



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

LANCOM IAP-54 Wireless LANCOM XAP-40-2 LANCOM XAC-40-1

- Handbuch
- Manual

LANCOM IAP-54 Wireless
LANCOM XAP-40-2
LANCOM XAC-40-1

© 2008 LANCOM Systems GmbH, Wuersele (Germany). All rights reserved.

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

The reproduction and distribution of the documentation and software 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 (eyay@cryptsoft.com).

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

This product includes the LZMA SDK written by Igor Pavlov.

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

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuersele

Germany

www.lancom.eu

Wuersele, Juli 2008

Preface

Thank you for placing your trust in this LANCOM Systems product.

The models LANCOM XAP-40-2, LANCOM XAC-40-1 and LANCOM IAP-54 Wireless offer professional access point technology at a maximum of WLAN performance.

Model variants

This documentation is for users of LANCOM WLAN products. Choose from different models:

- The LANCOM IAP-54 Wireless operates either according to the 802.11g standard with 2.4 GHz or according to the 802.11a standard at 5 GHz. It is additionally equipped with a specialized housing (IP50) for use in industrial environments such as in warehouses or production facilities.
- With two integrated 108 Mbps WLAN modules according to IEEE 802.11a/h or IEEE 802.11b/g the LANCOM XAP-40-2 works in the 2.4 and/or 5 GHz frequency range simultaneously. The LANCOM XAP-40-2 is equipped with a robust metal housing for mounting in switch cabinets and is supplied via 24 V voltage.
- The wireless LAN client LANCOM XAC-40-1 is the perfect supplement to WLAN base stations from LANCOM. The client can operate as a WLAN connection terminal, for example to provide a stationary or mobile network connection. It functions as a transparent WLAN- to-Ethernet translator and is suitable for operation under severe environmental conditions. The LANCOM XAC-40-1 offers a comprehensive range of security and QoS functions, and also a method of fast roaming to ensure reliable connection quality at all times.

Model
restriction

The sections of the documentation that refer only to a range of models are marked either in the corresponding text itself or with appropriate comments placed beside the text.

In the other parts of the documentation, all described models have been classified under the general term LANCOM.

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 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.

Content

1 Introduction	9
1.1 What is a wireless LAN?	9
1.1.1 Modes of operation of wireless LANs and access points	9
1.2 Just what can your LANCOM do?	10
2 Installation	14
2.1 Package contents	14
2.2 System requirements	15
2.2.1 Configuring the LANCOM devices	15
2.2.2 Operating access points in managed mode	15
2.3 Status displays, interfaces and hardware installation	15
2.3.1 LANCOM XAP-40-2 and LANCOM XAC-40-1	16
2.3.2 LANCOM IAP-54 Wireless	26
2.4 Software installation	31
2.4.1 Starting Software Setup	31
2.4.2 Which software should I install?	32
3 Basic configuration	33
3.1 What details are necessary?	33
3.1.1 TCP/IP settings	34
3.1.2 Configuration protection	35
3.1.3 Settings for the wireless LAN	36
3.2 Instructions for LANconfig	37
3.3 Instructions for WEBconfig	38
3.4 TCP/IP settings to workstation PCs	43

4 Security settings	44
4.1 Security for the Wireless LAN	44
4.1.1 Closed network	44
4.1.2 Access control via MAC address	45
4.1.3 LANCOM Enhanced Passphrase Security	45
4.1.4 Encryption of the data transfer	46
4.1.5 802.1x / EAP	46
4.1.6 IPSec over WLAN	47
4.2 Tips for handling keys	47
4.3 The security settings wizard	47
4.3.1 Wizard for LANconfig	48
4.3.2 Wizard for WEBconfig	49
4.4 The security checklist	49
5 Advanced wireless LAN configuration	53
5.1 WLAN configuration with the wizards in LANconfig	53
5.2 Point-to-point connections	55
5.2.1 Geometric dimensioning of outdoor wireless network links	56
5.2.2 Antenna alignment for P2P operations	60
5.3 Configuration of P2P connections	62
5.3.1 Access points in relay mode	64
5.3.2 Security for point-to-point connections	65
5.4 Client mode	67
5.4.1 Client settings	69
5.4.2 Set the SSID of the available networks	69
5.4.3 Encryption settings	70
6 Setting up Internet access	72
6.1 The Internet Connection Wizard	73
6.1.1 Instructions for LANconfig	73
6.1.2 Instructions for WEBconfig	74
6.2 The Firewall Wizard	74
6.2.1 LANconfig Wizard	74
6.2.2 Configuration under WEBconfig	75

7 Options and accessories	76
7.1 Optional LANCOM WLAN antennas	76
7.1.1 Antenna Diversity	77
7.1.2 Installation of AirLancer Extender antennas	77
7.2 LANCOM Public Spot Option	79
8 Troubleshooting	80
8.1 No DSL connection is established	80
8.2 DSL data transfer is slow	80
8.3 Unwanted connections under Windows XP	81
9 Appendix	82
9.1 Performance data and specifications	82
9.2 Contact assignment	83
9.2.1 Ethernet interface 10/100Base-TX, DSL interface	83
9.2.2 Configuration interface (Outband)	84
9.3 Declaration of conformity	84
10 Index	85

1 Introduction

1.1 What is a wireless LAN?



The following sections describe the functionality of wireless networks in general. You can see from the table 'What your LANCOM can do' further below which functions your device supports. Please refer to the reference manual for further information on this topic.

A wireless LAN connects individual end-user devices (PCs and mobile computers) to form a local network (also called – **Local Area Network**). In contrast to a traditional LAN, communication takes place over a wireless connection and not over network cables. For this reason it is called a **Wireless Local Area Network (WLAN)**.

A wireless LAN provides the same functionality as a cable-based network: Access to files, servers, printers etc. as well as the integration of individual work stations into a corporate mail system or access to the Internet.

There are obvious advantages to wireless LANs: Notebooks and PCs can be installed where they are needed—problems with missing connections or structural changes are a thing of the past with wireless networks.

Apart from that, wireless LANs can also be used for connections over longer distances. Expensive leased lines and the associated construction measures can be saved.



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

1.1.1 Modes of operation of wireless LANs and access points

Wireless LAN technology and access points in wireless LANs are used in the following modes of operation:

- Simple, direct connection between terminal devices with an access point (ad-hoc mode)
- Extensive wireless LANs, possibly connected to a LAN, with one or more access points (infrastructure network)

■ Chapter 1: Introduction

- Establishing access to the Internet
- Connecting two LANs over a wireless link (point-to-point mode)
- Connecting devices with an Ethernet interface via an access point (client mode)
- Extending an existing Ethernet network with a wireless LAN (bridge mode)
- Relay function for connecting networks via multiple access points
- Central administration using a LANCOM WLAN Controller

1.2 Just what can your LANCOM do?

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

	LANCOM IAP-54 Wireless	LANCOM XAP-40-2	LANCOM XAC-40-1
Operating modes			
Point-to-point mode (six P2P paths can be defined per WLAN interface)	✓	✓	
Access point mode	✓	✓	
Client mode	✓	✓	✓
Relay function to link two P2P connections		✓	
Managed mode for central configuration of WLAN modules by a WLAN Controller	✓	✓	
IP router	✓	✓	
Applications			
Industrial operation in IP50 protected housing for mast, wall or rail mounting	✓		
Industrial operation in compact housing for cabinet or rail mounting with 24 V supply (extended temperature range)		✓	✓
Internet access	✓	✓	
Stateful Inspection Firewall	✓	✓	
DHCP and DNS server (for LAN)	✓	✓	✓

	LANCOM IAP-54 Wireless	LANCOM XAP-40-2	LANCOM XAC-40-1
DHCP and DNS client (for WAN)	✓	✓	
Advanced Routing and Forwarding (ARF networks)	8	8	
N:N mapping for routing networks with the same IP-address ranges	✓	✓	✓
Policy-based routing	✓	✓	✓
Backup solutions and load balancing with VRRP	✓	✓	✓
PPPoE Server	✓	✓	✓
WAN RIP	✓	✓	✓
Spanning Tree protocol	✓	✓	✓
Layer 2 QoS tagging	✓	✓	✓
WLAN			
Wireless transmission by IEEE 802.11g and IEEE 802.11b	✓	✓	✓
Wireless transmission by IEEE 802.11a and IEEE 802.11h	✓	✓	✓
Turbo Mode: Double the bandwidth at 2.4 GHz and 5 GHz	✓	✓	✓
Super AG incl. hardware compression and bursting	✓	✓	✓
Multi SSID	✓	✓	
Roaming function	✓	✓	Client only
802.11i / WPA with hardware AES encryption	✓	✓	✓
WEP encryption (up to 128 Bit key length, WEP152)	✓	✓	✓
IEEE 802.1x/EAP Authenticator and supplicant in client mode	✓	✓	
IEEE 802.1x/EAP supplicant only in client mode			✓
MAC address filter (ACL)	✓	✓	
Individual passphrases per MAC address (LEPS)	✓	✓	
Closed network function	✓	✓	
Integrated RADIUS server	✓	✓	

■ Chapter 1: Introduction

	LANCOM IAP-54 Wireless	LANCOM XAP-40-2	LANCOM XAC-40-1
VLAN	✓	✓	✓
Intra-Cell Blocking	✓	✓	
WLAN QoS (IEEE 802.11e, WME)	✓	✓	✓
LAN connection			
Fast Ethernet LAN port (10/100Base-TX)	✓	2	1
Power-over-Ethernet (PoE)	✓	2-fach	1-fach
DHCP and DNS server	✓	✓	✓
WAN connection			
Connection for DSL modem (DSLol)	✓	✓	✓
Internet connection (IP-Router)			
Stateful Inspection Firewall	✓	✓	✓
Firewall filters (IP addresses, ports)	✓	✓	✓
IP-Masquerading (NAT, PAT)	✓	✓	✓
Quality of Service (QoS)	✓	✓	✓
Power supply			
Power-over-Ethernet (PoE) IEEE 802.3af	✓	double, redundant	✓
12 V via separate power adapter (DC)		✓	✓
24 V (DC) via industrial interface		double, redundant	double, redundant
Redundant power supply via PoE, 12 V or 24 V		✓	✓
Configuration and firmware			
Configuration with LANconfig or with web browser, additionally terminal mode for Telnet or other terminal programs, SNMP interface and TFTP server function, SSH connection	✓	✓	✓
Setup wizards	✓	✓	✓
FirmSafe with firmware versions for absolutely secure software upgrades	✓	✓	✓
Monitoring and management of the WLAN with Rogue AP Detection	✓	✓	

	LANCOM IAP-54 Wireless	LANCOM XAP-40-2	LANCOM XAC-40-1
Optionale Software- Erweiterungen			
LANCOM Public Spot Option	✓	✓	
LANCOM Service-Option	✓	✓	✓
Optional software extensions			
LANCOM Public Spot Option	✓	✓	
Optional hardware extensions			
AirLancer Extender antennas for increased range	✓	✓	✓
LANCOM Modem Adapter Kit for connection of analog or GSM modems to the serial interface	✓	✓	✓
Housing			
Industrial housing (IP50) for industrial operation	✓		
Industrial housing (IP40) for cabinet or rail mounting		✓	✓

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 contents

Please check the package contents for completeness before starting the installation. In addition to the base station itself, the package should contain the following accessories:

	LANCOM IAP-54 Wireless	LANCOM XAP-40-2	LANCOM XAC-40-1
12 V DC power adapter		✓	✓
Dualband antennas with screw connection	2	2	2
2 RP-SMA terminators to avoid interspersions on unused antenna connections		2	1
4-pin 24 V plug for custom assembly		✓	✓
Connector cable for serial configuration interface		✓	✓
Wall, mast and rail mounting accessories	✓		
Wall and rail mounting accessories		✓	✓
PoE ethernet cable (green plugs)	✓	✓	✓
PoE port injector (not included in bulk version)	✓		
LANCOM CD	✓	✓	✓
Printed documentation	✓	✓	✓

If anything should be 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, Windows Millennium Edition (Me), Windows 2000, Windows 98, Linux, BSD Unix, Apple Mac OS, OS/2.
- Access to the LAN via the TCP/IP protocol.
- Wireless LAN adapter or LAN access (if the access point is to be connected to the LAN).



