



. . . c o n n e c t i n g y o u r b u s i n e s s

LANCOM WLC-4006 LANCOM WLC-4025+ LANCOM WLC-4100

- Handbuch
- Manual

LANCOM WLC-4006
LANCOM WLC-4025+
LANCOM WLC-4100

© 2010 LANCOM Systems GmbH, Wuerselen (Germany). All rights reserved.

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

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

Windows®, Windows Vista™, Windows NT® and Microsoft® are registered trademarks of Microsoft, Corp.

The LANCOM Systems logo, LCOS and the name LANCOM are registered trademarks of LANCOM Systems GmbH. All other names or descriptions used may be trademarks or registered trademarks of their owners.

Subject to change without notice. No liability for technical errors or omissions.

Products from LANCOM Systems include software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org>).

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

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

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

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom.eu

Wuerselen, January 2010

Preface

Thank you for your confidence in us!

The WLAN Controllers LANCOM WLC-4006, LANCOM WLC-4025+ and LANCOM WLC-4100 are state-of-the-art hardware components for medium- and large-scale WLAN-installation management that is just as simple as it is secure. All settings are entered just once into a central profile in the WLAN Controller—the rest is pure and simple "Plug&Play". New Access Points are found automatically. All of the configuration settings required for optimized wireless network operations, such as the channel settings and security policies, are automatically transferred to all of the Access Points. Operations are also monitored centrally (e.g. background scanning) by the WLAN Controller. Greatly simplified WLAN management offers significant costs savings. WLAN networks are extended easily and securely simply by "plugging in" new access points. Even remote sites can be seamlessly integrated—any IP connection will do. Smaller sites also benefit from the RADIUS/EAP server integrated into the LANCOM WLAN Controller.

At the same time the LANCOM WLAN Controllers ensure maximum security as all of the LANCOM Access Points in the network strictly observe corporate security policies automatically. Potential security loopholes are eliminated by permanent monitoring across all company sites.

Special highlights of the LANCOM WLAN Controller include, among others:

- "'Smart controller" for application-related or user-related WLAN networking
- Reliability due to self-sufficient operations
- No separate cabling necessary—any IP connection will do
- "Split management" for LANCOM WLAN Routers
- Automatic discovery and commissioning of access points and WLAN routers
- Central administration of WLAN configuration profiles
- Monitoring and assurance of encryption and QoS policy
- Integrated RF optimization
- Full support of VLAN, RADIUS and 802.x/EAP functions
- Integrated router, firewall and VPN gateway
- Scalable by adding Controllers; redundancy included

- Unparalleled operational reliability which prevents "single points of failure"

Security settings

To maximize the security available from your product, we recommend that you undertake all of the security settings (e.g. firewall, encryption, access protection) that were not already activated when you purchased the product. The LANconfig Wizard 'Security Settings' will help you with this task. Further information is also available in the chapter 'Security settings'.

We would additionally like to ask you to refer to our Internet site www.lancom.eu for the latest information about your product and technical developments, and also to download our latest software versions.

Components of the documentation

The documentation of your device consists of the following parts:

- Installation Guide
- User manual
- Reference manual
- Menu Reference Guide

You are now reading the user manual. It contains all information you need to put your device into operation. It also contains all of the important technical specifications.

The Reference Manual is to be found as an Acrobat document (PDF file) at www.lancom.eu/download or on the CD supplied. It is designed as a supplement to the user manual and goes into detail on topics that apply to a variety of models. These include, for example:

- The system design of the operating system LCOS
- Configuration
- Management
- Diagnosis
- Security
- Routing and WAN functions
- Firewall
- Quality of Service (QoS)
- Virtual Private Networks (VPN)
- Virtual Local Networks (VLAN)

- Wireless networks (WLAN)
- Backup solutions
- Further server services (DHCP, DNS, charge management)

The Menu Reference Guide (also available at www.lancom.eu/download or on the CD supplied) describes all of the parameters in LCOS, the operating system used by LANCOM products. This guide is an aid to users during the configuration of devices by means of WEBconfig or the telnet console.

This documentation was created by ...

... several members of our staff from a variety of departments in order to ensure you the best possible support when using your LANCOM product.

Should you find any errors, or if you would like to suggest improvements, please do not hesitate to send an e-mail directly to:

info@lancom.eu



Our online services www.lancom.eu are available to you around the clock if you have any questions on the content in this manual, or if you require any further support. The area 'Support' will help you with many answers to frequently asked questions (FAQs). Furthermore, the knowledgebase offers you a large reserve of information. The latest drivers, firmware, utilities and documentation are constantly available for download.

In addition, LANCOM Support is available. For telephone numbers and contact addresses for LANCOM Support, please refer to the enclosed leaflet or the LANCOM Systems Web site.

Information symbols



Very important instructions. Failure to observe these may result in damage.



Important instruction that should be observed.



Additional information that may be helpful but is not essential.

Content

1	Centralized WLAN management	10
1.1	Introduction	10
1.2	Technical concepts	11
1.2.1	The CAPWAP standard	11
1.2.2	Smart controller technology	11
1.2.3	Communication between the Access Point and the WLAN Controller	13
1.2.4	Zero-touch management	16
1.2.5	Split management	16
1.3	Just what can your LANCOM WLAN Controller do?	17
2	Installation	20
2.1	Package content	20
2.2	System requirements	20
2.2.1	Configuring the LANCOM devices	20
2.2.2	Operating access points in managed mode	21
2.3	Status displays and interfaces	21
2.3.1	Status displays	22
2.3.2	Device connectors	27
2.4	Hardware installation	29
2.5	Software installation	30
2.5.1	Starting the software setup	30
2.5.2	Which software should I install?	31
3	Basic configuration	32
3.1	Details you will need	32
3.1.1	TCP/IP settings	32
3.1.2	Configuration protection	34
3.2	Instructions for LANconfig	34
3.3	Instructions for WEBconfig	36
3.4	TCP/IP settings for Access Points	40
3.5	TCP/IP settings for PC workstations	40

4	Configuring the WLAN Controller	42
4.1	Basic configuration of the LANCOM WLAN Controller	42
4.1.1	Setting the time on the LANCOM WLAN Controller	42
4.1.2	Generating a default configuration	43
4.1.3	Assigning the default configuration to the new Access Points	47
4.2	Extended settings	48
4.2.1	General settings	48
4.2.2	Profiles	50
4.2.3	Access point configuration	58
4.2.4	AP update	65
4.2.5	Stations	70
4.2.6	RADIUS server	73
4.2.7	Options for the WLAN Controller	74
4.2.8	Inheritance of parameters	76
4.3	Sample configurations	78
4.3.1	Accepting new Access Points into the WLAN infrastructure manually	78
4.3.2	Deactivating Access Points or permanently removing them from the WLAN infrastructure	80
4.3.3	Backing up the certificates	82
4.3.4	Backing up and restoring further files from the SCEP-CA	85
4.3.5	LANCOM WLAN Controller backup	86
4.3.6	Load balancing between WLAN Controllers	89
4.3.7	Dynamic VLAN assignment	90
4.3.8	Virtualization and guess access via the LANCOM WLAN Controller	93
4.3.9	Checking WLAN clients with RADIUS (MAC filter)	106
4.3.10	Internal and external RADIUS servers combined	107
4.4	Displays and commands in LANmonitor	111
4.5	Automatic RF optimization with LANCOM WLAN Controllers	113
4.6	Configuring the Access Points	115

5 Security settings	117
5.1 Security in the wireless LAN	117
5.1.1 Encrypted data transfer	117
5.1.2 802.1x / EAP	118
5.1.3 LANCOM Enhanced Passphrase Security	118
5.1.4 Access control by MAC address	119
5.1.5 IPSec over WLAN	119
5.2 Tips for the proper treatment of keys and passphrases	119
5.3 Security settings Wizard	120
5.3.1 LANconfig Wizard	120
5.3.2 WEBconfig Wizard	121
5.4 The security checklist	121
6 Setting up Internet access	126
6.1 The Internet Connection Wizard	126
6.1.1 Instructions for LANconfig	126
6.1.2 Instructions for WEBconfig	127
7 Connecting two networks	128
7.1 Which details are necessary?	128
7.1.1 General information	128
7.1.2 Settings for the TCP/IP router	130
7.1.3 Settings for NetBIOS routing	131
7.2 Instructions for LANconfig	131
7.3 1-Click-VPN for networks (site-to-site)	132
7.4 Instructions for WEBconfig	134
8 Providing dial-in access	135
8.1 Which details are necessary?	135
8.1.1 General information	135
8.1.2 Settings for TCP/IP	136
8.1.3 Settings for NetBIOS routing	136
8.2 Settings on the dial-in computer	137
8.3 Instructions for LANconfig	137
8.4 1-Click-VPN for LANCOM Advanced VPN Client	138
8.5 Instructions for WEBconfig	139

9 Appendix	140
9.1 Performance and characteristics	140
9.2 Connector wiring	141
9.2.1 Ethernet interface 10/100/1000Base-TX, DSL interface	141
9.2.2 Configuration interface (outband)	141
9.3 CE-declarations of conformity	142
10 Index	143

1 Centralized WLAN management

1.1 Introduction

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. Possibly some Access Points are missed during the update procedure, which will result in inconsistent configurations.
- 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.

Centralized WLAN management is the solution to these problems. The configuration of the Access Point 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 that devices are stolen. Only in "standalone" operation is the con-

figuration optionally saved for a defined period to flash memory (in an area that cannot be read out with LANconfig or other tools).

1.2 Technical concepts

1.2.1 The CAPWAP standard

The CAPWAP protocol (Control And Provisioning of Wireless Access Points) was adopted by the IETF (Internet Engineering Task Force) in March 2009 as a standard for the centralized management of large WLAN infrastructures.

CAPWAP uses two channels for data transfer:

- Control channel, encrypted with DTLS. This channel is used to exchange administration information between the WLAN Controller and the Access Point.



Datagram Transport Layer Security (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

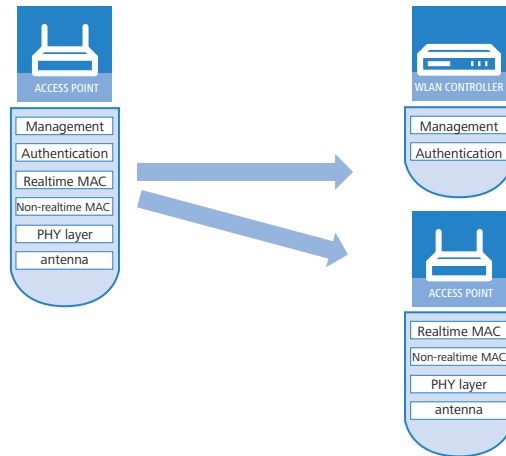
In a decentralized WLAN structure with stand-alone Access Points (operating as so-called "rich access points") all functions for data transfer take place in the PHY layer, the control functions in the MAC layer, and the management functions are integrated in the Access Points. Centralized WLAN management 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 for authentication of WLAN clients (which can also be the case in stand-alone WLANs).

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

Smart Controller Technology from LANCOM Systems uses the local MAC procedure. This method 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.



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, which has to process large portions of the overall data traffic, from becoming a central bottleneck. In remote MAC and split MAC architectures, **all** payload data is forced to run centrally via the WLAN Controller. However, in local MAC architectures data can alternatively be directly released from the Access Points into the LAN, so providing high-performance data transfer. This makes WLAN Controllers from LANCOM suitable for WLANs adhering to the IEEE 802.11n standard, so offering significantly higher bandwidths than conventional WLANs. 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.

CAPWAP tunneling and layer-3 roaming

From one of the later LCOS versions, LANCOM WLAN Controllers also support transfer of the 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 even during a call—between Ethernet subnets.
- 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 the Access Point and the WLAN Controller



As of firmware version LCOS 7.20 there is a difference between LANCOM Access Points (such as the LANCOM L-54ag) and LANCOM Wireless Routers (such as the LANCOM 1811n Wireless) with regard to the ex-factory standard settings in the WLAN modules. In the following specifications, the general term Access Point will be used for the most part.

For a successful starting up the Access Points must comply with the following requirements:

- The Access Point has an IP address (static or assigned via DHCP)
- The Access Point can reach a WLAN Controller in the LAN via broadcast
- Alternatively: The Access Point can resolve the address on a WLAN Controllers in the WAN using a DNS server (the “WLC-Address” is resolved using “.company.intern”).
- For a WLAN Controller in the WAN the firewall allows the communication for DNS, CAPWAP at UDP Port 1027 and HTTP for SCEP.

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:

- A LANCOM Access Point has the factory settings and is not yet configured. In these settings the WLAN modules are deactivated; the Access Point searches for a WLAN Controller in the LAN.

- A LANCOM Access Point is already configured; at least one WLAN module is manually set to operate as 'managed' ('Configuring the access points'). The Access Point searches for a WLAN Controller in the network on behalf of the one or more corresponding WLAN modules.
- A LANCOM Wireless Router is already configured; at least one WLAN module is manually set to operate as 'managed'. The wireless router searches for a WLAN Controller in the network on behalf of the one or more corresponding WLAN modules.

At the beginning of communications, the Access Point sends a "Discovery Request Message" to find any 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.

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 DNS suffixes learned via DHCP. In this way, a DNS server can automatically suffix the controller's standard name to 'WLC-address.company.internal'. This also makes it possible to reach WLAN Controllers that are not located in the same network, without having to configure the Access Points.

Please note that the access points must have an IP address in order to communicate with the WLAN Controller. The IP address can either be entered into the access point as a fixed value, or retrieved from a DHCP server.



If the access point is to retrieve an IP address from a DHCP server but the server is unobtainable, then an access point which is restarting may not have an IP address, and thus be unable to communicate with the WLAN Controller.

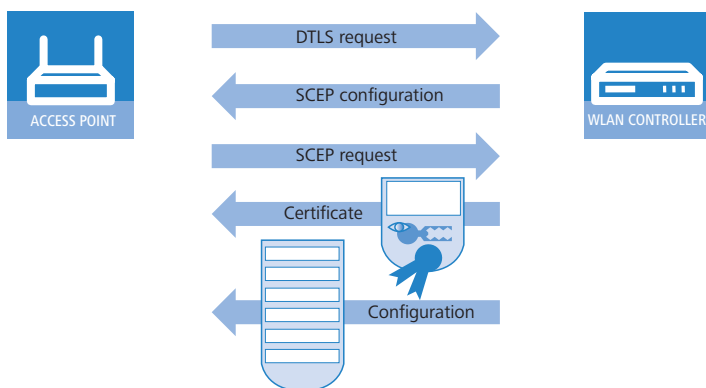
From the available WLAN Controllers, the Access Point selects the best one and queries it for the structure of the DTLS connection. The "best" WLAN Controller for the Access Point is the one with the least load, i.e., the lowest ratio of managed Access Points compared to the maximum possible Access Points. In case of two or more equally "good" WLAN Controllers, the Access Point selects the nearest one in the network, i.e., the one with the fastest response time.

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



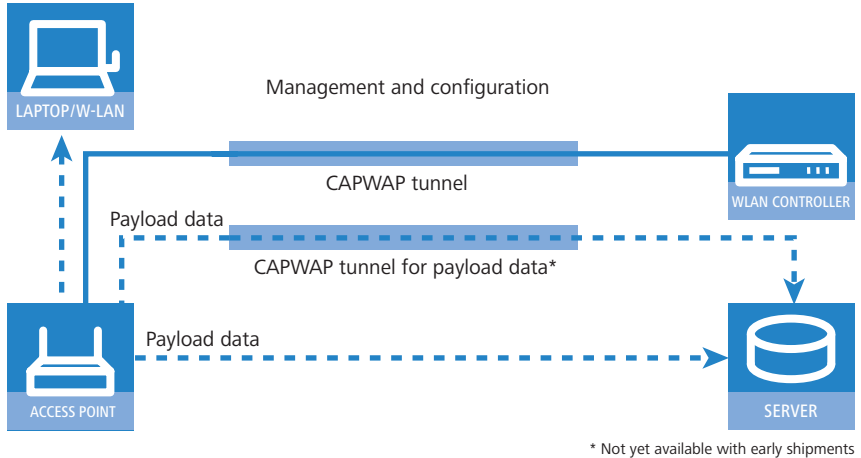
SCEP stands for Simple Certificate Enrollment Protocol; CA for Certification Authority.

The WLAN Controller then uses an internal random number to determine a unique and secure session key which it uses to protect 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's relationship 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.



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 CAP-WAP 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 locate your WLAN Controller in remote networks—a simple IP connection, such as via a VPN path, is all that you need. As the WLAN Controllers only influence the WLAN part of the configuration in the Access Point, all 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 Just what can your LANCOM WLAN Controller do?

The following table provides a comparison of the properties and functions of your device depending on the model.

	LANCOM WLC- 4006	LANCOM WLC- 4025+	LANCOM WLC- 4100
WLAN controlling			
Number of managed devices (factory setting / upgrade optional to maximum number)	6 / 12	25 / 100	100 / 1000
Automatic detection of WLAN controllers by the LANCOM Access Points or WLAN routers	✓	✓	✓
Automatic or manual authentication of the Access Points	✓	✓	✓
Communication between controller and Access Points via simple IP connection with CAPWAP	✓	✓	✓
Encryption of the control data with DTLS, including HW crypto accelerator	✓	✓	✓
Inheritance of configuration profiles, also multi-level	✓	✓	✓
Self-sufficient operations for continued operation even when the connection to the WLAN Controller is interrupted	✓	✓	✓
Advanced routing and forwarding (ARF) with customized DHCP, DNS, routing, firewall and VPN functions for these networks, assignment of the networks to SSIDs in the WLAN profile via VLAN IDs.	16 networks	16 networks	64 networks
Dynamic VLAN assignment for target user groups based on MAC addresses, BSSID or SSID by means of an external RADIUS server.	✓	✓	✓
Integrated RADIUS server for MAC address list management	✓	✓	✓
Integrated EAP server for authentication of 802.1x clients using EAP-TLS, EAP-TTLS, PEAP, MSCHAP or MSCHAPv2.	✓	✓	✓
Proxy mode for external RADIUS/EAP servers (forwarding and realm handling)	✓	✓	✓
802.11e / WME: Automatic VLAN tagging (802.1p) in the Access Points. Conversion to DiffServ attributes in the WLAN controller, provided it is used as a layer-3 router	✓	✓	✓
Fast roaming via PMK caching and pre-authentication	✓	✓	✓
Further applications			
Internet access	✓	✓	✓
LAN-LAN connectivity over VPN	✓	✓	✓

	LANCOM WLC- 4006	LANCOM WLC- 4025+	LANCOM WLC- 4100
RAS server (over VPN)	✓	✓	✓
IP router	✓	✓	✓
DHCP and DNS server (separate for all ARF networks)	✓	✓	✓
N:N mapping for routing networks with the same IP-address ranges over VPN	✓	✓	✓
LAN port can be configured to be a WAN port	✓	✓	✓
Policy-based routing	✓	✓	✓
NAT Traversal (NAT-T)	✓	✓	✓
PPPoE servers	✓	✓	✓
Layer 2 QoS tagging	✓	✓	✓
Spanning Tree Protocol	✓	✓	✓
802.1p	✓	✓	✓
LAN connection			
Uplink interface for connection to the LAN. Alternatively switchable as a LAN interface or as a WAN interface for connecting an SDSL modem.	1		
Individual Gigabit Ethernet LAN ports, auto-crossover, individually switchable, for example as LAN or DMZ ports. Alternatively switchable as a WAN interface for connecting an external DSL modem/router.	4	4	4
USB connector			
USB 2.0 host port (high speed: 480 Mbps) for connecting a USB printer and for future extensions	✓	✓	✓
Security functions			
5 integrated VPN tunnels for secure network connections	✓	✓	✓
DTLS and IPsec encryption via hardware	✓	✓	✓
IP masquerading (NAT, PAT) to conceal individual LAN workstations behind a single public IP address.	✓	✓	✓
Stateful-inspection firewall	✓	✓	✓
Firewall filter for blocking individual IP addresses, protocols and ports	✓	✓	✓

	LANCOM WLC- 4006	LANCOM WLC- 4025+	LANCOM WLC- 4100
Protection of the configuration from brute-force attacks.	✓	✓	✓
Configuration			
Configuration with LANconfig or via web browser; additional terminal mode for Telnet or equivalent terminal programs; SNMP interface and TFTP server function.	✓	✓	✓
Serial configuration interface	✓	✓	✓
FirmSafe for no-risk firmware updates	✓	✓	✓
Optional software extensions			
LANCOM WLC-PSPOT Option for guest-access accounts and chargeable WLAN access to the managed access points	integrated	✓	✓
LANCOM 2-Year Warranty Extension	✓	✓	✓
LANCOM Next Business Day Service Extension	✓	✓	✓

2 Installation

This chapter will assist you to quickly install hardware and software. First, check the package contents and system requirements. The device can be installed and configured quickly and easily if all prerequisites are fulfilled.

2.1 Package content

Before beginning with the installation, please check that nothing is missing from your package. Along with the device itself, the box should contain the following accessories:

	LANCOM WLC-4006	LANCOM WLC-4025+	LANCOM WLC-4100
IEC cable		✓	✓
Power adapter	✓		
CAT5 LAN connector cable (green connectors)	✓	✓	✓
RS232 connector cable for the configuration interface	✓	✓	✓
Rubber pads, 19" mounting brackets		✓	✓
LANCOM CD	✓	✓	✓
Printed Installation Guide	✓	✓	✓
Printed User Manual	✓	✓	✓
LANCOM Configuration Service Ticket	✓	✓	✓


Should anything be missing, please take up immediate contact to your dealer or to the address on the delivery note supplied with your device.

2.2 System requirements

2.2.1 Configuring the LANCOM devices


Computers that connect to a LANCOM must meet the following minimum requirements:

- Operating system with TCP/IP support, such as Windows, Linux, BSD Unix, Apple Mac OS, OS/2.
- Access to the LAN via the TCP/IP protocol.

 The LANtools also require a Windows operating system. A web browser under any operating system provides access to WEBconfig.

2.2.2 Operating access points in managed mode

LANCOM Wireless Routers and LANCOM Access Points can be operated either as self-sufficient Access Points with their own configuration ("Access Point mode") or as components in a WLAN infrastructure, which is controlled from a central WLAN Controller ("managed mode").


