LANCOM WLC-4006
LANCOM WLC-4025

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 included with this product is subject to written permission by LANCOM Systems. We reserve the right to make any alterations that arise as the result of technical development.

All explanations and documents for registration of the products you find in the appendix of this documentation, if they were present at the time of printing.

Trademarks

Windows®, Windows Vista™, Windows XP® 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 mentioned may be trademarks or registered trademarks of their respective owners.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit http://www.openssl.org/.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

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

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom.eu

Wuerselen, September 2007

110550/0907

Preface

Thank you for your confidence in us!

The WLAN Controllers LANCOM WLC-4025 and LANCOM WLC-4006 are state-of-the-art hardware components for medium-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
- 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"

EN

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.

User manual and reference manual

The documentation of your device consists of the following parts:

- Installation guide
- User manual
- Reference manual

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 can be found on the LANCOM product CD as an Acrobat (PDF) document. 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)

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.

In case you encounter any errors, or just want to issue critics enhancements, please do not hesitate to send an email directly to:
info@lancom.eu

Our online services www.lancom.eu are available to you around the clock should you have any queries regarding the topics discussed in this manual or 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 of LANCOM support, please see the enclosed leaflet or the LANCOM Systems website.

Information symbols	
	Very important instructions. Failure to observe this may result in damage.
	Important instruction that should be observed.
	Additional information that may be helpful but which is not required.

EN

Contents

EN

EN

1 Introduction

1.1 Centralized WLAN management

The widespread use of wireless Access Points and wireless routers has made accessing networks in businesses, universities and other organizations considerably more convenient and flexible.

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

- All wireless Access Points must be configured and require appropriate monitoring in order to recognize unwelcome WLAN clients, etc. The administration of the Access Points, especially for larger WLAN infrastructures with the appropriate security mechanisms, requires advanced qualifications and experience on the part of those responsible, and it ties up considerable resources in the IT departments.
- The manual customization of the configurations in the Access Points when changes are made to the WLAN infrastructure can be time-consuming, with the result that different configurations can be present in the WLAN at the same time.
- Combined utilization of the shared communications medium (air) requires effective coordination of the Access Points to avoid frequency interference and optimize network performance.
- Access Points in public places pose a potential security risk because the devices themselves and also 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. As the configuration provided by the WLAN Controller is generally **not** stored in the Access Point's flash memory but in RAM, security-related data cannot fall into the hands of unauthorized persons in the event that devices are stolen. Only in "self-sufficient" operation (‘Self-sufficient operation’ → Page 53) is the configuration optionally saved for a

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

1.1.1 The CAPWAP standard

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

CAPWAP uses two channels for data transfer:

- Control channel, encrypted with 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 less reliable 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.

1.1.2 Smart controller technology

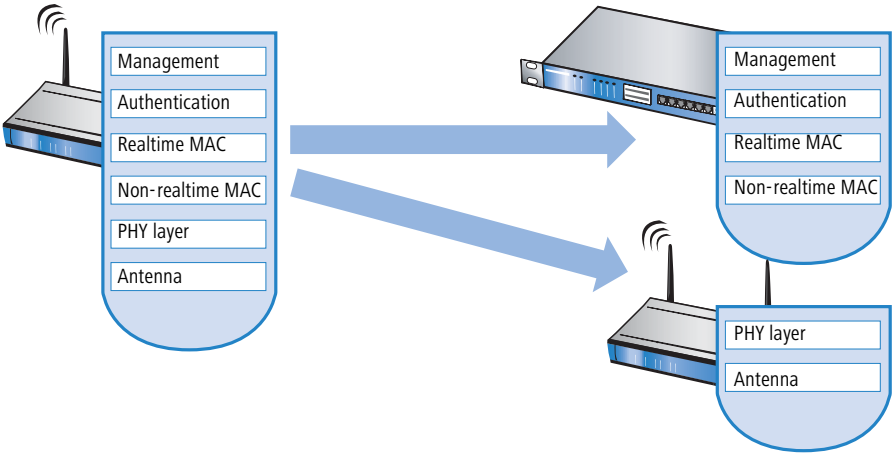
In a decentralized WLAN structure with stand-alone Access Points (operating as so-called "rich access points") all functions for data transfer take place in the PHY layer, the control functions in the MAC layer, and the management functions are integrated in the Access Points. Centralized WLAN management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

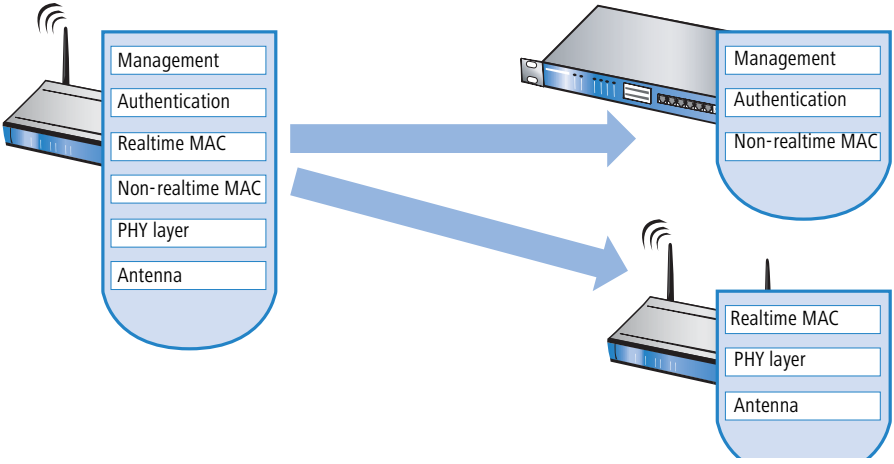
EN

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

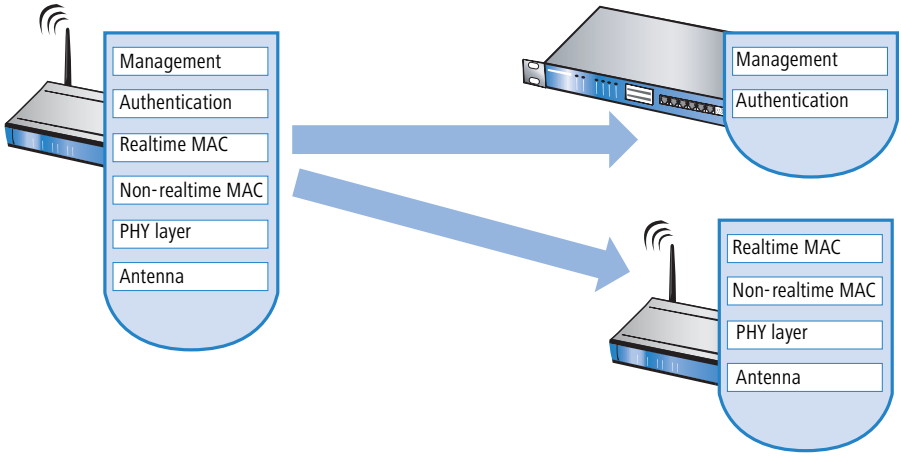
- Remote MAC: In this case, all of the WLAN functions are transferred from the Access Point to the WLAN Controller. Here, the Access Points only serve as "extended antennas" without independent intelligence.



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



- Local MAC: The third possibility provides for complete management and monitoring of the WLAN data traffic directly in the Access Points. The only information exchanged between the Access Point and the WLAN Controller are messages to ensure a uniform configuration of the Access Points and to manage the network .



Smart Controller Technology from LANCOM Systems uses the local MAC procedure. Thanks to the reduction of centralized tasks, these WLAN infrastructures offer optimum scalability. At the same time, infrastructure of this type prevents the WLAN Controller from becoming a central bottleneck that has to process large portions of the overall data traffic. In remote MAC and split MAC architectures, **all** payload data is forced to run centrally via the WLAN Controller. 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. During the release into the

LAN, data can also be directly routed into special VLANs, which 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.
- 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.

1.1.3 Communication between the Access Point and the WLAN Controller

As of firmware version LCOS 7.20 there is a difference between LANCOM Access Points (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. In the following specifications, the general term Access Point will be used for the most part.

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

- 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' → Page 79). The Access Point searches for a WLAN Controller in the LAN on behalf of the one or more corresponding WLAN modules.
- A LANCOM Wireless Router is already configured; the operating mode is manually set to 'managed' for at least one WLAN module. The wireless router searches for a WLAN Controller in the LAN on behalf of the one or more corresponding WLAN modules.

The Access Point sends a "discovery request message" at the beginning of communication to determine the available WLAN Controllers. This request is sent as a broadcast. However, because in some structures a potential WLAN Controller cannot be reached by a broadcast, special addresses from additional WLAN Controllers can also be entered into the configuration of the Access Points.

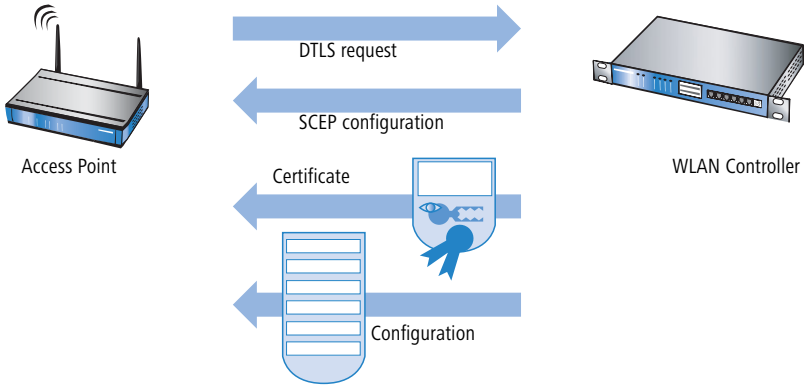
DNS names of WLAN Controllers can also be resolved. All Access Points with LCOS 7.22 or higher have the default name 'WLC-Address' pre-configured so that a DNS server can resolve this name to a LANCOM WLAN Controller. This also makes it possible to reach WLAN Controllers that are not located in the same network, without having to configure the Access Points.

From the available WLAN Controllers, the Access Point selects the best one and queries it for the structure of the DTLS connection. For the Access Point, the "best" WLAN Controller is the one with the least load, i.e., the lowest ratio of managedAccess 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 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 WLAN Controller also automatically creates a self-signed certificate for the Access Point with which it can later uniquely identify itself to the WLAN Controller.

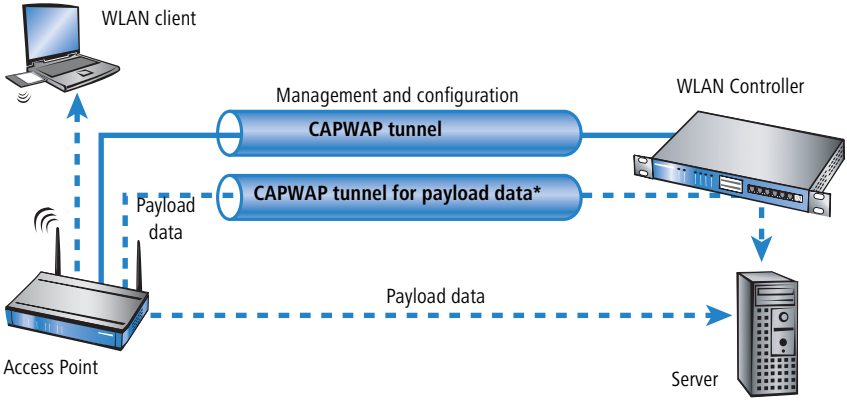
The Access Point is provided with the configuration for the integrated SCEP client via the secure DTLS connection – the Access Point is then able to retrieve its certificate from the SCEP CA via SCEP. Once this is done, the assigned configuration is transferred to the Access Point.

SCEP stands for Simple Certificate Encryption Protocol; CA for Certification Authority. Refer to the LCOS reference manual for further information about digital certificates, CAs and SCEP.



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

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



* Not yet available with early shipments

1.1.4 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". New Access Points now only need to be connected 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.

1.1.5 Split management

LANCOM Access Points can locate your WLAN Controller in distant networks—a simple IP connection, e. g., via a VPN path is all that is needed. 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 building a company-wide WLAN infrastructure at the headquarters that includes all branch and home offices connected to it.

1.2 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
WLAN controlling		
Number of managed devices	6	25
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.	✔	✔

EN

	LANCOM WLC-4006	LANCOM WLC-4025
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
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 coupling over VPN	✔	✔
RAS server (over VPN)	✔	✔
IP router	✔	✔
DHCP and DNS server (for each ARF network)	✔	✔
N:N mapping for routing networks with the same IP-address ranges over VPN	✔	✔
Configuring one LAN port as WAN port	✔	✔
Policy-based routing	✔	✔
NAT Traversal (NAT-T)	✔	✔
PPPoE servers	✔	✔
Layer 2 QoS tagging	✔	✔
802.1p	✔	✔
WAN connections		
Connection for DSL modem	✔	✔

	LANCOM WLC-4006	LANCOM WLC-4025
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	1
Separate Fast Ethernet LAN ports, individually switchable, e.g., as LAN switch or separate DMZ ports; auto crossover. Alternatively switchable as a WAN interface for connecting SDSL modems.	4	4
Security functions		
IPSec encryption via external software (VPN client)	✔	✔
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	✔	✔
MAC address filter regulates, for example, LAN-workstation access to the IP routing function	✔	✔
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 WLAN Controller 12 Option for managing up to 12 access points	✔	
LANCOM WLAN Controller 50 option for managing up to 50 Access Points		✔

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

EN

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
Cable for integrated power supply		✔
Power adapter	✔	
CAT5 LAN connector cable (green connectors)	✔	✔
Connector cable for the configuration interface	✔	✔
Rubber base, 19" mounting kit		✔
LANCOM CD	✔	✔
Printed Installation Guide	✔	✔
Printed User Manual	✔	✔
Printed Reference Manual		✔

If anything is missing, please contact your retailer or the address stated on the delivery slip of the unit.

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 that supports TCP/IP, e.g. Windows Vista™, Windows XP, Millennium Edition (Me), Windows 2000, Windows 98, 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).

2.3 Introducing the LANCOM WLAN Controller

This section introduces your device. We will give you an overview of all status displays, connections and switches.

While the information in this section is useful for the installation of the device, it is not absolutely essential. You may therefore skip this section for the time being and go straight forward to 'Hardware installation'.

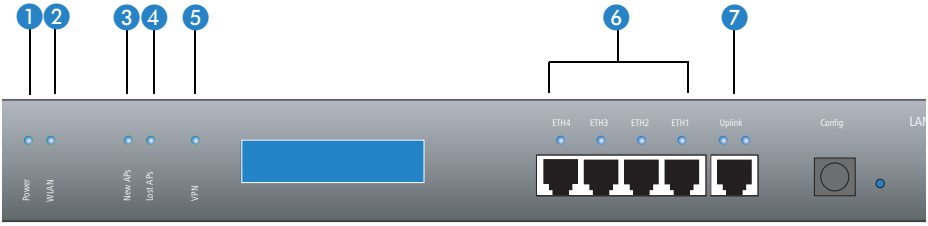
2.3.1 Status displays

The front panel of the device feature a series of light emitting diodes (LEDs) that provide information on the status of the device.