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 Status displays, interfaces and hardware installation

Meanings of the LEDs

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

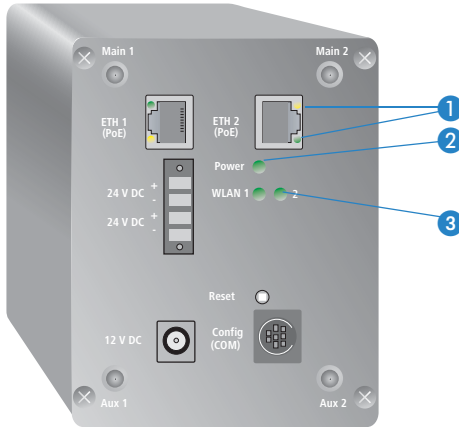
- ▶ **Blinking** means, that the LED is switched on or off at regular intervals in the respective indicated colour.
- ▶ **Flashing** means, that the LED lights up very briefly in the respective colour and stay then clearly longer (approximately 10x longer) switched off.
- ▶ **Inverse flashing** means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

2.3.1 LANCOM XAP-40-2 and LANCOM XAC-40-1

LEDs of LANCOM XAP-40-2 and LANCOM XAC-40-1

Model example:
LANCOM XAP-40-2



1 ETH 1 and
ETH 2
(LANCOM
XAP-40-2 only)

Status of the LAN ports:

off		No network device connected
green	constantly on	Connection to network device operational, no data traffic
yellow	flickering	Data traffic

2 Power

This LED indicates that the device is operational. After the device has been switched on, it will flash green for the duration of the self-test.

green	constantly on	Device ready for use
red/ green	blinking slow	Device insecure: configuration password not assigned
red	blinking	Time or connect-charge reached
red	blinking (fast)	hardware error

i The power LED flashes red when a charge limit is reached ('Flashing Power LED but no connection?' → page 17).

- 3 WLAN 1
WLAN 2
(LANCOM
XAP-40-2 only)

Gives information about the wireless LAN access and the data traffic of the internal WLAN modules:

off		No wireless networks configured, no beacons being broadcasted.
green		At least one wireless network is configured. The WLAN module is active and broadcasting beacons.
green	inverse flashing	Activity in wireless LAN (blinking frequency indicates the number of registered stations)
green	blinking	DFS or other scanning sequence.
green	flickering	TX data traffic
red	flickering	WLAN error (TX error, e.g. sending error because of bad connection quality)
red	blinking	Hardware error in WLAN module

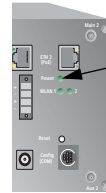
Flashing Power LED but no connection?

There's no need to worry if the Power LED blinks red and you can no longer connect to the WAN. This simply indicates that a preset time or connect-charge limit has been exceeded. There are three methods available for unlocking:

- Reset connect charge protection.
- Increase the limit that has been reached.
- Completely deactivate the lock that has been triggered (set limit to '0').

If a time or connect charge limit has been reached, you will be notified in LANmonitor. To reset the connect charge protection, select **Reset Charge and Time Limits** in the context menu (right mouse click). You can configure the connect charge settings in LANconfig under **Management / Costs** (you will only be able to access this configuration if 'Complete configuration display' is selected under **View / Options...**).

You will find the connect charge protection reset in WEBconfig and all parameters under **Expert Configuration / Setup / Charges-module**.

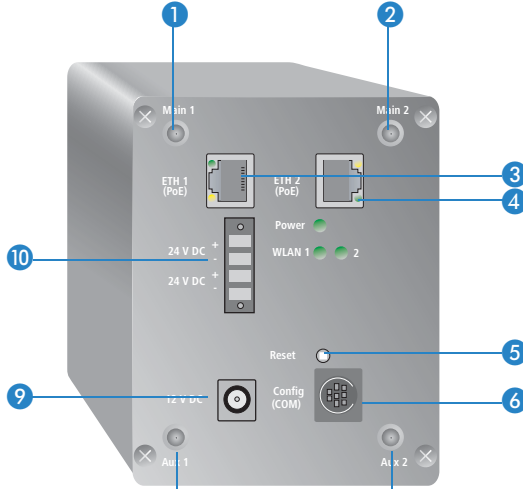


Signal for
exceeded time
or connect-
charge limit

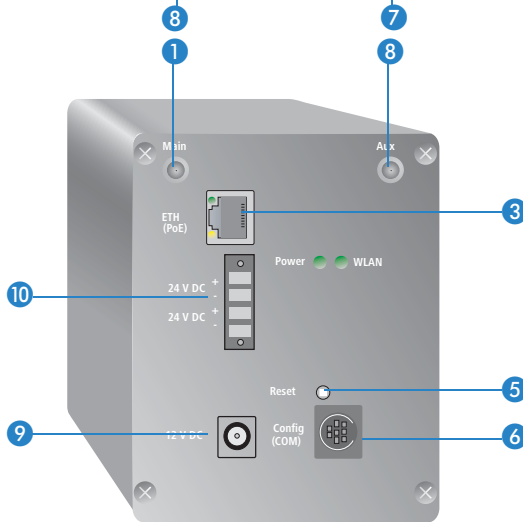
Interfaces of LANCOM XAP-40-2 and LANCOM XAC-40-1

All interfaces of the LANCOM XAP-40-2 and LANCOM XAC-40-1 are located on the front panel.

LANCOM XAP-40-2



LANCOM XAC-40-1



- ① Main connector for first WLAN module.
- ② Main connector for second WLAN module.

- 3 First 10/100Base-Tx ethernet connector for connection to the LAN.
- 4 Second ethernet connector.

Both 10 Mbps or 100 Mbps connections are supported. The available transfer rate is detected automatically (autosensing). The LAN connection features an automatic MDI/MDIX detector omitting the use of cross-over cables.

The LAN connector on the LANCOM access point supports the Power over Ethernet standard IEEE 802.3af (PoE). Further information about the operations with PoE can be found in the information box 'Power over Ethernet—elegant power supply over LAN cabling'.

By activated DSSoL option, the LAN connector can also be used for connecting the access point to a broadband modem.

- 5 Reset button (see "Reset button functions")
- 6 Serial configuration port
- 7 Aux connector for second WLAN modul.
- 8 Aux connector for first WLAN modul.
- 9 Connection for the included power adapter
- 10 Connection for 24 V DC via 4-pin plug (Phoenix Contact, Combicon RM 3,81mm). Two 24 V voltage sources can be connected to the redundant power supply.



The 24 V input in particular has been optimized for industrial settings. Variation of the input voltage between 20 V to 28 V can be tolerated.

Reset button functions

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

Some 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 the suitable setting, the behavior of the reset button can be controlled.

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



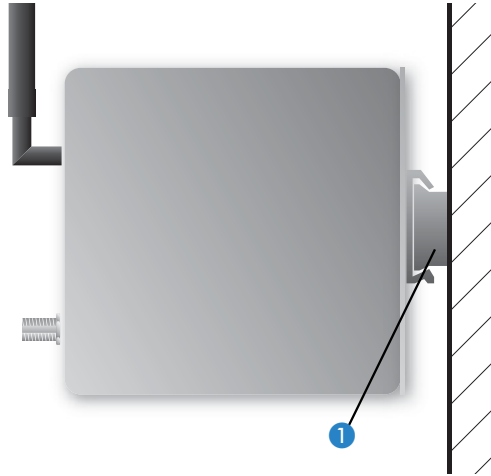
After resetting, the device starts completely unconfigured and **all** settings are lost. If possible be sure to backup the current device configuration **before** resetting.



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

Top hat rail mounting

- ① Mount your device in the required position on the top hat rail ①.



EN

Wall mounting

- ① Place the supplied top hat rail using the screws in the required position on the wall.
- ② Mount your device on the top hat rail as described above.

Connecting



When mounting the device, please observe the information on lightning protection in the LANCOM Outdoor Wireless Guide (download from www.lancom.eu). Mounting without adequate lightning protection could lead to serious damage to the access point and the network infrastructure connected to it.

Installation of the access point devices involves the following steps:

- ① **Antennas** —screw the two supplied diversity antennas onto the front side of the device:
 - Use the individual main connectors to build up separate Wireless networks (e.g. for point-to-point applications).
 - Apply the main and the aux connector of a single WLAN module to use the diversity function. The diversity function increases the quality

of the connection by transmitting and receiving via the antenna that provides the best contact to the client.



Antennas are only to be attached or changed when the device is switched off. Mounting or demounting antennas while the device switched on may cause the destruction of the WLAN module!



When assembling separately purchased mobile radio antennas please note that the maximum allowed transmission power of the wireless LAN according to EIRP in the country in question may not be exceeded. The system operator is responsible for adhering to the threshold values.

The employment of the AirLancer Extender SA-5L for internal lightning protection is **essential under all circumstances**—the AirLancer Extender SA-5L is always mounted between the Access Point and the antenna, preferably as near as possible to the antenna.



Unused connectors should be fitted with the terminators as supplied. This prevents stray signals from one WLAN module from interfering with the other WLAN module.



If the device is operated inside a switching cabinet, please take the attenuation caused by the cabinet itself into consideration when selecting the antenna to be used. For applications of this type, we recommend the use of an external antenna. For further information on external antennas and their mountings, please refer to 'Options and accessories' → page 74.

- ② **LAN** – You can first connect the access point to your LAN. For that purpose, plug the included network cable (green plugs) into the LAN connector of the device ③ or ④ and the other end into a free network connecting socket of your local network (resp. into a free socket of a hub/switch). Alternatively, you can connect also a single PC.

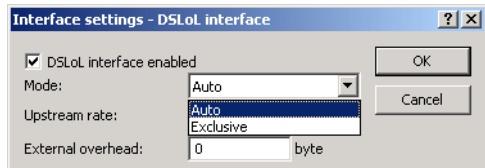
The LAN connector identifies automatically the transfer rate (10/100 Mbp) of the connected network device (autosensing).

For information about the installation of PoE see the info box 'Power-over-Ethernet – elegant power supply through the LAN wiring' → page 20.

- ③ **DSLol** – If you want to use your access point in DSLol mode, you can either connect the device directly to the DSL modem (exclusive mode) or to a hub resp. switch of the cable-bound LAN (automatic mode).

LAN interface: exclusive or in parallel for DSLol

There are two principle DSLol operation modes available. Either use the exclusive mode when connecting your LANCOM Access Point directly to a DSL modem, or use the automatic mode when connecting the Access Point to a hub or switch of a cable-bound LAN, and connect this hub/switch again to the DSL modem. If the Access Point is broadcasted as gateway via DHCP, computers in LAN and WLAN can use the internet connection **simultaneously** via one physical interface. Set the desired mode in LANconfig in the Interface settings of the DSLol interface.



DSLol supports all PPPoE-based Internet access lines, as well as those that are supplied with an access router with multiple fixed IP addresses (such as many SDSL business lines).

- For the exclusive mode insert the included network cable (green plugs) into the LAN connector of the device ③ or ④ and the other end into the corresponding interface of the DSL modem.
 - For the automatic mode for simultaneous operating with LAN and DSLol insert the included network cable (green plugs) into the LAN connector of the device ③ or ④ and the other end into a free network connecting socket of your local network (resp. into a free socket of a hub/switch).
- ④ Connect up the power supply – There are three options for supplying power to the device:
- Use the supplied power supply unit to provide the device with power via connector ⑨.



Use only the supplied power supply unit! The use of the wrong power supply unit can be of danger to the device or persons.

- For power supplied via the Ethernet cable (PoE), use the device's LAN connectors ③ or ④. Information about the installation of PoE can be

found in the information box 'Power-over-Ethernet – elegant power supply through the LAN wiring' → page 20



The PoE supply for the LANCOM XAP-40-2 is equipped for redundancy, i.e. both LAN interfaces can be supplied by separate PoE Injectors.

- Provide power to the device via one of the 24 V connectors **10**. Use the supplied 24 V plug (wiring described in the Appendix) or another suitable 24 V plug (Phoenix Contact, Combicon RM 3.81 mm).



The 24 V supply for the device is equipped for redundancy, i.e. both 24 V connectors can be supplied by separate power supplies.

Multiple power sources can be connected in any combination, which ensures that the power supply is redundant and fail safe. The device itself selects the power source to be used.

If a power outage causes a switch between power sources, the device reboots so that the power feed is reactivated, if appropriate.