 For operation in managed mode the Access Points require firmware of version 7.22 or higher and a current loader (version 1.86 or higher).

Split management can be used to separate the WLAN configuration from the rest of the router configuration. This allows router settings and VPN settings to be adjusted locally, for example in a branch office or home office installation, and the WLAN configuration is regulated by a LANCOM WLAN Controller at the main office.

2.3 Status displays and interfaces

Meanings of the LEDs

The following section describes the meaning of the LEDs.

 Please be aware that LANmonitor shows far more information about the status of the WLAN Controller than the LEDs '→ Monitoring the LANCOM switch with LANmonitor'.

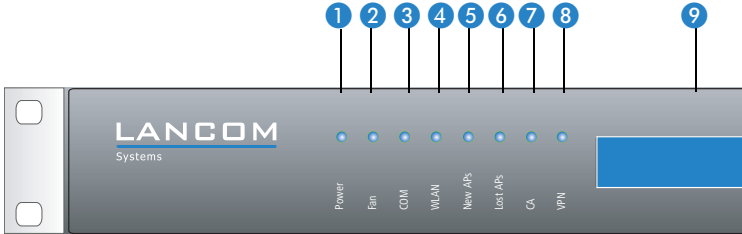
In the following sections we will use different terms to describe the behaviour of the LEDs:

- **Blinking** means, that the LED is switched on or off at regular intervals in the respective indicated colour.
- **Flashing** means, that the LED lights up very briefly in the respective colour and stay then clearly longer (approximately 10x longer) switched off.
- **Inverse flashing** means the opposite. The LED lights permanently in the respective colour and is only briefly interrupted.
- **Flickering** means, that the LED is switched on and off in irregular intervals.

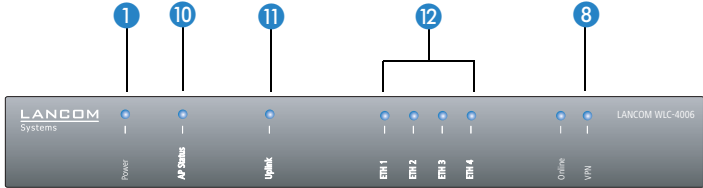
2.3.1 Status displays

The LANCOM WLAN Controllers are equipped with the following status displays:

LANCOM WLC-4025+
LANCOM WLC-4100

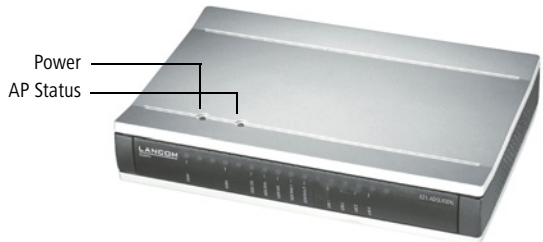


LANCOM WLC-4006



LANCOM WLC-4006 only

The two top-mounted LEDs enable the main function status to be assessed even if the device is positioned vertically:



1 Power

This LED provides information on the device's operating state.

Off		Device switched off
Green	blinking	Self-test after power-up

Green	On (permanently)	Device operational
Red/green	Blinking alternately	Device insecure: Configuration password not set
Red	blinking	Time limit for online connections has been reached



The power LED blinks alternately in red/green until a configuration password has been set. Without a configuration password, the configuration data in the LANCOM is unprotected. Normally you would set a configuration password during the basic configuration (instructions in the following chapter). Information about setting a configuration password at a later time is available in the section 'The Security Wizard'.

2 Fan

The Fan LED displays the fan's status:

Green	On (permanently)	CPU temperature OK
Orange	On (permanently)	CPU temperature > 55°
Red	blinking	Hardware failure of the fan or CPU temperature > 60°; additional acoustic signal

To prevent damage to the hardware, this LED is complemented by an acoustic signal. If the fan is blocked or the CPU temperature exceeds 60°, a pulsed acoustic signal is emitted.

3 COM

Connection status of the serial configuration interface

Off		No session logged on
Green	On (permanently)	Serial configuration session logged on
Orange	Flickering	Data transmission during the configuration session

4 WLAN

Provides information on the operational state of the device and the connected Access Point. The WLAN display can show the following:

Red	On (permanently)	The LANCOM WLAN Controller is not yet operational; one of the following elements is missing: <ul style="list-style-type: none"> ■ Root certificate ■ Device certificate ■ Current time
Red	blinking	The device is operational but not connected to an active access point.
Green	On (permanently)	At least one active access point connected and authenticated.



The reason for non-operability is shown in more detail in the display.

5 New APs

Provides information on new access points. The New AP display can show the following:

Orange	blinking	At least one new access point for authentication has been found.
--------	----------	--

6 Lost APs

Provides information on lost access points. The Lost AP display can show the following:

Red	blinking	At least one expected access point has not been found.
-----	----------	--

7 CA

Internal CA status

Off		CA off
Green	On (permanently)	CA on and ready
Red	On (permanently)	CA on; an error has occurred
Orange	On (permanently)	CA on and ready; request pending

8 VPN

Status of a VPN connection.

Off		No VPN tunnel established
Green	blinking	connection establishment
Green	Flashing	First connection
Green	Inverse flashing	Other connections
Green	On (permanently)	VPN tunnels are established

9 LCD display

The LC display has two lines of 16 characters each to display the following information in rotation:

- ▶ Device name
- ▶ Firmware version
- ▶ Device temperature
- ▶ Date and time
- ▶ CPU load
- ▶ Memory load
- ▶ Number of VPN tunnels
- ▶ Number of authenticated Access Points
- ▶ Number of expected Access Points (actively configured)
- ▶ Number of new discovered and as yet unauthenticated Access Points.
- ▶ Number of unfound expected Access Points.

If the WLAN LED constantly illuminates in red, the display also displays the following information:

- ▶ SNTP status
- ▶ SCEP status

■ Chapter 2: Installation

10 AP status (LANCOM WLC-4006 only)

Provides information on the operational state of the device and the connected Access Point. The AP status display can show the following:

Red	On (permanently)	The LANCOM WLAN Controller is not yet operational; one of the following elements is missing: <ul style="list-style-type: none"> ■ Root certificate ■ Device certificate ■ Current time ■ Random number for the DTLS encryption
Red	Blinking	At least one of the expected Access Points is missing.
Green/orange	Blinking	At least one new Access Point
Green	On (permanently)	At least one active access point is connected and authenticated; no new and no missing Access Point.

11 Uplink

Provide information on the connection to the WAN and to the LAN. The WAN LED is only active when the uplink port is configured as a DSL interface. The Uplink display can show the following:

		Left LED (WAN)	Right LED
Off		No active WAN connection has been established	No connection
Green	Blinking	Connection establishment	
Green	Flashing	Connection establishment: First connection	
Green	Inverse flashing	Connection establishment: Other connections	
Green	On (permanently)	Connection established	Connection established
Green	Flickering		Data traffic (send or receive)
Red	On (permanently)	The last connection request failed. Error status is deleted when a connection is made or when it is deleted in LANmonitor.	

12 ETH

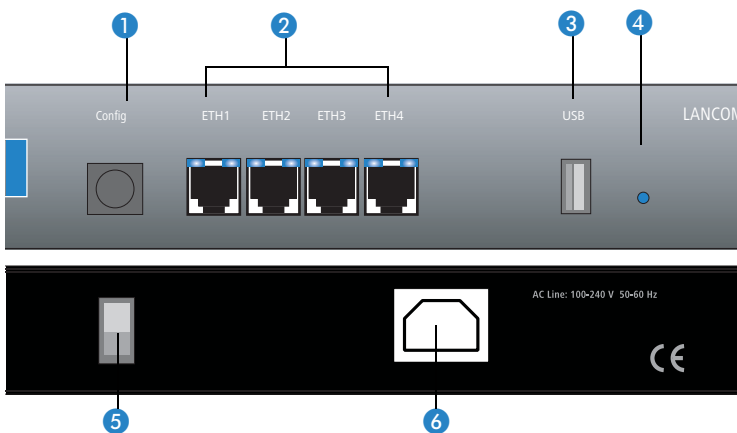
LAN connector status in the integrated switch:

Off		No networking device attached
Green	On (permanently)	Connection to network device operational, not data traffic
Green	Flickering	Data traffic
Red	Flickering	Data packet collision

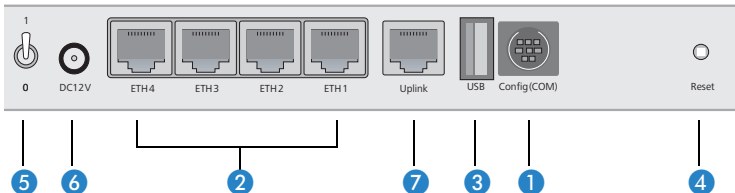
2.3.2 Device connectors

The LANCOM WLAN Controllers are equipped with the following device connectors:

LANCOM WLC-4025+
LANCOM WLC-4100



LANCOM WLC-4006



1 COM

Connector for the serial configuration cable.

2 ETH 1 to 4

Ethernet sockets (10/100/1000Base-Tx) for connection to the LAN. 10 Mbit, 100 Mbit or 1000 Mbit connections are supported. The available transfer rate is detected automatically (autosensing).

Each Ethernet socket has two LEDs (green and yellow).

Green	Off	No networking device attached
Green	On (permanently)	Connection to network device operational, not data traffic
Green	Flickering	Data traffic
Yellow	Off	1000 Mbps
Yellow	On (permanently)	10/100 Mbps

- 3 USB USB connector (USB host)
- 4 Reset Reset button (see 'Reset button functions')
- 5 Power switch Switch for detaching the device from the power supply.



Please note:

For a complete detachment from the power supply please unplug the power connection.

- 6 Power connection Connector for the IEC cable (LANCOM WLC-4025+, LANCOM WLC-4100) or power supply unit (LANCOM WLC-4006)
- 7 Uplink Uplink connection

Reset button functions

The reset button offers two basic functions—boot (restart) and reset (to the factory settings)—which are called by pressing the button for different lengths of time.

It is not always possible to install a device under lock and key. There is consequently a risk that the configuration will be deleted by mistake if a co-worker presses the reset button too long. You can define the behavior of the reset button with a setting in WEBconfig (LCOS menu tree ► Setup ► Config):

■ Reset button

This option controls the behavior of the reset button when it is pressed:

- Ignore: The button is ignored.
- Boot only: With a suitable setting, the behavior of the reset button can be controlled; the button is then ignored or a press of the button prompts a re-start only, however long it is held down.



A hard reset causes the device to start with the default factory settings; all previous settings are lost! Any access points managed from this WLAN Controller could lose their configuration, depending on how standalone operation has been set up ('StandaloneOperation').



Please observe the following notice: The settings 'Ignore' or 'Boot only' makes it impossible to reset the configuration to the factory settings. If the password is lost for a device with this setting, there is no way to access the configuration! In this case the serial communications interface can be used to upload a new firmware version to the device—this resets the device to its factory settings, which results in the deletion of the former configuration. Instructions on firmware uploads via the serial configuration interface are available in the LCOS reference manual.

- Reset-or-boot (standard setting): Press the button briefly to re-start the device. Pressing the button for 5 seconds or longer restarts the device and resets the configuration to its factory settings. All LEDs on the device light up continuously.

Once the switch is released the device will restart with the restored factory settings.



After resetting, the device starts completely unconfigured and **all** settings are lost. If possible be sure to backup the current device configuration **before** resetting.



After resetting, the LANCOM Access Point returns to managed mode, in which case the configuration cannot be directly accessed via the WLAN interface!

2.4 Hardware installation

Installing the LANCOM WLAN Controller involves the following steps:

- ① **Mounting** – The device is designed for mounting in an available 19" unit in a server cabinet. If necessary fix the rubber pads to the underside of the device to prevent any scratching to other equipment.
- ② **LAN** – First of all connect your LANCOM WLAN Controller to the LAN. Plug one end of the supplied network cable (green connectors) into an

LANCOM WLC-4025+
LANCOM WLC-4100

LANCOM WLC-4025+
LANCOM WLC-4100

LANCOM WLC-4006

EN

Ethernet port on the device ②, and the other end into an available network connector socket in your local network.

- ③ **LAN** – First of all connect your LANCOM WLAN Controller to the LAN. Plug in one end of the supplied network cable (green connectors) to the uplink connector on the device ⑦ and the other end into an available network connector socket in your local network, or a free socket on a switch.

The Ethernet ports use autosensing to recognize the data rate (10/100/1000 Mbit) and the type (node/hub) of attached network devices. It is possible to connect devices of different speeds and types in parallel.

- ④ **Further network devices** – you can optionally connect further network devices to the LAN interfaces ②.
- ⑤ **Configuration interface** – optionally, the LANCOM WLAN Controller can be connected directly to the serial interface (RS-232, V.24) of a PC. Use the connection cable supplied for this. Connect the LANCOM configuration interface ① to an available serial interface on the PC.
- ⑥ **Supply power and switch on** – Using the power connection ⑥, supply power to the device and switch it on using the switch ⑤ located on the rear panel.

2.5 Software installation

The following section describes the installation of the Windows-compatible system software LANtools, as supplied.



You may skip this section if you use your WLAN Controller exclusively with computers running operating systems other than Windows.

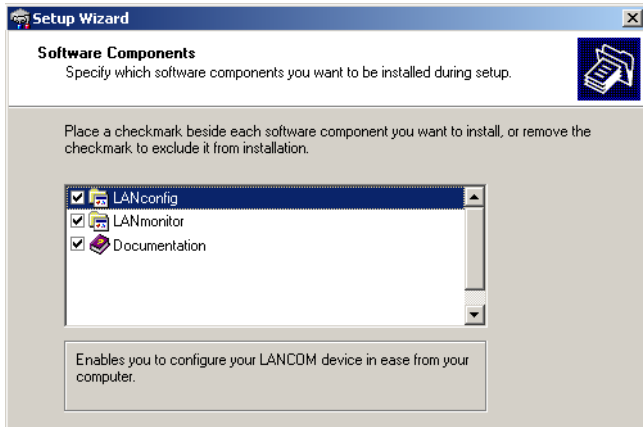
2.5.1 Starting the software setup

Place the product CD into your drive. The setup program will start automatically.



If the setup does not start automatically, run AUTORUN.EXE in the root directory of the LANCOM CD.

In Setup, select **Install software**. The following selection menus will appear on screen:



2.5.2 Which software should I install?

- **LANconfig** is the Windows configuration program for all LANCOM devices. WEBconfig can be used alternatively or in addition via a web browser.
- With **LANmonitor** you can use a Windows computer to monitor all of your LANCOM devices.
- **WLANmonitor** enables the observation and surveillance of wireless LAN networks. Clients connected to the access points are shown, and even non-authenticated access points and clients can be displayed as well (rogue AP detection and rogue client detection).
- With **Documentation** you copy the documentation files onto your PC.

Select the appropriate software options and confirm your choice with **Next**. The software is installed automatically.

3 Basic configuration

The basic configuration is conducted with a convenient Setup Wizard that provides step-by-step guidance through the configuration and that requests any necessary information.

First of all this chapter presents the information that has to be entered for the basic configuration. This first section will help you to gather up all of the necessary data before you start the Wizard.

You subsequently enter this information into the Setup Wizard. Starting the program and the following procedure are described step by step. LANconfig and WEBconfig each have their own description. With all of the necessary information collected in advance, this basic configuration can now take place quickly and in ease.

At the end of this chapter we show you the necessary settings for the workplace computers in the LAN so that they can access the device without problem.

3.1 Details you will need

The Basic Settings Wizard is used to set the WLAN Controllers basic TCP/IP parameters and to protect the device with a configuration password. The following description of the information required by the wizard is divided into the following configuration sections:

- TCP/IP settings
- Protecting the configuration
- Security settings

3.1.1 TCP/IP settings

TCP/IP configuration can be performed in two different ways: Either fully automatically or manually. No user input is required if TCP/IP configuration is performed automatically. All parameters are set by the Setup Wizard on its own. When manual TCP/IP configuration is performed the wizard prompts for the usual TCP/IP parameters: IP address, network mask etc. (more on this later)

The fully automatic TCP/IP configuration is only possible in certain network environments. For this reason the Setup Wizard analyses the connected LAN to see whether fully automatic configuration is possible or not.

New LAN – fully automatic configuration possible

The setup wizard offers to configure TCP/IP fully automatically if no network devices connected have yet been configured. This usually happens in the following situations:

- Only a single PC is going to be attached to the WLAN Controller
- Setting up a new network

Fully automatic TCP/IP configuration will not be offered if you are integrating the WLAN Controller into an existing TCP/IP LAN. In this case please continue with the section 'Required information for manual TCP/IP configuration'.

The result of fully automatic TCP/IP configuration is as follows: The WLAN Controller is assigned the IP address '172.23.56.254' (network mask '255.255.255.0'). The integrated DHCP server is also activated so that the WLAN Controller can assign the devices in the LAN IP addresses automatically.

Should you still configure manually?

Fully automatic TCP/IP configuration is optional. Instead of this you can select manual configuration. Make this selection after considering the following:

- Select automatic configuration if you are **not** familiar with networks and IP addresses.
- Select the manual TCP/IP configuration if you are familiar with networking and IP addresses, and you would like to specify the IP address for the router yourself (from one of the address ranges reserved for private use, for example '10.0.0.1' with a network mask of '255.255.255.0'). If you do this you simultaneously specify the address range that the DHCP server will subsequently use for the other devices in the network (provided the DHCP server is activated).

Required information for manual TCP/IP configuration

When performing manual TCP/IP configuration the Setup Wizard prompts you for the following information:

- **DHCP mode of operation**
 - Off: The IP addresses required must be entered manually.
 - Server: The WLAN Controller operates as DHCP server in the network; as a minimum its own IP address and the network mask must be assigned.
 - Client: The WLAN Controller obtains its address information from another DHCP server; no address information is required.

■ IP address and network mask for the WLAN Controller

Assign the WLAN Controller a free IP address from your LAN's address range and enter the network mask.

■ Gateway address

Enter the gateway's IP address if you have selected 'Off' as the DHCP mode of operation or if another network device is assuming the role of gateway in the 'Server' mode of operation.

■ DNS server

Enter the IP address of a DNS server to resolve domain names if you have selected 'Off' as the DHCP mode of operation or if another network device is assuming the role of DNS server in the 'Server' mode of operation.

3.1.2 Configuration protection

Using a password secures access to the WLAN Controller's configuration and thus prevents unauthorized modification. The device's configuration contains a great deal of sensitive data such as data for Internet access and should be protected by a password in all cases.



Multiple administrators can be set up in the configuration of the LANCOM, each with different access rights. Up to 16 different administrators can be set up for a WLAN Controller. Further information can be found in the LCOS reference manual under "Managing rights for different administrators".

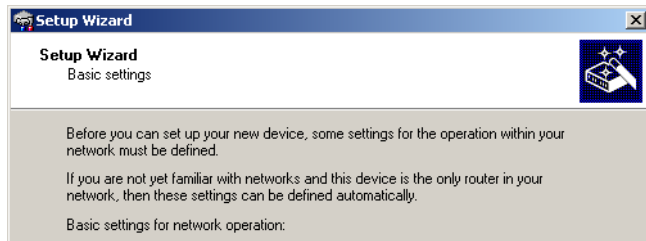



In the managed mode the LANCOM Wireless Routers and LANCOM Access Points automatically receive the same root password as the WLAN Controller, assuming that no root password has been set in the device itself.


3.2 Instructions for LANconfig



- ① Start LANconfig with **Start ▶ Programs ▶ LANCOM ▶ LANconfig**. LANconfig automatically detects new LANCOM devices in the TCP/IP network.
- ② If the search detects an unconfigured device, the Setup Wizard launches to help you with its basic settings, or indeed to handle the entire process

on your behalf (assuming that the appropriate networking environment exists).




 If you cannot access an unconfigured WLAN Controller, the problem may be the LAN netmask: In case there are less than 254 potential hosts available (netmask >'255.255.255.0'), you must ensure that the IP address 'x.x.x.254' is available in your subnet or a DHCP server is available respectively.



If you choose automatic TCP/IP configuration, you can continue with step .


-  Give the LANCOM an address from the applicable IP address range. Confirm with **Next**.
-  In the window that follows, you first set the password to the configuration. Entries are case sensitive and should be at least 6 characters long.

You also define whether the device can be configured from the local network only, or if remote configuration via WAN is to be permitted.

 Be aware that releasing this option also allows remote configuration over the Internet. Whichever option you select, make sure that configuration access is password protected.

If no main password is set the power LED will blink and the WAN configuration is not possible, even if the WAN configuration is activated.

-  Charge protection is a function which can place a limit on the costs from WAN connections. Accept your entries with **Next**.
-  Close the configuration with **Finish**.

 See the section 'TCP/IP settings for PC workstations' for information on the settings that are required for computers in the LAN.

3.3 Instructions for WEBconfig

Device settings can be configured from any Web browser. WEBconfig configuration software is an integral component of the LANCOM. A Web browser is all that is required to access WEBconfig. WEBconfig offers similar Setup Wizards to LANconfig and hence provides the perfect conditions for easy configuration of the LANCOM – although, unlike LANconfig, it runs under any operating system with a Web browser.

Secure with HTTPS

WEBconfig offers secure (remote) configuration by encrypting the configuration data with HTTPS.

```
https://<IP address or device name>
```



Always use the latest version of your browser to ensure maximum security.

Accessing the device with WEBconfig

To carry out a configuration with WEBconfig, you need to know how to contact the device. Device behavior and accessibility for configuration via a Web browser depend on whether the DHCP server and DNS server are active in the LAN already, and whether these two server processes share the assignment in the LAN of IP addresses to symbolic names. WEBconfig accesses the LANCOM either via its IP address, the device name (if configured), or by means of any name if the device has not yet been configured and has assigned itself as DNS server.

Following power-on, unconfigured LANCOM devices first check whether a DHCP server is already active in the LAN. Depending on the situation, the device can either enable its own DHCP server or enable DHCP client mode. In the second operating mode, the device can retrieve an IP address for itself from a DHCP server in the LAN.



If a LANCOM Wireless Router or LANCOM Access Point is centrally managed from a LANCOM WLAN Controller, the DHCP mode is switched from auto-mode to client mode upon provision of the WLAN configuration or a fixed IP address is assigned respectively.

