



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

LANCOM OAP-54-1 Wireless
LANCOM OAC-54-1 Wireless
LANCOM OAP-54-1 Wireless Bridge Kit

- Handbuch
- Manual

**LANCOM OAP-54-1 Wireless
LANCOM OAC-54-1 Wireless
LANCOM OAP-54-1 Wireless Bridge Kit**

© 2009 LANCOM Systems GmbH, Wuerselen (Germany). All rights reserved.

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

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

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

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

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

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

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

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

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

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom.eu

Wuerselen, Januar 2010

Preface

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

The LANCOM OAP/OAC-54-1 Wireless are designed to offer high-performance wireless LAN in tough environments.

The housing that conforms with IP66 and the facilities for sturdy mounting on walls or poles all make the LANCOM OAP-54-1 Wireless ideally suited for locations where the demands on stability and robustness are at their highest—in temperatures from -30° up to +70°C.

With the integrated 54/108 Mbps WLAN module according to IEEE 802.11a/h or IEEE 802.11b/g the LANCOM OAP-54-1 Wireless work in the 2,4 or 5 GHz frequency range.

The models of the LANCOM OAP/OAC-54-1 Wireless series can be configured in standalone, managed and client mode (LANCOM OAC-54-1 Wireless client mode only). In managed mode, the access point can be securely managed by the LANCOM WLAN Controller.

Model variants

This documentation is intended for LANCOM OAP/OAC-54-1 Wireless users. The following models are available:

- The LANCOM OAP-54-1 Wireless with one integrated WLAN module and one integrated antenna for access point operation or as hot spot with additional software option.
- The LANCOM OAC-54-1 Wireless with one integrated WLAN module and one integrated antenna for client mode operation only.
- The LANCOM OAP-54-1 Wireless Bridge Kit comes as bundle with two LANCOM OAP-54-1 Wireless for the quick set up of point to point connections (WLAN bridge).



In the following parts of this documentation the LANCOM OAP-54-1 Wireless Bridge Kit is referenced only, when special features of the bundle are described. In all other cases the descriptions for the LANCOM OAP-54-1 Wireless are valid for the LANCOM OAP-54-1 Wireless Bridge Kit too.

Model
restrictions

Passages applying only to certain models are identified either in the text itself or by a comment in the margin.

Otherwise the documentation refers to all models collectively as the LANCOM OAP/OAC-54-1 Wireless series.

Security settings

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

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

Components of the documentation

The documentation of your device consists of the following parts:

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

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

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

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

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

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

This documentation was created by ...

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

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

info@lancom.eu

Content

1 Introduction	9
1.1 What is a wireless LAN?	9
1.1.1 Modes of operation of wireless LANs and access points	10
1.2 Just what can your LANCOM OAP/OAC-54-1 Wireless 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 and interfaces	15
2.3.1 LEDs of LANCOM OAP-54-1 Wireless and LANCOM OAC-54-1 Wireless	16
2.3.2 Connectors of LANCOM OAP-54-1 Wireless and LANCOM OAC-54-1 Wireless	17
2.3.3 Mounting and connecting the LANCOM OAP-54-1 Wireless and LANCOM OAC-54-1 Wireless	19
2.4 Software installation	25
2.4.1 Starting the software setup	25
2.4.2 Which software should I install?	26
3 Basic configuration	27
3.1 Details you will need	27
3.1.1 TCP/IP settings	28
3.1.2 Configuration protection	29
3.1.3 Settings for the wireless LAN	30
3.2 Instructions for LANconfig	31
3.3 Instructions for WEBconfig	32
3.4 TCP/IP settings for PC workstations	36

4 Security settings	38
4.1 Security in the wireless LAN	38
4.1.1 Encrypted data transfer (802.11i/WPA or WEP)	38
4.1.2 802.1x / EAP	39
4.1.3 LANCOM Enhanced Passphrase Security	39
4.1.4 Access control by MAC address	40
4.1.5 IPSec over WLAN	40
4.2 Tips for the proper treatment of keys and passphrases	41
4.3 Security settings Wizard	41
4.3.1 LANconfig Wizard	42
4.3.2 WEBconfig Wizard	43
4.4 The security checklist	43
5 Advanced wireless LAN configuration	48
5.1 WLAN configuration with the wizards in LANconfig	48
5.2 Point-to-point connections	50
5.2.1 Geometric dimensioning of outdoor wireless network links	50
5.2.2 Antenna alignment for P2P operations	54
5.2.3 Measuring wireless bridges	56
5.2.4 Activating the point-to-point operation mode	56
5.2.5 Configuration of P2P connections	57
5.2.6 Access points in relay mode	60
5.2.7 Security for point-to-point connections	61
5.3 Client mode	62
5.3.1 Client settings	63
5.3.2 Set the SSID of the available networks	64
5.3.3 Encryption settings	64
6 Setting up Internet access	66
6.1 The Internet Connection Wizard	67
6.1.1 Instructions for LANconfig	67
6.1.2 Instructions for WEBconfig	67

7 Options and accessories	69
7.1 Optional AirLancer Extender antennas	69
7.1.1 Antenna diversity	69
7.1.2 Polarization diversity	70
7.1.3 MIMO	70
7.1.4 Installing the AirLancer Extender antennas	70
7.2 LANCOM Public Spot Option	72
8 Troubleshooting	74
8.1 No DSL connection is established	74
8.2 DSL data transfer is slow	74
8.3 Unwanted connections under Windows XP	75
9 Appendix	76
9.1 Performance data and specifications	76
9.2 Connector wiring	77
9.2.1 Ethernet interface 10/100Base-TX, DSL interface	77
9.2.2 Configuration interface (outband)	77
9.3 CE-declarations of conformity	78
10 Index	79

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").

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

Please observe the corresponding notices to this in this documentation or in the LCOS reference manual.