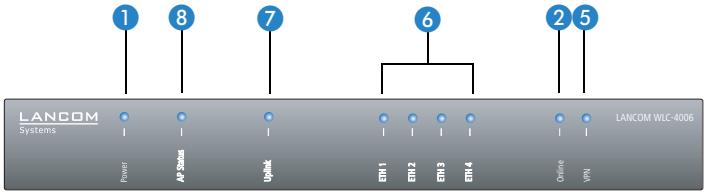
Front side

The various LANCOM WLAN Controller models have different numbers of indicators on the front panel depending on their functionality.

LANCOM WLC-4025



LANCOM WLC-4006



EN

Top

LANCOM WLC-4006 only

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

Meanings of the LEDs

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.

1 Power

This LED provides information on the device's operating state. After being switched on, it blinks green during the self-test. The LED then shines con-

stantly to indicate operational readiness, unless an error is detected as indicated by a code blinked in red.

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
Orange/green	In the housing cover; blinking alternately with the online LED	At least one WLAN module is in managed mode and has not found a WLAN Controller yet. The corresponding WLAN module(s) is/are switched off until a WLAN Controller is found to supply a configuration, or until being switched manually into another operating mode.
Orange /red	In the housing cover; blinking alternately with the online LED	At least one WLAN module is in managed mode and has found a WLAN Controller. However, the WLAN Controller cannot assign a configuration because the firmware and/or the device's loader version is not compatible with the WLAN Controller.
Red	Blinking	Charge limit for online connections 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 are 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'.

EN

The power LED is blinking and no connection can be made?

Signal that a charge or time limit has been reached

If the power LED blinks red and no WAN connections can be established, there is no cause for concern. This merely means that a pre-set charge or time limit has been reached.

There are three ways to remove the lock:

- Reset the toll protection.
- Increase the limit.
- Deactivate the lock completely (set limit to '0').

LANmonitor shows you when a charge or time limit has been reached. To reset the toll protection, activate the context menu (right-mouse click) **Reset charge and time limits**. The charge settings are defined in LANconfig under **Management** ▶ **Costs** (these settings are only available if the 'Complete configuration display' is activated under **Tools** ▶ **Options**).

With WEBconfig, resetting the toll protection and all parameters are found under **Expert configuration** ▶ **Setup** ▶ **Charges**.

2 WLAN (LANCOM WLC-4025 only)

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: ■ Root certificate ■ Device certificate ■ Current time ■ Random number for the DTLS encryption
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.

3 New APs (LANCOM WLC-4025 only)

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.

4 Lost APs (LANCOM WLC-4025 only)

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.

5 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

6 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

7 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	

EN

		Left LED (WAN)	Right LED
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.	

8 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: ■ 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.

Status display at the Access Points

The Access Points show the status of their connection with the LANCOM WLAN Controller by means of their LEDs.

- If an Access Point is in managed mode and is searching for a WLAN Controller, the LEDs in the device cover blink alternately **green** and **orange**.
- Once an Access Point in managed mode has found a WLAN Controller, but configuration is not possible due to an incompatible firmware or loader version, then the LEDs in the device cover blink alternately in **red** and **orange**. The firmware and/or loader have to be updated before the Access Point can be accepted by a WLAN Controller.

As soon as the Access Point has made contact to the WLAN Controller, the LEDs resume their normal function as described in the user manual for the relevant model.

EN

2.3.2 LC display

LANCOM WLC-4025 only

The LC display on the LANCOM WLC-4025 uses two lines with 16 characters each to display the following information in rotation:

- Device name
- Firmware version
- 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.

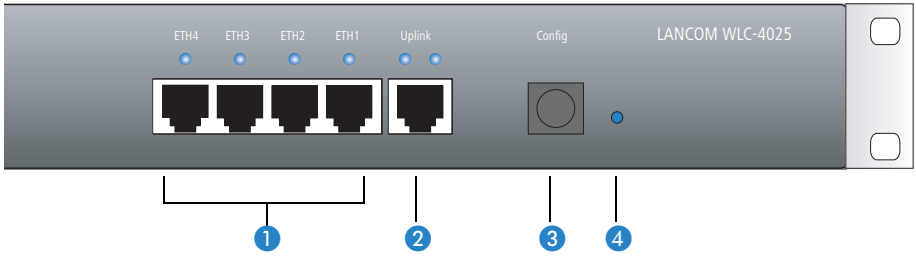
If the WLAN LED constantly illuminates in red, the display also displays the following information:

- Occupied random-number memory
- SNTP status
- SCEP status

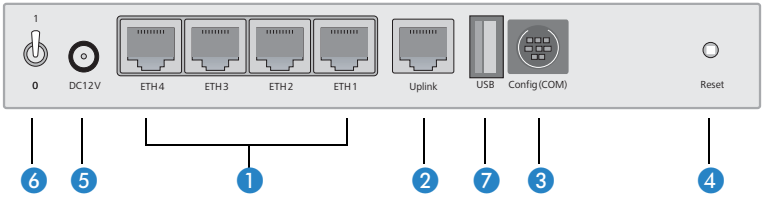
2.3.3 Device connectors

All of the router's connectors and switches are located on the front and back panel:

LANCOM WLC-4025



LANCOM WLC-4006



The following connectors are located on the front and back panel of the LANCOM WLC-4025 and on the back panel of the LANCOM WLC-4006.

1. Four 10/100Base-Tx connectors for local networks
2. Uplink connector
3. Serial configuration interface
4. Reset button

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.

Some devices simply cannot be installed under lock and key. There is consequently a risk that the configuration will be deleted by someone pressing the reset button too long. With the suitable setting, the behavior of the reset button can be controlled accordingly.

Configuration tool	Call
WEBconfig, Telnet	Expert configuration > Setup > Config

Reset button

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

- ☐ Ignore: The button is ignored.

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, then 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.

- Boot only: A press of the button prompts a restart, regardless of how long the it is held down.
- Reset-or-boot (standard setting): Press the button briefly to restart 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.

This hard reset causes the device to start with the default factory settings; all previous settings are lost!

Note that resetting the device leads to a loss on the WLAN encryption settings within the device and that the default WEP key is active again.

5 Connector for the IEC cable (LANCOM WLC-4025) or power supply unit (LANCOM WLC-4006)

6 Power switch

7 USB connector (LANCOM WLC-4006 only)

2.3.4 Hardware installation

Installation of the LANCOM Router involves the following steps:

① **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 2 and the other end into an available network connector socket in your local network, or a free socket on a switch or hub.

Avoid having multiple unconfigured LANCOMs at once within a single network segment. Any unconfigured LANCOM takes on the same IP address (ending in '254'), and so address conflicts could arise. To avoid problems, multiple LANCOMs should be configured one after the other with the respective device being assigned with a new and unique IP address (not ending in '254') each time.

EN

② **Further network devices** – you can optionally connect further network devices to the LAN interfaces 1.

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

③ **Configuration interface** – optionally, the router 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 3 to an available serial interface on the PC.

④ **Power supply** – the socket 5 is for connecting the supplied power supply unit.

With the LANCOM WLC-4006 use only the supplied power adapter! The use of the wrong power adapter can be of danger to the device or persons.

⑤ **Supply power and switch on** – Using the IEC cable, supply power to the device and switch it on using the switch 6.

⑥ **Installation complete** – This step completes the installation of the hardware. The next steps are to install the management software and to configure the LANCOM WLAN Controller.

2.4 Software installation

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

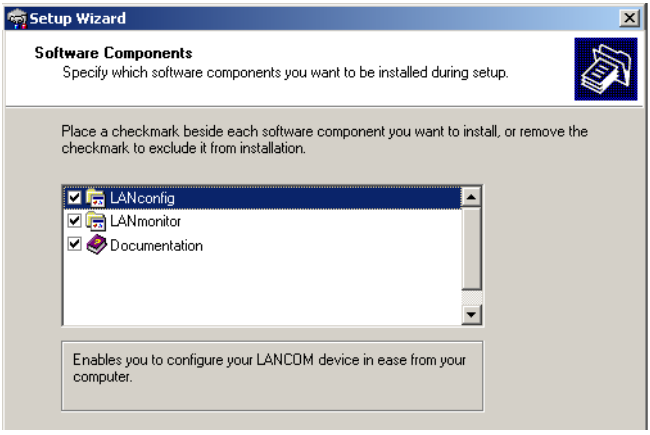
You may skip this section if you use your LANCOM Router exclusively with computers running operating systems other than Windows.

2.4.1 Starting 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 product CD.

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



2.4.2 Which software should I install?

- **LANconfig** is the Windows configuration program for all LANCOM routers and LANCOM access points. 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 routers and LANCOM access points.
- **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).
- The **LANCOM Advanced VPN Client** enables VPN connections to be established over the Internet from a remote computer to a VPN router.
- 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.

EN

3 Basic configuration

The basic configuration can be performed on a step-by-step basis using a convenient setup wizard to guide you through the setup process and prompt you for the required information.

First, this chapter will tell you which information is required for the basic configuration. Use this section to assemble the information you will need before you launch the wizard.

Next, enter the data in the setup wizard. Launching the wizard and the process itself are described step by step — with separate sections for LANconfig and WEBconfig. Thanks to the information that you have collected in advance, the basic configuration is quick and effortless.

At the end of this chapter we will show you the settings that are needed for the LAN's workstations to ensure trouble-free access to the device.

3.1 Which information is necessary?

The basic configuration wizard will take care of the basic TCP/IP configuration of the device and protect the device with a configuration password. The following descriptions of the information required by the wizard are grouped in these configuration sections:

- TCP/IP settings
- protection of the configuration
- configuring connect charge protection
- security settings

3.1.1 TCP/IP settings

The TCP/IP configuration can be realized in two ways: either as a fully automatic configuration or manually. No user input is required for the fully automatic TCP/IP configuration. All parameters are set automatically by the setup wizard. During manual TCP/IP configuration, the wizard will prompt you for the usual TCP/IP parameters: IP address, netmask etc. (more on these topics later).

Fully automatic TCP/IP configuration is only possible in certain network environments. The setup wizard therefore analyses the connected LAN to determine whether it supports fully automatic configuration.

EN

New LAN—fully automatic configuration possible

If all connected network devices are still unconfigured, the setup wizard will suggest fully automatic TCP/IP configuration. This may be the case in the following situations:

- a single PC is connected to the WLAN Controller
- setup of a new network

Fully automatic TCP/IP configuration will not be available when integrating the WLAN Controller in an existing TCP/IP LAN. In this case, continue with the section 'Information required for manual TCP/IP configuration'.

The result of the fully automatic TCP/IP configuration: the router will be assigned the IP address '172.23.56.1' (netmask '255.255.255.0'). In addition, the integrated DHCP server will be enabled so that the WLAN Controller can automatically assign IP addresses to the devices in the LAN.

Configure manually nevertheless?

The fully automatic TCP/IP configuration is optional. You may also select manual configuration instead. Make your selection after the following considerations:

- Choose automatic configuration if you are **not** familiar with networks and IP addresses.
- Select manual TCP/IP configuration if you are familiar with networks and IP addresses, and one of the following conditions is applicable:
  - You have not yet used IP addresses in your network but would like to do so now. You would like to specify the IP address for your router, selecting it from the address range reserved for private use, e.g. '10.0.0.1' with the netmask '255.255.255.0'. At the same time you will set the address range that the DHCP server uses for the other devices in the network (provided that the DHCP server is switched on).
  - You have previously used IP addresses for the computers in your LAN.

Information required for manual TCP/IP configuration

During manual TCP/IP configuration, the setup wizard will prompt you for the following information:

- **IP address and netmask for the WLAN Controller**
  Assign a free IP address from the address range of your LAN to the WLAN Controller and specify the netmask.

EN

3.1.2 Configuration protection

The password for configuration access to the LANCOM protects the configuration against unauthorized access. The configuration of the device contains a considerable amount of sensitive information such as your Internet access information. We therefore strongly recommend protecting it with a password.

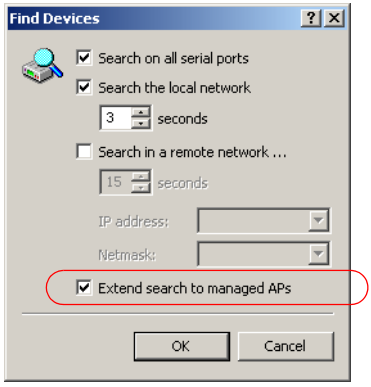
Multiple administrators can be set up in the configuration of the LANCOM, each with differing access rights. For a LANCOM, up to 16 different administrators can be set up. Further information can be found in the section 'Managing rights for different administrators' in the LCOS reference manual.

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.

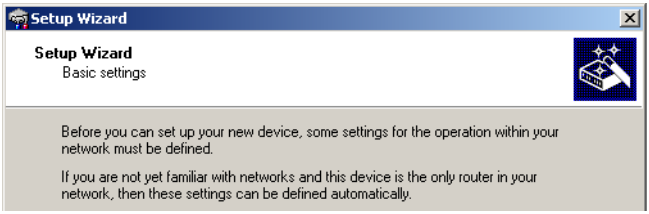
3.2 Instructions for LANconfig

① Start up LANconfig by clicking **Start** ▶ **Programs** ▶ **LANCOM** ▶ **LANconfig**. LANconfig automatically detects the new LANCOM devices in the TCP/IP network.

② As standard, LANCOM Wireless Routers and LANCOM Access Points in managed mode are **not** displayed by LANconfig carrying out its device search. To display these devices, activate the option 'Extend search for managed APs'.



③ If an unconfigured device is being found during searching, the setup wizard starts that will help you make the basic settings of the device or will even do all the work for you (provided a suitable network environment exists).



If you cannot access an unconfigured LANCOM, the problem may be due to the netmask of the LAN: with less than 254 possible hosts (netmask > '255.255.255.0'), please ensure that the IP address 'x.x.x.254' is located in your own subnet.

If you have chosen automatic TCP/IP configuration, please continue with Step ④.

④ If you would like to configure the TCP/IP settings manually, assign an available address from a suitable address range to the LANCOM. Confirm your choice with **Next**.

⑤ Specify whether or not the router should act as a DHCP server. Make your selection and confirm with **Next**.

⑥ In the following window, specify the password for configuration access. Note that the password is case-sensitive and ensure that it is sufficiently long (at least 6 characters).