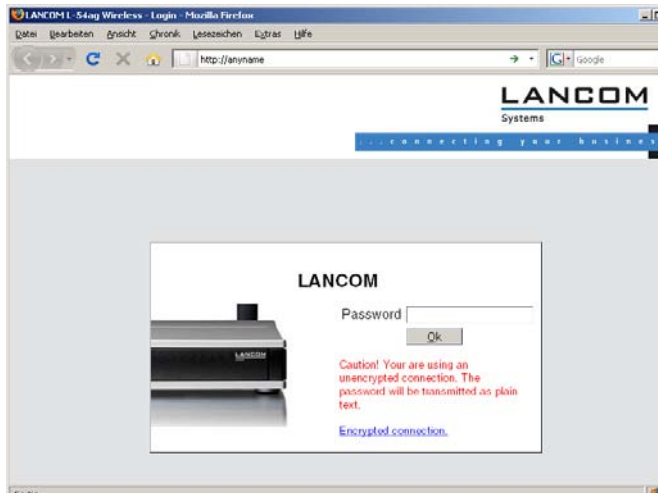
Not for centrally managed LANCOM Wireless Routers or LANCOM Access Points

Network without a DHCP server

In a network without a DHCP server, unconfigured LANCOM devices enable their own DHCP server service when switched on and assign IP addresses, information on gateways, etc. to other computers in the LAN (provided they are set to automatic retrieval of IP addresses – auto DHCP). In this constellation, the device can be accessed by every computer with the auto DHCP function enabled with a Web browser under IP address **172.23.56.254**.



With the factory settings and an activated DHCP server, the device forwards all incoming DNS requests to the internal Web server. This means that a connection can easily be made to set up an unconfigured LANCOM by entering any name into a Web browser.

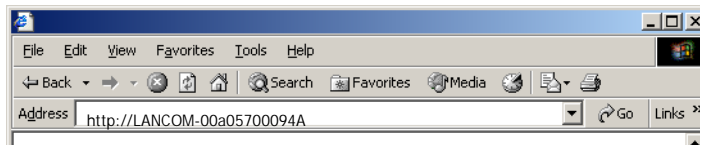


If the configuration computer does not retrieve its IP address from the LANCOM DHCP server, it determines the current IP address of the computer (with **Start ▶ Run ▶ cmd** and command **ipconfig** at the prompt under Windows 2000 or Windows XP or Windows Vista, with **Start ▶ Run ▶ cmd** and command **winipcfg** at the prompt under Windows Me or Windows 9x, or with command **ifconfig** in the console under Linux). In this case, the LANCOM can be accessed with address **x.x.x.254** (the “x”s stand for the first three blocks in the IP address of the configuration computer).

Network with DHCP server

If a DHCP server for the assignment of IP addresses is active in the LAN, an unconfigured LANCOM device disables its own DHCP server, switches to DHCP client mode and retrieves an IP address from the DHCP server in the LAN. However, this IP address is initially unknown and accessing the device depends on the name resolution:

- If the LAN also has a DNS server for name resolution and this communicates the IP address/name assignment to the DHCP server, the device can be reached under name "LANCOM-<MAC address>", e.g. "LANCOM-00a057xxxxx".



The MAC address on a sticker on the base of the device.

- If there is no DNS server in the LAN, or if it is not coupled to the DHCP server, the device cannot be reached via the name. In this case the following options remain:
 - Under LANconfig use the function "Find devices", or under WEBconfig use the "search for other devices" option from any other networked LANCOM.
 - Use suitable tools to find out the IP address assigned to the LANCOM by DHCP and access the device directly using this IP address.
 - Use the serial configuration interface to connect a computer running a terminal program to the device.

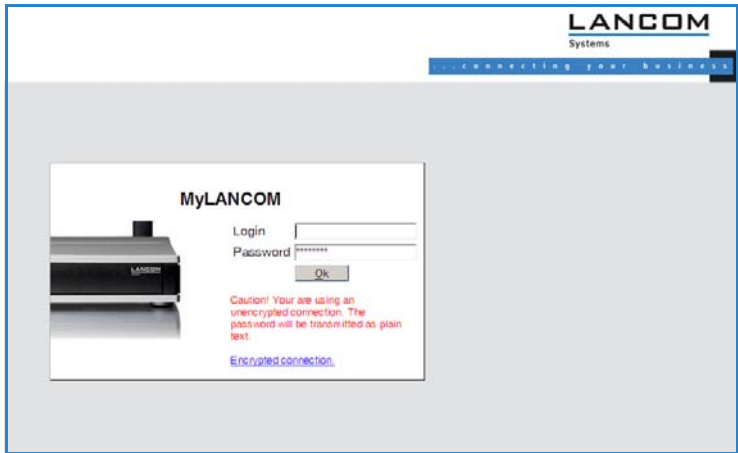
Login

When prompted for user name and password when accessing the device, enter your personal data in the appropriate fields. Observe the use of upper and lower case.

If you used the general configuration access, only enter the corresponding password. The user name field remains blank in this case.

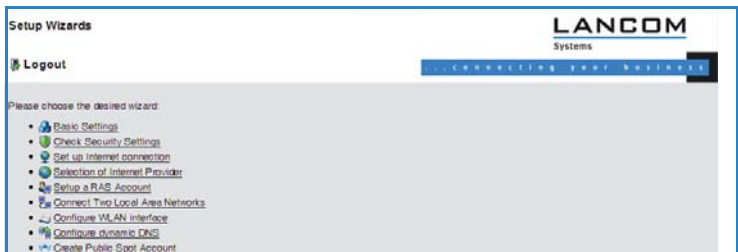


As an alternative, the login dialog provides a link for an encrypted connection over HTTPS. Always use the HTTPS connection for increased security whenever possible.



Setup Wizards

The setup Wizards allow quick and easy configuration of the most common device settings. Select the Wizard and enter the appropriate data on the following screens.



The settings are not stored in the device until inputs are confirmed on the last screen of the Wizard.

TCP/IP setting for the access points Please note that the access points must have an IP address in order to communicate with the WLAN Controller. The IP address can either be entered into the access point as a fixed value, or retrieved from a DHCP server.



If the access point is to retrieve an IP address from a DHCP server but the server is unobtainable, then an access point which is restarting may not have an IP address, and thus be unable to communicate with the WLAN Controller.

3.4 TCP/IP settings for Access Points

Please note the the Access Points needs a IP address to connect to the WLAN Controller. The IP address may either be set up fixed in the Access Point or assigned via DHCP server.



If the IP address is assigned via DHCP server and this server cannot be reached, the Access Point has no IP address after restart and therefore cannot connect to the WLAN Controller.

3.5 TCP/IP settings for PC workstations

It is extremely important to assign the correct addresses to all of the devices in the LAN. Also, all of these computers must know the IP addresses of two central stations in the LAN:

- Standard gateway – receives all packets which are not addressed to computers in the local network
- DNS server – translates network and computer names into their actual IP addresses.

The WLAN Controller can fulfill the functions of a standard gateway and also of a DNS server. It can also operate as a DHCP server, which automatically assigns IP addresses to all of the computers in the LAN.

The correct TCP/IP configuration of a PC in the LAN depends essentially on the method used for assigning IP addresses in the LAN:

■ IP address allocation by a LANCOM

In this operating mode, a LANCOM uses DHCP to allocate not only an IP address to each PC in the LAN and WLAN (for devices with a radio module), but it also communicates its own IP address as the standard gateway and DNS server. For this reason, the PCs have to be set up to automatically retrieve their own IP address and those of the standard gateway and DNS server via DHCP.

■ IP address allocation by a separate DHCP server

For this reason, the workstation PCs have to be set up to automatically retrieve their own IP address and those of the standard gateway and DNS server via DHCP. The DHCP server is to be programmed such that the IP address of the LANCOM is communicated to the PCs in the LAN as the standard gateway. The DHCP server should also communicate that the LANCOM is the DNS server.

■ Manual IP address assignment

If IP addresses in a network are statically assigned, then the IP address of the LANCOM is to be set as the standard gateway and DNS server in the TCP/IP configuration of each PC in the LAN.



Further information and help on the TCP/IP settings for your WLAN Controller is available in the Reference Manual. For information on the network configuration of workstation PCs, refer to the documentation for the installed operating system.

4 Configuring the WLAN Controller

LANCOM WLAN Controllers handle the management of Access Points in larger WLAN infrastructures. The configuration data of the Access Points is stored in profiles in the WLAN Controller and, from there, these are transmitted to the Access Points.



LANCOM WLAN Controllers manage the configurations of LANCOM wireless devices with WLAN modules set to the 'Managed' operating mode.

- LANCOM Access Points (L-315agn dual, L-310agn, L-305agn, L-54g, L-54ag, L-54 dual, IAP, XAP, OAP) with firmware of LCOS 7.20 or higher are set to managed mode as standard when shipped.
- Conversely, LANCOM Wireless Routers (18xx, 3x50) are set to the Access Point mode.

Instructions on setting the operating mode for WLAN modules are to be found under 'Configuring the Access Points' → page 115.

4.1 Basic configuration of the LANCOM WLAN Controller

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 configuration that the WLAN Controller can provide 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.

4.1.1 Setting the time on 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 Enrolment Protocol (SCEP).



For further information on SCEP refer to the LCOS reference manual.

The LANCOM WLAN Controller can only check the temporal validity of these certificates if it is set with the current time. If the time is not set in the WLAN Controller, the WLAN LED illuminates in red and the device is not operational. 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 the models LANCOM WLC-4006 the time information **must** be retrieved from a time server, because these devices doesn't incorporate a battery buffered 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) and it determines a random number. 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' → page 82).

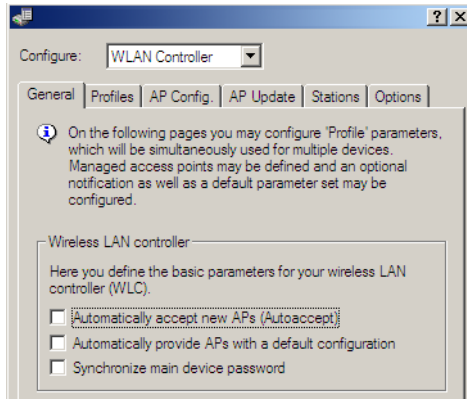
4.1.2 Generating a default configuration

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' → page 115), the WLAN Controller soon displays these as "New Access Points" in that the New APs LED blinks orange. The LANmonitor and the device's display additionally shows 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.

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

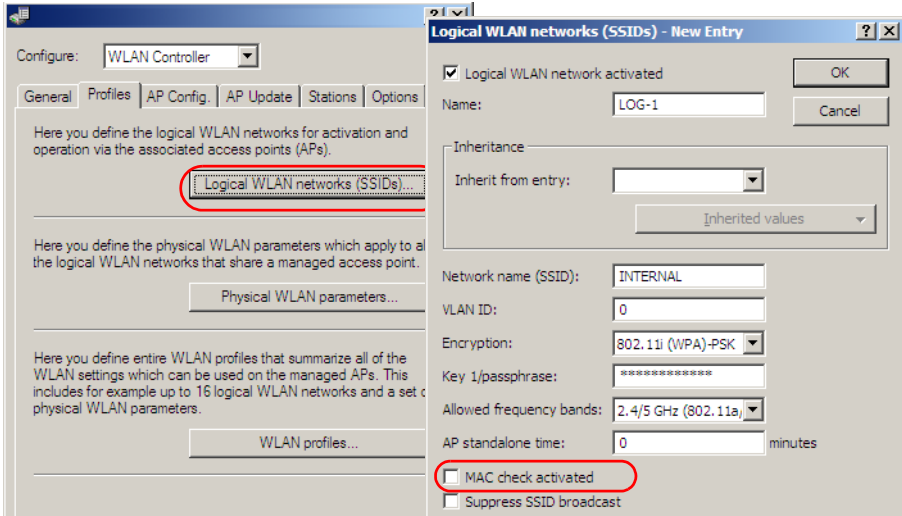
- ② In the configuration section 'WLAN Controller' on the 'General' tab, activate the options for the automatic acceptance of new Access Points and the provision of a default configuration.



- Automatically accept new Access Points: 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.
- Automatic provision of the default configuration: This enables the WLAN Controller to assign a default configuration to any 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' tab, select the logical WLAN networks. Add a new entry with the following values:



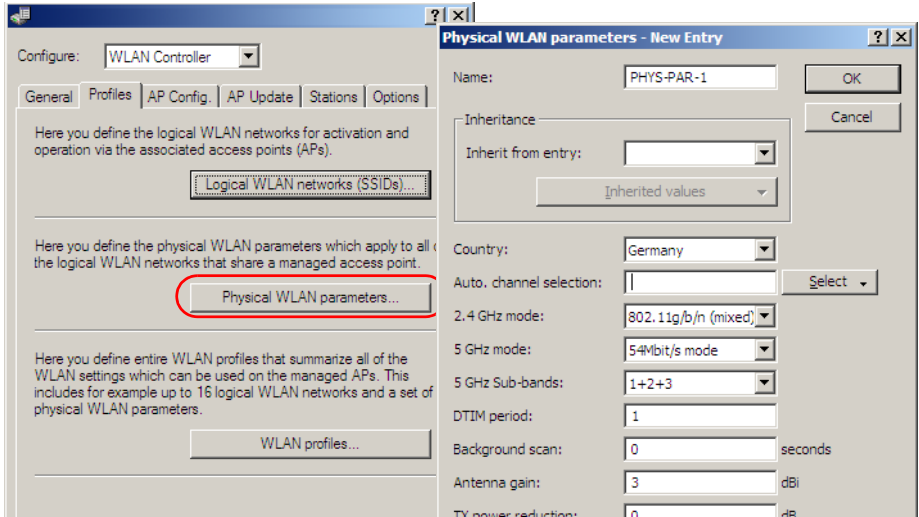
- (Network) name: Give the WLAN a name. This name is used only for administrative purposes in the LANCOM WLAN Controller.
 - SSID: This SSID is used for the WLAN clients to connect.
 - Encryption: Select the encryption method suitable for the WLAN clients being used, and enter a key or passphrase, as 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)' → page 106.
- 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.



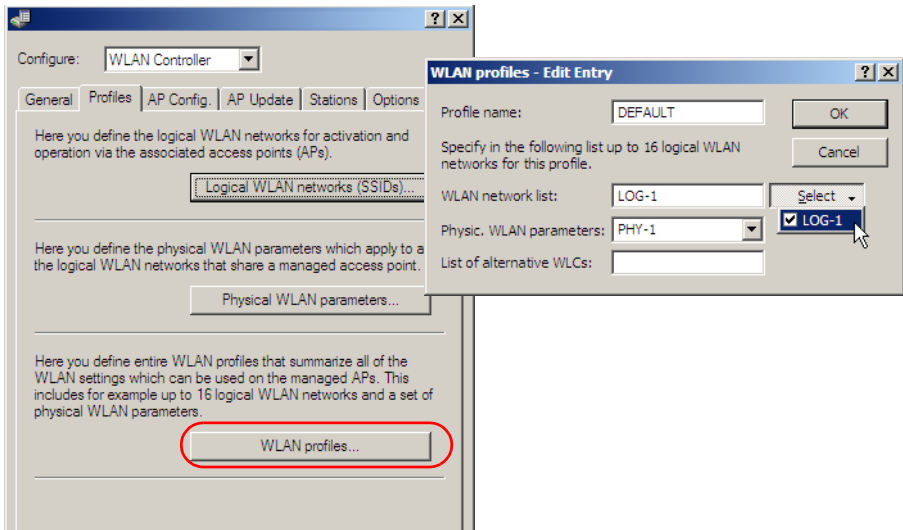
For normal access point applications you should use only the 5-GHz subbands 1 and 2. Subband 3 is for special applications only (e.g. BFWA, Broadband Fixed Wireless Access).

Chapter 4: Configuring the WLAN Controller


EN

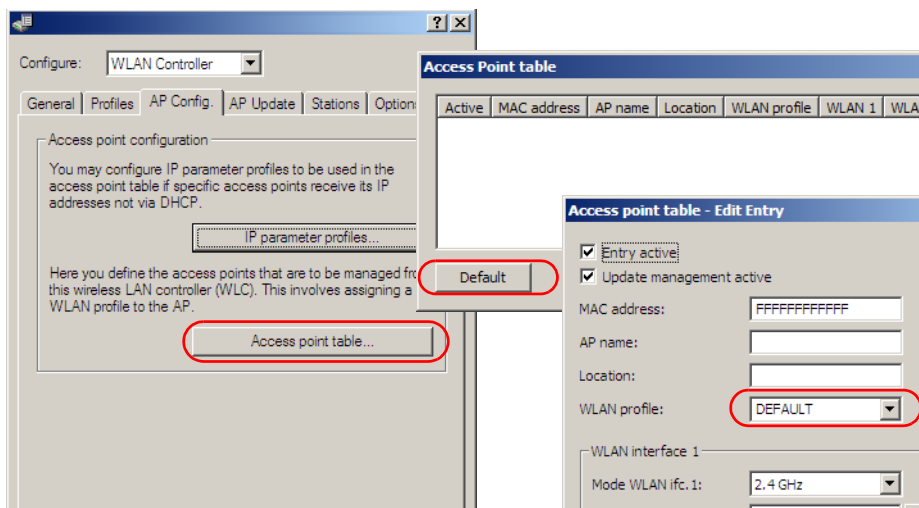


- ⑤ Create a new WLAN profile, give it a unique name, and assign the above logical WLAN network and physical WLAN parameters to it.



- ⑥ Change to the 'AP config.' tab and add a new entry by clicking on the **Default** button. Assign the WLAN profile defined above to it. You can 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 in this table with its MAC address.



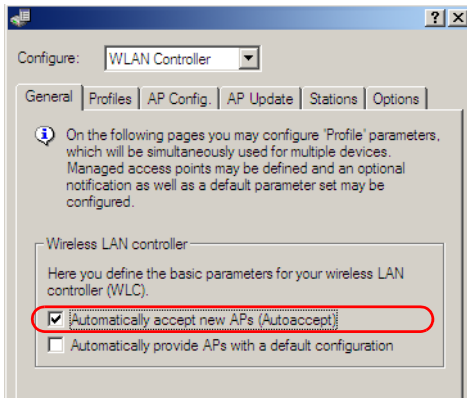
4.1.3 Assigning the default configuration to the new Access Points

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

In the configuration of the WLAN Controller, each Access Point receives an entry in the Access Point table and is fed with the default configuration.

 After the initial start-up phase, the option 'Automatically provide APs with the default configuration' can be deactivated again so that no further Access Points are automatically accepted into the network.

The option 'Automatically accept new APs' can remain active so that, after a reset, the WLAN Controller can automatically provide expected Access Points—as entered into the AP table—with valid certificates.

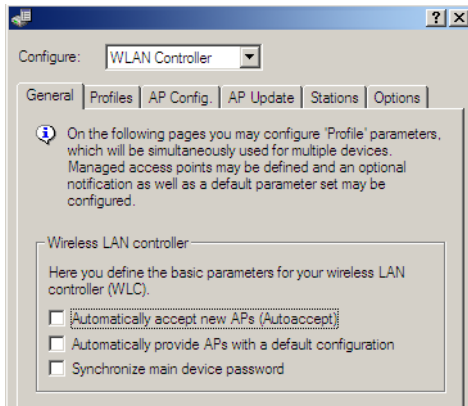


4.2 Extended settings

Most of the parameters for configuring the LANCOM WLAN Controller correspond with those of the Access Points. For this reason, this documentation does not explicitly describe all of the WLAN parameters, but only those aspects necessary for operating the WLAN Controller. Information on the available WLAN parameters can be found in the LCOS reference manual.

4.2.1 General settings

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



LANconfig: WLAN Controller ► General ► WLAN profiles

WEBconfig: LCOS menu tree ► Setup ► WLAN management

■ Automatically accept new APs (Auto-accept)

Enables the WLAN Controller to provide a certificate to all new Access Points **without** a valid certificate. One of these two conditions must be fulfilled for this:

- A configuration for the Access Point is entered into the AP table 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, 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 can be managed by one WLAN Controller). Any Access Points accepted by default are also entered into the MAC list.



This option can also 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 no Access Points can connect unintentionally with the LAN and thus be accepted into the WLAN infrastructure.
On	Off	Controlled rollout phase: Use this combination if you have entered all of the approved Access Points into the AP table along with their MAC addresses, assuming that these are to be automatically accepted into the WLAN infrastructure.
Off	Off	Normal operation: No new Access Points will be accepted into the WLAN infrastructure without the administrator's approval.

■ Synchronize the main device password

Activating this function sets the main device password for the access point each time it registers. This ensures that the password is synchronized with that of the WLAN controller.

If this function is deactivated, the main device password will only be set if the access point has no password when it registers. Once a password is set, it will not be overwritten and will get different when changing the WLC password.

4.2.2 Profiles

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

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:

Logical WLAN networks (SSIDs) - New Entry

Logical WLAN network activated OK

Name: Cancel

Inheritance

Inherit from entry: Inherited values

Network name (SSID):

VLAN ID:

Encryption:

Key 1/passphrase:

Allowed frequency bands:

AP standalone time: minutes

MAC check activated

Suppress SSID broadcast

WPA version:

WPA1 session key type:

WPA2 session key type:

Broadcast rate:

Client Bridge Support:

Maximum count of clients:

Use long preamble for 802.11b

802.11n

Spatial streams count:

Allow short guard interval

Use frame aggregation

LANconfig: WLAN Controller ▶ Profiles ▶ Logical WLAN networks

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN management ▶ AP configuration ▶ Network profiles

■ Name

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

Possible values:

- Maximum 32 ASCII characters.

Default:

- Blank

■ Inheritance

Selection of a logical WLAN network defined earlier and from which the settings are to be inherited ('Inheritance of parameters' → page 76).

■ Network name (SSID)

Define an unambiguous SSID (the network name) for each of the logical wireless LAN networks. Only WLAN clients that have the same SSID can register with this wireless LAN network.

Possible values:

- Maximum 32 ASCII characters.

Default:

- Blank

■ VLAN ID

VLAN ID for this logical WLAN network.