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)
- Transmission of VPN-encrypted connections with VPN pass through
- 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
- WDS (Wireless Distribution Systems)
- Central administration using a LANCOM WLAN Controller

1.2 Just what can your LANCOM OAP/OAC-54-1 Wireless do?

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

	LANCOM OAP-54-1 Wireless	LANCOM OAC-54-1 Wireless
Operating modes		
Point-to-point mode (six P2P paths can be defined per WLAN interface)	✓	
Access point mode	✓	
Client mode	✓	✓
Managed mode for central configuration of WLAN modules by a WLAN Controller	✓	
IP router	✓	✓
Applications		

	LANCOM OAP-54-1 Wireless	LANCOM OAC-54-1 Wireless
Outdoor operation in tough environments with extreme temperature ranges(-30 °C up to +70 °C)	✓	✓
Internet Access	✓	
Stateful Inspection Firewall	✓	
DHCP and DNS server (for LAN)	✓	✓
DHCP and DNS client (for WAN)	✓	
N:N mapping for routing networks with the same IP-address ranges	✓	✓
Policy-based routing	✓	✓
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	✓	✓
Integrated antenna with antenna gain 13.5 dBi at 2.4 GHz and 15.5 dBi at 5 GHz	✓	✓
Turbo Modus: Bandbreitenverdopplung im 2,4 GHz- und 5 GHz-Bereich	✓	✓
Super AG inkl. Hardware-Compression und Bursting	✓	✓
Multi SSID	✓	
Roaming function	✓	Client only
802.11i / WPA with hardware AES encryption	✓	✓
WEP encryption (up to 128 Bit key length, WEP152)	✓	✓

■ Chapter 1: Introduction

	LANCOM OAP-54-1 Wireless	LANCOM OAC-54-1 Wireless
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	✓	
VLAN	✓	✓
Intra-Cell Blocking	✓	
WLAN QoS (IEEE 802.11e, WME)	✓	✓
LAN connection		
Fast Ethernet LAN port (10/100Base-TX)	✓	✓
Power-over-Ethernet (PoE)	✓	✓
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) according to IEEE 802.3af	✓	✓

	LANCOM OAP-54-1 Wireless	LANCOM OAC-54-1 Wireless
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	✓	
Optional software extensions		
LANCOM Public Spot Option	✓	
LANCOM 2-Year Warranty Extension	✓	✓
LANCOM Next Business Day Service Extension	✓	✓
Optional hardware extensions		
AirLancer Extender antennas for increased range	✓	✓
Housing		
IP66-rated housing for deployment in extreme environments	✓	✓

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 OAP-54-1 Wireless	LANCOM OAC-54-1 Wireless	LANCOM OAP-54-1 Wireless Bridge Kit
LANCOM OAP-54-1 Wireless	1		2
LANCOM OAC-54-1 Wireless		5	
LAN cable for connecting to PoE Injector with waterproof screw connections, 15 m	1	5	2
External 360° dualband antennas with N-plug	2		
Mast and wall mount accessories	✓	✓	✓
PoE Port Injektor	1	5	2
Power cable for PoE Power Injector	1	5	2
Grounding cable with screws	1	5	2
Terminator for a free antenna connector	1	5	2
Serial configuration cable	1	1	1
Plug for resetting the device via serial interface	1	1	1
Surge protector AirLancer Extender SA-LAN			2
LANCOM CD	✓	✓	✓
Printed documentation	✓	✓	✓

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

2.2 System requirements

2.2.1 Configuring the LANCOM devices

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

- Operating system with TCP/IP support, such as Windows, 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").

2.3 Status displays and interfaces

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 LEDs of LANCOM OAP-54-1 Wireless and LANCOM OAC-54-1 Wireless

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



1 2 3

1 Power

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

Off		Device switched off
Green	On (permanently)	Device operational



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

2 WLAN Link

Provides information about the WLAN connections via the internal WLAN module.

The following can be displayed for WLAN link:

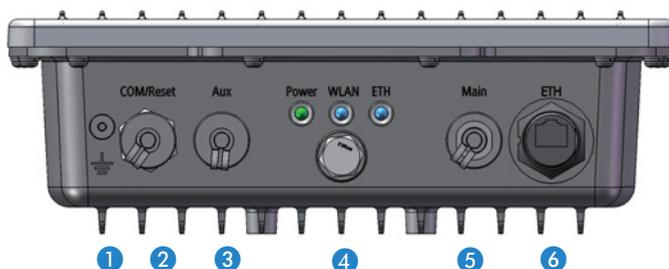
Off		No WLAN network defined or WLAN module deactivated. The WLAN module is not transmitting beacons.
Green		At least one WLAN network is defined and WLAN module activated. The WLAN module is transmitting beacons.
Green	Inverse flashing	Number of flashes = number of connected WLAN stations and P2P wireless connections, followed by a pause (default). Alternatively, the frequency of the flashed can indicate the received signal strength of a P2P link or the received signal strength from an access point, to which this device is connected in client mode..
Green	Blinking	DFS scanning or other scan procedure.

3 ETH

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

2.3.2 Connectors of LANCOM OAP-54-1 Wireless and LANCOM OAC-54-1 Wireless

The connections and switches of the LANCOM OAP-54-1 Wireless and LANCOM OAC-54-1 Wireless are located on the bottom side.



- 1 Earth cable connector.
- 2 Connector for serial configuration cable and reset plug (see 'The reset function').