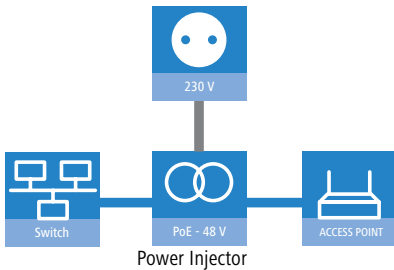
- ⑤ **Operational?** – After a short device self-test the Power LED will be permanently lit green resp. will blink alternately red and green as long as no configuration password has been given.

Power over Ethernet – the elegant power supply via LAN cabling

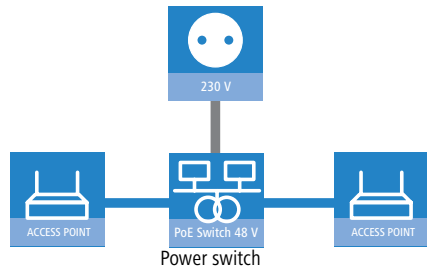
LANCOM Access Points are prepared for the PoE power supply (Power-over-Ethernet), corresponding to the 802.3af standard. PoE-enabled network devices can be comfortably supplied with power feeding through the LAN wiring. A separate external power supply for each base station is unnecessary, which reduces the installation complexity considerably.

The power feeding into the LAN happens at a central position, either via a PoE power injector, or via a so-called powerhub/powerswitch. For the LAN wiring is to note that all 8 wires must be available by the cabling. PoE feeds the power over those four wires, which are normally not used for data transfer.

Installation of single devices



Installation of several devices



The PoE supply works only in such network segments, in which exclusively PoE-capable devices are operating. The protection of network devices without PoE support is guaranteed by an intelligent mechanism, that tests the network segment for devices without PoE support before starting the PoE power feeding. The power is only switched onto the segment, if only devices with PoE support were detected.



In a PoE installation use exclusively devices which correspond to the 802.3af standard! For damages caused by inadmissible devices no warranty may be claimed.

For the LANCOM XAP-40-2, two LAN sockets can be used for redundant power supply. The device itself selects the power source to be used. If a power outage causes a switch between power sources, the device reboots so that the power feed is reactivated, if appropriate.

2.3.2 LANCOM IAP-54 Wireless

LEDs of LANCOM IAP-54 Wireless



1 Power

This LED indicates that the device is operational. After the device has been switched on, it will flash green for the duration of the self-test. After the self-test, either an error is output by a flashing red light code or the device starts and the LED remains lit green.

off		Device off
green	blinking	Self-test when powering up
green		Device ready for use
red/green	blinking alternately	Device insecure: configuration password not assigned
red	blinking	Time or connect-charge reached



The power LED flashes red/green in alternation until a configuration password has been specified. Without a configuration password, the configuration data of the LANCOM is insecure. Under normal circumstances, you would assign a configuration password during the basic configuration (instructions in the following chapter).

2 WLAN Link

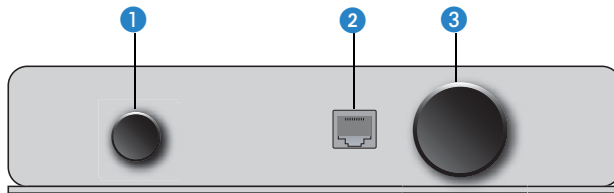
Gives information about the Wireless LAN access of the internal wireless network adapter of the base station.

The WLAN link display can assume three different conditions:

off		no Wireless LAN adapter found
green		Wireless LAN adapter ready for use
green	blinking	activity in the Wireless LAN (blink frequency indicates the number of registered stations)

Interfaces of LANCOM IAP-54 Wireless

With the LANCOM IAP-54 Wireless the access point's connectors are located on the base of the device:



- 1 Voltage connector for an external power supply (not included in delivery), protected by an IP50 sealing cap.
- 2 10/100Base-Tx for connection to the LAN. Supported are 10-Mbit or 100-Mbit connections. The data transfer speed is recognized automatically (autosensing).

The LANCOM IAP-54 Wireless LAN connector supports the Power-over-Ethernet standard (PoE). Further information about PoE is available in the info box 'Power-over-Ethernet – elegant power supply through the LAN wiring' → page 20.

By activated DSLoL option, the LAN connector can also be used for connecting the LANCOM Wireless Router to a broadband modem.

- 3 Connection for the serial configuration cable (not included in delivery) and access to the reset button, protected by an IP50 sealing cap (see "The reset button function").

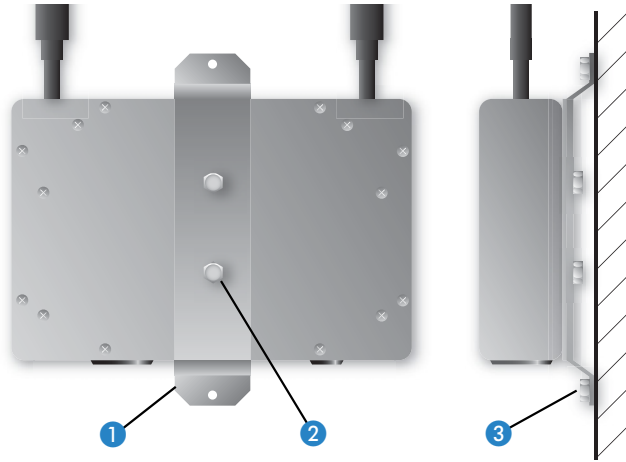
Wall mounting

- 1 Fit the wall-mounting bracket 1 with the help of the two M6 hexagonal screws 2 to the reverse side of the housing.

Chapter 2: Installation

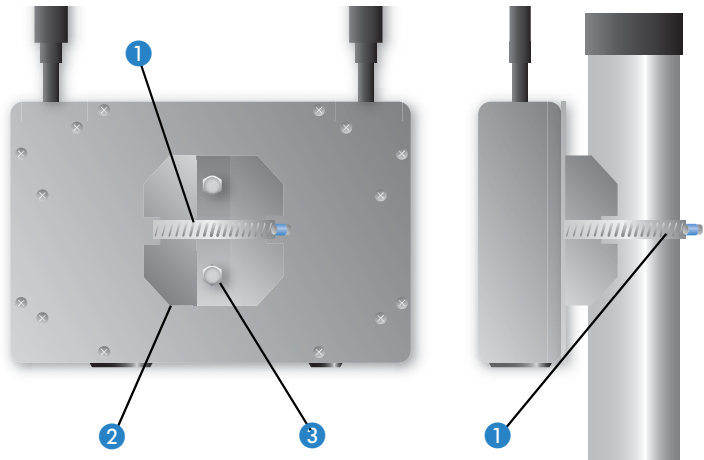
- ② Mount your LANCOM IAP-54 Wireless on the wall with suitable fixing screws/bolts ③ in the location. The wall-mounting screws are not supplied as standard.

Wall mounting

**Pole mounting**

- ① Place the hose clip ① that is best suited to the size of your pole around the pole-mounting bracket ②. Two hose clips for posts of differing diameter are supplied as standard.
- ② Fix the pole-mounting bracket ② with the two M6 hexagonal screws ③ to the reverse side of the housing.
- ③ Finally, mount your LANCOM IAP-54 Wireless with the hose clip ① in the position required on the post.

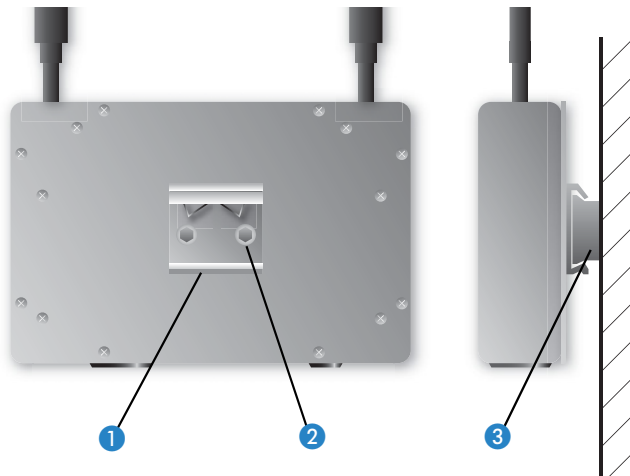
Pole mounting



Top-hat rail mounting

- ① Fix the bracket for top-hat rail mounting ① with the two M6 hexagonal screws ② to the reverse side of the housing.
- ② Now mount your LANCOM IAP-54 Wireless in the desired position on the top-hat rail ③.

Top-hat rail mounting



Connecting



When mounting the device, please observe the information on lightning protection in the LANCOM Outdoor Wireless Guide (download from www.lancom.eu). Mounting without adequate lightning protection could lead to serious damage to the access point and the network infrastructure connected to it.

- ① Plug the supplied network cable (green plug) into the LAN connector of the LANCOM IAP-54 Wireless and into the 'Data/Power Out' socket of the PoE Power Injector.
- ② Connect the 'Data In' connector on the PoE Power Injector with an available network socket of your local network (or a free socket of a hub or switch). The cable to connect the PoE Power Injector to the LAN is not supplied.



- If the PoE Power Injector is not connected to a switch or hub but directly to a computer's network connector, please be sure to use a suitable crossover cable.
- ③ Connect the PoE Power Injector to the power supply (as described in the manual supplied with the PoE Power Injector).
 - ④ After a brief self-test, the device illuminates the power LED on the LANCOM IAP-54 Wireless with a steady green, or blinks alternately in green and red if the configuration password has not been set.

Remove the sealing caps for the serial connector and reset button

The connector for the serial configuration cable and the reset button are recessed into the housing and are protected by two black plastic screws.

If necessary, undo the sealing screws carefully with a suitable screwdriver. After resetting or carrying out the configuration via the serial cable, you should seal the device again carefully with the sealing screws.

Information about the function of the reset button can be found under 'The reset button function'.

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.

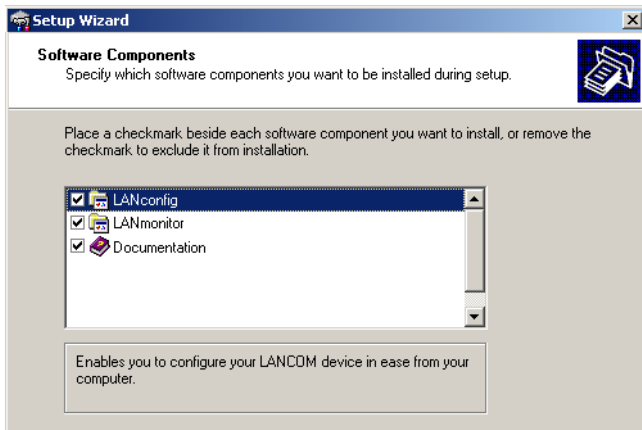
2.4.1 Starting Software Setup

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).
- With **Documentation** you copy the documentation files onto your PC.

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

3 Basic configuration

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



Unconfigured LANCOM Access Points with standard factory settings cannot be commissioned by means of the WLAN interface.

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

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

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

For LANCOM Access Points that are unconfigured and in their factory settings, the WLAN modules are switched off and set to the "Managed" operating mode. The WLAN modules search the LAN for a LANCOM WLAN Controller from which they can receive their WLAN-interface configuration profiles.

Once executed, the Basic Settings Wizard automatically resets the WLAN-module operating mode to "Access Point". The WLAN interface then has to be configured manually.



Only activate the Basic Settings Wizard if the Access Point is not to be configured from a WLAN-Controller. Subsequently execute the WLAN Wizard → WLAN Configuration.

3.1 What details are necessary?

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

- TCP/IP settings
- Protecting the configuration

- Wireless LAN details
- Security settings

3.1.1 TCP/IP settings

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

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

New LAN – fully automatic configuration possible

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

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

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

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

Should you still configure manually?

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

- Select automatic configuration if you are **not** familiar with networks and IP addresses.
- Select manual TCP/IP configuration if you are familiar with networks and IP addresses and one of the following statements is true:
 - You have not yet used any IP addresses in your network but would like to now; You would like to specify the IP address for the router yourself and would like to assign it a user-defined address from one of the

address ranges reserved for private use, for example '10.0.0.1' with a network mask of '255.255.255.0'. If you do this you simultaneously specify the address range that the DHCP server will subsequently use for the other devices in the network (provided the DHCP server is activated).