Possible values:

- 1 to 4096

Default:

- 0

Special values:

- 1: Logical wireless LAN works untagged (no VLAN tag).
- 2 to 4096: Logical wireless LAN uses the VLAN with the specified ID, assuming that the management VLAN ID is not equal to 0.



Please note that to use VLAN IDs in a logical WLAN network requires a management VLAN ID to be set ('Management VLAN ID' → page 55). If a VLAN ID is specified for a wireless LAN profile, the VLAN module is automatically activated for access points managed by it.

■ Self-sufficient operation

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 can be reached 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 data theft as all security-related configuration parameters are automatically deleted after this time has expired.

Possible values:

- 0 to 9999

Default:

- 0

Special values:

- 0: Switches the WLAN module off the moment that the connection to the Controller is lost. With this setting, the configuration provided by the WLAN Controller is not stored in flash memory but in RAM, meaning that a power outage causes the configuration to be lost immediately.
- 9999: Continues working indefinitely with the current configuration, even if the WLAN Controller is permanently unavailable. The WLAN configuration in the flash memory is only deleted after a reset.



Please note that the delay before deletion of the flash configuration is the time of self-sufficient operation, not the time after power loss!



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:

The screenshot shows a dialog box titled "Physical WLAN parameters - New Entry". It contains the following fields and options:

- Name: PHYS-PAR-1
- Inheritance: Inherit from entry: (dropdown), Inherited values: (dropdown)
- Country: Germany
- Auto channel selection: 1, Select (dropdown)
- 2.4 GHz mode: 802.11g/b/n (mixed)
- 5 GHz mode: 54Mbit/s mode
- 5 GHz Sub-bands: 1+2+3
- DTIM period: 1
- Background scan: 0 seconds
- Antenna gain: 3 dBi
- TX power reduction: 0 dB
- Management VLAN-ID: 0
- Enable QoS according to 802.11e (WME)
- Indoor only mode activated



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).

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.

Possible values:

- Maximum 31 ASCII characters.

Default:

- Blank

■ Inheritance

Selection of a logical WLAN network defined earlier and from which the settings are to be inherited ('Inheritance of parameters' → page 76).

■ Country

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

Possible values:

- Select from the list of countries.

Default:

- Blank

Special values:

- 'Default' makes use of the country setting defined in the 'Options' area.

■ Automatic channel selection

As standard the Access Points can use all of the channels permitted in the country of operation. To limit the selection to certain channel, the desired channels can be entered here as a comma-separated list (e.g. '1,6,11'). Ranges can also be defined.

Possible values:

- Maximum 16 characters.

Default:

- Blank

■ Management VLAN ID

The VLAD ID for the management network that is to manage the Access Points.

Possible values:

- 0 to 4094

Default:

- 0

Special values:

- 0: In general the VLAN function should be switched off—also for all logical WLANs (SSIDs), whatever VLAN configuration they may have.

- 1: Switches the use of VLAN **on**; the management network remains untagged, however.
- 2 to 4094: Switches the use of VLAN **on**; the management network uses the VLAN ID set here.



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.

WLAN profiles

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 ► Common profiles

■ Profile name

Name of the profile under which the settings are saved.

Possible values:

- Maximum 31 ASCII characters.

Default:

- Blank

■ WLAN network list

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

Possible values:

- Maximum of 16 WLAN networks, multiple values separated by commas or activated in the selection list.

Default:

- Blank



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.

EM

■ Physical WLAN parameters

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

Possible values:

- Selection from the list of physical WLAN networks.

Default:

- Blank

■ 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 via DNS or 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).

Possible values:

- IP addresses, multiple values separated by commas. Maximum 159 characters, i.e. 9 to 10 entries depending on the length of the IP addresses.

Default:

- Blank

4.2.3 Access point configuration

This area contains a list of all available Access Points and the IP parameter profiles. You can use these profiles if certain Access Points should not receive their IP addresses via DHCP.

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.

LANconfig: WLAN Controller ► AP config. ► IP parameter profiles

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' → page 76).

■ Domain name

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

Possible values:

- Max. 63 characters

Default:

- Blank

■ Network mask

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

■ DNS default

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

Possible values:

- Valid IP address

Default:

- Blank

■ DNS backup

Second, alternative DNS if the first is unavailable.

Possible values:

- Valid IP address

Default:

- Blank

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:

Access point table - New Entry

Entry active OK

Update management active Cancel

MAC address:

AP name:

Location:

WLAN profile:

WLAN interface 1

Mode WLAN ifc. 1:

Auto. channel selection: Select ▾

Antenna gain: dB

TX power reduction: dB

WLAN interface 2

Mode WLAN ifc. 2:

Auto. channel selection: Select ▾

Antenna gain: dB

TX power reduction: dB

Encryption:

802.11n

Double bandwidth:

Antenna grouping:

Fixed IP addresses

IP address:

IP parameter profile:

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.

Possible values:

- Yes, No

Default:

- Yes

■ **MAC address**

MAC address of the ethernet interface of each Access Point.

Possible values:

- 12 hexadecimal characters.

Special values:

- FFFFFFFFFF defines the default configuration ('Automatic provision of the default configuration' → page 49).

Default:

- Blank

■ **AP name**

Name of the Access Point in managed mode.

Possible values:

- Maximum 16 ASCII characters.

Default:

- Blank

■ **Location**

Location of the Access Point in managed mode.

Possible values:

- Maximum 251 ASCII characters.

Default:

- Blank

■ **WLAN profile**

WLAN profile from the list of defined profiles ('WLAN profile').

Possible values:

- Select from the list of defined WLAN profiles, max. 31 ASCII characters.

Default:

- Blank

■ WLAN interface 1

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

Possible values:

- 2.4 GHz, 5 GHz, off, default

Special values:

- 'Default' makes use of the frequency setting defined in the 'Options' area.

■ Auto. channel selection lfc 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 this channel only 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 country of operation as defined. Invalid channels are ignored. This value is as well used for the automatic channel optimization for assigning a fixed channel to the Access Point.

Possible values:

- Comma-separated list with max. 48 characters

Default:

- Blank

■ WLAN interface 2

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

Possible values:

- 2,4 GHz, 5 GHz, off, default

Default:

- Blank

Special values:

- 'Default' makes use of the frequency setting defined in the 'Options' area.

■ Auto. channel selection lfc 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.

Possible values:

- DTLS, no, default

Default:

- DTLS

Special values:

- 'Default' makes use of the encryption method defined in the 'Options' area.

■ Double bandwidth

LANCOM Access Points compliant with IEEE 802.11n optionally offer the activation of double the bandwidth.

A wireless LAN module normally uses a frequency range of 20 MHz in which data to be transmitted is modulated to the carrier signals. 802.11a/b/g use 48 carrier signals in a 20MHz channel. The use of double the frequency range of 40 MHz means that 96 carrier signals can be used, resulting in a doubling of the data throughput.

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

Possible values:

- Auto, No

Default:

- Auto

■ Antenna grouping

LANCOM access points with 802.11 support can use up to three antennas for transmitting and receiving data. Depending on the application the use of the antennas can be set.

Possible values:

- 1+2+3: When using the device in access point mode to connect wireless LAN clients it is generally recommended to use all three antennas in parallel in order to achieve good network coverage.
- 1+3: Antenna ports 1 and 3 are used for 2 parallel data streams for example in point to point connections with an appropriate dual slant antenna. The third antenna port is deactivated.
- 1: For applications with only one antenna (for example an outdoor application with just one antenna) the antenna is connected to port 1 and ports 2 and 3 are deactivated
- Auto: Automatic antenna selection

Default:

- Auto

Special values:

- Auto: The "Auto" setting means that all available antennas are used.

■ IP address

Static IP address for the AP if DHCP cannot be /should not be used.

Possible values:

- Valid IP address

Default:

- Blank

■ IP parameter profile

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

Possible values:

- Select from the list of defined IP parameter profiles, max. 31 ASCII characters.

Default:

- DHCP

4.2.4 AP update

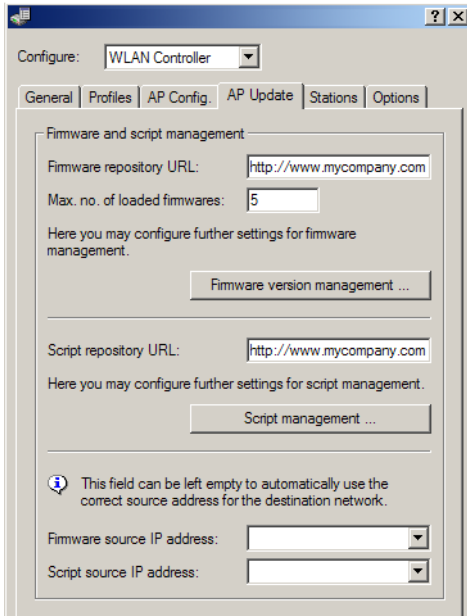
LANCOM WLAN Controllers allow the configurations of multiple LANCOM Access Points to be managed from a central location in a consistent and convenient manner. With central firmware and script management, uploads of firmware and scripts can be automated for all of the WLAN devices.

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 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.



LANconfig: WAN Controller ► AP Update

WEBconfig: Setup ► WLAN Management ► Central Firmware Management

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 valid on the WLAN Controller.

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.



Entries in the firmware management table are only necessary if certain firmware versions are to be uploaded, for example in the case of downgrades. If devices are to use the current firmware only, no entries are required here.

■ 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 valid on the WLAN Controller.

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 an 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 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 an 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 Configure/Wireless LAN/Central Firmware /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.

The screenshot shows the LANCOM Systems web interface. On the left is a navigation menu with items like Setup Wizards, System information, Configuration, LCOS Menu Tree, File management, Extras, HTTP-Session, and Logout. The main content area is titled 'Upload Certificate or File' and includes a 'Logout' button. Below the title, there is a 'Start Upload' button and a list of file types to upload. The list includes:

- SSL - Certificate (*.pem, *.crt *.cer [BASE64])
- SSL - Private Key (*.key [BASE64 unencrypted])
- SSL - Root CA Certificate (*.pem, *.crt *.cer [BASE64])
- SSL - Container as PKCS#12-File (*.pfx *.p12 [requires passphrase])
- SSH - RSA Key (*.key [BASE64 unencrypted])
- SSH - DSA Key (*.key [BASE64 unencrypted])
- SSH - accepted public keys
- VPN - Root CA Certificate (*.pem, *.crt *.cer [BASE64])
- VPN - Device Certificate (*.pem, *.crt *.cer [BASE64])
- VPN - Device Private Key (*.key [BASE64 unencrypted])**
- VPN - Container as PKCS#12-File (*.pfx *.p12 [requires passphrase])
- EAP/TLS - Root CA Certificate (*.pem, *.crt *.cer [BASE64])
- EAP/TLS - Device Certificate (*.pem, *.crt *.cer [BASE64])
- EAP/TLS - Device Private Key (*.key [BASE64 unencrypted])
- EAP/TLS - Container as PKCS#12-File (*.pfx *.p12 [requires passphrase])
- RADSEC - Root CA Certificate (*.pem, *.crt *.cer [BASE64])
- RADSEC - Device Certificate (*.pem, *.crt *.cer [BASE64])
- RADSEC - Device Private Key (*.key [BASE64 unencrypted])
- RADSEC - Container as PKCS#12-File (*.pfx *.p12 [requires passphrase])
- Public Spot - Welcome Page (*.html *.htm)

4.2.5 Stations

The station table defines which WLAN clients can associate with the WLAN networks of the LANCOM Access Points which are centrally managed by the WLAN Controller. Furthermore, the method offers a convenient way to assign an individual authentication passphrase and a VLAN ID to each WLAN client.

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, the passphrases

stored in the '802.11i/WEP' area will be used for each logical wireless LAN network (on the WLAN Controller in the definitions of logical WLANs (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 own settings to the base station when logging in. The Access Point 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.

4.2.6 RADIUS server

By default the WLAN Controller forwards account and access management requests 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, the settings for each individual access point must be entered into the RADIUS server and the managed access points needs to reach the RADIUS server from their management network. If the RADIUS server is located in another network, then the gateway must be determined in the IP parameter profile.

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 taht cannot be changed.

■ IP address

IP address of the RADIUS server that is communicated to 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:

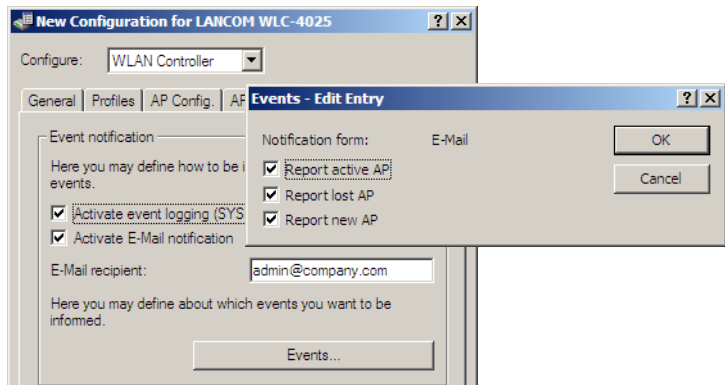
- Blank

4.2.7 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 or off

Default:

Off

■ E-mail

Activates notification by e-mail.

Possible values:

On or off

Default:

Off

■ Events

Selects the events that trigger notification.

Possible values:

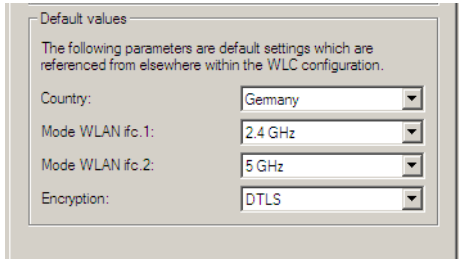
Active Access Point notification

Missing Access Point notification

New Access Point notification

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 ▶ Options ▶ Default parameters

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN management ▶ AP configuration

■ Country

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

■ 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

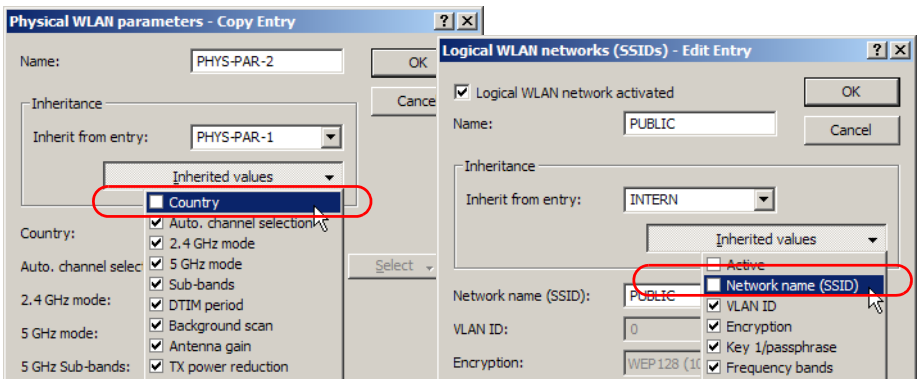
Encryption of communications over the control channel. Without encryption the control data is exchanged as plain text. In both cases authentication is by certificate.

4.2.8 Inheritance of parameters

A LANCOM WLAN Controller is capable of managing a wide range 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.



Changes to the parent entry take immediate effect on all entries which inherit from it. The parent entry itself may also inherit values from other entries. Complex inheritances of this type should be employed with great care, as this can quickly lead to incomprehensible configurations and even errors.



If a parent entry is deleted from the configuration, all settings inherited from it become invalid.

4.3 Sample configurations

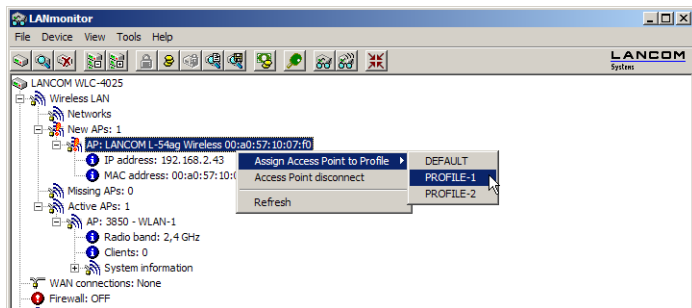
4.3.1 Accepting new Access Points into the WLAN infrastructure manually

If you prefer not to accept Access Points into the WLAN infrastructure automatically (auto-accept, 'Automatically accept new APs (Auto-accept)'), you can accept Access Points manually.

Accepting Access Point via LANmonitor

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.



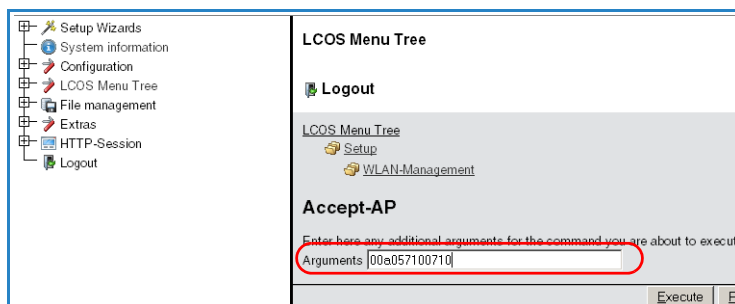
Assignment of the configuration causes the Access Point to be entered into the AP table in the WLAN Controller. It takes a few seconds for the WLAN Controller to assign a certificate to the Access Point and for this to become an active element in the central WLAN infrastructure.

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 LANCOM WLAN Controller configuration with 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 LANCOM WLAN Controller configuration with WEBconfig. If new Access Points have been found, WEBconfig displays this with a notification on the Device status page.

System data	Device status	Syslog
SCEP-CA	CA-Status: Active Pending-Requests: 0	
WLAN-Controller	Controller-State: Ready Expected-AP: 0 Connected-expected-AP: 0 Connected-new-AP: 1	Assign Access Points to Profiles
Update		
Refresh period (s): 30 Page will be reloaded in 0 seconds		

- ② Click on this 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.

192.168.2.34 - Assign Access Points to Profiles **LANCOM**
Systems

... connecting your

Step 3 of 4

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

Profile

! 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.

! A number of administrator accounts with different rights can be set up for configuring LANCOM devices. It may be worthwhile to set up an administrator account on a WLAN Controller for accepting access points, but which does not allow any other changes to the configuration. Instructions on creating administrator accounts are available in the LCOS Reference Manual.

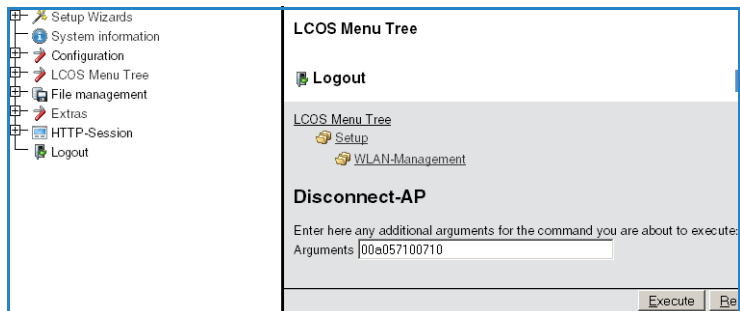
4.3.2 Deactivating Access Points or permanently removing them from the WLAN infrastructure

Occasionally it is necessary to temporarily deactivate or even permanently remove a WLAN Controller-managed Access Point.

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'.
- 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 ethernet MAC address of the Access Point to be disconnected and confirm with **Execute**.



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 ('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 simply by activating the entry in the AP table or by making a new entry in the AP table along with the appropriate MAC address.

If the connection to a deactivated 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, it is treated as a secondary WLAN Controller by the Access Point. If the Access Point finds a WLAN Controller then it will register with it.

Permanently removing Access Points 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 changing to **Status ▶ Certificates ▶ SCEP-CA ▶ Certificates** and accessing the **Certificate status table**. Here you delete the certificate for the MAC address of the Access Points which are to be removed from the WLAN infrastructure. The certificates are not actually deleted, but they are marked as expired.

4.3.3 Backing up the certificates

At system startup, a LANCOM WLAN Controller generates the own 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.

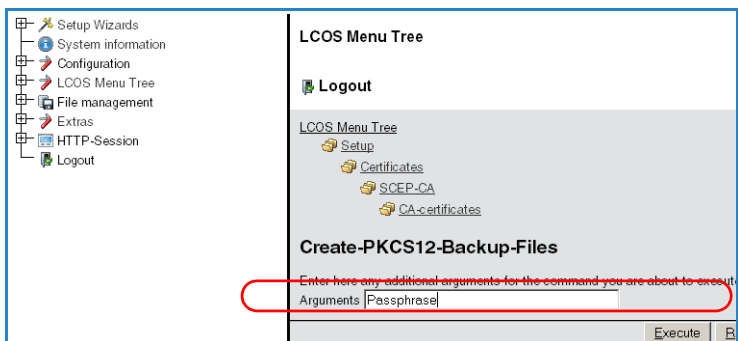
If multiple WLAN Controllers are employed in parallel in the same WLAN infrastructure (for load balancing) or if a device is being replaced or reconfigured, the same root certificates must always be used to avoid problems operating the managed Access Points.

Create backups of the certificates

To restore the CA or RA, the relevant root certificates with private keys will be required as generated automatically when the LANCOM WLAN Controller was started. Furthermore the following files with information on issued device certificates should also be backed up ('Backing up and restoring further files from

the SCEP-CA'). To ensure that this confidential information remains protected even when exported from the device, it is initially stored to a password-protected PKCS12 container.

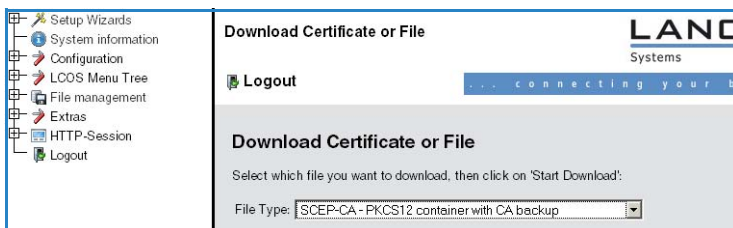
- ① Open the configuration of the LANCOM WLAN Controller with WEBconfig under **LCOS menu tree ▶ Setup ▶ Certificates ▶ SCEP-CA ▶ CA certificates**.
- ② Select the command **Create PKCS12 backup files** and enter the passphrase for the PKCS12 container as the additional argument.