- 3 Aux connector for external antennas. Diversity antennas are connected to the Aux connector.
- 4 Goretex membrane for compensation of fluctuations in pressure and humidity.
- 5 Main connector for external antennas. Additional AirLancer antennas are connected to the Main connectors if necessary. The integrated RF switch automatically changes to the usage of an external antenna.
- 6 10/100Base-Tx for connection to the LAN. Both 10 Mbit or 100 Mbit connections are supported. The available transfer rate is detected automatically (autosensing). The LAN connection features an automatic MDI/MDIX detector enabling the use of cross-over cables.
The LAN connector on the LANCOM OAP/OAC-54-1 Wireless supports Power over Ethernet (PoE).

The reset function

Via the serial interface the device can either be bootet (restarted) or reset (to the factory settings).

Unsrew the fitting of the "COM/Reset" interface at the bottom of the device. Insert the reset plug to the serial interface. Via this plug, two connectors of the interface are bridged, which starts the reset process.

Press the reset plug briefly to re-start the device. Pressing the button for 5 seconds or longer restarts the device and resets the configuration to its factory settings. All LEDs on the device light up continuously. Once the switch is released the device will restart with the restored factory settings.



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



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

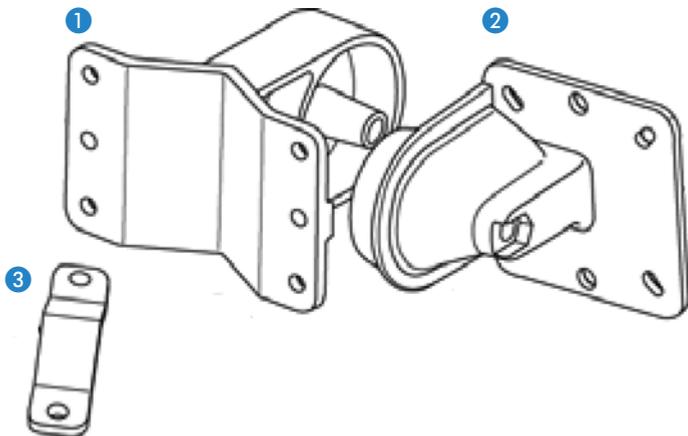
2.3.3 Mounting and connecting the LANCOM OAP-54-1 Wireless and LANCOM OAC-54-1 Wireless



Before mounting external antennas, please observe the information on lightning protection in the LANCOM Outdoor Wireless Guide. Mounting antennas without adequate lightning protection could lead to serious damage to the access point and the network infrastructure connected to it.

The material from the LANCOM OAP/OAC-54-1 Wireless includes beside the screws, nuts and locking rings the following components:

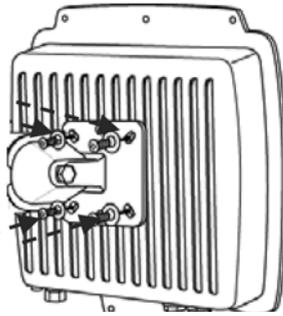
Material



- ① Mounting arm
 - ② Connector flange for the Access Point
 - ③ clamp profile
- ① Screw the Connector flange for the Access Point with the four M5 x 12-screws as well as the appropriate washers to the rear of the chassis.

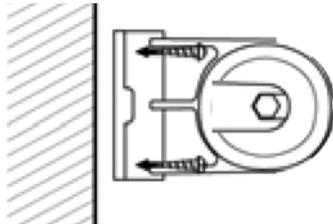
■ Chapter 2: Installation

Preparation



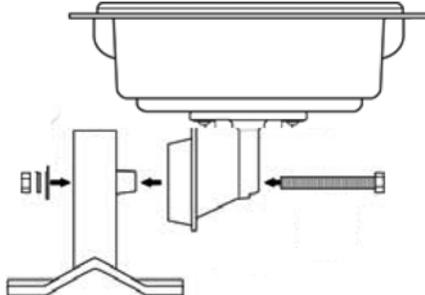
- ② Prepare for the mounting bores at the wall. Use for this the mounting arm as a stencil. Screw the mounting arm ① with the enclosed screws and dowels at the wall.

Wall mounting



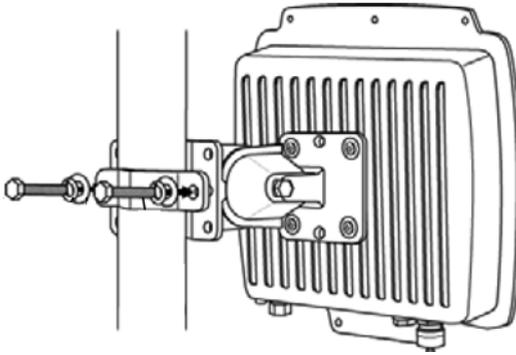
- ③ Attach the Access Point with the connector flange at the mounting arm. Use for this the M8 x 110-screw with the locking washer, washer and nut.

Wall mounting



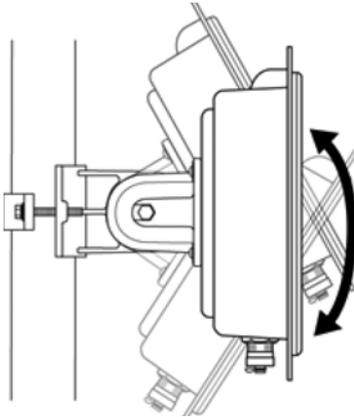
- ④ Place for the pole mounting the clamp profile around the pole. Screw the clamp profile with the M8 x 110-screws at the mounting arm.

Pole mounting



- ⑤ To change the main beam direction of the integrated antennas, you can bend the Access Point up or down with the connector flange opposite the mounting arm.

Adjusting of the Access Point

**Installation of the LANCOM OAP/OAC-54-1 Wireless**

For the installation of the LANCOM OAP/OAC-54-1 Wireless proceed as follows:

- ① Earth connection - attach the earth cable to the earth screw of the LANCOM OAP/OAC-54-1 Wireless and to a suitable earthed conductor.