- You have so far also used IP addresses on the computers in the LAN.

Required information for manual TCP/IP configuration

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

■ DHCP mode of operation

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

■ IP address and network mask for the LANCOM

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

■ Gateway address

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

■ DNS server

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

3.1.2 Configuration protection

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



Multiple administrators can be set up in the configuration of the LANCOM, each with differing access rights. Up to 16 different administrators can be set up for a LANCOM. Further information can be

found in the LCOS reference manual under "Managing rights for different administrators".



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

3.1.3 Settings for the wireless LAN

Network name (SSID)

The Basic Settings Wizard prompts for the access point's network name (frequently referred to as SSID – **S**ervice **S**et **I**dentifier). The name is of your own choice. Several access points with the same name form a common wireless LAN.

Open or closed wireless LAN?

Mobile wireless devices select the desired wireless LAN by specifying the network name. Two methods serve to facilitate the specification of network name:

- Mobile wireless devices can search ("scan") the vicinity for wireless LANs and offer the wireless LANs they find in a list for selection.
- By using the network name 'ANY' the mobile wireless device registers with the nearest available wireless LAN.

The wireless LAN can be "closed" in order to prevent this procedure. In this case it will not accept any devices attempting to register with the network name 'ANY'.

Selecting a radio channel

The access point operates in a specific radio channel. The radio channel is selected from a list of up to 13 channels in the 2.4 frequency band or up to 19 channels in the 5 GHz frequency band (individual radio channels are blocked in some countries. Please refer to the appendix for more details).

The channel and frequency range used determine the operation if the common wireless standard, with the 5 GHz frequency range corresponding to the IEEE 802.11a/h standard and the 2.4 GHz frequency range determining operation in the IEEE 802.11g and IEEE 802.11b standards.

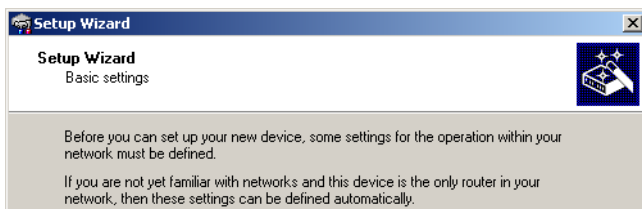
If no other access points are operating within the access point's range, any radio channel can be set. Otherwise the channels in the 2.4 GHz band must be selected in such a way that they do not overlap and are as far apart as possible. In the 5 GHz band the automatic setting, where the LANCOM Access Point uses TPC and DFS to select the best channel is normally sufficient.



Please refer to the LCOS reference manual for more information on TPC and DFS.

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 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 ⑤.


- ③ 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**.
- ④ Specify whether or not the router should act as a DHCP server. Make your selection and confirm with **Next**.

- ⑤ 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.

- ⑥ 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**.
- ⑦ 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**.
- ⑧ Connect charge protection can limit the cost of DSL connections to a pre-determined amount if desired. Confirm your choice with **Next**.
- ⑨ 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 device 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**.



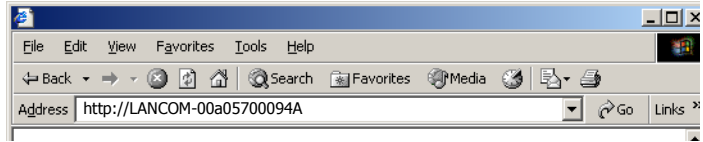
If the configuration PC does not obtain its IP address from the LANCOM DHCP server, figure out the current IP address of this PC (with **Start ▶ Execute ▶ cmd** and command **ipconfig** at the prompt under Windows 2000 or Windows XP, with **Start ▶ Execute ▶ cmd** and the command **winipcfg** at the 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-00a057xxxxx").



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:
 - 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 there:

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






(or with a name as described above)









If you cannot access an unconfigured device, 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:




Setup Wizards
Wizards enable you to handle frequent configuration jobs easily and quickly:

-  [Basic Settings](#)
-  [Security Settings](#)
-  [Set up Internet connection](#)
-  [Selection of Internet Provider](#)
-  [Assign Access Points to Profiles](#)


Device Configuration and Status
These menu options enable you to access the device's entire configuration:
Use the 'Configuration' for normal configuration jobs.
For experienced users, the expert configuration provides detailed access to all configuration options and the device status.

-  [Configuration](#)
-  [Expert Configuration](#)
-  [Save Configuration](#)
-  [Upload Configuration](#)
-  [Save Configuration Script](#)
-  [Execute Configuration Script](#)







File Handling

-  [Edit List of Allowed SSH Public Keys](#)
-  [Download Certificate or File](#)
-  [Upload Certificate or File](#)

Firmware Handling

-  [Perform a Firmware Upload](#)

Extras

-  [Show/Search Other Devices](#)
-  [Get Device SNMP MIB](#)
-  [Enable Software Option](#)
-  [Display Key Fingerprints](#)
-  [Change password](#)
-  [Create TCP/HTTP Tunnel](#)




The setup wizards are tailored precisely to the functionality of the specific LANCOM model. 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. Also set whether or not it is to operate as a DHCP server. Confirm your entry with **Apply**.

- 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).

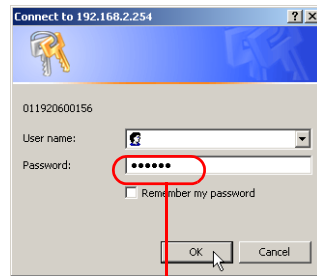
You may specify whether the device may only be configured from the local network or whether remote configuration via the WAN (i.e. a remote network) is also permissible.

-  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 pre-determined 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 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 (default)

In this operating mode the LANCOM 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 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 as a DNS server.

■ Manual IP address assignment

If the IP addresses in the network are assigned statically, then for each PC the IP address of the LANCOM 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, 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 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.



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

4.1 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

4.1.1 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.

4.1.2 Access control via MAC address

Each network device has a special identification number. This identification number is the so-called MAC address (**M**edia **A**ccess **C**ontrol), which is world-wide 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.

4.1.3 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.



Guest access with LEPS: LEPS can also be set up to allow access to guests. To this end, all users of the internal WLAN network are given individual passphrases. Guests can make use of their own dedicated SSID and a global passphrase. To avoid abuse, this global passphrase can be changed on a regular basis—every few days, for example.

4.1.4 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.

4.1.5 802.1x / EAP

The international industry standard IEEE 802.1x and the **Extensible Authentication Protocol (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.

4.1.6 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 have to upgrade the base stations of the with the LANCOM VPN option and the LANCOM Advanced VPN Client, which runs under the operating systems Windows Vista™, Windows 2000 and Windows XP. 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.

4.2 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.

4.3 The security settings wizard

Access to the configuration of a device permits not only to read out critical information (e.g. WEP key, 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.

4.3.1 Wizard for LANconfig

- 1 Mark your LANCOM 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 you can set the security settings for the WLAN. These include the name of the wireless network, the closed network function and the WEP encryption. You can type in the parameters for both wireless networks separately on devices with the option of a second WLAN interface.
- 6 Now you specify filter lists for stations (ACL) accessing the WLAN and protocols. Thereby, you restrict data exchange between the wireless network and the local network.
- 7 Now activate Stateful Inspection, ping-blocking and Stealth mode in the the firewall configuration.

- ⑧ The wizard will inform you when entries are complete. Complete the configuration with **Finish**.

4.3.2 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)
- security parameters as WLAN name, closed network function, WEP key, ACL list and protocol filters

4.4 The security checklist

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



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

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

With the help of 802.11i, WPA or WEP, you can encrypt the data in your wireless network with different encryption methods such as AES, TKIP or WEP. LANCOM Systems recommends the strongest possible encryption with 802.11i and AES. If the WLAN client adapters do not support these, then you should use TKIP or at least WEP. Make sure that the encryption function in your device is activated, and that at least one passphrase or WEP key has been entered and selected for application.

To check the WEP settings, open LANconfig, go to the configuration area and select 'WLAN security' on the '802.11i/WEP' tab to view the encryption settings for the logical and physical WLAN interfaces.

With the access control list (ACL) you can permit or prevent individual clients accessing your wireless LAN. The decision is based on the MAC

address that is permanently programmed into wireless network adapters. To check the access-control list, go to the configuration area in LANconfig and select 'WLAN security' on the 'Stations' tab.

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

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

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

■ **Have you permitted remote configuration?**

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

■ **Have you allowed configuration from the wireless LAN?**

If you do not need to configure the device from the wireless LAN, switch this function off. The field for disabling configuration from the wireless LAN is to be found in LANconfig in the 'Management' configuration area on the 'Admin' tab. Under 'Access rights – From the wireless LAN' select the option 'denied' for all methods of configuration.

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

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

■ **Have you activated the firewall?**

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

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

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

■ Have you activated IP masquerading?

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

■ Have you used filters to close critical ports?

The firewall filters in LANCOM devices offer filter functions for individual computers or entire networks. It is possible to set up source and destination filters for individual ports or port ranges. Furthermore, filters can be set for individual protocols or any combination of protocols (TCP/UDP/ICMP). It is especially convenient to set up the filters with the aid of LANconfig. Under 'Firewall/QoS', the 'Rules' tab contains the functions for defining and editing filter rules.

■ Have you excluded certain stations from accessing the device?

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

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

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

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

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

■ Have you activated the protection of your WAN access in case 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.

The scripting function can store the entire configuration in RAM only so that restarting the device will cause the configuration to be deleted. The configuration is not written to the non-volatile flash memory. A loss of power because the device has been relocated will cause the entire configuration to be deleted (for further information see the reference manual).

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

Some devices simply cannot be installed under lock and key. There is consequently a risk that the configuration will be deleted by mistake if a co-worker presses the reset button too long. The behavior of the reset button can be set so that a press is either ignored or it causes a re-start, depending on the time for which it is held pressed.

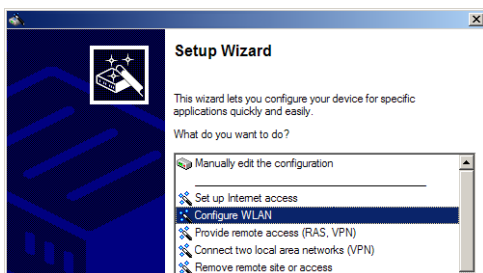
5 Advanced wireless LAN configuration

5.1 WLAN configuration with the wizards in LANconfig

Highly convenient installation wizards are available to help you with the configuration of LANCOM Access Points for your wireless LAN.

The settings include the general shared parameters and also the individual settings for one or more logical wireless LAN networks (WLAN radio cells or SSIDs).

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



- ② In the selection menu, select the Setup Wizard, **Configure WLAN interface** and confirm the selection with **Continue**.
- ③ Make the settings as requested by the wizard and as described as follows.

Country settings

Regulations for the operation of WLAN cards differ from country to country. The use of some radio channels is prohibited in certain countries. To operate the LANCOM Access Points while observing the regulations in various countries, all physical WLAN interfaces can be set up for the country where they are operated.

WLAN module operation

The WLAN modules can be operated in various operating modes:

- As a base station (Access Point mode), the device makes the link between WLAN clients and the cabled LAN. Parallel to this, point-to-point connections are possible as well.
- In Managed Mode the Access Points also accept WLAN clients into the network, although the clients then join a WLAN infrastructure that is con-

figured by a central WLAN-Controller. In this operating mode, no further WLAN configuration is necessary as all WLAN parameters are provided by the WLAN-Controller.

- In client mode, the device itself locates the connection to another Access Point and attempts to register with a wireless network. In this case the device serves, for example, to link a cabled network device to an Access Point over a wireless connection. In this operating mode, parallel point-to-point connections are **not** possible.

For further information please refer to section → Client Mode.

Physical WLAN settings

Along with the radio channels, the physical WLAN settings can also be used to activate options such as the bundeling of WLAN packets (TX Burst), hardware compression, or the use of QoS compliant with 802.11e. You also control the settings for the diversity behavior here.