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

Downloading certificate backups from the device

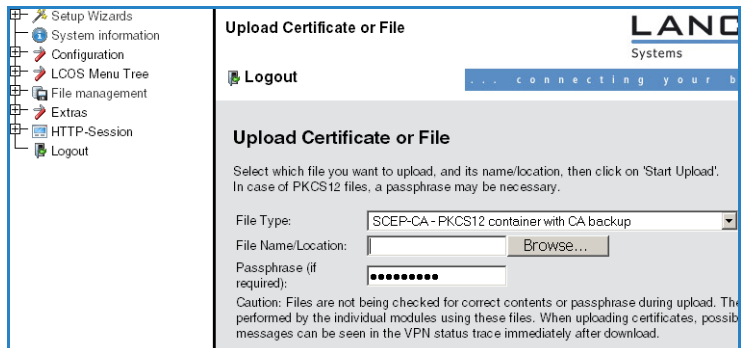
- ① On the WEBconfig entry page select the command **Download certificate or file**.
- ② Select the two entries for SCEP-CA as data type one after the other and confirm with **Start download**:
 - PKCS12 container with CA backup
 - PKCS12 container with RA backup



The backup file is then stored to your data medium. The passphrase will be required is when uploading the backup to a LANCOM WLAN Controller.

Uploading a certificate backup into the device

- ① On the WEBconfig entry page select the command **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**:



- 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 that, access the directory /Setup/Certificates/SCEP-Client and execute the command Reinit:


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

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

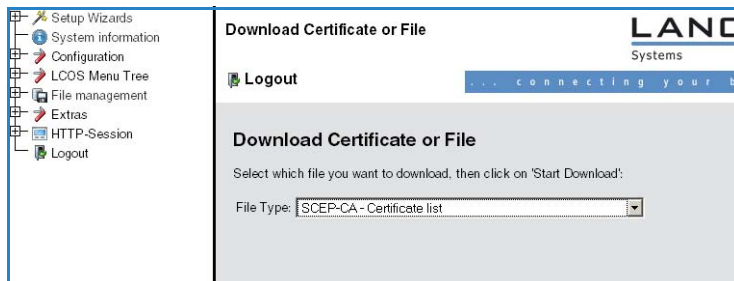
To be able to fully restore the SCEP-CA, it is important to have the information on the device certificates issued for the individual Access Points by the SCEP-CA.



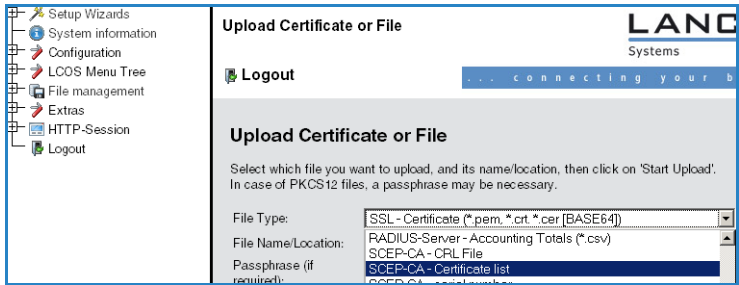
If the root certificates only were backed up, then any issued device certificates can no longer be revoked!

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

- SCEP CA certificate list: List of all certificates ever issued by the SCEP-CA.
 - SCEP CA serial number: Contains the next available serial number for the next certificate.
- ① On the WEBconfig entry page select the command **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 start 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**:



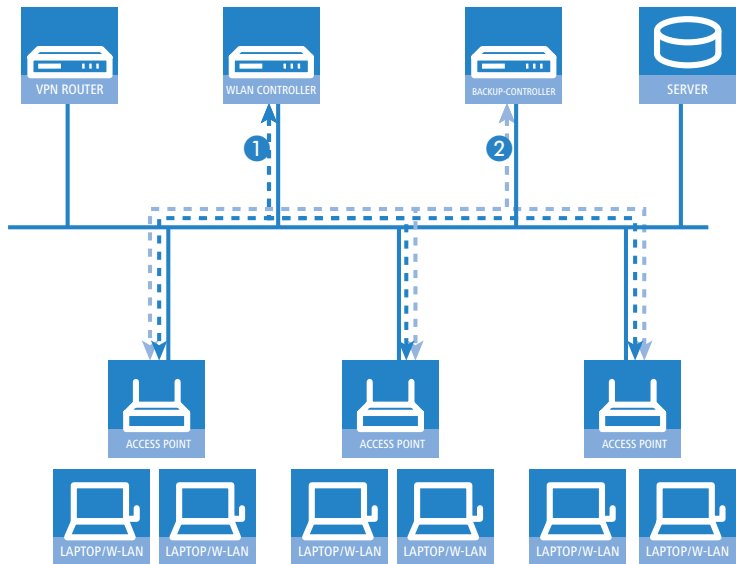
After installing a new certificate list, expired certificates are removed and a new CRL is created. Furthermore, the CA reinitializes itself automatically if certificates and keys are successfully extracted after loading the certificate backup.

4.3.5 LANCOM WLAN Controller backup

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.

- To achieve this, generate a backup certificate on one of the WLAN Controllers and upload this to all of the other WLAN Controllers (also see 'Backing up the certificates' → page 82).
- All of the WLAN Controllers should be set with same time information to ensure that checks on the certificate validity period all produce the same result.



- ① Set the same time on the two LANCOM WLAN Controllers ① and ②.
- ② Transfer the CA and RA certificates from a WLAN Controller ① to the second and backup Controller ②.
- ③ 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.
- ④ Save the configuration from the first WLAN Controller ① to a file, for example using LANconfig. In this configuration file assign an appropriate IP address for the backup controller.
- ⑤ Transfer this modified configuration 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.
- ⑥ 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.

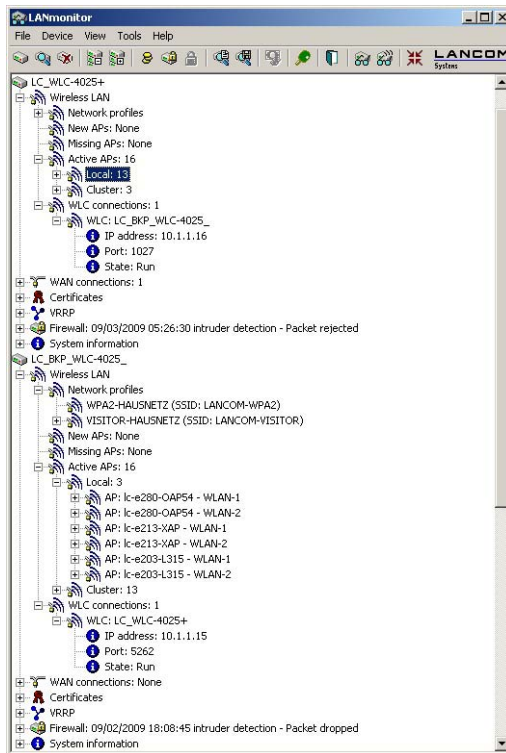


In this scenario, the Access Points remain under the management of the backup controller until this itself becomes unavailable or is manually disconnected ('Disconnect Access Point' → page 112).



If the Access Points are set up for standalone operation ('Self-sufficient operation' → page 52) they will remain operational while searching for a backup controller, and the WLAN clients will remain associated.

- ⑦ In LANmonitor the connections between the access points and controllers are displayed: At this time, local access points are managed by the relevant controller itself. Access Points in the "cluster" are managed by another controller, although they could also be taken over by the former controller.



4.3.6 Load balancing between WLAN Controllers

If multiple WLAN Controllers are available in a network, the Access Points are automatically distributed evenly between the WLAN Controllers.

At the beginning of communications, the Access Point sends a "Discovery Request Message" to find any available WLAN Controllers.

- From the available WLAN Controllers the Access Point selects the one with the lowest load, i.e. that with the lowest ratio of managed Access Points to the maximum possible 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.

In this way, e.g. by activating multiple WLAN Controllers via automatic assignment of configurations ('Automatically provide APs with a default con-

figuration'), all WLAN Controllers can be "filled" with equal numbers of configurations from a portion of the Access Points.

If a second WLAN Controller is to be integrated into a network in addition to an existing WLAN Controller, all of the access points initially remain registered with the older controller. The following is a convenient procedure to distribute the access points between the two controllers:

- ① Set the time on the second controller to be the same as that on the existing device.
- ② Transfer the CA and RA certificates from the existing WLAN Controller to the new device.
- ③ Activate 'Automatically accept new APs (Auto-accept)' in the new controller.
- ④ Save the configuration from the existing WLAN Controller to a file, for example using LANconfig. In this configuration file assign an appropriate IP address for the new controller.
- ⑤ Transfer this modified configuration to the new controller ②. The profiles and the AP tables with the Access Point MAC addresses are transferred to the new controller at the same time.
- ⑥ Switch the former controller off. The access points now search for an available controller. They find the new device, which already has the appropriate CA certificates and WLAN profiles. The new controller can now issue new device certificates on request from the access points, and it takes over the system management.
- ⑦ Switch the former controller on again. Initially, the Access Points remain under the management of the new controller. By manual means, a proportion of the access points are again disconnected from the new controller. These access points then search again for an available controller. They now connect with the former controller, as this has a lower traffic load.

4.3.7 Dynamic VLAN assignment

Larger WLAN infrastructures often require individual WLAN clients to be assigned to certain networks. In general the assignment can be realized via the SSID in connection with a particular IP network. For larger organizations it may not be useful to define a special SSID for each departement. Dynamically assigned VLANs can be used where WLAN clients are to remain within a

certain network and logically separated from the other users, **independent** of the WLAN network they are currently using. Unlike the situation where VLAN IDs are statically configured for a certain SSID ('VLAN ID'), in this case a RADIUS server directly assigns the VLAN ID to the WLAN client.

Example:

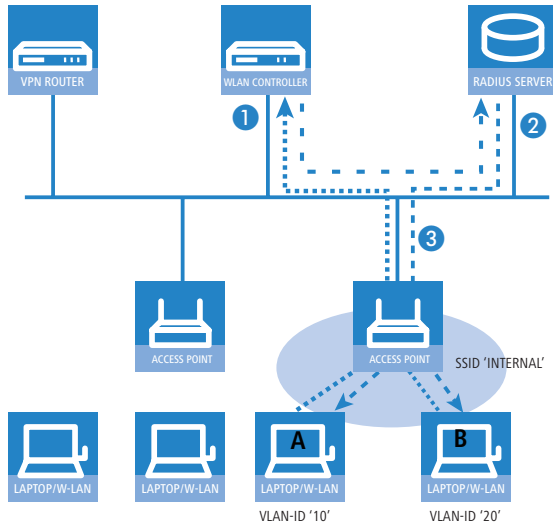
- The WLAN clients of two employees log into an Access Point in the WPA-secured network with the SSID 'INTERNAL'. During registration, the RADIUS requests from the WLAN clients are directed to the Access Point. If the corresponding WLAN interface is in the operating mode 'managed' the RADIUS requests 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 or user names when using 802.1x 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.



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 ('Station table (ACL table)').



- 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' (Management VLAN ID) 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 by IEEE 802.1x (e.g. '802.11i (WPA)-802.1x').
- ③ To check the MAC addresses, activate the MAC check for the profile's logical WLAN network.

i 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 Point are then directly forwarded to the WLAN Controller, which can either process the requests itself or forward them to an external RADIUS server. Alternatively the access points can communicate with the RADIUS server directly if the information about the RADIUS server is configured accordingly ('RADIUS server' → page 73).

- 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), see 'Configuring RADIUS forwarding' → page 109.

- 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.

4.3.8 Virtualization and guest access 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.

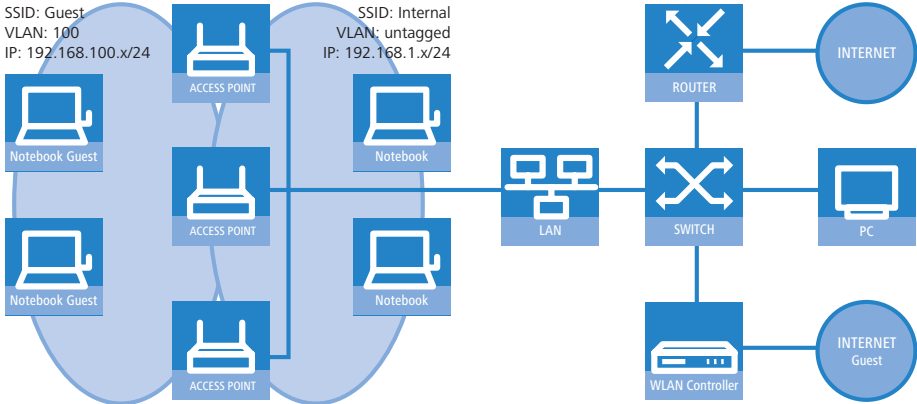
Objectives

- 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.

Structure

- 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:

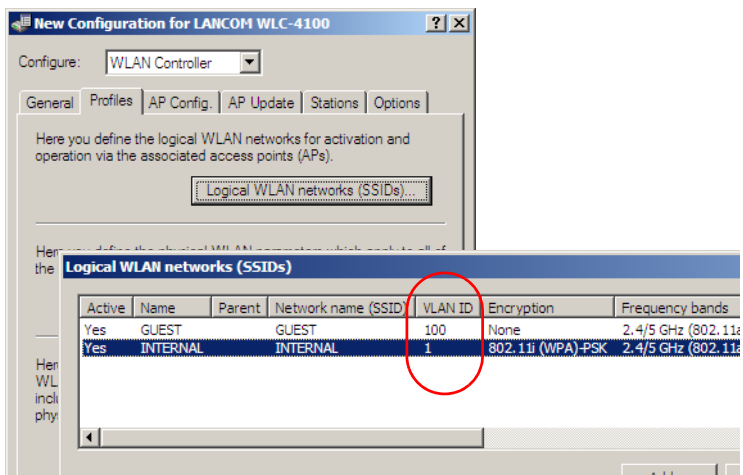
- The VLAN management of access points is handled by the LANCOM WLC.
- The VLAN management of the switches is handled separately by the switch configuration.
- The access points operate within the internal VLANs.



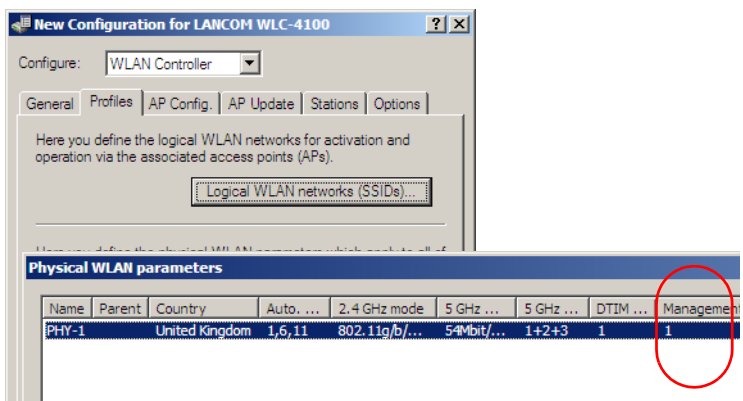
Wireless LAN configuration of the WLAN controllers

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

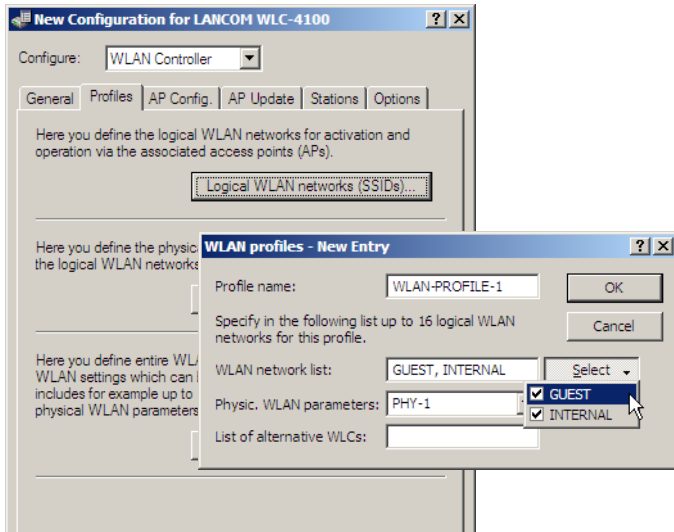
- ① Create a logical WLAN for guests and one for the internal employees:
 - The WLAN with the SSID 'GUESTS' uses the VLAN ID '100'. No encryption is employed here.
 - The WLAN with the SSID 'INTERNAL' uses the VLAN ID '1' (i.e. transmitted to the Ethernet without a VLAN tag), and WPA encryption is employed.



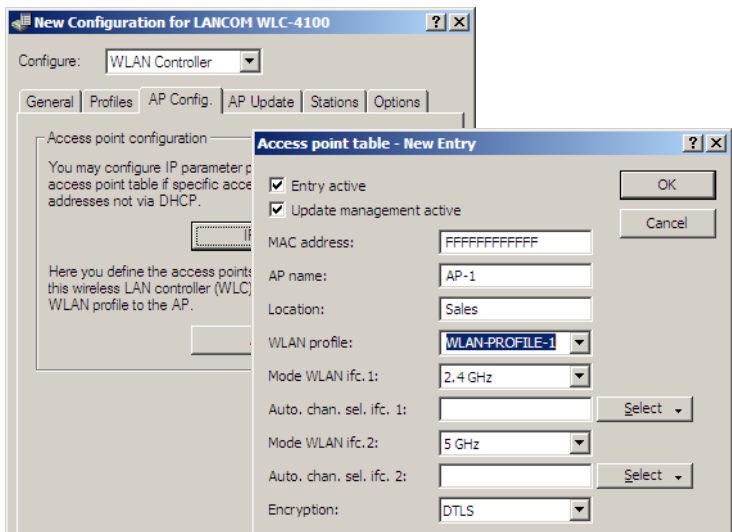
- ② Create a set of physical parameters for the access points. The management VLAN ID is set to '1', which serves to activate the VLAN function (but without a separate management VLAN for the device; the management data traffic is transmitted untagged).



- 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.



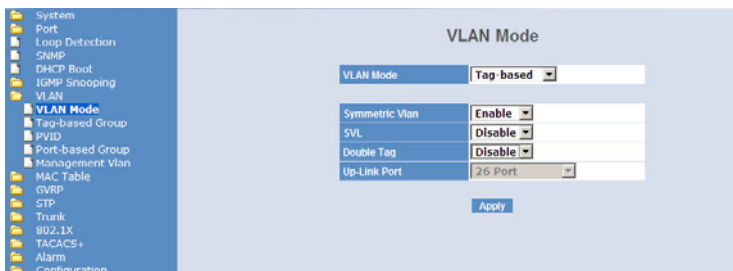
- ④ Assign this WLAN profile to the access points managed by the controller. Do this either by entering the individual access points with their MAC addresses or, alternatively, you can use the default profile.



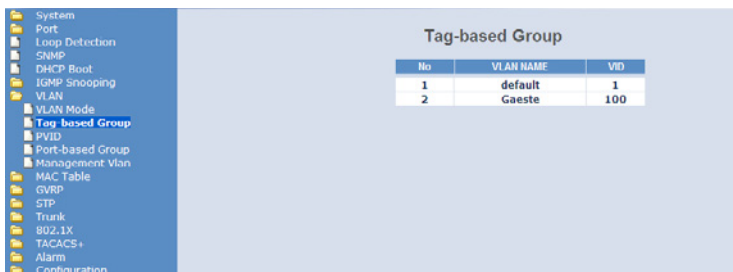
Configuring the switch

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

- ① Set the VLAN mode to "Tag based", as the access points handle the assignment of VLAN tags.



- ② 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 VLANs.



- ③ 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.

Tag-based Group

No	VLAN NAME	VID
1	default	1
2	Gaeste	100

VLAN name: default
 VID: 1
 GVRP Propagation: Enable

Member	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Untag	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

- ④ 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.

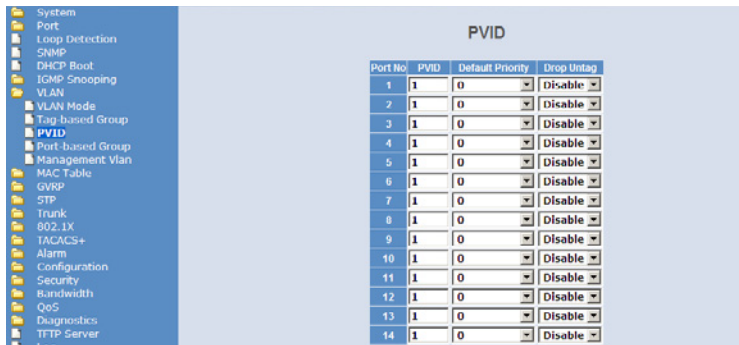
Tag-based Group

No	VLAN NAME	VID
1	default	1
2	Gaeste	100

VLAN name: Gaeste
 VID: 100
 GVRP Propagation: Disable

Member	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Untag	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

- ⑤ 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'.