In addition, you may specify whether the device may only be configured from the local network or whether remote configuration via the WAN (i.e. a remote network) is also permissible.

Please note that enabling this will also permit remote configuration via the Internet. You should always make sure that the configuration access is protected with a password.

⑦ Enter the wireless parameters. Select a network name (SSID) and a radio channel. Turn on if necessary the function for 'closed network'. Confirm your choice with **Next**.

⑧ In the next window, select your DSL provider from the list that is displayed. If you select 'My provider is not listed here,' you must enter the transfer protocol used by your DSL provider manually. Confirm your choice with **Next**.

⑨ Connect charge protection can limit the cost of DSL connections to a predetermined amount if desired. Confirm your choice with **Next**.

⑩ Complete the configuration with **Finish**.

Section 'TCP(IP settings to workstation PCs' will describe the settings required for the individual workstations in the LAN.

3.3 Instructions for WEBconfig

To configure the router with WEBconfig you must know how to address it in the LAN. The reaction of the devices, as well as their accessibility for configuration via web browser is dependent on whether a DHCP server and a DNS server are already active in the LAN, and whether these two server processes exchange the assignment of IP addresses to symbolic names within the LAN between each other.

After powered on, unconfigured LANCOM devices check first, whether a DHCP server is already active in the LAN. Dependent on the situation, the device is able to switch on its own DHCP server or, alternatively, to activate its DHCP client mode. In this second operating mode, the device itself can obtain an IP address from a DHCP server already existing in the LAN.

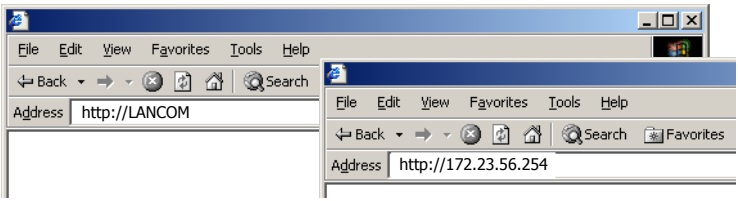
If a LANCOM Wireless Router or LANCOM Access Point is centrally managed from a LANCOM WLAN Controller, the DHCP mode is switched from auto-mode to client mode.

Network without DHCP server

Not for centrally managed LANCOM Wireless Router or LANCOM Access Points

In a network without DHCP server, unconfigured LANCOM devices activate their own DHCP server service after starting, and assign appropriate IP addresses and gateway information to the other workstations within the LAN, provided that the workstations are set to obtain their IP address automatically (auto-DHCP). In this constellation, the device can be accessed with any web

browser from each PC with activated auto-DHCP function through the name **LANCOM** or by its IP address **172.23.56.254**.

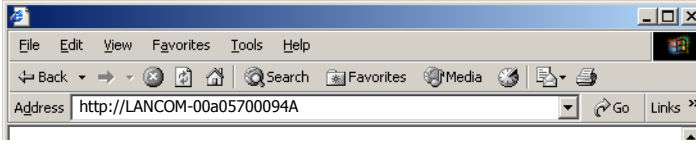


If the configuration PC does not obtain its IP address from the LANCOM DHCP server, figure out the current IP address of this PC (with **Start ▶ Execute ▶ cmd** and command **ipconfig** at the prompt under Windows 2000 or Windows XP, with **Start ▶ Execute ▶ cmd** and the command **winipcfg** at the prompt under Windows Me and Windows 9x, or with the command **ifconfig** on the console under Linux). In this case, the LANCOM is reachable under the IP address **x.x.x.254** ("x" stands for the first three blocks in the IP address of the configuration PC).

Network with DHCP server

If a DHCP server is active in the LAN to assign IP addresses, an unconfigured LANCOM device will turn off its own DHCP server. It will change into DHCP client mode and will obtain an IP address from the DHCP server of the LAN. This IP address is not known at first. The accessibility of the device depends on the name resolution:

- If there is a DNS server for name resolution in the LAN, which interchanges the assignment of IP addresses to names with the DHCP server, then the device can be accessed by the name "LANCOM <MAC address>" (e.g. "LANCOM-00a057xxxxxx").



The MAC address can be found on a label at the bottom of the device.

- If there is no DNS server in the LAN, or it is not linked to the DHCP server, then the device can not be reached by the name. The following options remain in this case:

EN

- Figure out the DHCP-assigned IP address of the LANCOM by suitable tools and contact the device directly with this IP address.
- Use LANconfig.

Starting the wizards in WEBconfig

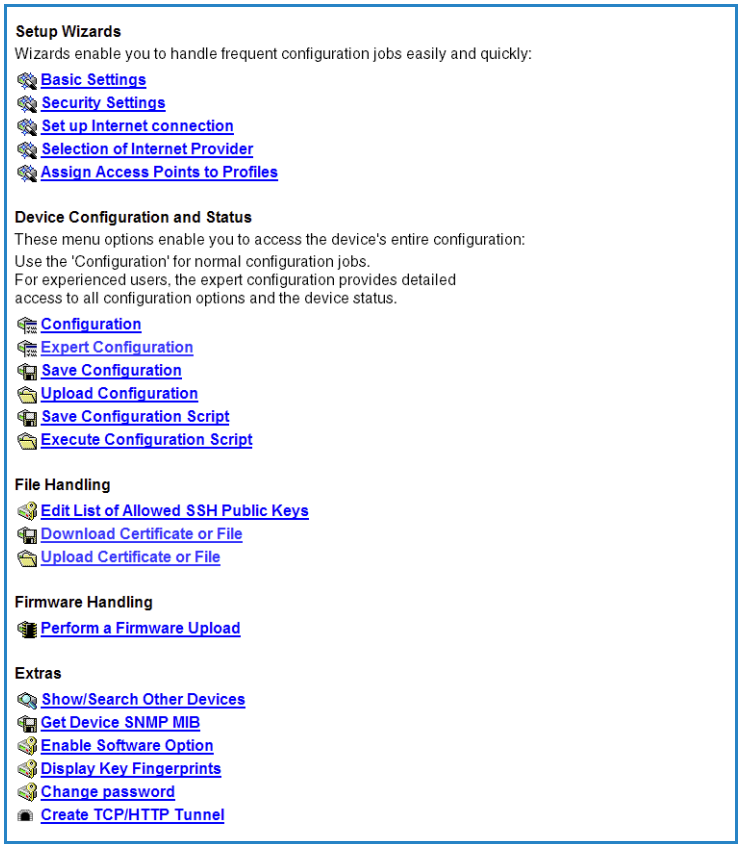
① Start your web browser (e.g. Internet Explorer, Firefox, Opera) and call the LANCOM Router there:

```
http://<IP address of the LANCOM>
```

(or with a name as discribed above)

If you cannot access an unconfigured LANCOM Router, the problem may be due to the netmask of the LAN: with less than 254 possible hosts (netmask > '255.255.255.0'), please ensure that the IP address 'x.x.x.254' is located in your own subnet.

The WEBconfig main menu will be displayed:



The setup wizards are tailored precisely to the functionality of the specific LANCOM Router. As a result, your device may offer different wizards than those shown here.

If you have chosen automatic TCP/IP configuration, please continue with Step ③.

② If you would like to configure the TCP/IP settings manually, assign an available address from a suitable address range to the LANCOM Router. Also set whether or not it is to operate as a DHCP server. Confirm your entry with **Apply**.

EN

③ Enter the wireless parameters. Select a network name (SSID) and a radio channel. Turn on if necessary the function for 'closed network'. Confirm your choice with **Next**.

④ In the following 'Security settings' window, specify a password for configuration access. Note that the password is case-sensitive and ensure that it is sufficiently long (at least 6 characters).

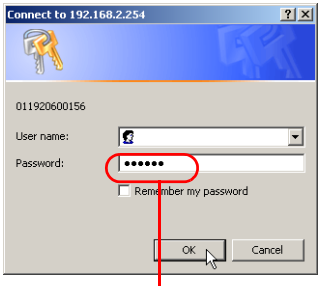
You may specify whether the device may only be configured from the local network or whether remote configuration via the WAN (i.e. a remote network) is also permissible.

Please note that enabling this will also permit remote configuration via the Internet. You should always make sure that the configuration access is suitably protected, e.g. with a password.

Entering the password in the web browser

When you are prompted for a user name and password by your web browser when accessing the device in the future, enter your personal values to the corresponding fields. Please note that the password is case-sensitive.

If you are using the common configuration account, enter the corresponding password only. Leave the user name field blank.



Entering the configuration password

⑤ In the next window, select your DSL provider from the list that is displayed. Confirm your choice with **Apply**.

If you select 'My provider is not listed here,' you must enter the transfer protocol used by your DSL provider manually in the next window. Confirm your choice with **Apply**.

⑥ Connect charge protection can limit the cost of DSL connections to a predetermined amount if desired. Confirm your choice with **Apply**.

⑦ The basic setup wizard reports that all the necessary information has been provided. You can end the wizard with **Go on**.

3.4 TCP/IP settings to workstation PCs

The correct addressing of all devices within a LAN is extremely important for TCP/IP networks. In addition, all computers must know the IP addresses of two central points in the LAN:

- Default gateway – receives all packets that are not addressed to computers within the local network.
- DNS server – translates network names (www.**lancom.de**) or names of computers (**www**.lancom.de) to actual IP addresses.

The LANCOM Router can perform the functions of both a default gateway and a DNS server. In addition, as a DHCP server it can also automatically assign valid IP addresses to all of the computers in the LAN.

The correct TCP/IP configuration of the PCs in the LAN depends on the method used to assign IP addresses within the LAN:

- **IP address assignment via the LANCOM Router (default)**

  In this operating mode the LANCOM Router not only assigns IP addresses to the PCs in the LAN, it also uses DHCP to specify its own IP address as that of the default gateway and DNS server. The PCs must therefore be configured so that they automatically obtain their own IP address and the IP addresses of the standard gateway and DNS server (via DHCP).

- **IP address assignment via a separate DHCP server**

  The workstation PCs must be configured so that they automatically obtain their own IP address and the IP addresses of the standard gateway and DNS server (via DHCP). The IP address of the LANCOM Router must be stored on the DHCP server so that the DHCP server transmits it to the PCs in the LAN as the standard gateway. In addition, the DHCP server should also specify the LANCOM Router as a DNS server.

- **Manual IP address assignment**

  If the IP addresses in the network are assigned static ally, then for each PC the IP address of the LANCOM Router must be set in the TCP/IP configuration as the standard gateway and as a DNS server.

For further information and help on the TCP/IP settings of your LANCOM Router, please see the reference manual. For more information on the network configuration of the workstation computers, please refer to the documentation of your 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-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 79.

4.1 Basic settings for 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 default configuration that the WLAN Controller can provide to the Access Points.

The information in this section enables the basic configuration of the WLAN Controllers for fast commissioning. It does not, however, go into detail on the full range of options and specifics of the individual parameters. A detailed description of the LANCOM WLAN Controller configuration parameters can be found under 'Extended settings' → Page 49.

EN

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 Enrolement 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, use WEBconfig and click on the link 'Set date and time' at the lower edge of the browser window.

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.

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 random number and the necessary certificates have been generated, the LANCOM WLAN Controller indicates that it is operational and the WLAN LED blinks red.

The WLAN Controller should be connected to the LAN in order to generate random numbers that are cryptographically sound. Depending on the network constellation, it may take a few minutes for the random number to be generated. Random numbers only have to be generated if the device was switched on and off a number of times, otherwise there should be sufficient random numbers in memory.

Once operational, you should make a backup copy of the certificates ('Backing up the certificates' → Page 65).

4.1.2 Generating a default configuration

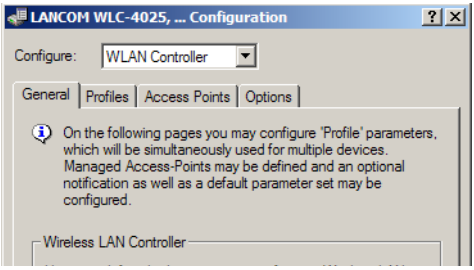
With the time information and the certificates, the LANCOM WLAN Controller is ready for operations. If the LAN contains Access Points in managed mode

(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 79), the WLAN Controller soon displays these as "New Access Points" in that the New APs LED blinks orange. The display of the LANCOM WLC-4025 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.

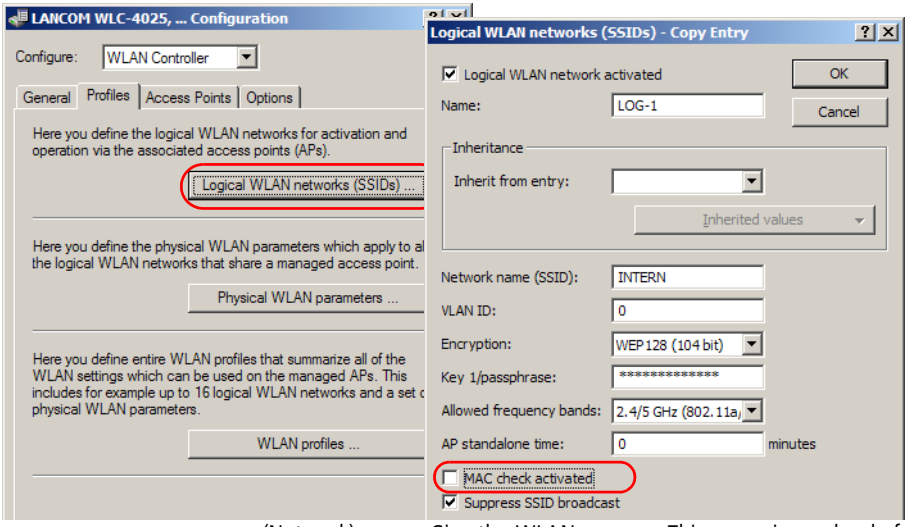
② In the configuration area 'WLAN Controller' on the 'General' tab, activate the options for the automatic acceptance of new Access Points and the provision of a default configuration.



- 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.