When mounting the LANCOM OAP/OAC-54-1 Wireless on poles or walls it may be necessary to earth the housing to avoid dangerous differences in potential. For grounding the LANCOM OAP/OAC-54-1

Wireless please observe the information on lightning protection in the attached LANCOM Outdoor Wireless Guide.

- ② Optional: Antenna terminal LANCOM OAP-54-1 Wireless – screw the supplied diversity antennas onto the two N connectors on the bottom side of the LANCOM OAP/OAC-54-1 Wireless.



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.



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!

- ③ LAN—The LAN connector is also used to supply power to the LANCOM OAP/OAC-54-1 Wireless. Plug in the water-proof power cable to the LAN port on the underside of the device and carefully tighten the threaded connector. Connect the other end of the power cable to the 'Power Out' connector on the supplied PoE Injector.
- ④ 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).
 - For the exclusive mode insert the included network cable (green plugs) into the LAN connector of the device 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 and the other end into a free network connecting socket of your local network (resp. into a free socket of a hub/switch).

More information about using a LAN interface for DSLoL can be found in the following information box → LAN interface: exclusive or in parallel for DSLoL.

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 a access router with multiple fixed IP addresses (such as many SDSL business lines).

- ⑤ PoE—the 'LAN In' connector of the supplied PoE Injector should be connected via a normal Ethernet cable to an available network connection socket in your local network (e.g. an available socket on a hub or switch) and the PoE Injector connected with the electricity supply.

Information about the installation of PoE can be found in the information box 'Power over Ethernet—elegant power supply over LAN cabling' above.

Please observe the information in the documentation supplied with the PoE Injector.



Use only the supplied PoE Injector for the power supply of the LANCOM OAP/OAC-54-1 Wireless. Pay particular care not to connect the PoE Injector to normal Ethernet devices!

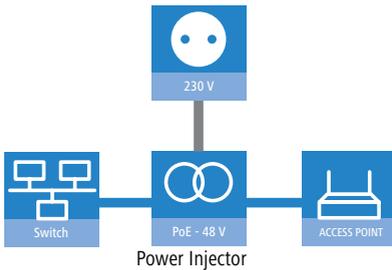
- ⑥ Ready for operation? —the Power LED permanently lights up in green as soon as the device receives power. The LEDs subsequently display the operational status.

Power over Ethernet – the elegant power supply via LAN cabling

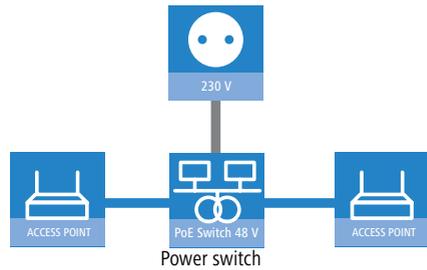
LANCOM Access Points are prepared for the PoE power supply (Power-over-Ethernet), corresponding to the 802.3af standard. PoE-enabled network devices can be comfortably supplied with power feeding through the LAN wiring. A separate external power supply for each base station is unnecessary, which reduces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

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 OAP/OAC-54-1 Wireless exclusively with computers running operating systems other than Windows.

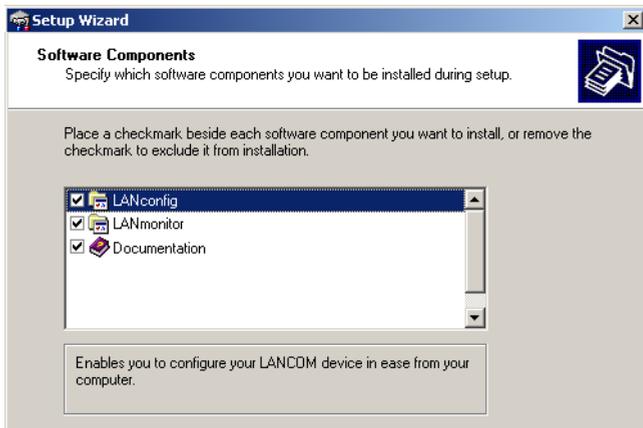
2.4.1 Starting the software setup

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



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

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



2.4.2 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).

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 Details you will need

The Basic Settings Wizard is used to set the LANCOM OAP/OAC-54-1 Wireless 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 OAP/OAC-54-1 Wireless
- Setting up a new network

Fully automatic TCP/IP configuration will not be offered if you are integrating the LANCOM OAP/OAC-54-1 Wireless 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 OAP/OAC-54-1 Wireless 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 OAP/OAC-54-1 Wireless can assign the devices in the LAN IP addresses automatically.

Should you still configure manually?

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

- Select automatic configuration if you are **not** familiar with networks and IP addresses.

- Select the manual TCP/IP configuration if you are familiar with networking and IP addresses, and you would like to specify the IP address for the router yourself (from one of the address ranges reserved for private use, for example '10.0.0.1' with a network mask of '255.255.255.0'). If you do this you simultaneously specify the address range that the DHCP server will subsequently use for the other devices in the network (provided the DHCP server is activated).

Required information for manual TCP/IP configuration

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

- **DHCP mode of operation**
 - Off: The IP addresses required must be entered manually.
 - Server: The LANCOM OAP/OAC-54-1 Wireless operates as DHCP server in the network; as a minimum its own IP address and the network mask must be assigned.
 - Client: The LANCOM OAP/OAC-54-1 Wireless obtains its address information from another DHCP server; no address information is required.
- **IP address and network mask for the LANCOM OAP/OAC-54-1 Wireless**

Assign the LANCOM OAP/OAC-54-1 Wireless 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 OAP/OAC-54-1 Wireless's configuration and thus prevents unauthorized modification. The device's configuration contains a great deal of sensitive data such as data for Internet access and should be protected by a password in all cases.