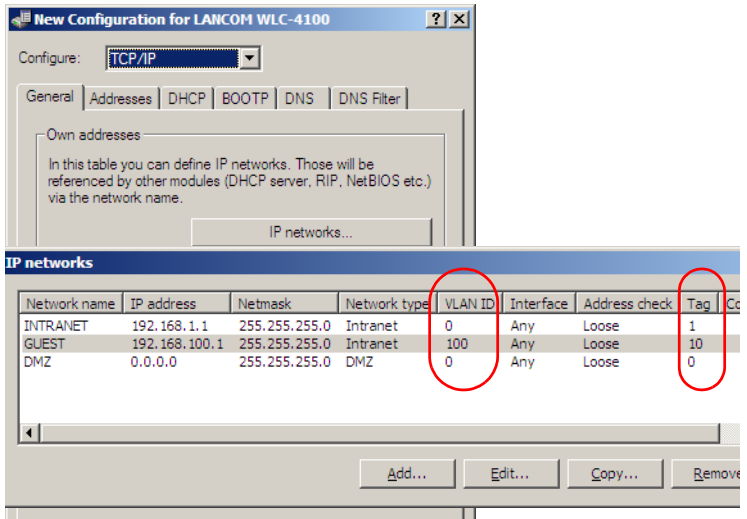
The screenshot shows the configuration interface for the PVID (Port VLAN ID) settings. On the left is a navigation tree with 'PVID' selected. The main area displays a table with the following data:

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

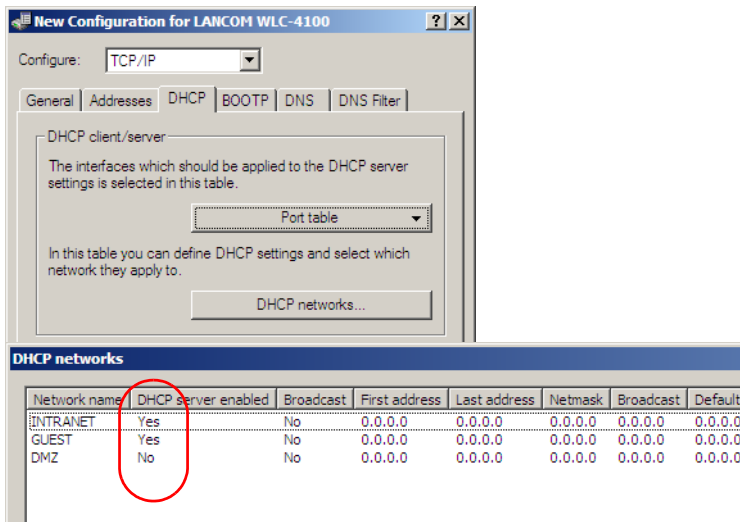
Configuring the IP networks in the WLAN controller

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

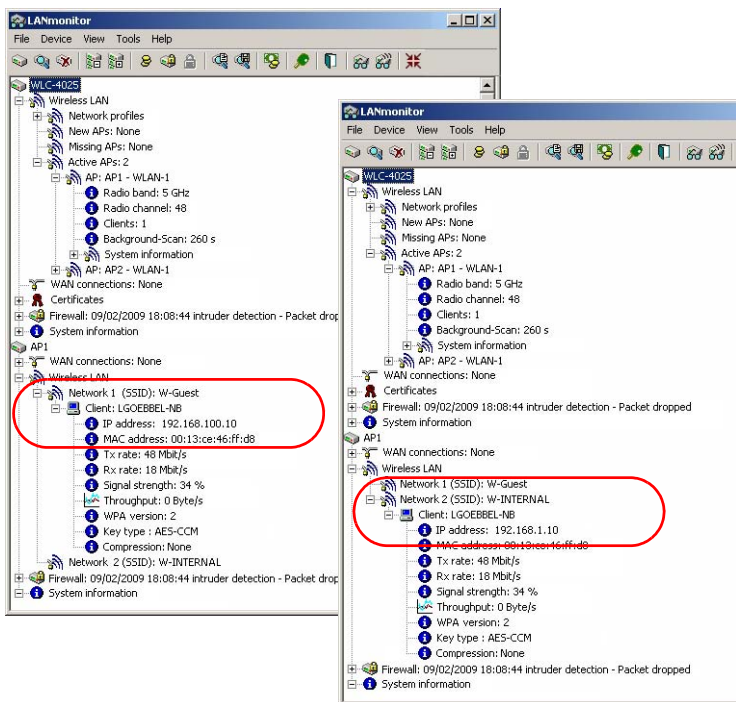
- ① The first step is to define the required IP networks.
 - For the internal network, set the 'Intranet' to the address '192.168.1.1'. This IP network uses the VLAN ID '0'. This assigns all untagged data packets to this network (the VLAN module in the controller itself must be activated for this). The 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.



- ② For both IP networks, an entry is created in the DHCP networks to permanently activate the DHCP server.



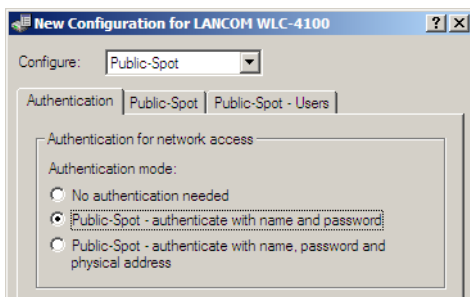
- ③ With these settings, the WLAN clients of the internal employees and guests are assigned to the appropriate networks.



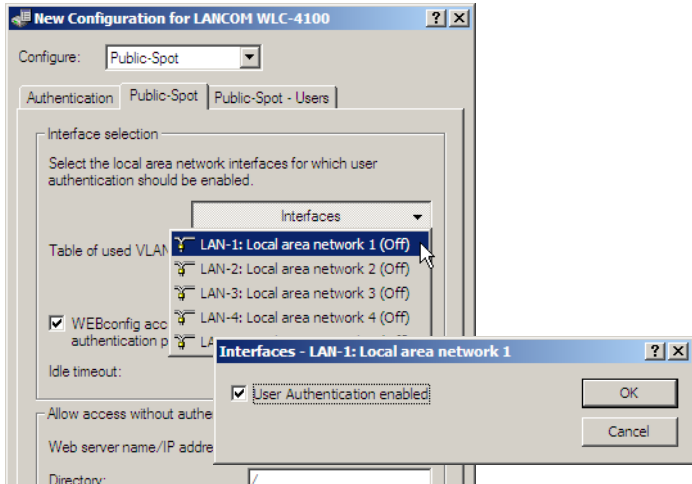
Configuring Public Spot access

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. If desired, access can be subject to time limits.

- ① Activate authentication for network access by name and password.



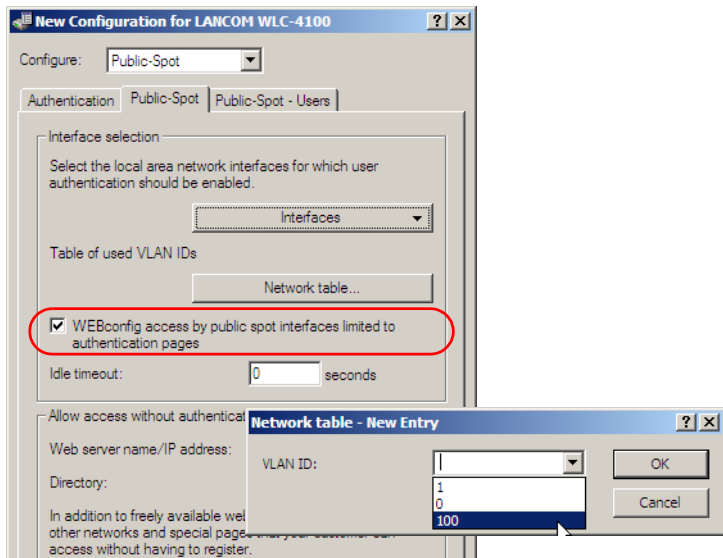
- ② Activate user authentication for the controller's interface that is connected to the switch.



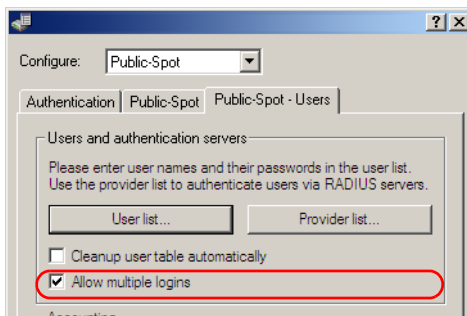
- ③ By entering the VLAN ID of '100' for the guest network into the VLAN table, the data packets for Public Spot users are restricted to this virtual LAN. Other data packets from other VLANs will be forwarded without a Public Spot login. Note that access to WEBconfig via the Public Spot interface is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



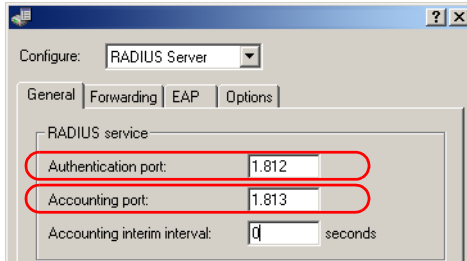
- ④ In the Public Spot module, activate the "Cleanup user table automatically" option to ensure that unwanted entries are automatically deleted.



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 1,812 and the accounting port 1,813.



- 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, 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.

- ③ Use the authentication and accounting port settings from the RADIUS server (1,812 and 1,813).

The screenshot shows a dialog box titled "Provider list - New Entry". It contains the following fields and values:

- Provider: RADIUS-INTERNAL
- Backup provider: (empty dropdown)
- Authentication server section:
 - Auth. server IP address: 12.0.0.0
 - Auth. server port: 1.812
 - Auth. server secret: (empty text box)
 - Source IP address: (empty dropdown)
- Accounting server section:
 - Acc. server IP address: 12.0.0.0
 - Acc. server port: 1.813
 - Acc. server secret: (empty text box)
 - Source IP address: (empty dropdown)

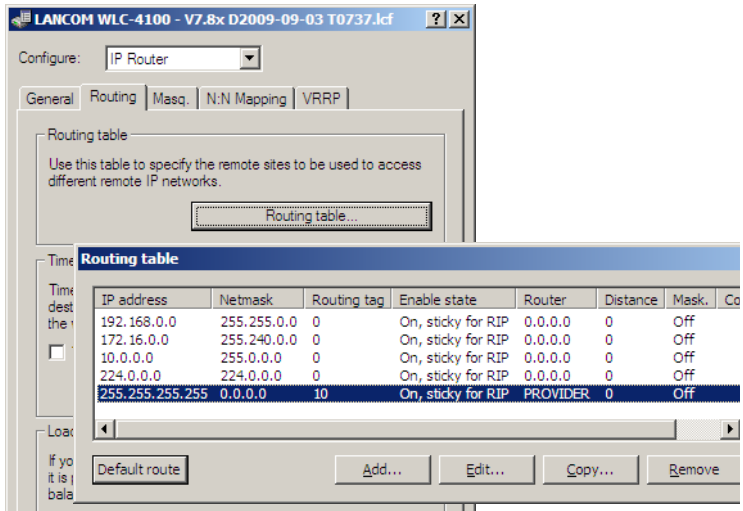
Buttons for "OK" and "Cancel" are located on the right side of the dialog.



After updating to LCOS 7.70, user accounts created in the Public Spot module's user list with previous versions of LCOS remain valid.

Configuring Internet access for the guest network

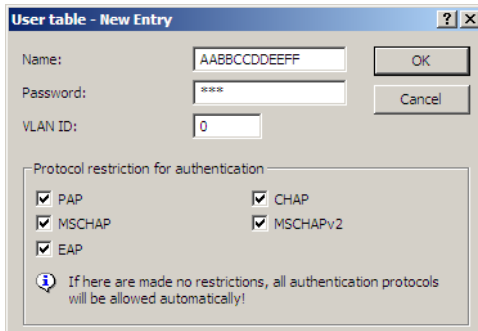
- ① In order to provide users of the guest network with Internet access, the wizards can be used to create access to the provider network.
- ② In order for this access to be available to users of the guest network only, the corresponding route is set for the routing tag '10'. This ensures that only data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



4.3.9 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.

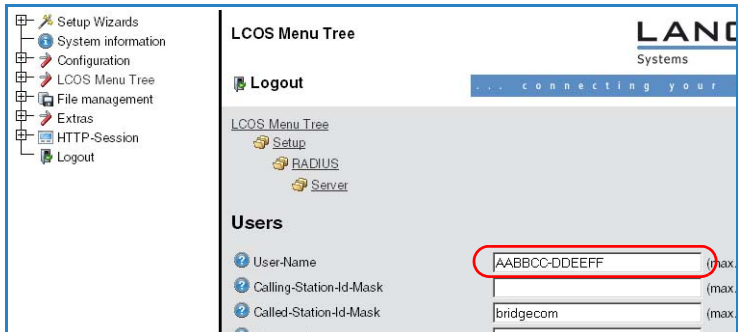
In LANconfig enter the approved MAC addresses into the RADIUS database in the configuration section 'RADIUS servers' on the 'General' tab. Enter the MAC address as 'Name' and as 'Password' and select the authentication method 'All'.



Alternatively, 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'.



4.3.10 Internal and external RADIUS servers combined

Some companies use an external RADIUS server to authenticate internal WLAN users by IEEE 802.1x. For applications with a WLAN controller and multiple access points, the access points initially address the WLAN controller as their RADIUS server. The WLAN controller then forwards the RADIUS requests to the external RADIUS server.



The settings described below are only necessary if you are operating an external RADIUS server in addition to the Public Spot in the LANCOM.

A Public Spot providing guest-access accounts requires the following settings:

- Authentication requests from internal employees are to be forwarded to an external RADIUS server.
- The authentication requests for Public Spot access accounts are to be handled by the internal RADIUS server.


Realm tagging for RADIUS forwarding

Authentication requests from the two user groups are to be handled separately. The WLAN controller uses what are known as "realms" to differentiate between these two groups. The purpose of realms is to address domains within which user accounts are valid. Realms can be sent with the authentication requests to the WLAN controller's RADIUS server. Alternatively, the

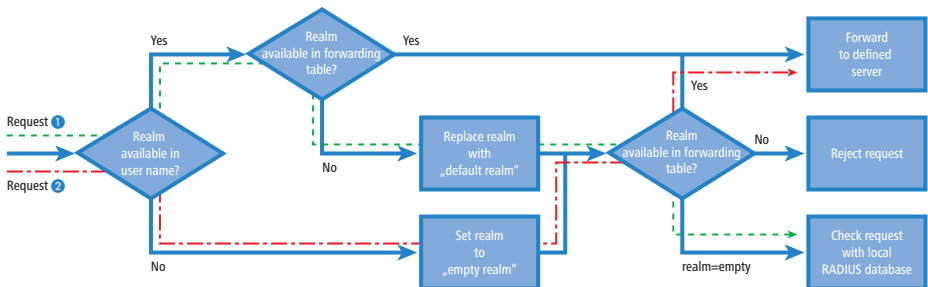
RADIUS server can change the realms in the user names for the purpose of RADIUS forwarding:

- The value defined for "Standard realm" replaces an existing realm of an incoming request if no forwarding is defined for that existing realm.
- The value defined under "Empty realm" is **only used** if the incoming user name **does not yet have** a realm.

An entry in the forwarding table causes all authentication requests with a certain realm to be forwarded to a RADIUS server. If no matching entry exists in the forwarding table, the request is refused.

 If a realm is found to be an empty realm, the authentication request is **always** checked with the internal RADIUS database in the LANCOM.

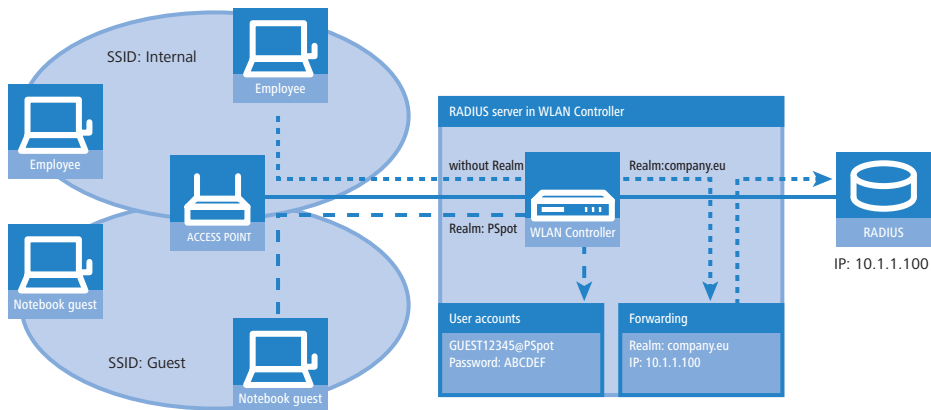
The following flow diagram illustrates the method used by the RADIUS server to process realms:



Using different realm tags allows different RADIUS servers to be targeted with requests. The way in which the LANCOM's RADIUS server makes decisions for the two requests is shown in the diagram.

- 1 Because the user names for guest access accounts are generated automatically, they are suffixed with an appropriate realm, such as "PSpot". Because the forwarding table does not contain this entry and the standard realm is empty, all authentication requests with this realm are forwarded to the internal RADIUS server.
- 2 To limit the amount of work required for the configuration, internal users are listed without a realm. The RADIUS server in the LANCOM can automatically replace an empty realm with another realm in order to identify internal users. In this example, the empty realm is replaced by the domain

of the company "company.eu". The information specified in the forwarding table allows all authentication requests with this realm to be forwarded to the external RADIUS server.



Configuring RADIUS forwarding

The following configuration steps allow you to specify the different manners in which internal users and guests are processed.

- ① In the Public Spot, adapt the pattern of user names such that a unique realm can be suffixed. For example, the pattern "GUEST%n@PSpot" generates user names that appear like "GUEST12345@PSpot".

Configure: Public-Spot

Authentication Public-Spot Public-Spot - Users

Users and authentication servers

Please enter user names and their passwords in the user list.
Use the provider list to authenticate users via RADIUS servers.

User list... Provider list...

Cleanup user table automatically
 Allow multiple logins

Accounting

Accounting update cycle: 0 seconds

Add user wizard

Public spot user accounts can be easily generated by the WEBconfig wizard. Both user name and password are generated automatically, and the next page offers to print out a page for the public spot user that contains all necessary data.

Default validity periods...

User name pattern: GUEST%n@Pspot

Password length: 6

SSID:

- ② In the WLAN controller's RADIUS server, define an "empty realm" (e.g. "COMPANY.EU"). This realm is attached to all user names which request authentication from the WLAN controller and which do not already have a realm. In this application, the internal users have no realm defined. In order to prevent the WLAN controller's RADIUS server from attaching a realm, the "Default realm" field must be left empty.

New Configuration for LANCOM WLC-4025+

Configure: RADIUS Server

General Forwarding EAP Options

RADIUS Forwarding

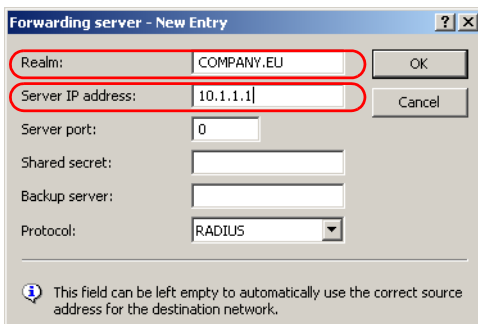
If RADIUS forwarding might be used further settings must be taken here.

Forwarding server...

Default-Realm:

Empty-Realm: COMPANY.EU

- ③ In order for authentication requests from internal users to be forwarded to the external RADIUS server, suitable entries must be entered into the forwarding settings. The realm "COMPANY.EU" causes all incoming RADIUS requests to be forwarded to the specified IP address.



Forwarding server - New Entry

Realm: COMPANY.EU

Server IP address: 10.1.1.1

Server port: 0

Shared secret:

Backup server:

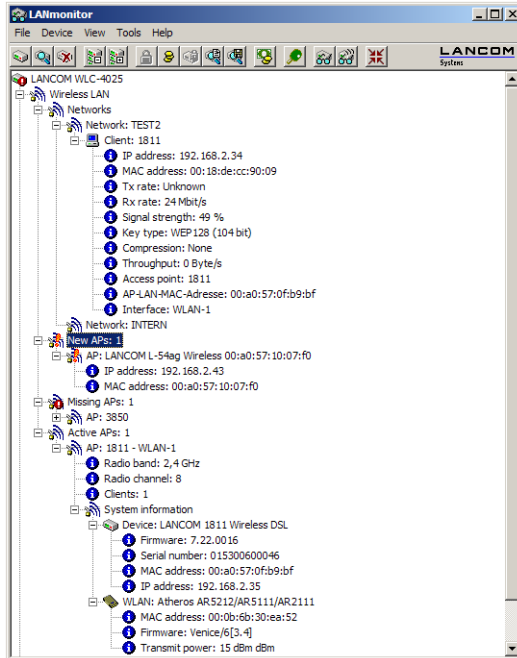
Protocol: RADIUS

This field can be left empty to automatically use the correct source address for the destination network.

- ④ Authentication requests from Public Spot users have the realm "@PSpot" and are received by the WLAN Controller. With no forwarding defined for this realm, the usernames are automatically checked with the internal RADIUS database. Because the Public Spot access accounts created with the Wizard are stored in this database, these requests can be authenticated as required.

4.4 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 Points 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 ('Access point acceptance via LANmonitor').
- **Disconnect Access Point**
Breaks the connection between Access Point and 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.

■ Update

Updates LANmonitor's display.

4.5 Automatic RF optimization with LANCOM WLAN Controllers

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



With a completely empty channel list, the 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 direct access points towards certain channels, the non-overlapping channels 1, 6, 11 can be activated in the channels list.

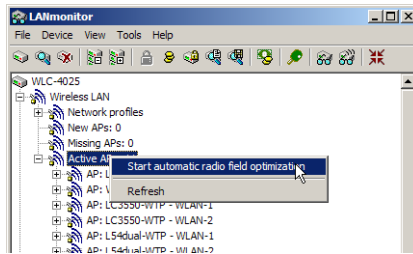
In larger installations with several Access Points it can be difficult to set a channel for every Access Point. With automatic radio-field (RF) optimization, the LANCOM WLAN Controllers provide an automatic method of setting the optimum channels for Access Points that work in the 2.4-GHz band.

WEBconfig: **Setup ▶ WLAN-management ▶ Start-automatic-radio-field-optimization**



Optimization can be initiated for a single Access Point by entering the MAC address as an argument 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 deletes the AP channel list in all of the Access Points in the 2.4-GHz range. Because the channel list for the Access Points is then empty, the channel list from their profile is assigned to them by means of a configuration update.
- ② The WLAN Controller switches off all radio modules operating at 2.4 GHz.
- ③ The Access Points are switched on again one after the other. They are processed in the same order that they were registered with the WLAN Controller.
- ④ Automatic calibration: After being switched on, the access point itself selects the most suitable channel from the list. 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 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.
- ⑤ The selected channel is then communicated back to the WLAN Controller and entered into the AP channel list there. For this reason, the Access Point receives the same channel the next time a connection is established. The AP channel list thus has a higher weighting than the profile channel list.



If an Access Point is equipped with multiple WLAN modules, this process is carried out separately for each WLAN module, one after the other.