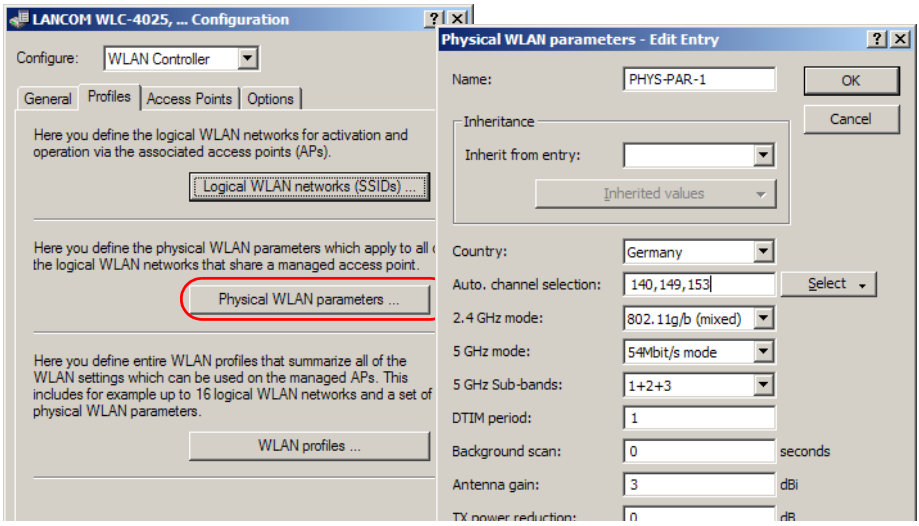
By combining these two options, the LANCOM WLAN Controller can automatically integrate any managed-mode Access Point found in the LAN into its WLAN infrastructure. This may, for example, be a temporary measure during the rollout phase of a WLAN installation.

③ On the 'Profiles' tab, select the logical WLAN networks. Add a new entry with the following values:

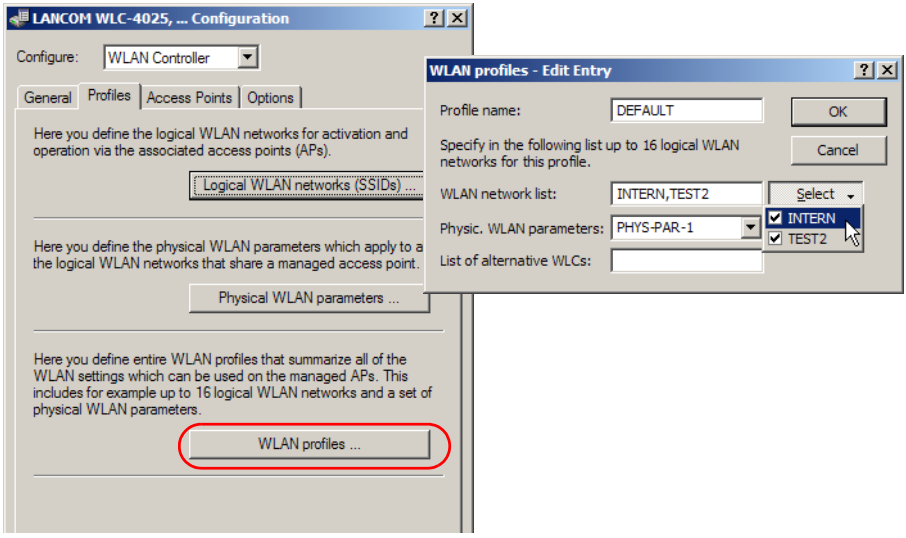


- (Network) name: Give the WLAN a name. This name is used only for administrative purposes in the LANCOM WLAN Controller.
- SSID: This SSID is used for the WLAN clients to connect.
- Encryption: Select the encryption method suitable for the WLAN clients being used, and enter a key or passphrase, as applicable.
- 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 75.

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.

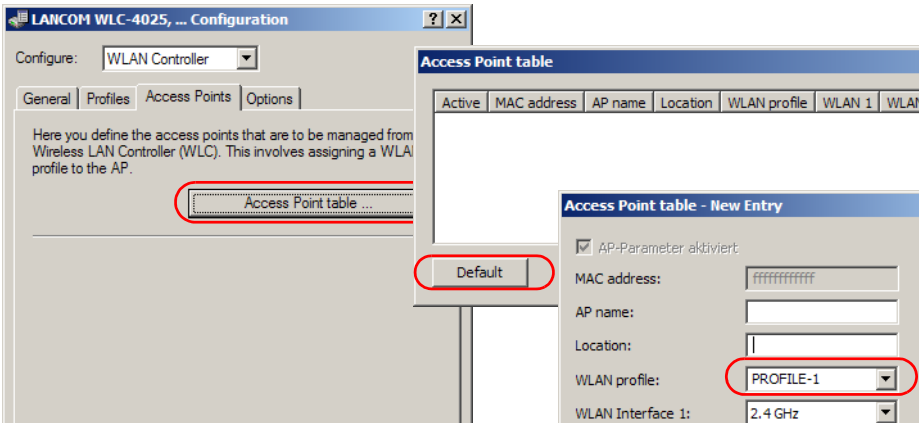


⑤ Create a new WLAN profile, give it an unique name, and assign the above logical WLAN network and physical WLAN parameters to it.



⑥ Change to the 'Access Point' 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 'ffffffffffff' 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.

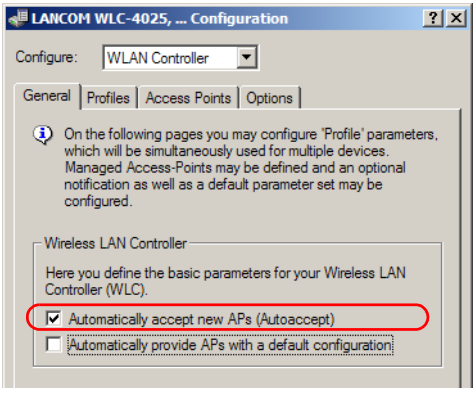


4.1.3 Assigning the default configuration to the new Access Points

With these settings you have defined all of the necessary values for the WLAN Controller to provide theAccess 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.

- **Automatically accept new APs (Auto-accept)**

  Enables the WLAN Controller to provide all new Access Points with a configuration, even those not in possession of a valid certificate.

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

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

- **Automatic provision of the default configuration**

  This enables the WLAN Controller to assign a default configuration to every new Access Point (even those **without** a valid certificate), even if no explicit configuration has been stored for it. In combination with auto-

accept, the LANCOM WLAN Controller can accept all managed-mode Access Points which are found in the WLAN infrastructure managed by it (up to the maximum number of Access Points that can be managed by one WLAN Controller).

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 if you can be sure that no unintended Access Points are connected with the LAN and thus accepted into the WLAN infrastructure.
On	Off	Controlled rollout phase: Use this combination if you have entered all of the approved Access Points into the AP table along with their MAC addresses, 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.

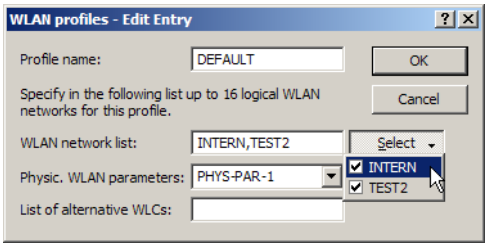
4.2.2 Profiles

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

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:



Configuration tool	Call
LANconfig	WLAN Controller ▶ Profiles ▶ WLAN profiles
WEBconfig, Telnet	Expert configuration > Setup > WLAN management > Profiles

■ **Profile name**

Name of the profile under which the settings are saved.

□ Maximum 31 ASCII characters.

■ **WLAN network list**

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

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

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

■ **Physical WLAN parameters**

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

■ **IP address of alternative WLAN Controllers**

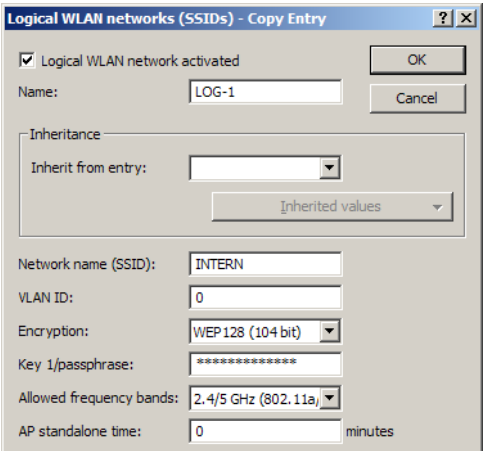
A list of WLAN Controllers that the Access Points should attempt to connect with. The Access Point starts searching for a WLAN Controller with a broadcast. Defining alternative WLAN Controllers is worthwhile when a broadcast cannot reach all WLAN Controllers (e.g. if the WLAN Controller is located in another network).

EN

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

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:



Configuration tool	Call
LANconfig	WLAN Controller ▶ Profiles ▶ Logical WLAN networks
WEBconfig, Telnet	Expert configuration > Setup > WLAN management > AP configuration > Networks

- **Network name**

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

  - Maximum 32 ASCII characters.

- **Inheritance**

  Selection of a logical WLAN network defined earlier and from which the settings are to be inherited (‘Inheritance of parameters’ → Page 64).

- **SSID**

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

- Maximum 32 ASCII characters.

■ **VLAN ID**

VLAN ID for this logical WLAN network ('Dynamic VLAN assignment' → Page 73).

- 0 to 4094
- Default: 0
- Special values: 0 switches off the use of VLAN with this WLAN network.

Please note that to use VLAN IDs in a logical WLAN network requires a management VLAN ID to be set ('Management VLAN ID' → Page 56).

■ **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 interrupted temporarily. Furthermore this represents an effective measure against theft as all security-related configuration parameters are automatically deleted after this time has expired.

If the Access Point establishes a backup connection to a secondary WLAN Controller then the countdown to the expiry of self-sufficient operation is halted ('Backup with primary and secondary WLAN

Controllers' → Page 70). The Access Point and its WLAN networks remain active as long as it has a connection to a WLAN Controller.

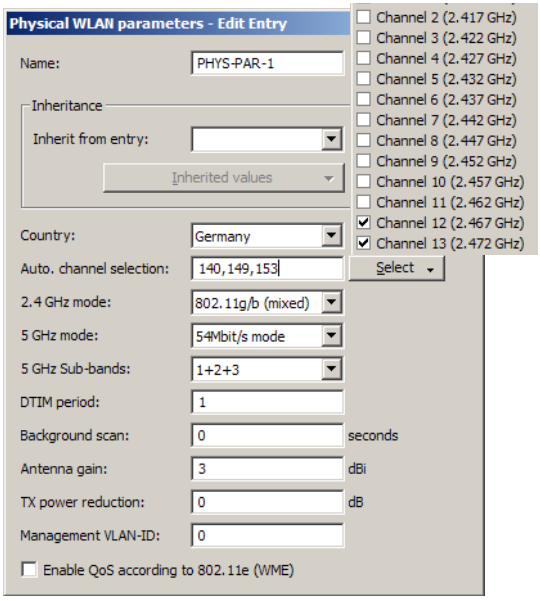
Please note that the delay before deletion of the flash configuration is the time of self-sufficient operation, not the time after power loss!

- 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.

All other WLAN network parameters correspond to those for the standard configuration of Access Points. Please refer to the LCOS reference manual for information.

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:



Configuration tool	Call
LANconfig	WLAN Controller ▶ Profiles ▶ Physical WLAN parameters
WEBconfig, Telnet	Expert configuration > Setup > WLAN management > AP configuration > AP parameters

- **Name**

  Unique name for this combination of physical WLAN parameters.

  - Maximum 31 ASCII characters.

- **Inheritance**

  Selection of a physical WLAN parameter set defined earlier and from which the settings are to be inherited ('Inheritance of parameters' → Page 64).

- **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.

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

EN

- **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. Ranges can also be defined (e.g. '7–9').

  - Maximum 16 characters.

- **Management VLAN ID**

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

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

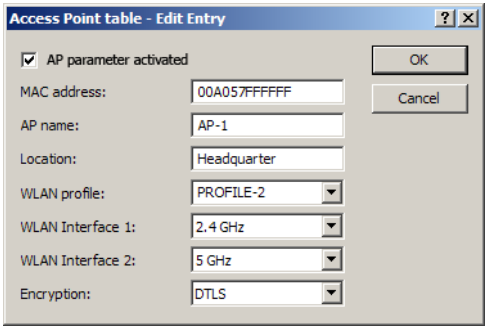
- 0 to 4094
- Default: 0
- Special values:
  - 0: Switches the use of VLAN **off**.
  - 1: Switches the use of VLAN **on**; the management network remains untagged, however.
  - 2 to 4094: Switches the use of VLAN **on**; the management network uses the VLAN ID set here.

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. Please refer to the LCOS reference manual for information.

4.2.3 List of Access Points

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



Configuration tool	Call
LANconfig	WLAN Controller ▶ Access Points ▶ AP table
WEBconfig, Telnet	Expert configuration > Setup > WLAN management > AP configuration > AP configuration

■ **MAC address**

MAC address of each Access Point.

□ Special values: FFFFFFFFFFFF defines the default configuration ('Automatic provision of the default configuration' → Page 49).

■ **AP name**

Name of the Access Point in managed mode.

□ Maximum 16 ASCII characters.

■ **Location**

Location of the Access Point in managed mode.

□ Maximum 251 ASCII characters.

■ **WLAN profile**

WLAN profile from the list of defined profiles ('WLAN profiles' → Page 50).

■ **WLAN interface 1**

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

□ Values: 2,4 GHz, 5 GHz, off, default

□ Special values: 'Default' makes use of the frequency setting defined in the 'Options' area.

- **WLAN interface 2**

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

  - Values: 2,4 GHz, 5 GHz, off, default
  - Special values: 'Default' makes use of the frequency setting defined in the 'Options' area.

- **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.

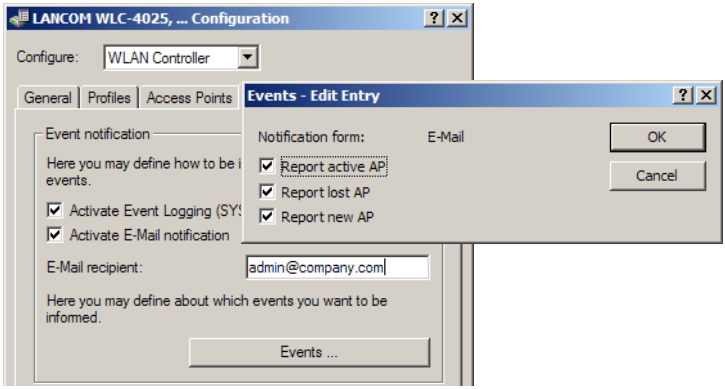
  - Values: DTLS, no, default
  - Special values: 'Default' makes use of the encryption method defined in the 'Options' area.

4.2.4 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:



Configuration tool	Call
LANconfig	WLAN Controller ▶ Options ▶ Event notification
WEBconfig, Telnet	Expert configuration > Setup > WLAN management > Notification

- **SYSLOG**

  Activates notification by SYSLOG.

  - Values: On/off.

- **E-mail**

  Activates notification by e-mail.

  - Values: On/off.

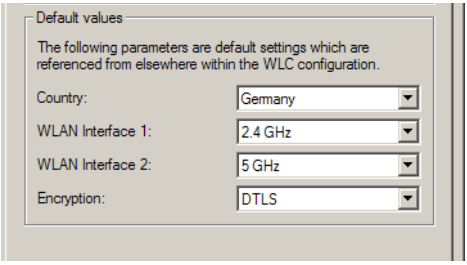
- **Events**

  Selects the events that trigger notification.