Logical WLAN networks

Each WLAN module can support up to eight logical WLAN networks for mobile WLAN clients to register with. The following parameters have to be set when configuring a logical WLAN network:

- The network name (SSID)
- Open or closed radio LAN
- Encryption settings
- MAC filter
- Client-bridge operation
- Filter settings

Point-to-point settings

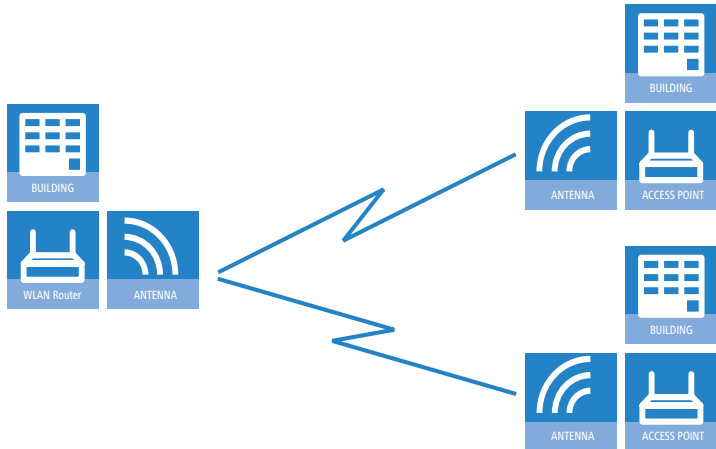
The configuration of P2P connections involves setting not only the operating mode but also the station name that the Access Point can connect to. Also, the role as "Master" or "Slave" is set here.

Along with the settings for the Access Point itself, also to be defined is the remote site that the Access Point can contact via the P2P connection.

For further information please refer to section → Point-to-point connections.

5.2 Point-to-point connections

LANCOM Access Points can serve not only as central stations in a wireless network, they can also operate in point-to-point mode to bridge longer distances. For example, they can provide a secure connection between two networks that are several kilometers apart — without direct cabling or expensive leased lines.

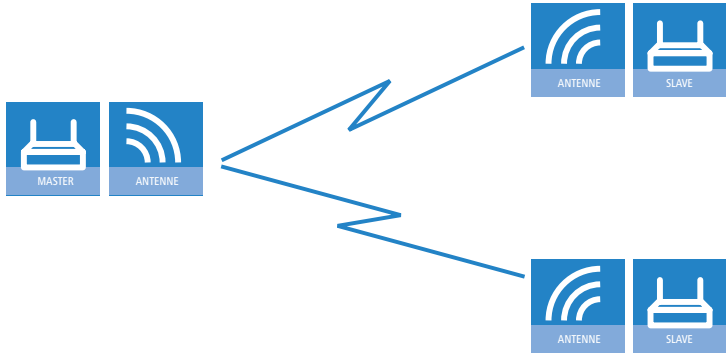


The behavior of an access point when exchanging data with other access points is defined in the "Point-to-point operation mode".

- **Off:** The access point only communicates with mobile clients
- **To:** The access point can communicate with other access points and with mobile clients
- **Exclusive:** The access point only communicates with other base stations

In the 5 -GHz band, the automatic search for vacant WLAN channels can lead to several simultaneous test transmissions from multiple access points, with the result that they do not find each other. This stalemate situation can be avoided with the appropriate "Channel selection scheme":

- **Master:** This access point takes over the leadership when selecting a free WLAN channel.
- **Slave:** All other access points will search for a channel until they have found a transmitting Master.



Thus it is recommended for the 5 GHz band that one central access point should be configured as 'Master' and all other point-to-point partners should be configured as 'Slave'. In the 2.4 GHz band, too, this setting simplifies the establishment of point-to-point connections if the automatic channel search is activated.



It is imperative that the channel selection scheme is configured correctly if the point-to-point connections are to be encrypted with 802.11i/WPA.

5.2.1 Geometric dimensioning of outdoor wireless network links

The following basic questions must be answered when designing wireless links:

- What antennas must be used for the desired application?
- How must the antennas be positioned to ensure a problem-free connection?
- What performance characteristics do the antennas need to ensure sufficient data throughput within the legal limits?

Selection of antennas using the LANCOM Antenna Calculator

You can use the LANCOM Antenna Calculator to calculate the output power of the access points as well as the achievable distances and data rates. The program can be downloaded from our website at www.lancom.eu.

After selecting your components (access points, antennas, lightning protection and cable) the calculator works out the data rates, ranges, and the antenna gain settings that have to be entered into the access point.



Please note that when using 5 GHz antennas additional technologies such as dynamic frequency selection (DFS) may be stipulated depending on the country of use. The operator of the wireless LAN system is responsible for ensuring that local regulations are met.

Antenna Distance Calculator

connecting your business

Point A

Accesspoint/Client Adapter: LANCOM IAP-54 Wireless

WLAN Module: WLANon OM20

Frequency Band: 802.11a (5 GHz)

Cable 1: AirLancom Cable N2-AP 5m

Surge Arrestor: Yes

Cable 2: O-5a Cable 3m

Antenna: AirLancom Extender O-5a

Point B

Accesspoint/Client Adapter: LANCOM IAP-54 Wireless

WLAN Module: WLANon OM20

Frequency Band: 802.11a (5 GHz)

Cable 1: AirLancom Cable N2-AP 5m

Surge Arrestor: Yes

Cable 2: O-5a Cable 3m

Antenna: AirLancom Extender O-5a

Distance (km) : 6.68

Mast Height [m] : 13.52

Data Rate (Mbps) : 6.0

10 dB "bad weather" Reserve: Yes

Data Rate to Distance

Data Rate (Mbps) | **Max. Distance (km)**

Data Rate (Mbps)	Max. Distance (km)
1.0	14.7
2.0	6.6
3.0	4.4
4.0	3.3
5.0	2.9
6.0	2.5
7.0	2.2
8.0	2.0
9.0	1.8
10.0	1.7
11.0	1.6
12.0	1.5
13.0	1.4
14.0	1.3
15.0	1.2
16.0	1.1
17.0	1.1
18.0	1.0
19.0	1.0
20.0	1.0

POINT A
Gain of Antenna System [dBS]

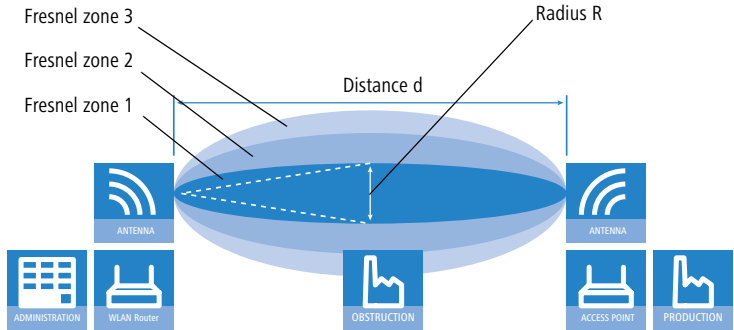
POINT B
Gain of Antenna System [dBS]

Calculated maximum distance between point A and B by using as maximum value antenna Point A & Point B in dBm (5GHz) respectively

Positioning the antennas

Antennas do not broadcast their signals linearly, but within an angle that depends on the model in question. The spherical expansion of the signal waves results in amplification of or interference to the effective power output

at certain intervals of the connection between the transmitter and receiver. The areas where the waves amplify or cancel themselves out are known as Fresnel zones.



The Fresnel zone 1 must remain free from obstruction in order to ensure that the maximum level of output from the transmitting antenna reaches the receiving antenna. Any obstructing element protruding into this zone will significantly impair the effective signal power. The object not only screens off a portion of the Fresnel zone, but the resulting reflections also lead to a significant reduction in signal reception.

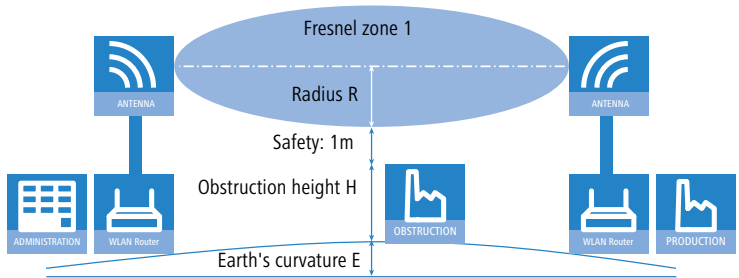
The radius (R) of Fresnel zone 1 is calculated with the following formula assuming that the signal wavelength (λ) and the distance between transmitter and receiver (d) are known.

$$R = 0.5 * \sqrt{\lambda * d}$$

The wavelength in the 2.4 GHz band is approx. 0.125 m, in the 5 GHz band approx. 0.05 m.

Example: With a separating distance of 4 km between the two antennae, the radius of Fresnel zone 1 in the 2.4-GHz band is **11 m**, in the 5-GHz band **7 m**.

To ensure that the Fresnel zone 1 remains unobstructed, the height of the antennas must exceed that of the highest obstruction by this radius. The full height of the antenna mast (M) should be as depicted:



$$M = R + 1\text{m} + H + E \text{ (earth's curvature)}$$

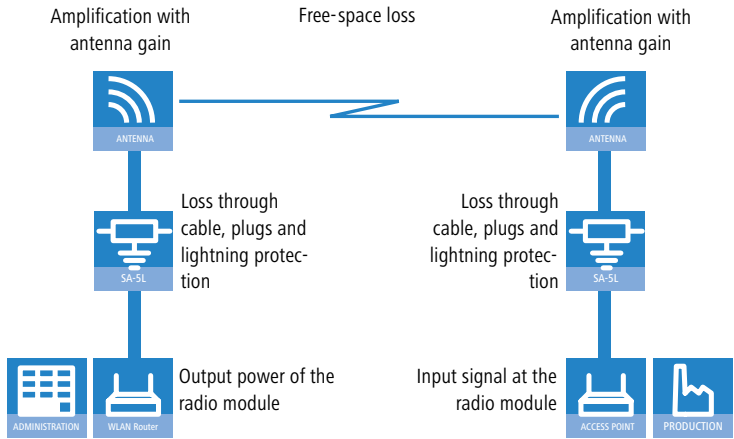
The allowance for the curvature of the earth (E) can be calculated at a distance (d) as $E = d^2 * 0.0147$ – i.e. at a distance of 8 km this is almost 1m

Example: With a distance of 8 km between the antennae, the result in the 2.4-GHz band is a mast height above the level of the highest obstruction of approx. **13 m**, in the 5-GHz band **9 m**.

Antenna power

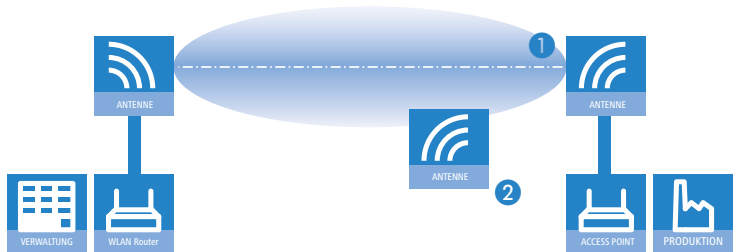
The power of the antennas must be high enough to ensure acceptable data transfer rates. On the other hand, the country-specific legal regulations regarding maximum transmission power should not be exceeded.

The calculation of effective power considers everything from the radio module in the transmitting access point to the radio module in the receiving access point. In between there are attenuating elements such as the cable, plug connections or simply the air transmitting the signals and amplifying elements such as the external antennas.



5.2.2 Antenna alignment for P2P operations

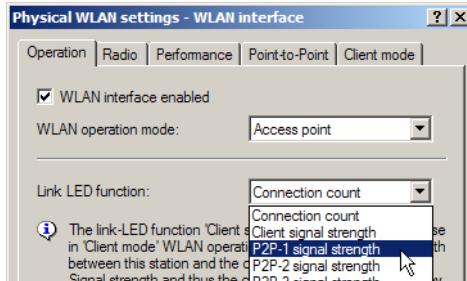
The precise alignment of the antennas is of considerable importance in establishing P2P connections. The more central the receiving antenna is located in the "ideal line" of the transmitting antenna, the better are the actual performance and the effective bandwidth **1**. If the receiving antenna is outside of this ideal area, however, significant losses in performance will be the result **2**.