4.6 Configuring the Access Points

Please note that the access points must have an IP address in order to communicate with the WLAN Controller. The IP address can either be entered into the access point as a fixed value, or retrieved from a DHCP server.



If the access point is to retrieve an IP address from a DHCP server but the server is unobtainable, then an access point which is restarting may not have an IP address, and thus be unable to communicate with the WLAN Controller.

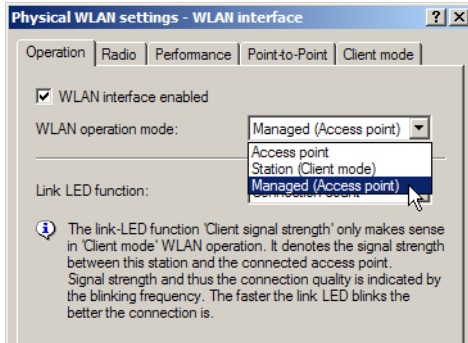
As of firmware version LCOS 7.20 there is a difference between LANCOM Access Points (e. g. the LANCOM L-54ag) and LANCOM Wireless Routers (e. g. the LANCOM 1811 Wireless) with regard to the ex-factory standard settings in the WLAN modules.

- 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.
- When shipped, the WLAN modules in LANCOM Wireless Routers are set to the 'Access point' operating mode. In this mode, LANCOM Wireless Routers function as self-sufficient Access Points and use 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 (7.22 / 23.08.2007)
- lang English
- flash 0
- cd Setup/Interfaces/WLAN/Operational
- set WLAN-1 0 managed-AP 0
- # done
- exit

5 Security settings

Your LANCOM features numerous security functions. This chapter provides you with all of the information you need to optimally protect your device.



You can carry out the configuration of security settings very quickly and conveniently with the Security Wizards in LANconfig and WEBconfig.

5.1 Security in the wireless LAN

Wireless LANs are potentially a significant security risk. It is a common assumption that it is simple to misuse data transferred by wireless.

Wireless LAN devices from LANCOM Systems enable the latest security technologies to be used.

- Encrypted data transfer (802.11i/WPA)
- 802.1x / EAP
- LANCOM Enhanced Passphrase Security (LEPS)
- Access control by MAC address
- Optional IPSec-over-WLAN VPN

5.1.1 Encrypted data transfer

Encryption takes on a special role in the transfer of data in wireless LANs. Wireless communication with IEEE 802.11 is supplemented with the encryption standards 802.11i/WPA and WEP. The aim of the encryption methods is to provide wireless LAN with levels of security equivalent to those in cabled LANs.



LANCOM Systems's recommendation for the most secure passphrase variant is to employ 802.11i (WPA2) in combination with AES. The key should be randomly selected from the largest possible range of numbers and should be as long as possible (32 to 63 characters). The prevents dictionary attacks.

- Use encryption on the data transferred in the WLAN. Activate the strongest possible encryption method available to you ((802.11i with AES, TKIP or WEP) and enter the appropriate keys or passphrases into the access point and the WLAN clients.

- The passphrases for 802.11i or WPA do not have to be changed quite so regularly as new keys are generated for each connection anyway. This is not the only reason that the encryption with 802.11i/AES or WPA/TKIP is so much more secure than the now obsolete WEP method. If you use WEP encryption to maintain compatibility with older WLAN clients, regularly change the WEP key in your access point and limit these clients to a separate SSID for lower security requirements assigning a dedicated VLAN ID (if possible).
- If the data is of a high security nature, further improvements include additionally authenticating the client with the 802.1x method ('802.1x / EAP' → page 118) or activate an additional encryption of the WLAN connection as used for VPN tunnels ('IPSec over WLAN' → page 119). In special cases, a combination of these two mechanisms is possible.



Detailed information about WLAN security and the various encryption methods are to be found in the LCOS reference manual.

5.1.2 802.1x / EAP

The international industry standard IEEE 802.1x and the **Extensible Authentication Protocol (EAP)** enable access points to carry out reliable and secure access checks. The access data can be managed centrally on a RADIUS server (integrated RADIUS/EAP server in the WLAN Controller or external RADIUS/EAP server) and accessed by the access point when required. The dynamically generated and cryptographically secure key material for 802.11i (WPA1/2) replaces the manual key management.

The IEEE-802.1x technology has already been fully integrated since Windows XP. Client software exists for other operating systems. The drivers for the LANCOM AirLancer wireless cards feature an integrated 802.1x client.

5.1.3 LANCOM Enhanced Passphrase Security

With LEPS (**LANCOM Enhanced Passphrase Security**), LANCOM Systems has developed an efficient method that makes use of the simple configuration of IEEE 802.11i with passphrase, but that avoids the potential error sources in passphrase distribution. LEPS uses an additional column in the ACL to assign an individual passphrase consisting of any 4 to 64 ASCII characters to each MAC address. The connection to the access point and the subsequent encryption with IEEE 802.11i or WPA is only possible with the right combination of passphrase and MAC address.

LEPS can be used locally in the device and can also be centrally managed with the help of a RADIUS server, and it works with all WLAN client adapters currently available on the market without modification. Full compatibility to third-party products is assured as LEPS only involves configuration in the access point.

5.1.4 Access control by MAC address

Every network device has a unique identification number. This identification number is known as the MAC address (**M**edia **A**ccess **C**ontrol) and it is unique worldwide.

The MAC address is programmed into the hardware. Wireless LAN devices from LANCOM Systems display their MAC number on the housing.

Access to an infrastructure network can be limited to certain wireless LAN devices by defining MAC addresses. The WLAN controllers have a filter list (ACL – access control list) for storing authorized MAC addresses.

5.1.5 IPSec over WLAN

With the help of the IPSec-over-WLAN technology in addition to the security measures described already, a wireless network for the exchange of especially sensitive data can be optimally secured. Generally speaking this requires an external VPN gateway and the LANCOM Advanced VPN Client (for Windows 2000, XP and Vista™). The LANCOM WLAN Controller itself provides only a small number of VPN tunnels, such as those used for site-to-site connectivity. Client software from third parties is available for other operating systems.

5.2 Tips for the proper treatment of keys and pass-phrases

By observing a few vital rules on the treatment of keys you can significantly increase the security of encryption techniques.

■ Keep your keys as secret as possible.

Never write down a key. Popular but completely unsuitable are, for example: Notebooks, wallets and text files on the computer. Do not pass on a key unless it is absolutely necessary.

■ Choose a random key.

Use long random strings that combine letters and numbers (at least 32 to a maximum of 63 characters). Keys that are normal words are not secure.

■ **If you suspect anything, change the key immediately.**

When an employee with access to a key leaves the company, then it is high time to change the wireless LAN key. Even if there is the slightest suspicion of a leak, renew the key.

■ **LEPS avoids the global distribution of passphrases.**

Activate LEPS to enable the use of individual passphrases. 802.1x allows the user specific assignment of access settings and the locking of compromised user accounts.

5.3 Security settings Wizard

Access to the configuration of a device allows access to more than just critical information (e. g. WPA key, Internet password). Far more critical is that settings for security functions (e.g.the firewall) can be altered. Unauthorized access is not just a risk for the device itself, but for the entire network.

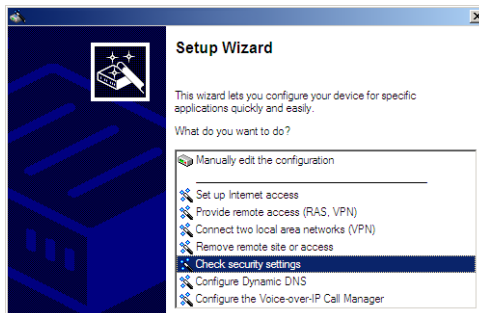
Your LANCOM offers password-protected access to its configuration. This is activated during the initial basic configuration simply by entering a password.

If the wrong password is entered a certain number of times, the device automatically blocks access to the configuration for a fixed period. You can modify the critical number of attempts and also the duration of the lock. By default, the device locks for five minutes after five incorrect entries of the password.

Along with these basic settings, you can use the Security settings Wizard to check the settings of your wireless network (if so equipped).

5.3.1 LANconfig Wizard

- ① Mark your LANCOM in the selection window. From the command line, select **Extras ▶ Setup Wizard**.



- ② In the selection menu, select the Setup Wizard, **Check security settings** and confirm the selection with **Next**.
- ③ In the dialogs that follow you can set the password and select the protocols to be available for accessing the configuration from local and remote networks.
- ④ In a subsequent step, you can set parameters for locking the configuration such as the number of incorrect password entries and the duration of the lock.
- ⑤ The Wizard will inform you as soon as the entries are complete. Close the configuration with **Finish**.

5.3.2 WEBconfig Wizard

With WEBconfig you have the option to launch the **Check security settings** Wizard to check and change any settings. The following values are edited:

- Device password
- The protocols to be available for accessing the configuration from local and remote networks
- The parameters for locking the configuration (the number of incorrect password entries and the duration of the lock)

5.4 The security checklist

The following checklists provide an overview of all security settings that are important to professionals. Most of the points in this checklist are uncritical for simple configurations. In these cases, the security settings in the basic configuration or that were set with the Security Wizard are sufficient.



Detailed information about the security settings mentioned here are to be found in the reference manual.

■ Have you secured your wireless network with encryption and access control lists?

With the help of 802.11i, WPA or WEP, you can encrypt the data in your wireless network with different encryption methods such as AES, TKIP or WEP. LANCOM Systems recommends the strongest possible encryption with 802.11i and AES. If the WLAN client adapters do not support these, then you should use TKIP or at least WEP. Make sure that the encryption

function in your device is activated, and that at least one passphrase or WEP key has been entered and selected for application.



For security reasons, LANCOM Systems strongly advises you not to use WEP! You should only ever use WEP under exceptional circumstances. When using WEP encryption, use additional security mechanisms additionally.

With the access control list (ACL) you can permit or prevent individual clients accessing your wireless LAN. The decision is based on the MAC address that is permanently programmed into wireless network adapters. To check the access-control list, go to the configuration area in LANconfig and select 'WLAN security' on the 'Stations' tab.

The LANCOM Enhanced Passphrase Security (LEPS) uses an additional column in the ACL to assign an individual passphrase consisting of any 4 to 64 ASCII characters to each MAC address. The connection to the access point and the subsequent encryption with IEEE 802.11i or WPA is only possible with the right combination of passphrase and MAC address.

■ **Have you protected the configuration with a password?**

The simplest way of protecting the configuration is to agree upon a password. If no password has been agreed for the device, the configuration is open to be changed by anybody. The field for entering the password is to be found in LANconfig in the 'Management' configuration area on the 'Security' tab. It is absolutely imperative to assign a password to the configuration if you want to enable remote configuration!

■ **Have you permitted remote configuration?**

If you do not require remote configuration, please ensure to switch it off. If you need to make use of remote configuration, ensure that you do not fail to password-protect the configuration (see the section above). The field for disabling remote configuration is to be found in LANconfig in the 'Management' configuration area on the 'Security' tab. Under 'Access rights – From remote networks' select the option 'denied' for all methods of configuration.

■ **Have you password-protected the SNMP configuration?**

Protect the SNMP configuration with a password too. The field for password-protecting the SNMP configuration is also to be found in LANconfig in the 'Management' configuration area on the 'Security' tab.

■ Have you activated the firewall?



The firewall in the LANCOM WLAN Controller only comes into effect if the WLAN Controller is operated as a Public Spot and provides direct Internet access. When operated for WLAN management only, the firewall in the WLAN Controller remains unused.

Only for WLAN
Controllers operating
as Public Spots

The stateful inspection firewall of LANCOM devices ensures that your local network cannot be attacked from the outside. Activate the firewall in LANconfig under 'Firewall/QoS' on the 'General' tab.



Note that firewall security mechanisms (incl. IP masquerading, port filters, access lists) are active only for data connections that are transmitted via the IP router. Direct data connections via the bridge are not protected by the firewall!

■ Are you using a 'deny all' firewall strategy?

Only for WLAN
Controllers operating
as Public Spots

Maximum security and control is initially achieved by denying all data traffic from passing the firewall. The only connections to be accepted by the firewall are those that are to be explicitly permitted. This ensures that Trojan horses and certain types of e-mail virus are denied communication to the outside. Activate the firewall rules in LANconfig under 'Firewall/QoS' on the 'Rules' tab. Instructions on this are to be found in the reference manual.

■ Have you activated IP masquerading?

Only for WLAN
Controllers operating
as Public Spots

IP masquerading refers to the concealment of local computers while they access the Internet. All that is revealed to the Internet is the IP number of the router module of the device. The IP address can be fixed or dynamically assigned by the provider. The computers in the LAN then use the router as a gateway and are not visible themselves. The router separates the Internet from the intranet like a wall. The application of IP masquerading is set in the routing table for every route individually. The routing table can be found in the LANconfig in the configuration area 'IP router' on the 'Routing' tab.

■ Have you used filters to close critical ports?

Only for WLAN
Controllers operating
as Public Spots

The firewall filters in LANCOM devices offer filter functions for individual computers or entire networks. It is possible to set up source and destination filters for individual ports or port ranges. Furthermore, filters can be set for individual protocols or any combination of protocols (TCP/UDP/

ICMP). It is especially convenient to set up the filters with the aid of LANconfig. Under 'Firewall/QoS', the 'Rules' tab contains the functions for defining and editing filter rules.

■ **Have you excluded certain stations from accessing the device?**

A special filter list can be used to limit access to the device's internal functions via TCP/IP. The phrase "internal functions" refers to configuration sessions via LANconfig, WEBconfig, Telnet or TFTP. As standard this table contains no entries, meaning that computers with any IP address can use TCP/IP and Telnet or TFTP to commence accessing the device. The first time an IP address is entered with its associated netmask, the filter is activated and only the IP addresses contained in this entry are entitled to make use of internal functions. Further entries can be used to extend the circle of authorized parties. The filter entries can describe individual computers or even entire networks. The access list can be found in the LANconfig in the configuration area 'TCP/IP' on the 'General' tab.

■ **Do you store your saved LANCOM configuration to a safe location?**

Protect your saved configurations in a location that is safe from unauthorized access. Otherwise, by way of example, an unauthorized person may load your stored configuration file into another device and they can access the Internet at your expense.

■ **Concerning the exchange of your particularly sensitive data via wireless LAN; have you set up the functions offered by IEEE 802.1x?**

If you move especially sensitive data via wireless LAN you can provide even stronger security by using the IEEE 802.1x technology. To check or activate the IEEE 802.1x settings in LANconfig select the configuration area '802.1x'.

■ **Is the storage of configuration files adapted to your security requirements?**

For self-sufficient operations, the configuration for a WLAN interface being managed by a LANCOM WLAN Controller is stored in flash memory for a certain time only, or even in the RAM only. This device configuration is deleted if contact to the WLAN Controller is lost or if the power supply is interrupted for longer than the set time period.

■ **Have you ensured that the reset button is safe from accidental configuration resets?**

Some devices simply cannot be installed under lock and key. There is consequently a risk that the configuration will be deleted by mistake if a co-worker presses the reset button too long. The behavior of the reset button

can be set so that a press is either ignored or it causes a re-start, depending on the time for which it is held pressed.

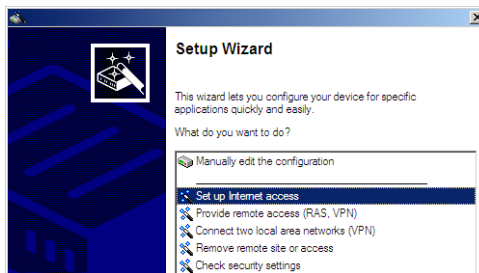
6 Setting up Internet access

LANCOM WLAN controllers also provide routing and firewall functions. If required, these devices can also operate as Internet access routers.

6.1 The Internet Connection Wizard

6.1.1 Instructions for LANconfig

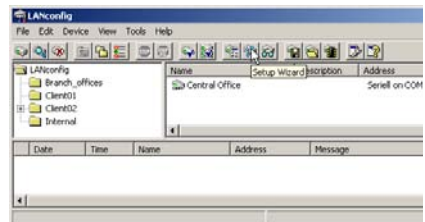
- 1 Mark your device in the selection window. From the command line, select **Extras ▶ Setup Wizard**.



- 2 In the selection menu, select the Setup Wizard, **Set up Internet connection** and confirm the selection with **Next**.
- 3 In the following windows you select your country, your Internet provider if possible, and you enter your access data.
- 4 Depending on availability the Wizard provides further options for your Internet connection.
- 5 The Wizard will inform you as soon as the entries are complete. Close the configuration with **Finish**.

LANconfig: Fast starting of the Setup Wizards

The fastest way of starting the Setup Wizards under LANconfig is to use the command button in the button bar.



6.1.2 Instructions for WEBconfig

- ① Select the entry **Set up Internet connection** from the main menu.
- ② In the following windows you select your country, your Internet provider if possible, and you enter your access data.
- ③ Depending on availability the Wizard provides further options for your Internet connection.
- ④ The wizard will inform you as soon as the entries are complete. Close the configuration with **Finish**.

7 Connecting two networks

Network connectivity, also known as LAN-LAN connectivity, with the LANCOM Router is used for interconnecting two local area networks. Connecting LANs over VPN ensures that the Internet-based connection between the two LANs has high-security protection. Each LAN must be equipped with a VPN-capable router.

Setting up LAN-LAN connectivity is carried out with the familiar convenience of a Setup Wizard.

Always configure both ends

Both of the routers for LAN-LAN connectivity must be configured. Note that the configuration information at both ends must match.



The following instructions assume that LANCOM Routers are being operated at both ends. It is possible to set up network connectivity between routers from other manufacturers. However, this mixed configuration frequently requires far-reaching modifications to both devices. In cases like this refer to the Reference Manual.

Security aspects

Of course your LAN has to be protected from unauthorized access. For this reason, a LANCOM provides a range of security mechanisms that offer an outstanding level of protection. VPN-based connectivity relies on IPsec for transferring data. The encryption methods employed are 3-DES, AES or Blowfish.

7.1 Which details are necessary?

The Wizard requests you for all of the necessary details step by step. If possible, you should have all of this information to hand before you start the Wizard.

The significance of the information required by the Wizard can be explained by an example: Connectivity between a branch office and your main office. The two routers are named 'MAIN OFFICE' and 'BRANCH OFFICE'.





The following tables indicate which entries are to be made for each of the two routers. Paths show how the entries relate to one another.

7.1.1 General information

The following information is required for setting up LAN-LAN connectivity.



For further information on VPN-based network connectivity by other methods, refer to the LANCOM Reference Manual.

Entry	Gateway 1		Gateway 2
Type of local IP address	Static/dynamic		Static/dynamic
Type of remote IP address	Static/dynamic		Static/dynamic
Name of the local device	'MAIN OFFICE'		'BRANCH OFFICE'
Name of the remote device	'BRANCH OFFICE'		'MAIN OFFICE'
Password for the secure transmission of the IP address	'Secret'		'Secret'
Shared Secret for encryption	'Secret'		'Secret'
IP address of remote device	'10.0.2.100'		'10.0.1.100'
IP-network address of the remote network	'10.0.2.0'		'10.0.1.0'
Netmask of the remote network	255.255.255.0		255.255.255.0
Domain descriptor in the remote network	'main office'		'branch office'
Hide own stations when accessing remote network (extranet VPN)?	Yes/No		Yes/No
NetBIOS routing for accessing the remote network?	Yes/No		Yes/No
Name of a local workgroup (for NetBIOS only)	'workgroup1'		'workgroup2'

Notes on the different settings:

- For VPN connections over the Internet, the type of IP address at each end must be specified. There are two **types of IP address**. Static and dynamic. The differences between these two IP address types are explained in the Reference Manual.

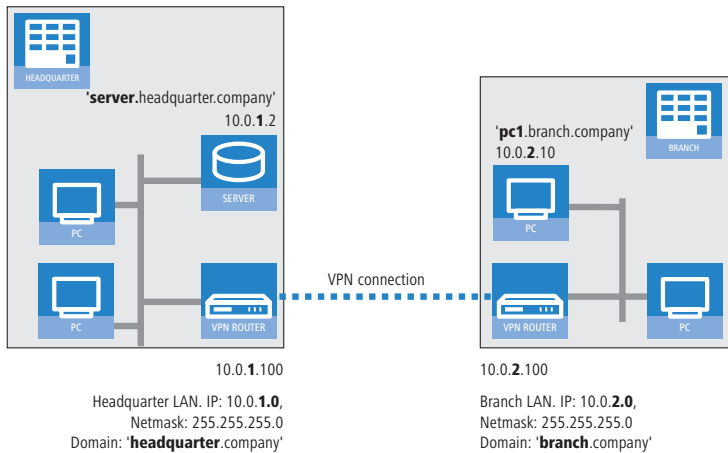
The Dynamic VPN function makes it possible to establish VPN connections between gateways with dynamic IP addresses, and not only between gateways with static (fixed) IP addresses.

- If you have not yet given a name to your LANCOM, the Wizard will ask you to enter a new **name for your device**. Entering a name will cause your LANCOM to be renamed. Ensure that you give different names to the two remote devices.
- The **name of the remote site** is required for identifying the devices.

- The **shared secret** is the central password for the VPN connection's security. It must be entered identically at both ends.

7.1.2 Settings for the TCP/IP router

In the TCP/IP network, correct addressing is of extreme importance. For network connectivity, it should be observed that both networks are logically separated. For this reason they require their own network number (e.g. '10.0.1.x' and '10.0.2.x'). The two network numbers must be different.



Unlike with Internet access, network connectivity makes all of IP addresses visible in all participating networks, including those in the remote LAN, and not just that of the router. The computer with the IP address 10.0.2.10 in the branch-office LAN sees the server 10.0.1.2 at the main office and, with the appropriate rights, has access to it. The same applies in the other direction.

DNS access to the remote LAN

Remote computers in a TCP/IP network can be accessed not only with their IP addresses, but also by freely definable names with the aid of DNS.

For example, the computer named 'pc1.branch_office.company' (IP 10.0.2.10) can access the server at the main office by using its IP address or the name 'server.main_office.company'. There is just one requirement: The domain of the remote network must be entered into the Wizard.