  - 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.



Configuration tool	Call
LANconfig	WLAN Controller ▶ Options ▶ Event notification
WEBconfig, Telnet	Expert configuration > Setup > WLAN management > Notification

- **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.

  - Values: 2,4 GHz, 5 GHz, off

- **WLAN interface 2**

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

  - Values: 2,4 GHz, 5 GHz, off

- **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.

  - Values: DTLS, no

EN

4.3 Further configuration details

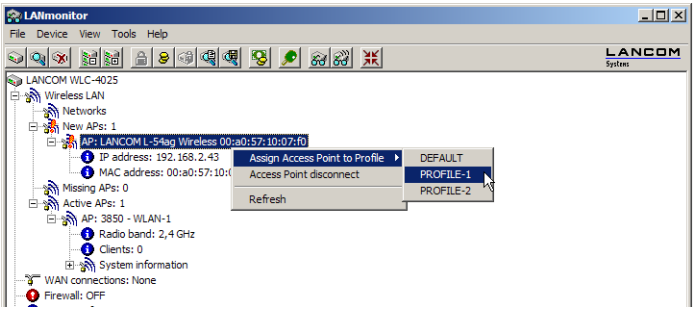
4.3.1 Accept new Access Points into the WLAN infrastructure manually

If you prefer not to accept Access Points into the WLAN infrastructure automatically (auto-accept, 'Automatically accept new APs (Auto-accept)' → Page 49), you can accept Access Points manually.

Access Point acceptance via LANmonitor

It is especially 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 assignment of a certificate

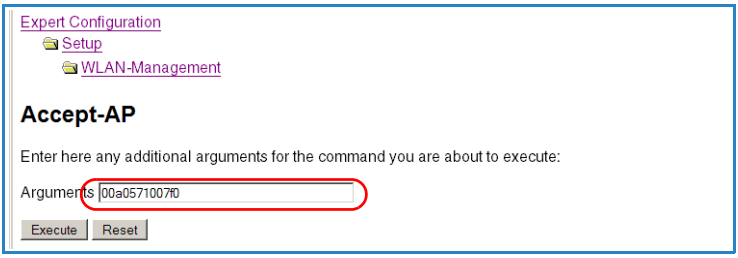
New Access Points that do not have a valid certificate but do have an entry in the AP table can be manually accepted with WEBconfig.

EN

① Open the LANCOM WLAN Controller configuration with WEBconfig.

② Under **Expert configuration** ▶ **Setup** ▶ **WLAN management** select the action **Accept AP**.

③ When requested for additional arguments, enter the MAC address of the Access Point for acceptance and confirm with **Execute**.

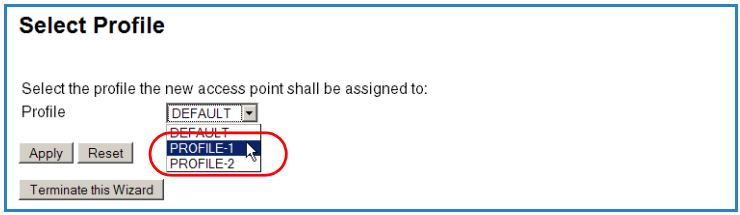


Accepting Access Points via WEBconfig with assignment of a certificate and configuration

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 entry page.

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.



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.

4.3.2 Manually removing Access Points from the WLAN infrastructure

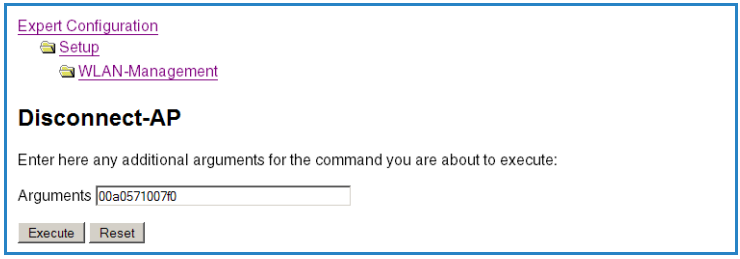
The following actions are required to remove an Access Point under management of the WLAN Controller from the WLAN infrastructure:

① Switch the WLAN operating mode of the WLAN module from 'Managed' to 'Client' or 'Access Point'.

② Delete the configuration for the Access Point and deactivate 'Automatically provide APs with a default configuration'.

③ Disconnect the Access Point in WEBconfig by selecting **Expert configuration ▶ Setup ▶ WLAN-Management** and the action **Disconnect AP**.

④ When requested for additional arguments, enter the MAC address of the Access Point to be disconnected and confirm with **Execute**.



EN

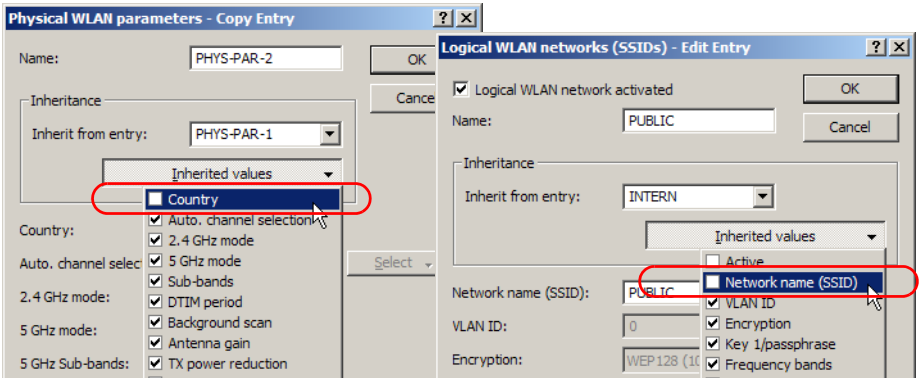
4.3.3 Inheritance of parameters

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. There are differences between the country settings and the device properties, for example.

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.

4.3.4 Backing up the certificates

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

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

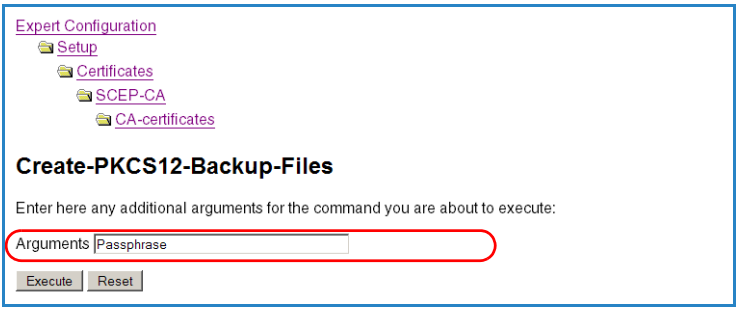
Create backups of the certificates

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' → Page 67). To ensure that this confidential information remains protected even when exported from the device, it is initially stored to a password-protected PCKS12 container.

① Open the configuration of the LANCOM WLAN Controller with WEBconfig under **Expert configuration** ▶ **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.

EN



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.

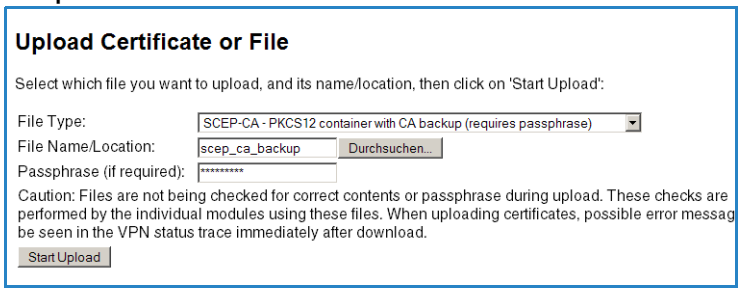
Uploading a certificate backup into the device

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**:



EN

4.3.5 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!

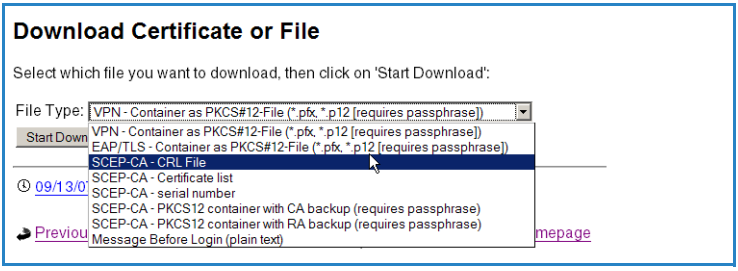
For this reason the following files have to be saved in addition to the certificates themselves:

- SCEP-CRL file: List of certificates issued and subsequently revoked by the SCEP-CA.
- SCEP certificate list: List of all certificates ever issued by the SCEP-CA.
- SCEP serial numbers: List with the serial numbers of issued certificates.

① On the WEBconfig entry page select the command **Download certificate or file**.

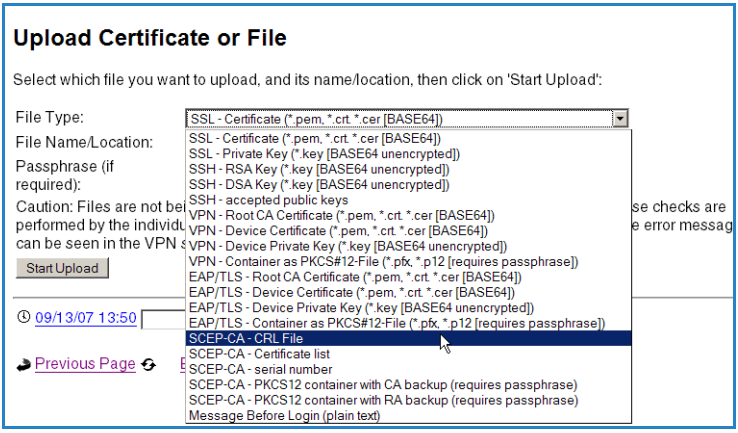
EN

② Select the entries listed above as data type one after the other and then confirm with **Start download**:



③ To upload these files to the device, go to the entry page of WEBconfig and select the command **Upload certificate or file**.

④ Select the entries listed above as data type one after the other, enter each file name and storage location and confirm with **Start upload**:



4.3.6 Backup solutions

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

In the event of a backup event, a managed Access Point should connect to another WLAN Controller. Because this connection will only function if the certificate in the Access Point has been authorized by the backup controller, it

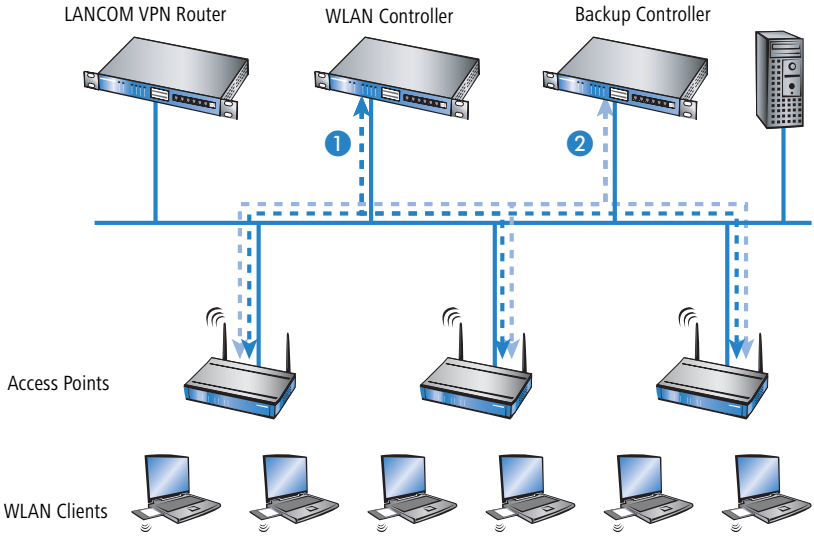
is essential that all WLAN Controllers sharing a backup solution have identical root certificates.

- 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 65).
- All of the WLAN Controllers should be set with similar time information to ensure that checks on the certificate validity period all produce the same result.

Apart from these basic settings you can choose between two different backup scenarios.

Backup with redundant WLAN Controllers

This is worthwhile for backing up a LANCOM WLAN Controller with a second WLAN Controller, the aim being to maintain full control over all managed Access Points at all times.



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.

EN

③ Configure the first WLAN Controller ❶ 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 Transfer the configuration from the first WLAN Controller ❶, for example using LANconfig, to the backup controller ❷. 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.

⑤ Should WLAN Controller ❶ fail, the Access Points will automatically search for another WLAN Controller and they will find the backup controller ❷. 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 78).

If the Access Points are set up for self-sufficient operation ('Self-sufficient operation' → Page 53) they will remain operational while searching for a backup controller, and the WLAN clients will remain associated.

Backup with primary and secondary WLAN Controllers

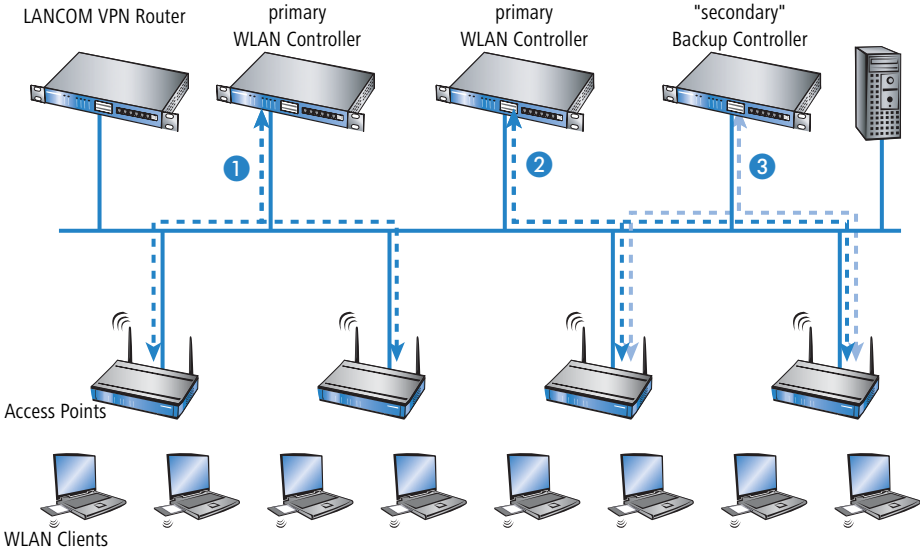
This second type of backup you can provide a larger number of "primary" WLAN Controllers with one common "secondary" backup controller. In case a WLAN Controller should fail, the Access Points remain operational but they work with the current configuration of the WLAN modules. As a secondary controller,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

Primary and secondary controllers

The establishment of a WLAN Controller/Access Point connection is always initiated by the Access Point. A LANCOM Access Point in managed mode will search the LAN for a WLAN Controller that will provide the configuration. During this search the Access Point may find various suitable WLAN Controllers:

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

This is an example of a backup solution with three LANCOM WLC-4025s for 50 managed Access Points: Two of the WLAN Controllers each manage 25 Access Points and the third is available as a backup:



① Set the same time on all LANCOM WLAN Controllers 1, 2 and 3.