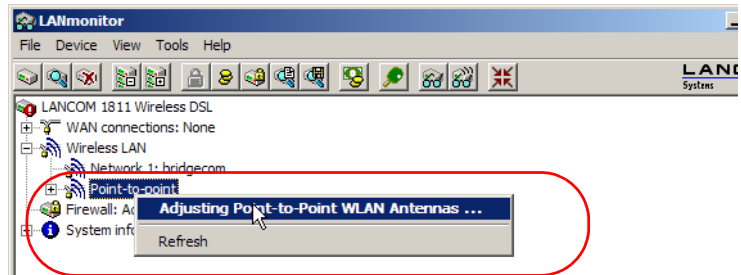
i You can find further information on the geometrical design of wireless paths and the alignment of antennas with the help of LANCOM software in the LCOSreference manual.

The current signal quality over a P2P connection can be displayed on the device's LEDs or in the LANmonitor in order to help find the best possible alignment for the antennas.

The display of signal quality on the LEDs must be activated for the wireless LAN interface (LANconfig: **Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Operation**). The faster the LED blinks the better the connection (a blinking frequency of 1 Hz represents a signal quality of 10 dB, double the frequency indicates that the signal strength is twice as high).



In LANmonitor the connection quality display is opened with the context menu. Right-clicking with the mouse on 'Point-to-point' activates the option 'Adjusting Point-to-Point WLAN Antennas...'



i The 'Point-to-point' entry is only visible in the LANmonitor if the monitored device has at least one base station defined as a remote station for a P2P connection (LANconfig: **Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Point-to-Point**).

In the dialog for setting up point-to-point connections, LANmonitor prompts for the information required to establish the P2P connection:

- Is the P2P connection configured at both ends (remote base station defined with MAC address or station name)?
- Is the point-to-point mode of operation activated?
- Which access point is to be monitored? All of the base stations defined as P2P remote stations in the device concerned can be selected here.

Chapter 5: Advanced wireless LAN configuration

- Are both antennas approximately aligned? The basic P2P connection has to be working before fine-tuning can be performed with the aid of LANmonitor.

Once signal monitoring has commenced, the P2P dialog displays the absolute values for the current signal strength and the maximum value since starting the measurement. The development of the signal strength over time and the maximum value are displayed in a diagram, too.



Initially only one of the two antennas should be adjusted until a maximum value is achieved. This first antenna is then fixed and the second antenna is then adjusted to attain the best signal quality.

5.3 Configuration of P2P connections

In the configuration of point-to-point connections, entries have to be made for the point-to-point operation mode, the channel selection scheme and the MAC addresses of the remote sites.

Configuration with LANconfig


For configuration with LANconfig you will find the settings for P2P connections under the configuration area 'Interfaces' on the 'Wireless LAN' tab.

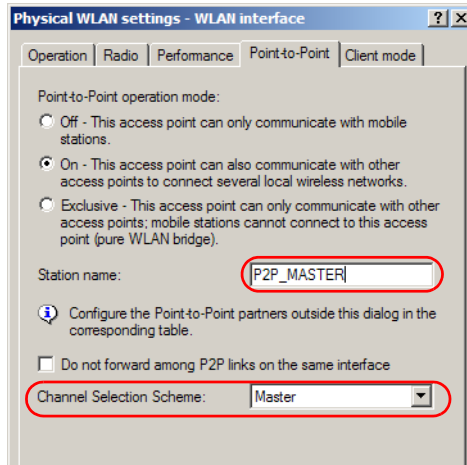


The configuration of the P2P connections can also be carried out with the WLAN Wizards in LANconfig.

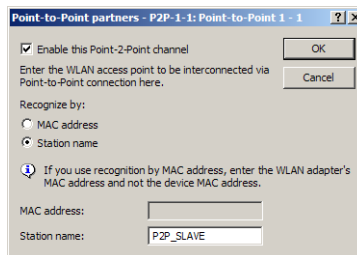
- Click on the button **Physical WLAN settings** to open the corresponding WLAN interface and select the tab for 'Point-to-Point'.
- Activate the suitable point-to-point operation mode here and set the channel selection scheme to either 'Master' or 'Slave'. If the peers of the


P2P connections are to be identified via their station names, then enter a unique name for this WLAN station.

-  For models with multiple WLAN modules, the station name can be entered separately for each physical WLAN interface.



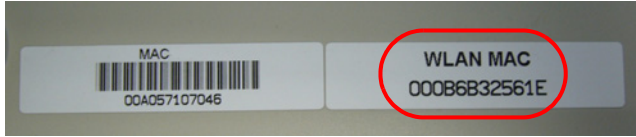
- ③ Close the physical WLAN settings and open the list of **Point-to-point partners**. For each of the maximum of six P2P connections, enter either the MAC address of the WLAN card at the remote station or enter the WLAN station's name (depending on the chosen method of identification).



-  Please observe that only the MAC addresses of the WLAN cards at the other end of the connections are to be entered here! Not the access point's own MAC address, and not the MAC addresses from any other interfaces that may be present in the access points.

Chapter 5: Advanced wireless LAN configuration

You will find the WLAN MAC address on a sticker located under each of the antenna connectors. Only use the string that is marked as the "WLAN MAC" or "MAC-ID". The other addresses that may be found are not the WLAN MAC address but the LAN MAC address.



Alternatively you will find the MAC addresses for the WLAN cards in the devices under WEBconfig, Telnet or a terminal program under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Status ▶ WLAN-statistics ▶ Interface-statistics
Terminal/Telnet	Status/WLAN-statistics/Interface-statistics

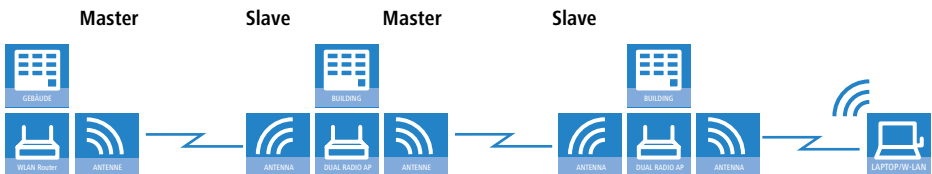
Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you can set the settings for the point-to-point connections under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ Interfaces ▶ WLAN-Interfaces ▶ Interpoint-Settings
Terminal/Telnet	cd /Setup/Interfaces/WLAN-Interfaces/Interpoint-Settings

5.3.1 Access points in relay mode

Access points equipped with two wireless modules can be used to establish wireless bridges across multiple stations. Each wireless module is configured as a 'Master' and then 'Slave' in turn.





The use of relay stations each equipped with two WLAN modules simultaneously solves the problem of the "hidden station", by which the MAC addresses of the WLAN clients are not transferred over multiple stations.

5.3.2 Security for point-to-point connections

IEEE 802.11i can be used to attain a significant increase in the security of WLAN point-to-point connections. All of the advantages of 802.11i such as the simple configuration and the powerful encryption with AES are thus available for P2P mode, as are the improved security of the passphrase from the LANCOM Enhance Passphrase Security (LEPS).

Encryption with 802.11i/WPA

To activate the 802.11i encryption for a correctly configured P2P connection, adjust the settings for the first logical WLAN network in the appropriate WLAN interface (i.e. WLAN-1 if you are using the first WLAN card for the P2P connection, WLAN-2 if you are using the second card, e.g. as with an access point with two WLAN modules).

- Activate the 802.11i encryption.
- Select the method '802.11i (WPA)-PSK'.
- Enter the passphrase to be used.



The passphrases should consist of a random string of at least 22 characters long, corresponding to a cryptographic strength of 128 bits.

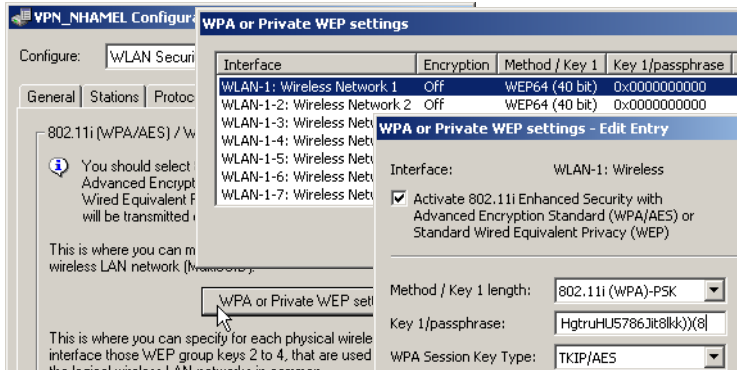
When set as P2P Master, the passphrase entered here will be used to check the Slave's authorization to access. When set as P2P Slave, the access point transfers this information to register with the remote site.

For configuration with LANconfig you will find the encryption settings under the configuration area 'Wireless LAN' on the '802.11i/WEP' tab.

Configuration with
LANconfig

Chapter 5: Advanced wireless LAN configuration

EN



Configuration with WEBconfig or Telnet

The encryption settings for the individual logical WLAN networks can be found under WEBconfig or Telnet under the following paths:

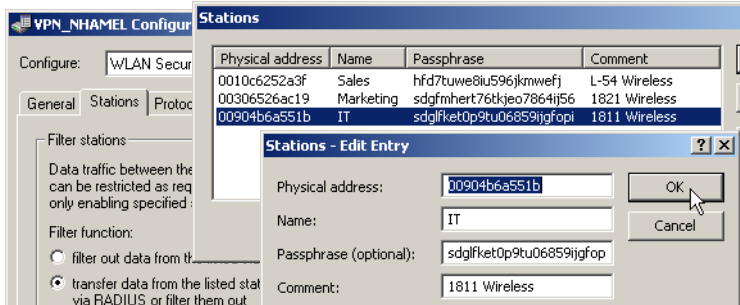
Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ Interfaces ▶ WLAN-Interfaces ▶ Encryption-Settings
Terminal/Telnet	/Setup/Interfaces/WLAN-Interfaces/Encryption-Settings

LEPS for P2P connections

A further gain in security can be attained by additionally using LANCOM Enhanced Passphrase Security (LEPS) which involves the matching of MAC address and passphrase.

LEPS can be used to secure single point-to-point (P2P) connections 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 secure.

When using LANconfig for the configuration, you enter the passphrases of the stations approved for the WLAN in the configuration area 'Wireless LAN' on the 'Stations' tab under the button **Stations**.



Configuration with
WEBconfig or Telnet

The access list for the matching of MAC addresses to the passphrases (LEPS) can be found under WEBconfig or Telnet under the following paths:

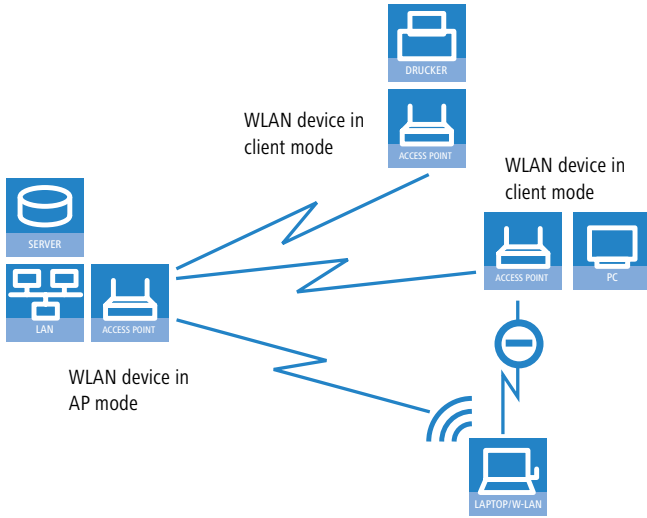
Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ WLAN-module ▶ Access-list
Terminal/Telnet	Setup/WLAN-module/Access-list

5.4 Client mode

To connect individual devices with an Ethernet interface into a wireless LAN, LANCOM devices with a WLAN module can be switched to "client mode", whereupon they act as conventional wireless LAN adapters and not as access points (AP). The use of client mode therefore allows devices fitted with only an Ethernet interface, such as PCs and printers, to be integrated into a wireless LAN.