The domain can only be specified in the LANconfig Wizard. With WEBconfig, the necessary changes are made later in the Expert Con-

figuration. Refer to the LANCOM Router reference manual for more detailed information.

VPN extranet

In the case of LAN-LAN connectivity via VPN, you can mask the individual computers behind another IP address. The operating mode referred to as 'extranet VPN' enables computers to be made visible from the remote LAN not with their own IP address, but with a freely definable address such as that of the VPN gateway.

This avoids giving stations in a remote LAN direct access to the computers in your own LAN. For example, if extranet VPN mode is set up to provide access from the branch-office LAN to the main office from the IP address '10.10.2.100', and computer '10.10.2.10' then accesses the server '10.10.1.2', the server receives a request from the IP '10.10.2.100'. The actual address of the computer is masked.

If LAN connectivity uses the extranet mode, the remote site does not receive the actual (masked) LAN addresses, but the IP address published by the LAN ('10.10.2.100' in the above example). The netmask in this case is '255.255.255.255'.

7.1.3 Settings for NetBIOS routing

NetBIOS routing is quick to set up: In addition to the specifying the TCP/IP protocol being used, the only other information required is the name of a Windows workgroup in the LAN used by the router.

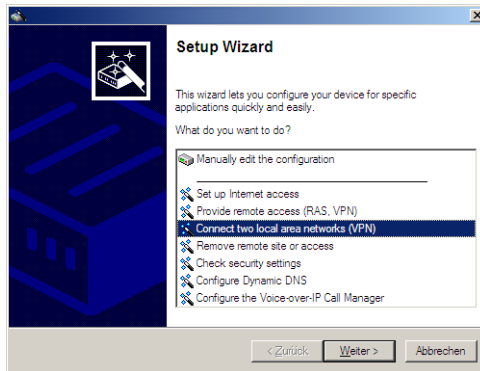


Remote Windows workgroups do not appear in the Windows network environment, but they can be contacted directly (e.g. by searching for a computer of known name).

7.2 Instructions for LANconfig

Carry out the configuration on both routers, one after the other.

- ① Launch the Wizard 'Connect two local area networks'. Follow the Wizard's instructions and enter the necessary data.



- ② The Wizard will inform you when the required information is complete. You can then close the Wizard with **Finish**.
- ③ Once you have completed the set-up of both routers, you can start testing the network connection. Try to communicate with a computer in the remote LAN (e. g. with ping). The LANCOM Router should automatically connect to the remote site and make contact to the requested computer.

Ping – the quick test of a TCP/IP connection

To test a TCP/IP connection, simply send a ping from your computer to a computer in the remote network. Details on the ping command are available from the documentation for your operating system.

```

Command Prompt
C:\>ping 10.0.2.0

Pinging 10.0.2.0 with 32 bytes of data:

Reply from 10.0.2.0: bytes=32 time<10ms TTL
Reply from 10.0.2.0: bytes=32 time<10ms TTL
Reply from 10.0.2.0: bytes=32 time<10ms TTL
Reply from 10.0.2.0: bytes=32 time<10ms TTL

Ping statistics for 10.0.2.0 :
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0m

C:\>

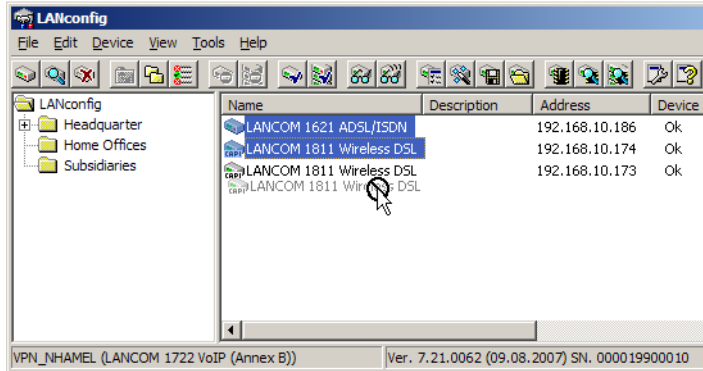
```

7.3 1-Click-VPN for networks (site-to-site)

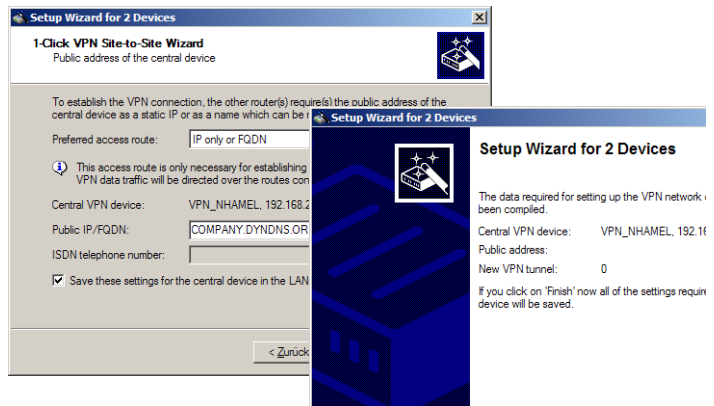
The site-to-site-to-site connectivity of networks is now very simple with the help of the 1-Click-VPN wizard. It is even possible to simultaneously couple multiple routers to a central network.

- ① In LANconfig, mark the routers at branch offices which are to be coupled to a central router via VPN.

- ② Use drag&drop by mouse to place the devices onto the entry for the central router.



- ③ The 1-Click-VPN Site-to-Site Wizard will be started. Enter a name for this access and select the address under which the router is accessible from the Internet.



- ④ Enter the address and/or name of the central router.
- ⑤ The final step is to define how the networks are to intercommunicate:
- The INTRANET at headquarters only is to be provided to the branch offices.
 - All private networks at the branch offices can also be connected to one another via headquarters.



All entries for the central device are made just once and are then stored to the device properties.

7.4 Instructions for WEBconfig



In WEBconfig, VPN-based network connectivity cannot be set up in the Wizard. The Expert Configuration has to be used instead. Refer to the reference manual for information on this.

Carry out the configuration on both routers, one after the other.

- ① In the main menu, launch the Wizard 'Connect two local area networks'. Follow the Wizard's instructions and enter the necessary data.
- ② The Wizard will inform you when the required information is complete. You can then close the Wizard with **Next**.
- ③ Once you have completed the set-up of both routers, you can start testing the network connection. Try to communicate with a computer in the remote LAN (e.g. with `ping`). The LANCOM Router should automatically connect to the remote site and make contact to the requested computer.

8 Providing dial-in access

Your LANCOM can be set up with dial-in access accounts enabling individual computers to dial-in to your LAN and fully participate in the network for the duration of the connection. This service is called RAS (**R**emote **A**ccess **S**ervice). RAS access via VPN provides a highly secure Internet-based connection between the LAN and the dial-in computer. The router in the LAN must support VPN; the dial-in computer needs any form of Internet access and a VPN client.

Setting up dial-in access is carried out with the familiar convenience of a Setup Wizard.

Security aspects

Of course your LAN has to be protected from unauthorized access.

VPN-based connectivity relies on IPsec for transferring data. The encryption methods employed are 3-DES, AES or Blowfish.

8.1 Which details are necessary?

The Wizard sets up an access account for just one user. For additional users, launch the Wizard again.

8.1.1 General information

The following information is required for setting up RAS access.



For further information on RAS access by other methods, refer to the LANCOM Reference Manual.

Entry

User name

Password

Shared Secret for encryption

Hide own stations when accessing remote network (extranet VPN)?

IP address(es) for one or more dial-in computer(s): Fixed or dynamic from the IP address pool

NetBIOS routing for accessing the remote network?

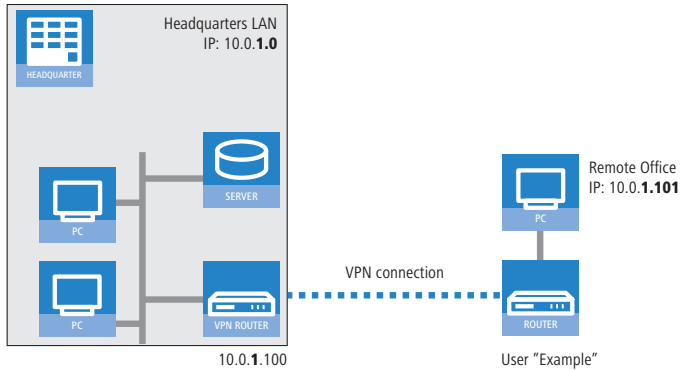
Name of a local workgroup (for NetBIOS only)

Notes on the different settings:

- **User name and password:** This access data serves to identify the user when dialing in.

8.1.2 Settings for TCP/IP

TCP/IP requires that every active RAS is assigned an IP address.



This IP address can be manually set to a fixed value when the user is created. A simpler option is to allow the LANCOM Router to assign the user with a free IP address when dialing in. In this case, all you have to do is to set the range of IP addresses which are to be available for assignment to the RAS users by the LANCOM Router.

For both manual and automatic IP address assignment, ensure that the addresses are freely available in your local network. In our example, the PC is assigned with the IP address '10.0.1.101' when it dials in.

This IP address allows the PC to fully participate in the LAN: With the appropriate rights, it can access any other device in the LAN. This relationship also applies in the other direction: The remote PC can be access from the LAN.

8.1.3 Settings for NetBIOS routing

When working with NetBIOS, the only information required is the name of a Windows workgroup in the LAN used by the router.



The connection is not established automatically. The RAS user first has to manually establish a connection to the LANCOM Router with the help of Dial-Up Networking. Once the connection has been estab-

lished, the computer can access and search the other network (click on **Search ► Computer**, do not use the Network Neighborhood).

8.2 Settings on the dial-in computer

For dialing-in to a network via VPN, a computer needs:

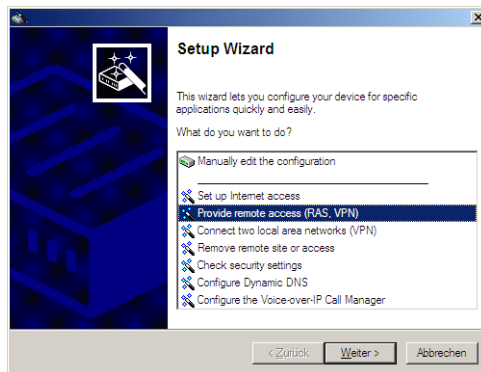
- Internet access
- A VPN client

LANCOM Systems offers you a 30-day test version of the LANCOM Advanced VPN Client on the CD supplied. A precise description of the VPN client and notes on its setup are also to be found on the CD.

The Wizard then requests the parameters that were specified when setting up the RAS access in the LANCOM Router.

8.3 Instructions for LANconfig

- ① Launch the 'Provide Remote Access (RAS, VPN, IPsec over WLAN)' Wizard. Follow the Wizard's instructions and enter the necessary data.



- ② The Wizard will inform you when the required information is complete. You can then close the Wizard with **Finish**.
- ③ Configure the access account on the dial-in PC as described. Subsequently test the connection (see box 'Ping – the quick test of a TCP/IP connection').

8.4 1-Click-VPN for LANCOM Advanced VPN Client

VPN accesses for employees who dial into the network with the LANCOM Advanced VPN Client are very easy to set up with the Setup Wizard and exported to a file. This file can then be imported as a profile by the LANCOM Advanced VPN Client. All of the information about the LANCOM VPN Router's configuration is also included, and then supplemented with randomly generated values (e.g. for the preshared key).

- ① Use LANconfig to start the 'Set up a RAS Account' wizard and select the 'VPN connection'.
- ② Activate the options 'LANCOM Advanced VPN Client' and 'Speed up configuration with 1-Click-VPN'.
- ③ Enter a name for this access and select the address under which the router is accessible from the Internet.
- ④ In the final step you can select how the access data is to be entered:
 - Save profile as an import file for the LANCOM Advanced VPN Client
 - Send profile via e-mail
 - Print out profile



Sending a profile via e-mail could be a security risk should the e-mail be intercepted en route!

To send the profile via e-mail, the device configuration must be set up with an SMTP account with the necessary access data. Further, the configuration computer requires an e-mail program that is set up as the standard e-mail application and that can be used by other applications to send e-mails.

When setting up the VPN access, certain settings are made to optimize operations with the LANCOM Advanced VPN Client, including:

- Gateway: If defined in the LANCOM VPN Router, a DynDNS name is used here, or alternatively the IP address
- FQDN: Combination of the name of the connection, a sequential number and the internal domain in the LANCOM VPN Router.
- Domain: If defined in the LANCOM VPN Router, the internal domain is used here, or alternatively a DynDNS name or IP address
- VPN IP networks: All IP networks defined in the device as type 'Intranet'.

- Preshared key: Randomly generated key 16 ASCII characters long.
- Connection medium: The LAN is used to establish connections.
- VoIP prioritization: VoIP prioritization is activated as standard.
- Exchange mode: The exchange mode to be used is 'Aggressive Mode'.
- IKE config mode: The IKE config mode is activated, the IP address information for the LANCOM Advanced VPN Client is automatically assigned by the LANCOM VPN Router.

8.5 Instructions for WEBconfig

- ① In the main menu, launch the Wizard 'Provide remote access (RAS)'. Follow the Wizard's instructions and enter the necessary data.
- ② Configure the access account on the dial-in PC as described. Subsequently test the connection (see box 'Ping – the quick test of a TCP/IP connection').

9 Appendix

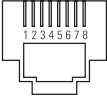
9.1 Performance and characteristics

		LANCOM WLC-4006	LANCOM WLC-4025+	LANCOM WLC-4100
Connectors	Ethernet LAN	5x 10/100Base-TX, auto-sensing, switch with node/hub autosensing	4x 10/100/1000Base-TX, Autosensing, Node/Hub Auto-sensing	
	WAN	Any Ethernet port can be switched as a WAN connector.		
	USB	USB 2.0 host port (high speed: 480 Mbps) for connecting a USB printer and for future extensions		
	Configuration	Serial V.24/RS-232 outband interface with Mini-DIN8 connector		
	Power supply	12V DC via external power supply	Internal power supply unit (110-230 V)	
Housing		210 mm x 143 mm x 45 mm (B x H x T), robust plastic housing, prepared for wall mounting	Robust metal housing, 19" 1 HU, (435 x 45 x 207 mm) with removable mounting brackets, network connectors on the front	
Approvals		EU (CE certification: EN 55022, EN 55024, EN 60950)		
Environment/ Temperature		41.00 °F to +95.00 °F at 80% max. humidity (non condensing)	41.00 °F to +104.00 °F at 80% max. humidity (non condensing)	
Package content		LAN cable (CAT.5, STP, 3 m), RS232 cable, IEC cable, printed manual (English, German), software CD	LAN cable (CAT.5, STP, 3 m), RS232 cable, IEC cable, printed manual (English, German), software CD	
Options		<ul style="list-style-type: none"> ■ LANCOM WLAN Controller options for managing up to 12 Access Points 	<ul style="list-style-type: none"> ■ LANCOM WLAN Controller options for managing up to 100 Access Points 	<ul style="list-style-type: none"> ■ LANCOM WLAN Controller options for managing up to 1000 Access Points
Accessories		<ul style="list-style-type: none"> ■ LANCOM modem adapter kit for connecting modems (analog or GSM) to the serial configuration interface item no. 110288 ■ LANCOM LCOS Reference Manual (DE), item no. 110405 		
		<ul style="list-style-type: none"> ■ LANCOM Next Business Day Service Extension CPE item no. 61411 ■ LANCOM 2-Year Warranty Extension CPE item no. 61414 	<ul style="list-style-type: none"> ■ LANCOM Next Business Day Service Extension Central Site item no. 61413 ■ LANCOM 2-Year Warranty Extension Central Site item no. 61416 	

9.2 Connector wiring

9.2.1 Ethernet interface 10/100/1000Base-TX, DSL interface


8-pin RJ45 sockets (ISO 8877, EN 60603-7)

Connector	Pin	Fast Ethernet	Gigabit Ethernet
	1	T+	BI_DA+*
	2	T-	BI_DA-
	3	R+	BI_DB+
	4		BI_DC+
	5		BI_DC-
	6	R-	BI_DB-
	7		BI_DD+
	8		BI_DD-

*BI_DA+ stands for "bi-directional pair +A"

9.2.2 Configuration interface (outband)

8-pin Mini DIN socket

Connector	Pin	Line
	1	CTS
	2	RTS
	3	RxD
	4	RI
	5	TxD
	6	DSR
	7	DCD
	8	DTR
	U	GND

9.3 CE-declarations of conformity

CE LANCOM Systems herewith declares that the devices of the type described in this documentation are in agreement with the basic requirements and other relevant regulations of the 1995/5/EC directive.

The CE declarations of conformity for your device can be found on the relevant product page on the LANCOM Web site (www.lancom.eu).

Index

Numerics

10/100Base-TX	27
100-Mbit network	27
3 DES	128, 135
802.11i	117, 118, 121
802.11i/	118
802.1p	17
802.1x	3, 117, 118

A

Access point	3, 10
Access point mode	21
Access-control list	119
ACL	118, 119
Advanced Routing and Forwarding	17
AES	117, 128, 135
Alternative WLAN Controller	57
Authentication	15, 17
Auto-accept	49
Automatic channel selection	55
Automatic provision of the default configuration	49, 81
Automatically accept new access points	44
Automatically accept new APs	48, 49
Automatically provide the default configuration	44, 47
Autosensing	27, 30

B

Background scanning	3
Blowfish	128, 135
Broadcast	57

C

CA	15
CAPWAP	11, 13, 15, 17
CAPWAP tunneling	13
Certificate	42, 43, 49, 78, 79, 82
Certificates	

Backup	82
Certification Authority	15
Charge protection	35
Configuration	49
Configuration access	35
Configuration cable	27
Configuration file	124
Configuration interface	19
Connector cable	20
Configuration password	122
Configuration protection	19, 34
Connector wiring	141
LAN interface	141
Outband	141
Control And Provisioning of Wireless Access Points	11
Control channel	11
CPU load	25
Cron job	65

D

Data channel	11
Datagram Transport Layer Security	11
Date	25
Declaration of conformity	142
Default configuration	43, 47, 61
Default gateway	40, 123
Device name	25
DHCP	40
DHCP server	18, 33, 41
Dial-in access	135
DiffServ	17
Discovery Request Message	14, 89
DNS	14
DNS access to the remote LAN	130
DNS server	18, 40
Domain	130
Download	5

■ Index

- DTLS 11, 14, 17, 26
- Dynamic VLAN assignment 17, 90
- E**
- EAP 12, 17, 117, 118
- E-mail 74
- Encryption 17, 45, 63, 76, 128, 135
- Expected access point 47
- F**
- Fast roaming 17
- Firewall 18, 123
 - Block stations 124
- FirmSafe 19
- Firmware 5
 - Central management 65
- Firmware version 25
- Flash 11, 52
- H**
- Hardware installation 29
- HTTPS 36
- I**
- ICMP 124
- IEEE 802.11n 12
- IETF 11
- Information symbols 5
- Inheritance 17, 52, 55, 58, 80
- Installation 20
 - Configuration interface 30
 - LAN 29, 30
- Internet access 17, 126
- Internet access setup 126
- IP
 - Block ports 123
 - Filter 123
- IP address 33, 34, 124
- IP masquerading 18, 123
- IP router 18
- IPsec 128, 135
- IPSec over WLAN 117
- IPX router 17
- L**
- LAN
 - Connector cable 20
 - LAN connection 27
 - LANCOM Enhanced Passphrase Security 117
 - LANconfig 31, 34
 - Starting the Wizards 126
 - LAN-LAN connectivity 17, 128
 - Required information 128
 - LANmonitor 31, 78, 111
 - Assign new access point to profile 112
 - Disconnect access point 112
 - LANtools
 - System requirements 21
 - Layer-3 roaming 13
 - LCD display 25
 - LED
 - Lost AP 24
 - New AP 24
 - WLAN 24
 - LEPS 118
 - Load balancing 89
 - Loader 21
 - Lost AP LED 24, 79, 80
- M**
- MAC check 45
- MAC filter 106
- MAC functions 11
- Managed mode 21
- Management VLAN ID 55
- Manual acceptance of access points 78
- Memory load 25
- N**
- NAT – see IP masquerading
- NetBIOS 131
- Network connectivity 128

Security aspects	128, 135	Security	
Network mask	33, 34, 124	Protecting the configuration	117
Network name	45	Security checklist	121
Network Time Protocol	43	self-sufficient	21
New access point	47	Serial configuration cable	27
New AP LED	24	Simple Certificate Encryption Protocol	15, 42
NTP	43	SIP telephone	13
Number of VPN tunnels	25	Smart controller	3, 11
P		SNMP	
Password	34, 35	Configuration protection	122
PAT – see IP masquerading		SNTP status	25
PCKS12 container	83	Software installation	30
PHY layer	11	Split management	3, 16
Ping	132	SSID	45, 52
PMK caching	17	Stand-alone operation	17, 52
Power supply unit	20	Statusanzeigen	
Pre-authentication	17	Power	22
R		Support	5
RADIUS	3, 12, 17, 106, 118	SYSLOG	74
RAM	53	System requirements	20
Random number	15	T	
Remote Access Service (RAS)		TCP	123
Configuring the dial-in computer	137	TCP/IP	20
NetBIOS	136	Connect test	132
Server	18	Settings	32
Setup	135	TCP/IP configuration	
TCP/IP	136	Fully automatic	32, 33
User name	136	Manual	32, 33
Windows workgroup search	136	TCP/IP filter	18, 123
Remote configuration	35	TCP/IP router	
Routing table	123	Settings	130
S		Telnet	124
Scalability	12	Temperature	25
SCEP	15, 42	TFTP	124
SCEP status	25	Time	25
Script		Time information	42
Central management	65	TLS	11
SDSL modem	18		

 ■ *Index*
U

UDP	123
USB connector	28

V

Virtual Private Networks (VPN)	17
VLAN	3
VLAN ID	52, 91
VPN client	137

W

WEBconfig	36
HTTPS	36
System requirements	21

WEP	117, 120, 121
Windows workgroup search	131
Wireless LAN Controllers	3, 10
Firmware management	65
Script management	65
WLAN LED	24, 43
WLAN profile	56, 61
WME	17
WPA	117, 118, 121

Z

Zero-touch management	16
-----------------------	----