② Transfer the CA and RA certificates from the first primary WLAN Controller 1 to the second primary 2 and to the secondary "backup controller" 3.

③ Configure the first WLAN Controller ❶ as required with the profiles and the associated AP table for one half of the Access Points. This WLAN Controller becomes the primary controller for the Access Points entered into it.

For a backup solution using a secondary WLAN Controller, be sure to set the time for self-sufficient operations such that the Access Point has time to find a backup controller. This is because the backup controller is not able to provide a new configuration for the Access Point.

Once the Access Point has established a backup connection to a secondary WLAN Controller the countdown until expiry of self-sufficient operation is halted. The Access Point and its WLAN networks remain active as long as it has a connection to a WLAN Controller.

④ Configure the second WLAN Controller ❷ for the other half of the Access Points, which subsequently treat this WLAN Controller as their primary controller.

⑤ For the backup controller ❸, only the time and the root certificate are set up. There is no further configuration.

⑥ After being started, the Access Points search for a WLAN Controller by emitting a discovery message. In this case, all three LANCOM WLAN Controllers respond to this message—the Access Points select "their" primary controller for the DTLS connection that follows. One half of the Access Points decides on WLAN Controller ❶ and the other half chooses WLAN Controller ❷. Because WLAN Controller ❸ does not function as primary controller for any of the Access Points, none of them log on to it.

⑦ In case of failure of, for example, WLAN Controller ❷, the Access Points automatically start searching for another WLAN Controller. They discover the WLAN Controller ❶ and ❸, whereby ❶ is already under full load with its 25 Access Points. Backup controller ❸ is able to check the validity of the certificates, i.e. it can authenticate the Access Points and accept them as managed Access Points. However, because the Access Points are **not** entered with their MAC numbers into the backup controller's AP table, the backup controller cannot manage the Access Points any further; they simply continue to operate with their current WLAN configurations.

If WLAN Controller ❶ is not under full load, for example because some of "its" Access Points are switched off, then some of the searching Access Points could log on here. WLAN Controller ❶ remains a

"secondary" controller for these Access Points because it does not have their configuration profiles. If in this case one of the Access Points with an entry in the AP table of WLAN Controller 1 is switched on again, then 1 accepts this reactivated Access Point and, in exchange, it disconnects one of the backup-event Access Points.

If the Access Points are set up for self-sufficient operation ('Self-sufficient operation' → Page 53) they will remain operational while searching for a backup controller, and the WLAN clients can continue to use all of their functions.

4.3.7 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.

- If the Access Point receives responses from primary and secondary WLAN Controllers, then primary controllers are preferred.
- 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 ('Automatic provision of the default configuration' → Page 49), all WLAN Controllers can be "filled" with equal numbers of configurations from a portion of the Access Points.

4.3.8 Dynamic VLAN assignment

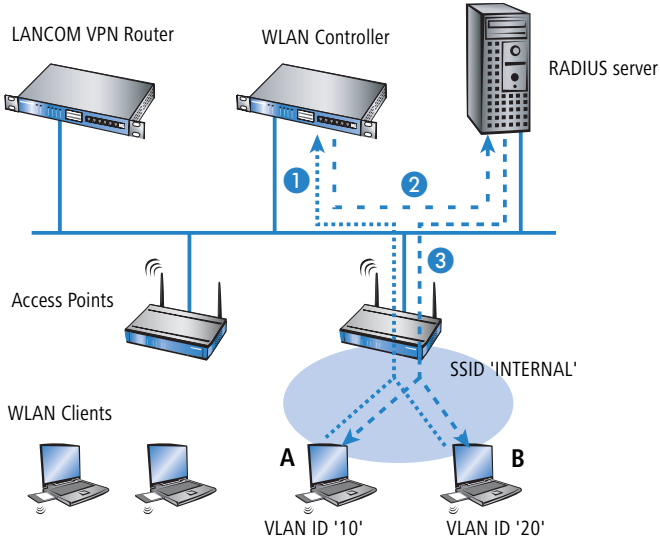
In larger WLAN infrastructures it can be worthwhile to assign individual WLAN clients to a certain network. Assuming that the WLAN clients are always within range of the same Access Points, then assignment can be realized via the SSID in connection with a particular IP network. If on the other hand the WLAN clients frequently change their position and logon to different Access Points then, depending on the configuration, they may find themselves in another IP network.

EN

For WLAN clients to remain within a certain network **independent** of their current WLAN network. dynamically assigned VLANs can be used. Unlike the situation where VLAN IDs are statically configured for a certain SSID (‘VLAN ID’ → Page 53), in this case a RADIUS server directly assigns the VLAN ID to the WLAN client.

Example: Two WLAN clients log into the same Access Point 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 configured RADIUS server. The RADIUS server can check the access rights of the WLAN clients. Furthermore it can also use the MAC address to assign a certain VLAN ID, for example. The WLAN client **A**, for example, receives the VLAN ID '10' and WLAN client **B** receives '20'.

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



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' → Page 56) for the management VLAN ID.

② For authentication via 802.1x, go to the encryption settings for the profile's logical WLAN network and choose a setting that triggers an authentication request.

③ To check the MAC addresses, activate the MAC check for the profile's logical WLAN network.

For the management of WLAN modules with a WLAN Controller, a RADIUS server is required to operate authentication via 802.1x and MAC-address checks. The WLAN Controller automatically defines itself as the RADIUS server in the Access Points that it is managing—all RADIUS requests sent to the Access Point are then directly forwarded to the WLAN Controller, which can either process the requests itself or forward them to an external RADIUS server. An external RADIUS server is required for the automatic assignment of a VLAN ID based on registration data.

④ To forward RADIUS requests to another RADIUS server, use LANconfig to enter its address into the list of forwarding servers in the configuration area 'RADIUS servers' on the 'Forwarding' tab. Alternatively, external RADIUS servers can be entered in WEBconfig under **Expert configuration ▶ Setup ▶ RADIUS ▶ Server ▶ Forward server**.

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.

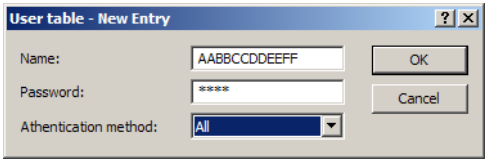
Further information about RADIUS is available in the LCOS reference manual and in the documentation for your RADIUS server.

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.

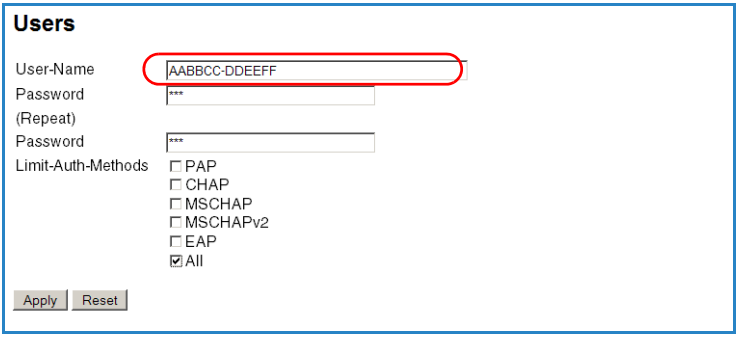
In LANconfig enter the approved MAC addresses into the RADIUS database in the configuration area 'RADIUS servers' on the 'General' tab. Enter the MAC

address as 'Name' and as 'Password' and select the authentication method 'All'.



Alternatively, approved MAC addresses can be entered in WEBconfig under **Expert configuration ▶ Setup ▶ RADIUS ▶ Server ▶ Users**.

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



4.3.10 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.

Access Point deactivation

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 self-sufficient operation (‘Self-sufficient operation’ → Page 53) 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 primary 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.

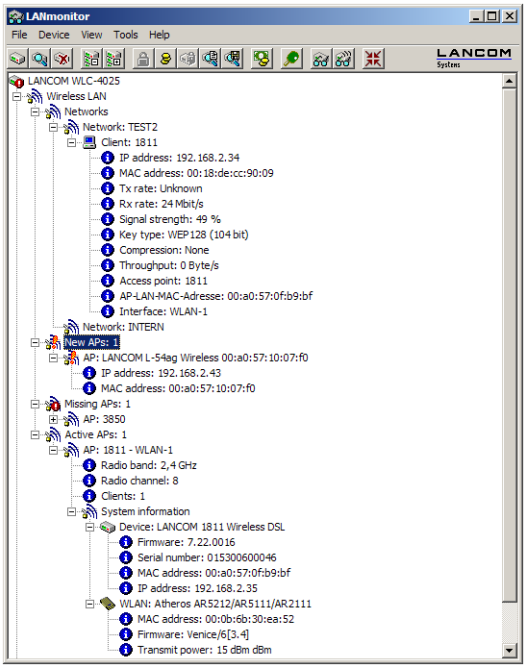
- If you have access to the Access Point, the certificates are quickly deleted by resetting the device.
- If the device has been stolen and consequently needs to be removed from the WLAN infrastructure, then the certificates in the WLAN Controller's CA have to be revoked. This is done in WEBconfig by 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.

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

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:

EN



- 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' → Page 61).

- **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.