Multiple administrators can be set up in the configuration of the LANCOM, each with different access rights. Up to 16 different administrators can be set up for a LANCOM OAP/OAC-54-1 Wireless. 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 LANconfig with **Start ▶ Programs ▶ LANCOM ▶ LANconfig**. LANconfig automatically detects new LANCOM devices in the TCP/IP network.
- ② If the search detects an unconfigured device, the Setup Wizard launches to help you with its basic settings, or indeed to handle the entire process on your behalf (assuming that the appropriate networking environment exists).



 If the Setup Wizard does not start automatically, you can search for new devices in the network manually (**File ▶ Find devices**).

 If you cannot access an unconfigured LANCOM OAP/OAC-54-1 Wireless, the problem may be the LAN netmask: In case there are less than 254 potential hosts available (netmask >'255.255.255.0'), you must ensure that the IP address 'x.x.x.254' is available in your subnet.

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

③ Give the LANCOM an address from the applicable IP address range. Confirm with **Next**.

④ In the window that follows, you first set the password to the configuration. Entries are case sensitive and should be at least 6 characters long.

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

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

⑤ Enter the wireless parameters. Set a network name (SSID) and a radio channel. If preferred, activate the "closed network" function. Accept your entries with **Next**.

⑥ Charge protection is a function which can place a limit on the costs from WAN connections. Accept your entries with **Next**.

⑦ Close the configuration with **Finish**.

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

3.3 Instructions for WEBconfig

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

Secure with HTTPS

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

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

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

Accessing the device with WEBconfig

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

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



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

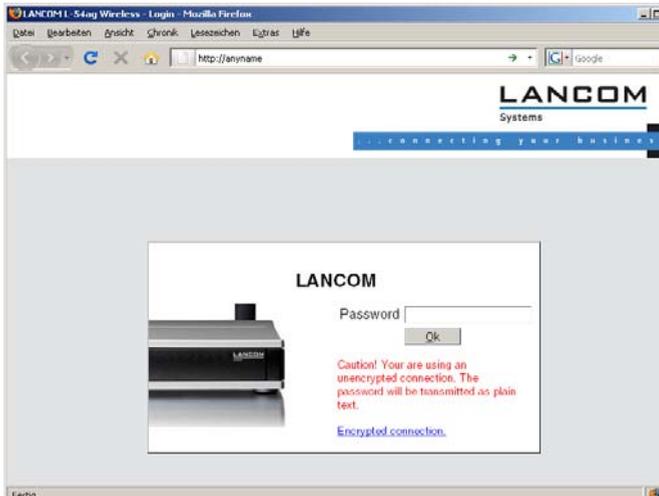
Network without a DHCP server

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



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

Not for centrally managed LANCOM Wireless Routers or LANCOM Access Points



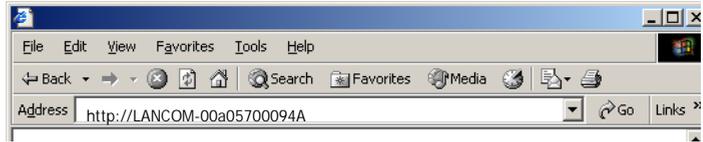
If the configuration computer does not retrieve its IP address from the LANCOM DHCP server, it determines the current IP address of the computer (with **Start ▶ Run ▶ cmd** and command **ipconfig** at the prompt under Windows 2000 or Windows XP or Windows Vista, with **Start ▶ Run ▶ cmd** and command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

Network with DHCP server

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

- If the LAN also has a DNS server for name resolution and this communicates the IP address/name assignment to the DHCP server, the device can

be reached under name "LANCOM-<MAC address>", e.g. "LANCOM-00a057xxxxx".



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

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

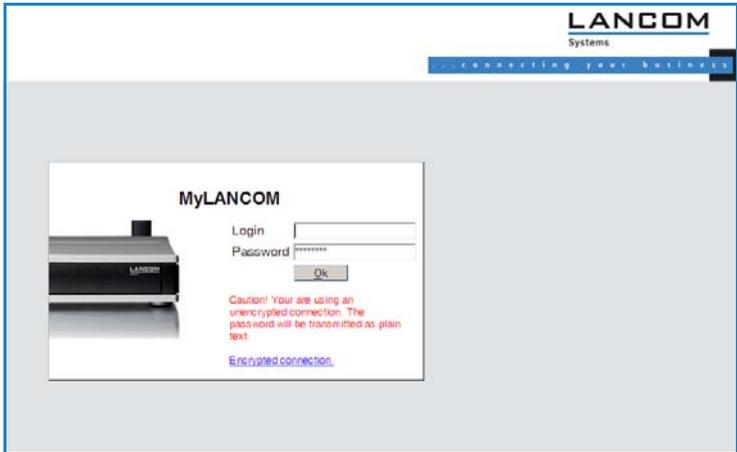
Login

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

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

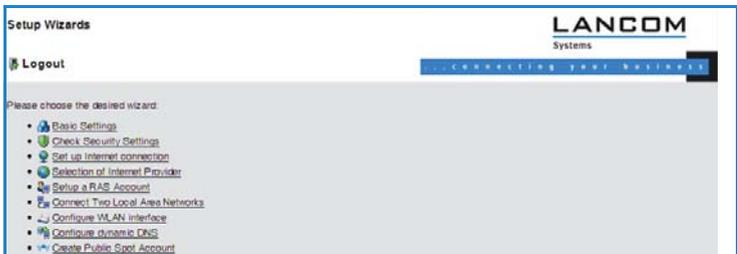


As an alternative, the login dialog provides a link for an encrypted connection over HTTPS. Always use the HTTPS connection for increased security whenever possible.



Setup Wizards

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



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

3.4 TCP/IP settings for PC workstations

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

- Standard gateway – receives all packets which are not addressed to computers in the local network

- DNS server – translates network and computer names into their actual IP addresses.