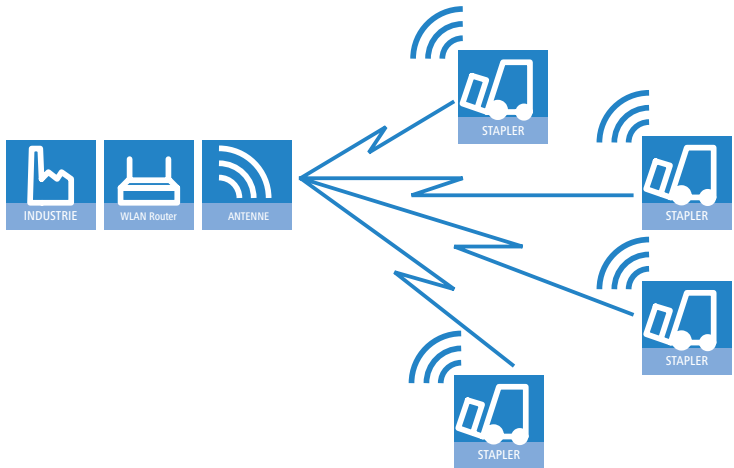
■ Chapter 5: Advanced wireless LAN configuration

EN



i Multiple WLAN clients can register with a WLAN device in AP mode, which is not the case for a WLAN device in client mode.

In industrial applications mobile WLAN clients can also be deployed, such as on a forklift truck, which then has permanent contact to the controller over the wireless connection.

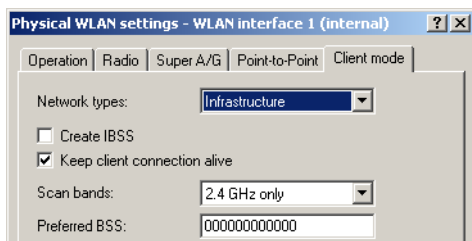


5.4.1 Client settings

For LANCOM Access Points and LANCOM Wireless Routers in client mode, further settings/client behavior can be configured from the 'Client mode' tab under the settings for the physical interfaces.



The configuration of the client settings can also be carried out with the WLAN Wizards in LANconfig.



- ① To edit the settings for client mode in LANconfig, go to the 'Client mode' tab under the physical WLAN settings for the desired WLAN interface.
- ② In 'Scan bands', define whether the client station scans just the 2.4 GHz, just the 5 GHz, or all of the available bands to locate an access point.

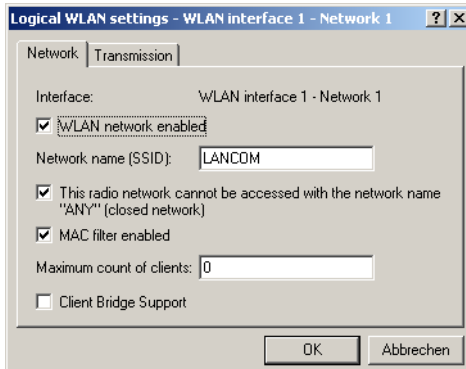
Under WEBconfig or Telnet the settings for client mode can be found under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ► Setup ► Interfaces ► WLAN ► Client modes
Terminal/Telnet	Setup/Interfaces/WLAN/ Client modes

5.4.2 Set the SSID of the available networks

In the WLAN clients, the SSIDs of the networks to which the client stations are to connect must be entered.

- ① To enter the SSIDs, change to the 'General' tab under LANconfig in the 'Wireless LAN' configuration area. In the 'Interfaces' section, select the **first** WLAN interface from the list of logical WLAN settings.



- ② Enable the WLAN network and enter the SSID of the network the client station should log onto.

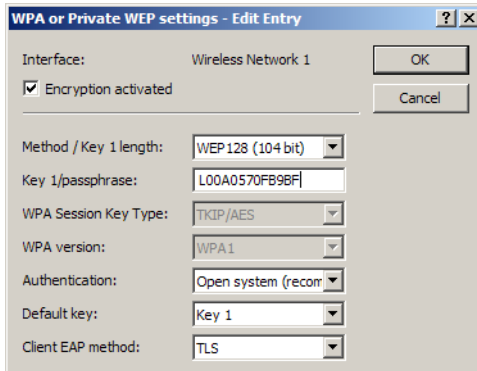
Under WEBconfig or Telnet the network settings for the logical WLAN interfaces can be found under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ► Setup ► Interfaces ► WLAN ► Network
Terminal/Telnet	Setup/Interfaces/WLAN/ Network settings

5.4.3 Encryption settings

For access to a WLAN, the appropriate encryption methods and key must be set in the client station.

- ① To enter the key, change to the '802.11i/WEP' tab under LANconfig in the 'Wireless LAN' configuration area. From 'WPA / private WEP settings', select the **first** WLAN interface from the list of logical WLAN settings.



- ② Enable encryption and match the encryption method to the settings for the access point.
- ③ In WLAN client operating mode, the LANCOM Access Points and LANCOM Wireless Routers can authenticate themselves to another access point using EAP/802.1X. For this, select the desired client EAP method here. Note that the selected client EAP method must match the settings of the access point that the device is attempting to log onto.

ⓘ Depending on the EAP method, the appropriate certificates must be stored in the device.

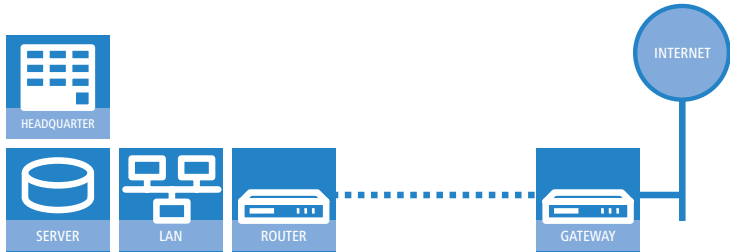
- For TTLS and PEAP - the EAP/TLS root certificate only; the key is entered as a combination username:password.
- For TLS in addition; the EAP/TLS device certificate including the private key.

Under WEBconfig or Telnet the network settings for the logical WLAN interfaces can be found under the following paths:

Configuration tool	Call
WEBconfig, Telnet	Expert configuration > Setup > Interfaces > WLAN > Encryption > WLAN 1

6 Setting up Internet access

The LANCOM provides a central point of Internet access for all of the computers in the LAN. The connection to the Internet provider can be established via the WAN connection which is connected to an ADSL or cable modem. For models not equipped with a WAN connector, a LAN interface is configured as a DSLoL connector and is connected to a compatible ADSL modem.



Does the Setup Wizard know your Internet provider?

The Wizard is preset with access data for the principal Internet providers in your country and offers you a selection list. If you find your Internet provider in this list, then you generally do not have to enter any additional parameters to set up your Internet access. All that is required is the authentication data as supplied to you by your Internet provider.

Internet provider unknown

If the list in the Setup Wizard does not contain your provider, you will be asked step-by-step for all of the necessary data. This access data will have been supplied to you by your Internet provider.

Other connection options

In addition you can use the Wizard to activate or deactivate additional options (if supported by your Internet provider):

- Billing by time or flatrate – select the method by which you are billed by your Internet provider.
 - In case of billing by time, you can set the LANCOM to cut connections automatically if no data flows for a certain time (the hold time).
You can also set up line polling that detects inactive remote stations very quickly and, in such cases, can close the connection before the hold time expires.

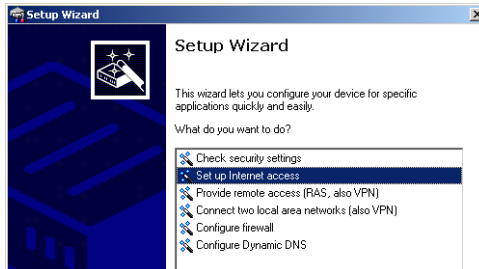
- In case of flatrate billing you can also set up line polling to monitor the function of the remote station.

Apart from that you can opt to keep flatrate connections permanently active ("keep-alive"). In case a connection should fail, it is re-established automatically.

6.1 The Internet Connection Wizard

6.1.1 Instructions for LANconfig

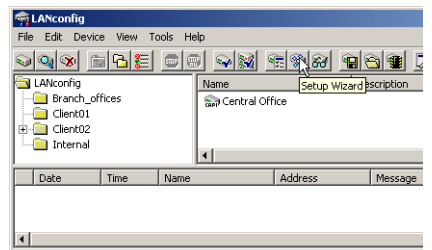
- ① Mark your device in the selection window. From the command line, select **Extras ▶ Setup Wizard**.



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

LANconfig: Fast activation of the Setup Wizards

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



6.1.2 Instructions for WEBconfig

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

6.2 The Firewall Wizard

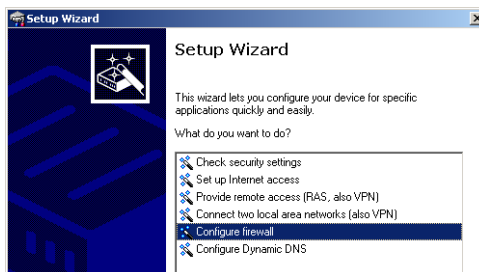
Your LANCOM features a stateful inspection firewall and firewall filter that provides effective protection from the Internet for your WLAN. The core concept of the stateful inspection firewall is that the only data transfers that are considered to be valid are those implemented by the protected device itself. All access attempts that were not requested from within the local network are invalid.

The Firewall Wizard assists you to generate new rules for the firewall quickly and conveniently.

More information on your LANCOM's firewall and its configuration are available in the reference manual.

6.2.1 LANconfig Wizard

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



- ② In the selection menu, select the Setup Wizard, **Configure firewall** and confirm the selection with **Continue**.

- ③ In the windows that follow you select the services/protocols that the rule is to relate to. In the next step you define the source and destination stations that the rule applies to, and the actions that are to be carried out by the rule on a data packet.
- ④ Finally the new rule is given a name, it is activated, and you define whether further rules are to be considered when the rule acts on a data packet.
- ⑤ The wizard will inform you as soon as the entries are complete. Close the configuration with **Finish**.

6.2.2 Configuration under WEBconfig

WEBconfig provides the option of checking and altering the parameters for Internet access under **Configuration ► Firewall / QoS ► Rules ► Rule table**.

7 Options and accessories

Your LANCOM device has numerous extensibilities and the possibility to use a broad choice of LANCOM accessories. You find in this chapter information about the available accessories and how to use them with your base station.

- The range of the base station can be increased by optional antennas of the AirLancer series and can be adapted to special conditions of environs.
- With the LANCOM Public Spot Option option it is possible to extend the LANCOM for additional billing and accounting functions in order to upgrade it to a Wireless Public Spot.

7.1 Optional LANCOM WLAN antennas

To increase the range of the LANCOM base station or to adapt the base station to special conditions of environs, you can connect LANCOM WLAN antennas at the base station. An overview of suitable antennas can be found on the LANCOM web site under www.lancom.eu.



For help with calculating the correct antenna setup for external LANCOM AirLancer Extender antennas or for antennas of other vendors, please refer to www.lancom.eu



When installing external antennas, ensure that you observe the statutory limitations of the country in which the WLAN device is being operated. To help with this, you can enter the transmitting power minus the cable loss into the LANCOM configuration. These data enable LCOS to automatically calculate the correct transmitting power for the selected country.



The employment of the AirLancer Extender SA-5L for internal lightning protection is **essential under all circumstances**—the AirLancer Extender SA-5L is always mounted between the Access Point and the antenna, preferably as near as possible to the antenna.



Antennas are only to be attached or changed when the device is switched off. Mounting or demounting antennas while the device switched on may cause the destruction of the WLAN module!

7.1.1 Antenna Diversity

LANCOM IAP-54
Wireless only

The transmission of radio signals can suffer from significant signal losses because of reflection and scatter, among other reasons. In some areas, the interaction with the reflected radio waves can cause a drop in signal strength, or even cause it to be cancelled out completely.

Transmission quality can be improved with so-called "diversity" methods. The principle of diversity methods relies on the fact that a transmitted signal is often received multiple times (generally twice). With appropriate processing, these signals can be re-combined into a single signal. The most common methods are space diversity and polarization diversity.

LANCOM Systems supplies a variety of polarization-diversity antennas as accessories for LANCOM Access Points and LANCOM Wireless Routers. These models enable two orthogonally polarized signals to be received with a single antenna. Further information about this technique is available in our "Polarization Diversity" techpaper.