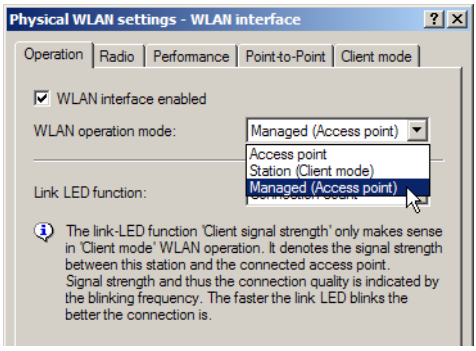
4.5 Configuring the Access Points

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 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
```

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

5 Security settings

Your LANCOM device has numerous security functions. You find in this chapter all information needed for an optimal protection of the base station.

5.1 Security for the Wireless LAN

Reflecting on Wireless LANs often entails substantial doubts concerning security. Many people suppose that abuse of data transmitted via radio links is relatively simple.

Wireless LAN devices by LANCOM Systems permit the employment of modern security technologies:

- Closed network
- Access Control (via MAC addresses)
- LANCOM Enhanced Passphrase Security
- Encryption of data transfer (802.11i/WPA or WEP)
- 802.1x / EAP
- optional IPSec over WLAN (VPN), in combination with external VPN gateway

5.1.1 Closed network

Each Wireless LAN according to IEEE 802.11 has its own network name (SSID). This network name serves as identification and enables administration of Wireless LANs.

A Wireless LAN can be established in such a way that any user gets access to this network. Such networks are called open networks. Any user can access an open network also without knowledge of the WLAN network name reserved specifically for this network. Only requirement is the input of the network name 'ANY'.

In a closed network the access via 'ANY' is not possible. User have to specify the correct network name. Unknown networks stay hidden to them.

Ad-hoc-networks are automatically installed as closed networks and cannot be opened. Infrastructure networks can be run either in open or closed condition. You make the settings for this at the respective base station.

EN

5.1.2 Access control via MAC address

Each network device has an special identification number. This identification number is the so-called MAC address (**M**edia **A**ccess **C**ontrol), which is worldwide unique per device.

The MAC address is programmed into the hardware and cannot be changed. Wireless LAN devices by LANCOM Systems have got a MAC address label on the casing.

The access to an infrastructure network can be restricted to known MAC addresses for certain Wireless LAN devices solely. To do so, Access Control lists are available within the LANCOM base stations, in which the granted MAC addresses can be deposited.

This method of access control is not available for ad-hoc networks.

5.1.3 LANCOM Enhanced Passphrase Security

With LEPS (**L**ANCOM **E**nhanced **P**assphrase **S**ecurity) LANCOM Systems has developed an efficient method which uses the simple configuration of IEEE 802.11i with passphrase and yet which avoids the potential error sources of passphrase sharing. 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.

An additional security aspect: LEPS can also be used to secure single point-to-point connections (P2P) with an individual passphrase. Even if an access point in a P2P installation is stolen and the passphrase and MAC address become known, all other WLAN connections secured by LEPS remain protected, particularly when the ACL is stored on a RADIUS server.

5.1.4 Encryption of the data transfer

A special role comes up to the encryption of data transfer for Wireless LANs. For IEEE 802.11 radio transfer the supplementing encryption standards are

802.11i/WPA and WEP. The function of the encryption is to ensure the security level of cable-bound LANs also in Wireless LANs.

- Use encryption on the data transferred in the WLAN. Activate the strongest possible encryption available to you ((802.11i with AES, WPA or WEP) and enter the appropriate keys or passphrases into the access point and the WLAN clients.
- Regularly change the WEP keys in your access points. The passphrases for 802.11i or WPA do not have to be changed 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 aged WEP method.
- If the data is of a high security nature, you can further improve the encryption by additionally authenticating the client with the 802.1x method or activate an additional encryption of the WLAN connection as used for VPN tunnels ('IPSec over WLAN'). In special cases, a combination of these two mechanisms is possible.

Further details to WLAN security and the used encoding methods can be found in the LCOS reference manual.

5.1.5 802.1x / EAP

The international industry standard IEEE 802.1x and the **E**xtensible **A**uthentication **P**rotocol (EAP) enables the realization of reliable and secure access controls for base stations. The access data is centrally administered on a RADIUS server then, and can be retrieved by the base station if required.

Moreover, this technology makes enables a secured dispatch and a regular automatic change of WEP keys. In this way IEEE 802.1x improves the protection efforts of WEP.

In Windows XP the IEEE-802.1x technology is already integrated by default. For other operating systems 802.1x client software is available.

The drivers for the LANCOM AirLancer wireless cards already feature an integrated 802.1x client.

5.1.6 IPSec over WLAN

By means of IPSec over WLAN a radio network can be optimally secured in addition to the already introduced securing mechanisms. In order to run IPSec over WLAN you need an external VPN gateway and the LANCOM Advanced VPN Client, which runs under the operating systems Windows 2000, Windows

XP and Windows Vista™. For other operating systems client software from other manufacturers is available. The drivers for the LANCOM AirLancer wireless adapter are already equipped with a 802.1x client.

5.2 Tips for handling keys

The security of encryption procedures can be substantially increased the by paying attention to some important rules for handling keys.

- **Keep keys as secret as possible.**
  Never note a key. Popular, but completely unsuitable are for example: notebooks, wallets and text files in PCs. Do not share a key unnecessarily.
- **Select a random key.**
  Use randomized keys of character and number sequences. Keys from the general linguistic usage are insecure.
- **Change a key immediately in case of suspicion.**
  It is time to change the key of the Wireless LAN if an employee with access to a key leaves your company. The key should also be renewed in case of smallest suspicion of a leak.
- **LEPS prevents the global spread of passphrases.**
  Activate LEPS to enable the use of individual passphrases.

5.3 The security settings wizard

Access to the configuration of a device permits not only to read out critical information (e.g. Internet password). Rather, also the entire settings of the security functions (e.g. firewall) can be altered then. So an unauthorized configuration access endangers not only a single device, but the entire network.

Your LANCOM has a password protection for the configuration access. This protection is already activated during the basic configuration by entering a password.

The device locks access to its configuration for a specified period of time after a certain number of failed log-in attempts. Both the number of failed attempts and the duration of the lock can be set as needed. By default, access is locked for a period of five minutes after the fifth failed log-in attempt.

Besides these general settings you can also check the security settings of the wireless network with the security wizard as far as your device has a WLAN interface.

5.3.1 Wizard for LANconfig

① Mark your LANCOM Router in the selection window. Select from the command bar **Extras** ▶ **Setup Wizard**.

② Select in the selection menu the setup wizard **Control Security Settings** and confirm your choice with **Next**.

③ Enter your password in the following windows and select the allowed protocols for the configuration access from local and remote networks.

④ In a next step parameters of the configuration lock like number of failed log-in attempts and the duration of the lock can be adjusted.

⑤ Now activate Stateful Inspection, ping-blocking and Stealth mode in the the firewall configuration.

⑥ The wizard will inform you when entries are complete. Complete the configuration with **Finish**.

5.3.2 Wizard for WEBconfig

Under WEBconfig you have the possibility to run the wizard **Security settings** to control and change the settings. The following values are handled:

- password for the device
- allowed protocols for the configuration access of local and remote networks
- parameters of configuration lock (number of failed log-in attempts and duration of the lock)

5.4 The firewall wizard

The LANCOM Router incorporates an effective protection of your LAN when accessing the Internet by its Stateful Inspection firewall and its firewall filters. Basic idea of the Stateful Inspection firewall is that only self-initiated data

transfer is considered allowable. All unasked accesses, which were not initiated from the local network, are inadmissible.

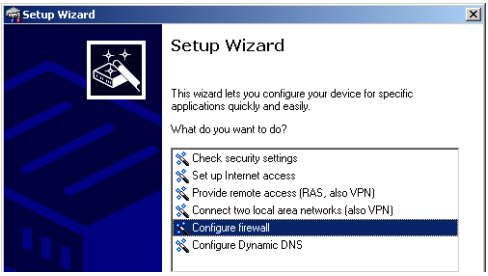
The firewall wizard assists you to create new firewall rules quickly and comfortably.

Please find further information about the firewall of your LANCOM and about its configuration in the reference manual.

EN

5.4.1 Wizard for LANconfig

① Mark your LANCOM Router in the selection window. Select from the command bar **Extras** ▶ **Setup Wizard**.



② Select in the selection menu the setup wizard **Configuring Firewall** and confirm your choice with **Next**.

③ In the following windows, select the services/protocols the rule should be related to. Then you define the source and destination stations for this rule and what actions will be executed when the rule will apply to a data packet.

④ You finally give a name to the new rule, activate it and define, whether further rules should be observed when the rule will apply to a data packet.

⑤ The wizard will inform you as soon as the entries are complete. Complete the configuration with **Finish**.

5.4.2 Configuration under WEBconfig

Under WEBconfig it is possible to check and modify all parameters related to the protection of the Internet access under **Configuration** ▶ **Firewall / QoS** ▶ **Rules** ▶ **Rule Table.**

5.5 The security checklist

The following checklist provides a comprehensive overview of all security settings for professionals. Most of the points on this checklist are no subject of concern in simple configurations, since these generally adequate security settings are already implemented during basic configuration and by the security wizard.

Detailed information on the security settings listed here can be found in the reference manual.

- **Have you assigned a password for the configuration?**

  The simplest option for the protection of the configuration is the establishment of a password. As long as a password hasn't been set, anyone can change the configuration of the device. The box for entering the password is located in LANconfig in the 'Management' configuration area on the 'Security' tab. It is particularly advisable to assign a password to the configuration if you want to allow remote configuration.

- **Have you permitted remote configuration?**

  If you do not require remote configuration, then deactivate it. If you require remote configuration, then be sure to assign a password protection for the configuration (see previous section). The field for deactivating the remote configuration is also contained in LANconfig in the 'Management' configuration area on the 'Security' tab. Select here under 'Access rights - of remote networks' for all types of configuration the option 'not allowed'.

- **Have you assigned a password to the SNMP configuration?**

  Also protect the SNMP configuration with a password. The field for protection of the SNMP configuration with a password is also contained in LANconfig in the 'Management' configuration area on the 'Security' tab.

- **Have you activated the Firewall?**

  The Stateful Inspection Firewall of the LANCOM ensures that your local network cannot be attacked from the outside. The Firewall can be enabled in LANconfig under 'Firewall/QoS' on the register card 'General'.

- **Do you make use of a 'Deny All' Firewall strategy?**

  For maximum security and control you prevent at first any data transfer through the Firewall. Only those connections, which are explicitly desired have to allowed by the a dedicated Firewall rule then. Thus 'Trojans' and

certain E-mail viruses loose their communication way back. The Firewall rules are summarized in LANconfig under 'Firewall/Qos' on the register card 'Rules'. A guidance can be found in the reference manual.

- **Have you activated the IP masquerading?**

  IP masquerading is the hiding place for all local computers for connection to the Internet. Only the router module of the unit and its IP address are visible on the Internet. The IP address can be fixed or assigned dynamically by the provider. The computers in the LAN then use the router as a gateway so that they themselves cannot be detected. The router separates Internet and intranet, as if by a wall. The use of IP masquerading is set individually for each route in the routing table. The routing table can be found in the LANconfig in the 'IP router' configuration section on the 'Routing' tab.

- **Have you closed critical ports with filters?**

  The firewall filters of the LANCOM Router devices offer filter functions for individual computers or entire networks. Source and target filters can be set for individual ports or for ranges of ports. In addition, individual protocols or any combinations of protocols (TCP/UDP/ICMP) can be filtered. It is particularly easy to set up the filters with LANconfig. The 'Rules' tab under 'Firewall/QoS' can assist you to define and change the filter rules.

- **Have you excluded certain stations from access to the router?**

  Access to the internal functions of the devices can be restricted using a special filter list. Internal functions in this case are configuration sessions via LANconfig, WEBconfig, Telnet or TFTP. This table is empty by default and so access to the router can therefore be obtained by TCP/IP using Telnet or TFTP from computers with any IP address. The filter is activated when the first IP address with its associated network mask is entered and from that point on only those IP addresses contained in this initial entry will be permitted to use the internal functions. The circle of authorized users can be expanded by inputting further entries. The filter entries can describe both individual computers and whole networks. The access list can be found in LANconfig in the 'TCP/IP' configuration section on the 'General' tab.

- **Is your saved LANCOM configuration stored in a safe place?**

  Protect the saved configurations against unauthorized access in a safe place. A saved configuration could otherwise be loaded in another device by an unauthorized person, enabling, for example, the use of your Internet connections at your expense.

EN

- **Have you secured your wireless network encryption, an ACL and LEPS?**

  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 by using 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.

  With the Access Control List (ACL) you can permit or prevent the access to your wireless LAN by individual clients. 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 set the 802.1x functions for particularly sensitive data exchange in the wireless network?**

  If you have a particularly sensitive data exchange in your wireless network, you can use the IEEE-802.1x technology for a more extensive protection. To control or to activate the IEEE-802.1x settings, select in LANconfig the configuration area 'User registration'.

- **Have you activated the mechanism that protects your WAN lines if the device is stolen?**

  After being stolen, the device can theoretically be operated at another location by unauthorized persons. Password-protected device configurations offer no protection from the operation of the RAS access, LAN coupling or VPN connections that are set up in the device; a thief could gain access to a protected network.

  The device's operation can be protected by various means; for example, it will cease to function if there is an interruption to the power supply, or if the device is switched on in another location.

  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.

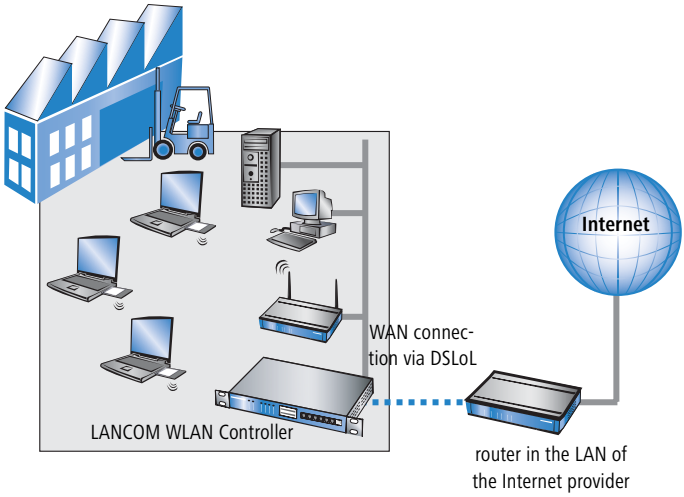
- **Have you ensured that the reset button is safe from accidental configuration resets?**

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

  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.

6 Setting up Internet access

All computers in the LAN can take advantage of the central Internet access of the LANCOM.



Does the setup wizard know your Internet provider?

A convenient wizard is available to help you set up Internet access. The wizard knows the access information of major Internet providers and will offer you a list of providers to choose from. If you find your Internet service provider on this list, you normally will not have to enter any further transfer parameters to configure your Internet access. Only the authentication data that are supplied by your provider are required.