The LANCOM OAP/OAC-54-1 Wireless can fulfill the functions of a standard gateway and also of a DNS server. It can also operate as a DHCP server, which automatically assigns IP addresses to all of the computers in the LAN.

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

- **IP address allocation by a LANCOM**

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

- **IP address allocation by a separate DHCP server**

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

- **Manual IP address assignment**

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



Further information and help on the TCP/IP settings for your LANCOM OAP/OAC-54-1 Wireless is available in the Reference Manual. For information on the network configuration of workstation PCs, refer to the documentation for the installed operating system.

4 Security settings

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



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

4.1 Security in the wireless LAN

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

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

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

4.1.1 Encrypted data transfer (802.11i/WPA or WEP)

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



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

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

- The passphrases for 802.11i or WPA do not have to be changed quite so regularly as new keys are generated for each connection anyway. This is not the only reason that the encryption with 802.11i/AES or WPA/TKIP is so much more secure than the now obsolete WEP method. If you use WEP encryption to maintain compatibility with older WLAN clients, regularly change the WEP key in your access point.
- If the data is of a high security nature, further improvements include additionally authenticating the client with the 802.1x method ('802.1x / EAP' →Seite 39) or activate an additional encryption of the WLAN connection as used for VPN tunnels ('IPSec over WLAN' →Seite 40). In special cases, a combination of these two mechanisms is possible.



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

4.1.2 802.1x / EAP

The international industry standard IEEE 802.1x and the **Extensible Authentication Protocol (EAP)** enable access points to carry out reliable and secure access checks. The access data can be managed centrally on a RADIUS server (integrated RADIUS/EAP server in the LANCOM OAP/OAC-54-1 Wireless or external RADIUS/EAP server) and accessed by the access point when required. The dynamically generated and cryptographically secure key material for 802.11i (WPA1/2) replaces the manual key management.

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

4.1.3 LANCOM Enhanced Passphrase Security

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

LEPS can be used locally in the device and can also be centrally managed with the help of a RADIUS server, and it works with all WLAN client adapters currently available on the market without modification. Full compatibility to

third-party products is assured as LEPS only involves configuration in the access point.

An additional security aspect: LEPS can also 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 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, the this global passphrase can be changed on a regular basis—every few days, for example.

4.1.4 Access control by MAC address

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

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

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

4.1.5 IPSec over WLAN

With the help of the IPSec-over-WLAN technology in addition to the security measures described already, a wireless network for the exchange of especially sensitive data can be optimally secured. Required for this is a base station with VPN support and the LANCOM Advanced VPN Client that operates under Windows 2000, XP and Windows Vista™. Client software from third parties is available for other operating systems.

4.2 Tips for the proper treatment of keys and passphrases

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

- **Keep your keys as secret as possible.**

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

- **Choose a random key.**

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

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

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

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

Activate LEPS to enable the use of individual passphrases.

4.3 Security settings Wizard

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

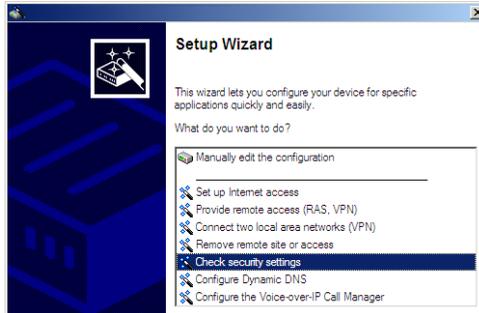
Your LANCOM offers password-protected access to its configuration. This is activated during the initial basic configuration simply by entering a password.

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

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

4.3.1 LANconfig Wizard

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



- ② In the selection menu, select the Setup Wizard, **Check security settings** and confirm the selection with **Next**.
- ③ In the dialogs that follow you can set the password and select the protocols to be available for accessing the configuration from local and remote networks.
- ④ In a subsequent step, you can set parameters for locking the configuration such as the number of incorrect password entries and the duration of the lock.
- ⑤ For devices with a WLAN interface, you have the option of specifying the security parameters of the wireless network. This includes the name of the wireless network, the closed-network function, and encryption by 802.11i/WPA or WEP. For devices with an optional second WLAN interface, you can set the parameters for both wireless networks separately.
- ⑥ For the WLAN interface, you can subsequently define the access control lists (ACL) and the protocols. This allows you to place limitations on the data exchange between the wireless network and the LAN.
- ⑦ For the firewall, you can activate stateful inspection, ping blocking, and the stealth mode.
- ⑧ The Wizard will inform you as soon as the entries are complete. Close the configuration with **Finish**.

4.3.2 WEBconfig Wizard

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

- Device password
- The protocols to be available for accessing the configuration from local and remote networks
- The parameters for locking the configuration (the number of incorrect password entries and the duration of the lock)
- Security parameters such as WLAN name, closed-network function, WPA passphrase, WEP key, ACL lists, 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.



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

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



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

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

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 do not stop third parties from operating RAS access, LAN connectivity 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).

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

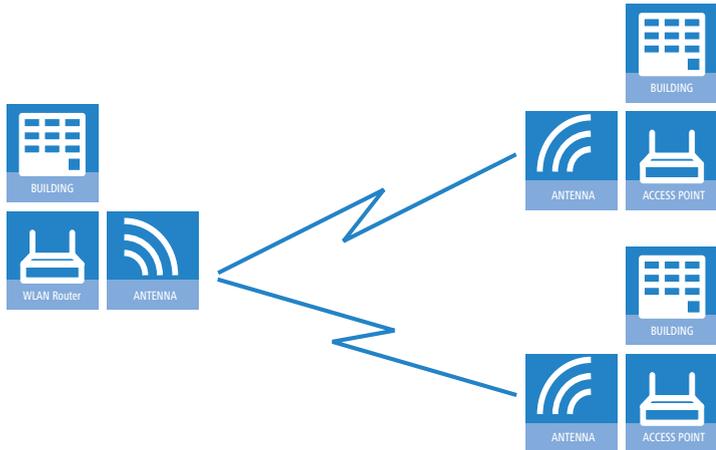
The configuration of P2P connections involves setting not only the operating mode but also the station name that the Access Point can connect to. Also, the role as "Master" or "Slave" is set here.