7.1.2 Installation of AirLancer Extender antennas

Polarization diversity antennas from LANCOM Systems:

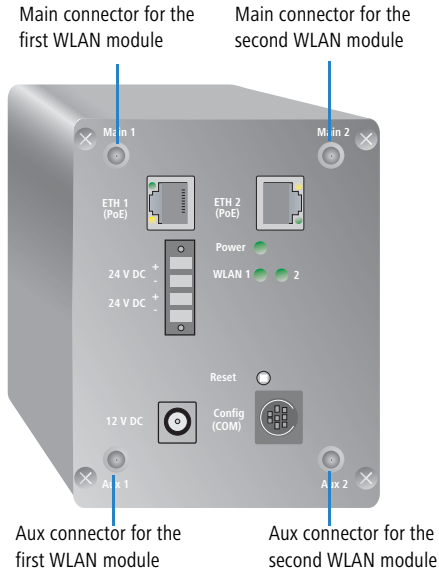
- AirLancer Extender O-D80g (2.4 GHz band), item no. 61221
- AirLancer Extender O-D60a (5 GHz band), item no. 61222
- AirLancer Extender O-D9a (5 GHz), item no. 61224



Before mounting external antennas, please observe the information on lightning protection in the LANCOM Outdoor Wireless Guide (available as a download from www.lancom.eu). Mounting antennas without adequate lightning protection could lead to serious damage to the access point and the network infrastructure connected to it.

LANCOM XAP-40-2
and LANCOM XAC-
40-1 only

To install the optional AirLancer Extender antenna, switch the LANCOM Wireless Router off by deactivating its power supply (via 12 V power-supply unit, 24 V interface or PoE). Then carefully unscrew the existing antenna and the terminators, if applicable. Connect the AirLancer Extender antenna to the appropriate 'Antenna Main' connector.



Relay operation requires the connection of AirLancer Extender antennas to the first and to the second WLAN modules.

Additionally, you can use the "Tx diversity" function with the LANCOM XAP-40-2 via the Aux connector of the appropriate WLAN module. Refer to the LCOS reference manual for further information.



The AirLancer Extender O-D60a and O-D80g are polarization diversity antennas that are equipped with two internal antennas that polarize the radio signals with a 90° offset. In the case of coverage in a warehouse or a production site, for example, the result is an improvement in signal quality of at least 3 dB. Improved connections with higher data rates become possible.

7.2 LANCOM Public Spot Option

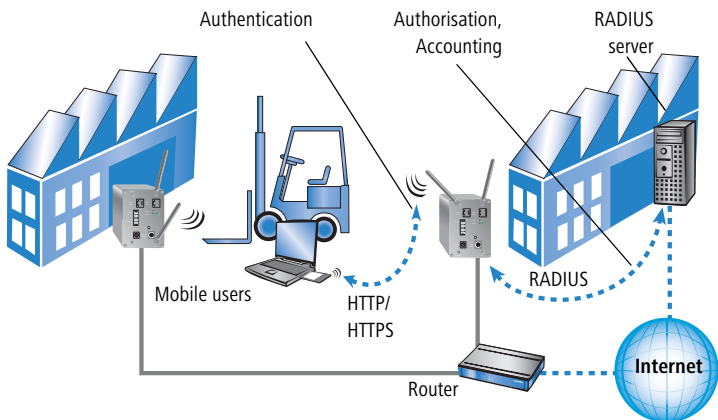
Wireless public spots are publicly accessible points, at which users with their own mobile computers can dial wirelessly into a network, usually into the Internet.



Please note that the operation of a LANCOM with LANCOM Public Spot Option (sometimes referred as HotSpot) is possibly subject to certain legal regulations. Please inform yourself concerning relevant regulations before installing a LANCOM. Further information to this topic can be found in our whitepaper „Public Spots - Operators' rights and obligations“, available as download from www.lancom.eu.

EN

The LANCOM Public Spot Option is ideal for use to authenticate staff who need access to a certain machine or network, for example. Access rights are controlled by a central server (e.g. in the production department). Staff members then have to register anew each time they wish to use a certain IP address range.



With the LANCOM Public Spot Option you extend a base station additionally with these functions and upgrade it to a Wireless Public Spot.

8 Troubleshooting

In this chapter, you will find suggestions and assistance for a few common difficulties.

8.1 No DSL connection is established

After start-up the router automatically attempts to connect to the DSL provider. During this process, the LAN-link LED will blink green. If successful, the LED will switch over to steady green. If, however, the connection can't be established, the LAN-link LED will light up red. The reason for this is usually one of the following:

Problems with the cabling?

Only the cable provided with your device should be used to connect to DSL. This cable must be connected to the Ethernet port of your broadband access device. The LAN link LED must light green indicating the physical connection.

Has the correct transfer protocol been selected?

The transfer protocol is set along with the basic settings. The basic setup wizard will enter the correct settings for numerous DSL providers automatically. Only if your DSL provider is not listed, you will have to enter manually the protocol being used. In any case, the protocol that your DSL provider supplies you with should definitely work.

You can monitor and correct the protocol settings under:

Configuration tool	Run command
LANconfig	Management ► Interfaces ► Interface settings ► WAN Interface
WEBconfig	Expert Configuration ► Setup ► Interfaces ► WAN Interface

8.2 DSL data transfer is slow

The data transfer rate of an broadband (Internet) DSL connection is dependent upon numerous factors, most of which are outside of one's own sphere of influence. Important factors aside from the bandwidth of one's own Internet connection are the Internet connection and current load of the desired target. Numerous other factors involving the Internet itself can also influence the transfer rate.

Increasing the TCP/IP window size under Windows

If the actual transfer rate of a DSL connection is significantly below the fastest rate listed by the provider, there are only a few possible causes (apart from the above-mentioned external factors) which may involve one's own equipment.

One common problem occurs when large amounts of data are sent and received simultaneously with a Windows PC using an asynchronous connection. This can cause a severe decrease in download speed. The cause of this problem is what is known as the TCP/IP receive window size of the Windows operating system that is set to a value too small for asynchronous connections.

Instructions on how to increase the Windows size can be found in the Knowledge Base of the support section of the LANCOM web site (www.lancom.eu).

8.3 Unwanted connections under Windows XP

Windows XP computers attempt to compare their clocks with a timeserver on the Internet at start-up. This is why when a Windows XP in the WLAN is started, a connection to the Internet is established by the LANCOM.

To resolve this issue, you can turn off the automatic time synchronization on the Windows XP computers under **Right mouse click on the time of day ► Properties ► Internet time**.

9 Appendix

9.1 Performance data and specifications

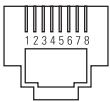
		LANCOM IAP-54 Wireless	LANCOM XAP-40-2	LANCOM XAC-40-1
Frequency band		2400 - 2483,5 MHz (ISM) or 5150 - 5750 MHz	Two WLAN modules with 2400 - 2483,5 MHz (ISM) or 5150 - 5750 MHz each	2400 - 2483,5 MHz (ISM) or 5150 - 5750 MHz
Connections	LAN	10/100Base-TX, Auto-sensing, Auto Node-Hub	2x 10/100Base-TX, Auto-sensing, Auto Node-Hub	10/100Base-TX, Auto-sensing, Auto Node-Hub
	WAN	Utilisation of one LAN connection for simultaneous DSL-over-LAN (DSLolL).		
	WLAN1	2x reverse SMA connectors with antenna diversity		
	WLAN2		2x reverse SMA connectors with antenna diversity	
Power supply		Via Power over Ethernet only, using included PoE injector.	<ul style="list-style-type: none"> ■ 12V DC over external power adapter ■ 2x Power-over-Ethernet as per IEEE 802.3af (redundant) ■ 2x 24 V DC with 4-pin plug (Phoenix Contact, Combicon RM 3,81mm) (redundant) 	<ul style="list-style-type: none"> ■ 12V DC over external power adapter ■ Power-over-Ethernet as per IEEE 802.3af (redundant) ■ 2x 24 V DC with 4-pin plug (Phoenix Contact, Combicon RM 3,81mm) (redundant)
Antennas		Two dualband dipole antennas supplied. Please respect the restrictions given in your country when setting up an antenna system. For information about calculating the correct antenna setup, please refer to www.lancom.com .		
Housing		IP50 protected housing, 225 mm x 145 mm x 45 mm (BxHxT), robust metal housing, ready for wall, mast and top hat rail mounting.	IP40 protected housing, ca. 8 x 12 x 13 cm (W x H x D), robust metal housing, ready for wall and top hat rail mounting.	IP40 protected housing, ca. 8 x 12 x 13 cm (W x H x D), robust metal housing, ready for wall and top hat rail mounting.
Approvals		The device is compliant to the following approvals: EN 300328, EN 301893, EN 301489-1, EN 301489-17, EN 61000-6-2, EN 60950		
Regulations		Notified in Germany, Belgium, Netherlands, Luxembourg, Austria, Switzerland, United Kingdom, Italy, France, Czechia, Denmark, Spain		

LANCOM IAP-54 Wireless		LANCOM XAP-40-2	LANCOM XAC-40-1
Environment/Temperature		Temperature range 0 °C to +50 °C at 95 % max. humidity (non condensing)	Temperature range –20 °C to +50 °C at 95 % max. humidity (non condensing)
Service		Warranty: 3 years	
Support		Via hotline and Internet	

9.2 Contact assignment


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

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

Numerics

10/100Base-TX	27
100-Mbit network	27
802.11i	11, 44, 45, 46, 49
802.1x	11, 44, 46
802.3af- standard	25

A

Access point mode	9, 15
ACL	45
Anschlussbelegung	
Konfigurationsschnittstelle	84
Antenna	
Outdoor	76
Antenna Calculator	56
Antenna power	59
Autosensing	19, 22, 27

C

charge lock	17
Client mode	67, 69
Closed network	11
Configuration access	38, 42
Configuration cable	27, 30
Configuration file	52
Configuration password	50
Configuration port	19
Configuration protection	35
Connect charge protection	38, 42
Contact assignment	83
DSL interface	83
LAN interface	83
Outband	84

D

Default gateway	43, 51
DFS	57
DHCP	12, 43
DHCP server	34, 37, 41, 43

DNS	12
DNS server	10, 11, 43
Documentation	14
Download	5
DSL	
provider	38, 42
transfer protocol	42

DSL connection	
problems establishing the connection	80
DSL transfer protocol	38
DSLolL	19, 23, 27
Dynamic Frequency Selection	57
Dynamic frequency selection	57

E

EAP	11, 44, 46
Encryption methods	70

F

Firewall	10, 12, 51
Block stations	51
Firewall filters	74
FirmSafe	12
Firmware	5
Flatrate	72
Fresnel zone	58

I

ICMP	51
Information symbols	5
Installation	14
LAN	22
LANtools	31
Power supply unit	23
Internet access	10, 72
Authentication data	72
Flatrate	72
Internet access setup	72

■ Index

Internet provider	72	Public Spot Option	79
IP		Q	
Block ports	51	QoS	12
Filter	51	Quality of Service	12
IP address	34, 35, 51	R	
IP masquerading	12, 51	RADIUS	11
L		Relay function	10
LAN connector	27	Remote configuration	38, 42
LANCOM Enhanced Passphrase Security	44	Reset connect charge protection.	17
LANCOM setup	31	Routing table	51
LANconfig	32, 37	S	
Starting the Wizards	73	Security	
LANmonitor	32	Wireless LAN	44
LANtools		Security checklist	49
System requirements	15	self-sufficient	9, 15
LEPS	11, 45	Serial configuration cable	27, 30
Loader	15	SNMP	
M		Configuration protection	50
MAC address filter	11	Software installation	31
Managed mode	9, 15	SSID	36, 38, 42, 69
Multi SSID	11	Stateful Inspection Firewall	10
N		Stateful-inspection firewall	74
NAT – see IP masquerading		Status displays	
Netmask	34, 51	Power	17
Network mask	35	Statusanzeigen	
O		Power	16, 26
Optional antennas	76	Wireless Link	17, 26
Options and accessories	76	Super AG	11
P		Support	5
P2P	45	System requirements	15
Password	35, 38	T	
PAT – see IP masquerading		TCP	51
Point-to-Point	45	TCP/IP	15
Point-to-point	55	Settings	34, 37, 41
point-to-point	10	Settings to PCs in the LAN	43
Power adapter	19	Windows size	81
Power-over-Ethernet	25	TCP/IP configuration	
		Automatic	41

Fully automatic	34	W	
Manual	34, 35	WEBconfig	38
TCP/IP filter	12, 51	password	42
Technische Daten	82	System requirements	15
Telnet	51	WEP	11, 49
TFTP	51	Wireless LANs	
Transfer protocol	80	Operating modes	9
Turbo Mode	11	WLAN	
U		Bands scanned	69
UDP	51	Client mode	69
		WPA	11, 44, 45, 46, 49