Additional information for unknown Internet providers

If the setup wizard does not know your Internet provider, it will prompt you for all of the required information step by step. Your provider will supply this information.

Additional connection options

You may also enable or disable further options in the wizard, depending on whether or not they are supported by your Internet provider:

- Time-based billing or flat rate – select the accounting model used by your Internet provider.

EN

- When using time-based billing, you can set the LANCOM Router to automatically close existing connections if no data has been transferred within a specified time (the so-called idle time).

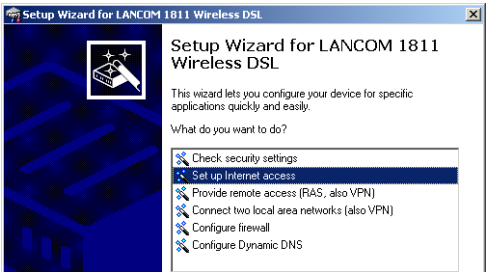
  In addition, you can activate a line monitor that identifies inactive remote stations faster and therefore can close the connection before the idle time has elapsed.

- Active line monitoring can also be used with flat rate billing to continuously check the function of the remote station.

  You also have the option of keeping flat rate connections alive if required. Dropped connections are then automatically re-established.

6.1 Instructions for LANconfig

① Highlight the LANCOM Router in the selection window. From the menu bar, select **Tools** ▶ **Setup Wizard**.



② From the menu, select the **Setup Internet access** wizard and click **Next**.

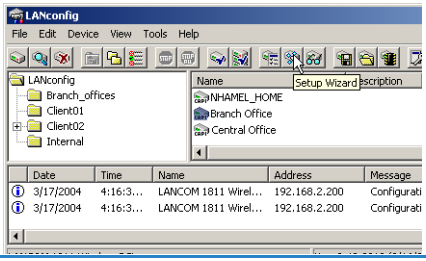
③ In the following window select your country and your Internet provider if possible, and enter your access information.

④ Depending on their availability, the wizard will display additional options for your Internet connection.

⑤ The wizard will inform you as soon as the entered information is complete. Complete the configuration with **Finish**.

LANconfig: Quick access to the setup wizards

Under LANconfig, the fastest way to launch the setup wizards is via the button on the toolbar.



EN

6.2 Instructions for WEBconfig

① In the main menu, select **Setup Internet access**.

② In the following window select your country and your Internet provider if possible, and enter your access information.

③ Depending on their availability, the wizard will display additional options for your Internet connection.

④ The wizard will inform you as soon as the entered information is complete. Complete the configuration with **Apply**.

EN

7 Linking two networks

With the network interconnection (also known as LAN to LAN coupling) of the LANCOM Router, two local networks are linked.

For coupling via VPN, the connection between both LANs is established over a specially secured connection through the public Internet. A router with VPN support is required in both LANs.

Always configure both sides

Both routers involved in the network interconnection must be configured. Care must be taken to ensure that the configuration information provided matches.

The following instructions will assume that LANCOM Router devices are being used on both sides. A network interconnection may also be realized with routers from other manufacturers. A mixed setup usually requires more extensive configuration measures for both devices, however. Please refer to the reference manual for more information in this regard.

A setup wizard handles the configuration of the connection in the usual convenient manner.

Security aspects

You must, of course, protect your LAN against unauthorized access. A LANCOM Router therefore offers a whole range of security mechanisms that can provide an outstanding level of protection: Network couplings via VPN transmit data by IPSec. The data are encrypted by AES, 3-DES, Blowfish or CAST encryption algorithms.

7.1 What information is necessary?

The wizard will prompt you for the necessary information on a step-by-step basis. If possible, however, you should have it available before launching the wizard.

To explain the significance of the information requested by the wizard, we will be using a typical deployment as an example: setting up a link between a branch office and its headquarters. The routers involved are named 'HEAD_OFFICE' and 'BRANCH'.

Please refer to the following tables for the entries to be made for each of the routers. Arrows mark the dependencies between the entries.

7.1.1 General information

The following details are required for the installation of LAN to LAN couplings.

Further details to network couplings via VPN using enhanced methods (e.g. digital certificates) can be found in the LCOS reference manual.

EN

Entry	Gateway 1		Gateway 2
Type of the local IP address	static/dynamic		static/dynamic
Type of the remote IP address	static/dynamic		static/dynamic
Name of the local device	'HEAD'		'BRANCH'
Name of the remote station	'BRANCH'		'HEAD'
Password for secure transmission of the IP address	'Password'		'Password'
Shared secret for encryption	'Secret'		'Secret'
IP address of remote station	'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 name of the remote network	'head'		'branch'
Hide local stations for access to remote network (Extranet VPN)?	yes/no		yes/no
NetBIOS routing for access to remote network?	yes/no		yes/no
Name of remote workgroup (NetBIOS only)	'workgroup1'		'workgroup2'

- The type of IP address must be stated for both sides for VPN connections via the Internet. There are two types of IP addresses: static and dynamic. An explanation of the two **IP address types** can be found in the reference manual.

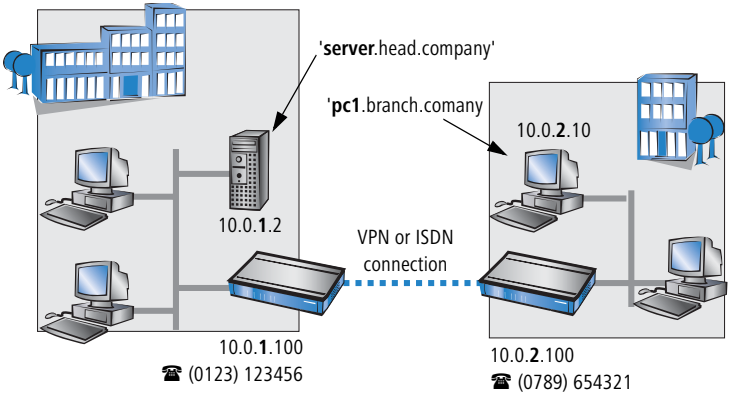
  Thanks to Dynamic VPN, connections can be enabled not only between gateways with fixed, static IP addresses, but even between gateways with dynamic IP addresses.

- If you haven't already named your LANCOM Router, the wizard will ask you for a new, **unique device name.** With this entry, you will rename your LANCOM Router. Be sure to give the two devices different names.
- The **name of the remote station** is needed for its identification.
- The **Shared Secret** is the central password for security within the VPN. The exact same password has to be entered on both sides

EN

7.1.2 Settings for the TCP/IP router

In TCP/IP networks, addressing has a special significance. Please note that two interconnected networks are logically separate from one another. Each must therefore have its own network number (in our example, '10.0.1.x' and '10.0.2.x'). These network numbers may not be identical.



Unlike when accessing the Internet, all of the IP addresses in the involved networks are visible on the remote side when coupling networks, not just those 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 in the headquarters and can access it (assuming it has the appropriate rights), and vice versa.

DNS access to the remote LAN

Thanks to DNS, it is not only possible to access remote computers in a TCP/IP network via their IP address, but also by using freely defined names.

For example, the computer with the name 'pc1.branch.company' (IP 10.0.2.10) will not only be able to access the server of the head office via its IP address, but also via its name, 'server.head.company'. The only precondition: the domain of the remote network in the wizard must be specified.

The domain can only be specified in the LANconfig wizard. In WEBconfig, enter the appropriate information later in the expert configuration. For more information, see the LANCOM reference manual.

Extranet VPN

Finally, one can decide whether access to local stations is permitted. In this 'Extranet VPN' operating mode, the IP stations do not expose their IP address to the remote LAN, rather they will be hidden behind the VPN gateway's IP address instead.

Therefore, the stations within the remote LAN cannot access IP stations in the other LAN directly. For example, if a headquarters. LAN in 'Extranet VPN' mode is hidden behind its gateway's address '10.10.2.100', and on of its IP stations (e.g. '10.10.2.13') accesses the IP station '10.10.1.2' of the branch office, then the branch office.s IP stations deems to be a accessed by '10.10.2.100'. The true IP address of the accessor ('10.10.2.13') is hidden.

If two LANs shall be coupled in Extranet mode, please ensure to enter the 'outbound' Extranet IP address of the remote site, not its Intranet address. According to the example, this was '10.10.2.100'. The appropriate netmask for the Extranet IP address would be '255.255.255.255' then.

7.1.3 Settings for NetBIOS routing

NetBIOS routing can be set up quickly: All that is required in addition to the information for the TCP/IP protocol used is the name of a Windows workgroup from in the router's own LAN.

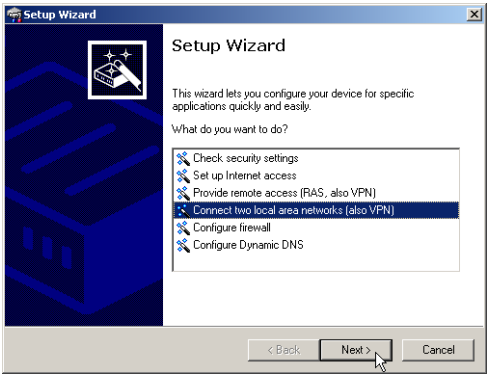
Remote Windows workgroups do not appear in the Windows Network Neighbourhood, but can only be contacted directly (e.g. via Find Computers).

7.2 Instructions for LANconfig

Perform the configuration on both routers, one at a time.

① Launch the 'Connect two local area networks' wizard. Follow the wizard's instructions and enter the required information.

EN



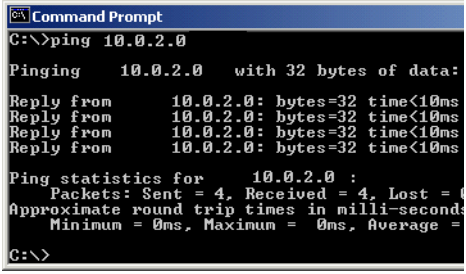
② The wizard will return a message to indicate that it has all the information it needs. Close the wizard with **Finish**.

③ After finishing the configuration of both routers, you can test the network connection. Try to contact a computer in the remote LAN (e.g. with a `ping`). The LANCOM Router should automatically set up a connection to the remote station and contact the required computer.

Ping – quick testing for TCP/IP connections

To test a TCP/IP connection, simply send a `ping` from your computer to a computer in the remote network. For more information on the 'ping' command, please see the documentation of your operating system.

IPX and NetBIOS connection can be tested by searching for a remote Novel Server or a computer in the remote Windows workgroup from your computer.



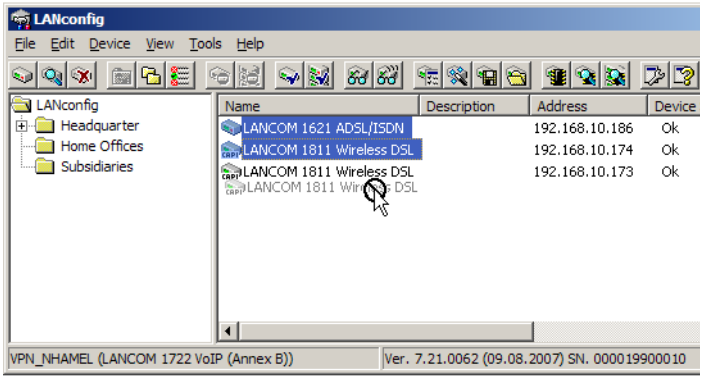
7.3 1-Click-VPN for networks (site-to-site)

The site-to-site coupling 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.

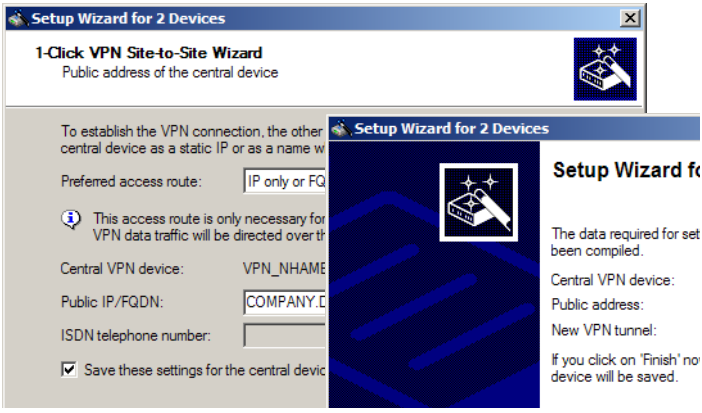
EN

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 or the 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

Under WEBconfig, the coupling of networks via VPN cannot be configured using the wizard. It can only be set up in the expert configuration. For details, please see the reference manual.

Perform the configuration on both routers, one at a time.

1. From the main menu, launch the 'Connect two local area networks' wizard. Follow the wizard's instructions and enter the required information.
2. The wizard will return a message to indicate that it has all the information it needs. Close the wizard with **Terminate**.
3. After finishing the configuration of both routers, you can test the network connection. Try to contact a computer in the remote LAN (e.g. with a `ping`). The LANCOM Router should automatically set up a connection to the remote station and contact the required computer.

EN

8 Providing dial-in access

Your LANCOM Router supports dial-in connections to permit individual computers full access to your network. This service is also known as RAS (Remote Access Service).

For a RAS access via VPN, the connection between the LAN and the dial-in PC is established over a specially secured connection through the public Internet. The router in the LAN requires VPN support, the dial-in PC an access to the Internet and the LANCOM VPN Client.

A setup wizard handles the configuration of the dial-in connection in the usual convenient manner.

Security aspects

You must, of course, protect your LAN against unauthorized access.

Network couplings via VPN transmit data by IPSec. The data are encrypted by AES, 3-DES, Blowfish or CAST encryption algorithms.

8.1 Which information is required?

The wizard will set up dial-up access for only one user. Please run the wizard again for each additional user.

8.1.1 General information

The following entries are required to set up a RAS connection.

Further details to network couplings via VPN using enhanced methods (e.g. digital certificates) can be found in the LCOS reference manual.

Entry
User name
Password
Shared secret for encryption
Hide local stations for access to remote network (Extranet VPN)?
IP addresses for the dial-up PCs: static or dynamic by address range (IP address pool)
NetBIOS routing for access to remote network?
Name of remote workgroup (NetBIOS only)

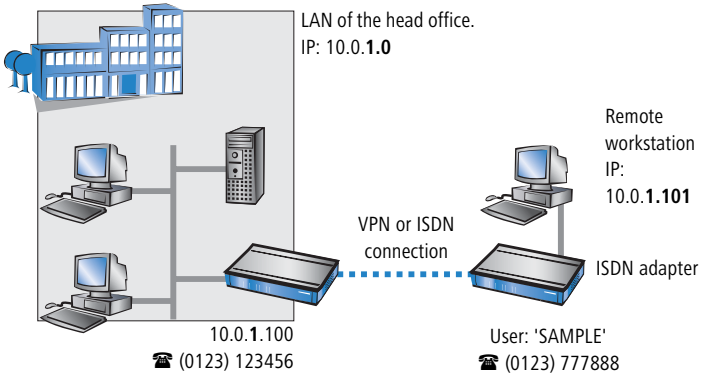
EN

Notes to the individual values:

- **User name and password**: Users authenticate themselves with this information when dialling in.

8.1.2 Settings for TCP/IP

Each active RAS user must be assigned an IP address when using the TCP/IP protocol.



This IP address can be permanently assigned when setting up a user. However, it is simpler to let the LANCOM Router automatically assign free IP addresses to users when they dial in. In this case you only need to specify the IP address range that the LANCOM Router should use for RAS users.

During both manual and automatic IP address assignment, please ensure that only free addresses from the address range of your local network are used. In our example, the IP address '10.0.1.101' will be assigned to the PC when connecting.

This IP address makes the computer a fully-fledged member of the LAN: with the appropriate rights, it can access all of the other devices in the LAN. The same applies in the other direction as well: computers in the LAN will also be able to access the remote machine.

8.1.3 Settings for NetBIOS routing

All that is required to use NetBIOS is the name of a Windows workgroup from the router's own LAN.

The connection is not established automatically. The RAS user must manually establish a connection to the LANCOM Router via Dial-Up Networking first. When connected, they can search for and access computers in the remote network (via **Find** ▶ **Computer**s, not through the Network Neighbourhood).

8.2 Settings for the dial-in computer

For dialing into a network via VPN a workstation requires:

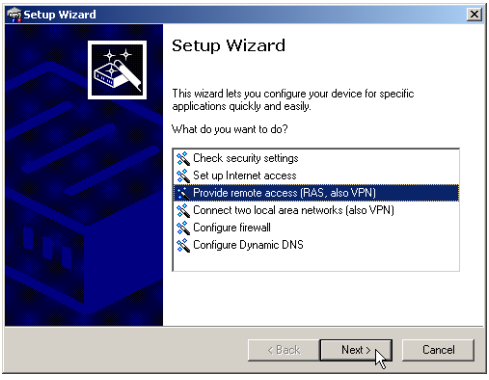
- an Internet access
- a VPN client

LANCOM Systems offers a 30 days trial version of the LANCOM Advanced VPN Client on the LANCOM CD. A detailed description of the LANCOM Advanced VPN Client and a description of its installation can also be found on the CD.

The wizard asks then for the values that have been defined during the installation of the RAS access in the LANCOM Router.

8.3 Instructions for LANconfig

① Launch the 'Provide Dial-In access (RAS)' wizard. Follow the wizard's instructions and enter the required information.



② The wizard will return a message to indicate that it has all the information it needs. Close the wizard with **Finish**.

③ Configure Dial-Up Networking access on the dial-in PC as described. Next, test the connection (see box 'Ping – quick testing for TCP/IP connections' → Seite 46).

8.4 1-Click-VPN for LANCOM Advanced VPN Client

EN

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 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

RAS access via VPN cannot be configured using the wizard under WEBconfig yet. It can only be set up in the expert configuration. For details, please refer to the reference manual.

⑤ From the main menu, launch the 'Connect two local networks' wizard. Follow the wizard's instructions and enter the required information.

⑥ Configure Dial-Up Networking access on the dial-in PC as described. Next, test the connection (see box 'Ping – quick testing for TCP/IP connections' → Seite 46).

EN

9 Appendix

9.1 Performance and characteristics

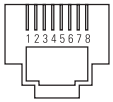
		LANCOM WLC-4006	LANCOM WLC-4025
Connectors	Ethernet LAN	5x 10/100Base-TX, autosensing, switch with node/hub autosensing	
	WAN	Any Ethernet port can be switched as a WAN connector.	
	Configuration	Serial V.24/RS-232 outband interface with Mini-DIN8 connector	
	Power supply	12V DC via external power supply	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, external power supply unit, printed manual (English, German), software CD	LAN cable (CAT.5, STP, 3 m), RS232 cable, IEC cable, printed manual (English, German), software CD
Options		■ LANCOM WLAN Controller-12-Option for managing up to 12 Access Points ■ LANCOM Service Option (4-year warranty, advance replacement) (item no. 61401)	■ LANCOM WLAN Controller-50-Option for managing up to 50 Access Points ■ LANCOM Service Option (4-year warranty, advance replacement) (item no. 61401)
Accessories		■ 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	

EN

9.2 Contact assignment

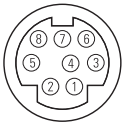
9.2.1 Ethernet interface 10/100Base-TX

8-pin RJ45 socket, corresponding to ISO 8877, EN 60603-7

Connector	Pin	IAE
	1	T+
	2	T-
	3	R+
	4	PoE/G
	5	PoE/G
	6	R-
	7	PoE/-48 V
	8	PoE/-48 V

9.2.2 Configuration interface (Outband)

8-pin mini-DIN socket

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

9.3 Declaration of conformity

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 are available in the appropriate product area on the LANCOM Systems web site (www.lancom.eu).

Index

EN

EN

EN

EN