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.



This chapter introduces the basic principles involved in designing point-to-point links and provides tips on aligning the antennas.

5.2.1 Geometric dimensioning of outdoor wireless network links

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

- Which antennas are necessary for the desired application?
- How do the antennas have to be positioned to ensure problem-free connections?
- What performance characteristics do the antennas need to ensure sufficient data throughput within the legal limits?

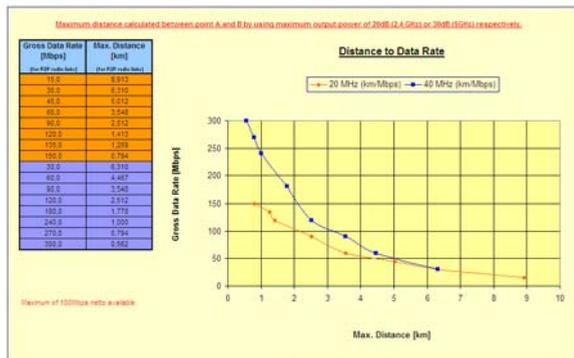
Selection of antennas using the LANCOM Antenna Calculator

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 Web site 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.



Positioning the antennas

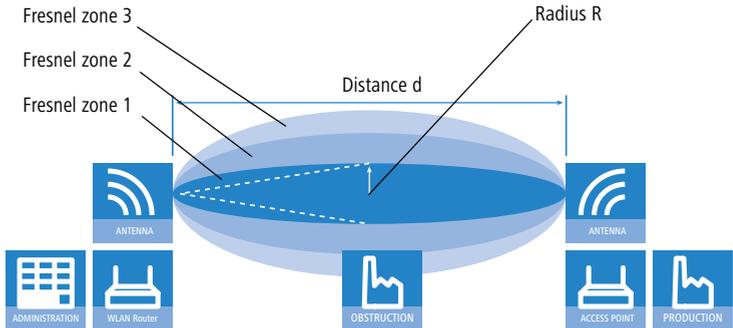
Antennas do not broadcast their signals linearly, but within an angle that depends on the model in question. The spherical expansion of the signal waves produces amplification or interference of the effective power output at certain distances along the connection between the transmitter and receiver.

The areas where the waves amplify or cancel themselves out are known as Fresnel zones.



Protecting the components employed from the consequences of lightning strikes and other electrostatic influences is one of the most important aspects to be considered when designing and installing wireless LAN systems for outdoor use. Please refer to the appropriate notes on 'Lightning and surge protection' as otherwise LANCOM Systems cannot provide any guarantee for damage to LANCOM and AirLancer components.

Information on the installation of WLAN systems for outdoor deployment is available in the 'LANCOM Outdoor Wireless Guide'.



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.

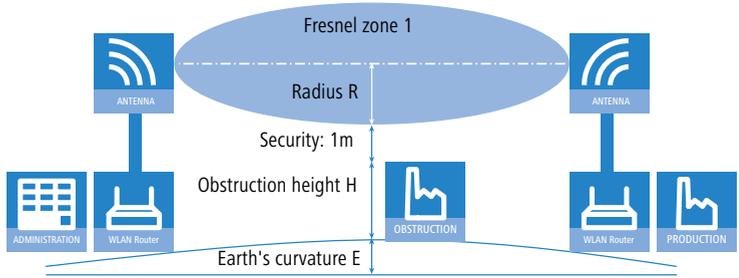
The radius (R) of Fresnel zone 1 is calculated with the following formula assuming that the signal wavelength (λ) and the distance between transmitter and receiver (d) are known.

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

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:



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

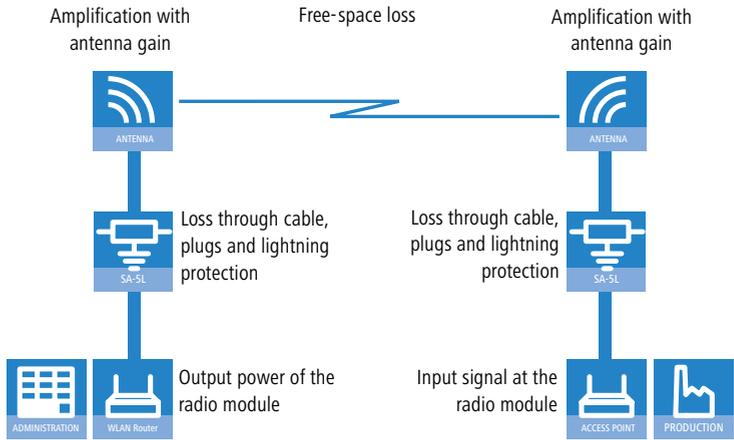
The allowance for the curvature of the earth (E) can be calculated at a distance (d) as $E = d^2 * 0.0147$ – i.e. at a distance of 8 km this is almost 1 m

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

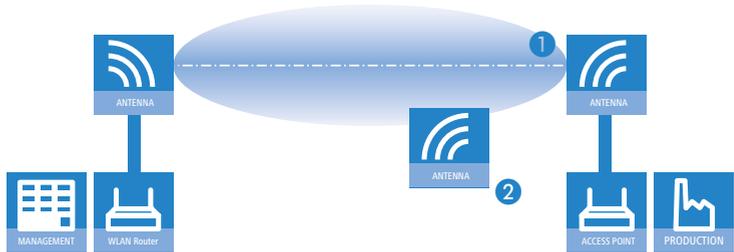
The power of the antennas must be high enough to ensure acceptable data transfer rates. On the other hand, the country-specific legal regulations regarding maximum transmission power should not be exceeded.

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

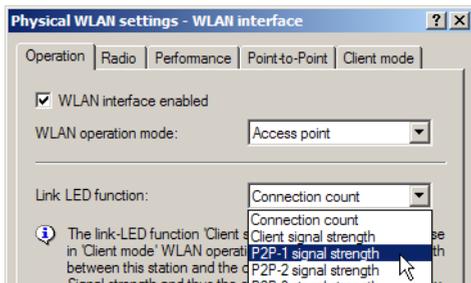
The precise alignment of the antennas is of considerable importance in establishing P2P connections. The more central the receiving antenna is located in the "ideal line" of the transmitting antenna, the better are the actual performance and the effective bandwidth **1**. If the receiving antenna is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



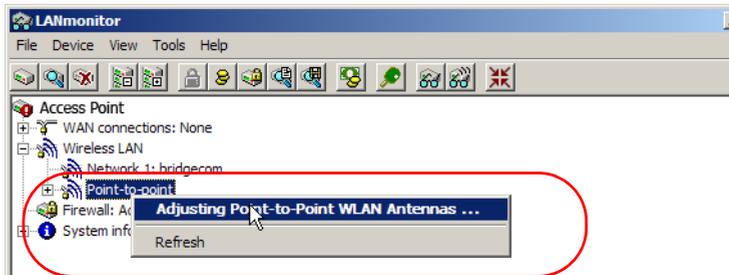
You can find further information on the geometrical design of wireless paths and the alignment of antennas with the help of LANCOM software in the LCOSreference manual.

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 site 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 sites 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.

5.2.3 Measuring wireless bridges

After planning and installation, the wireless bridge can be analyzed to determine the actual data throughput. Further information about the available tools and taking measurements can be found in the LANCOM Techpaper "The performance of outdoor P2P connections", available as a download from www.lancom.eu.

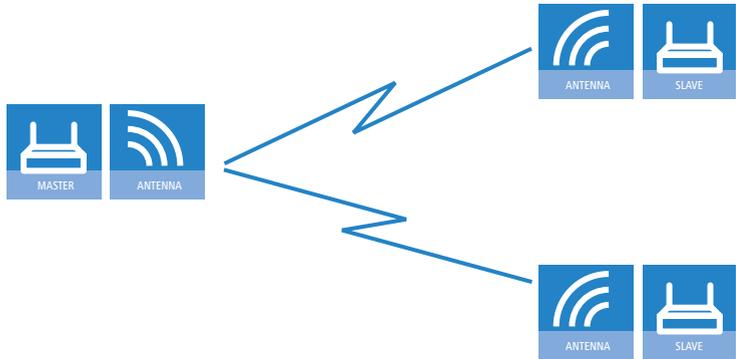
5.2.4 Activating the point-to-point operation mode

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 (a master as authentication server and a slave as client).

5.2.5 Configuration of P2P connections

In the configuration of point-to-point connections, entries have to be made for the point-to-point operation mode and the channel selection scheme, along with the MAC addresses or station names 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.

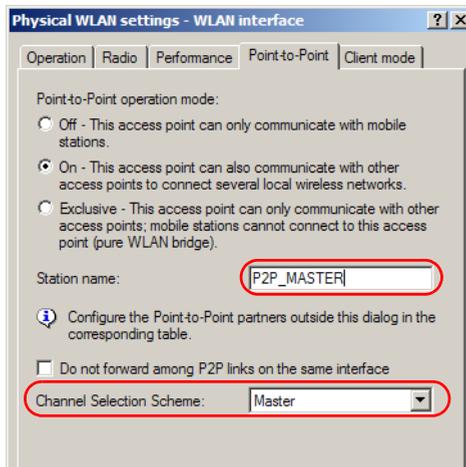


The configuration of the P2P connections can also be carried out with the WLAN Wizards in LANconfig.

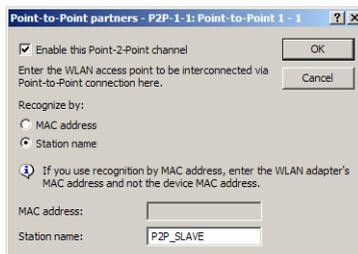
- ① Click on the button **Physical WLAN settings** to open the corresponding WLAN interface and select the tab for 'Point-to-Point'.
- ② Activate the suitable point-to-point operation mode here and set the channel selection scheme to either 'Master' or 'Slave'. If the peers of the P2P connections are 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.

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.



Connecting point-to-point remote stations by station name

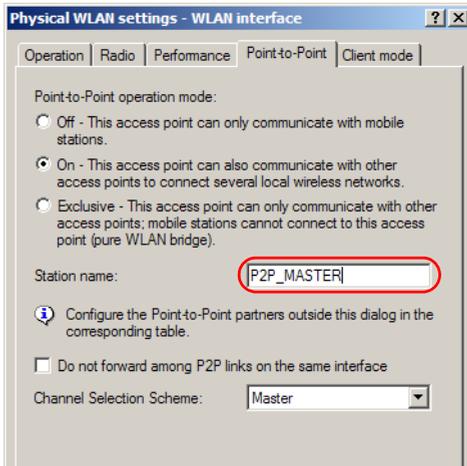
When configuring point-to-point connections, an alternative to the MAC addresses is to use the station names of the remote stations.

First of all the station name is entered into the point-to-point settings in the Wireless Routers or Access Points.

- LANconfig: **Wireless LAN** ▶ **General** ▶ **Physical WLAN settings** ▶ **Point to point**
- WEBconfig: **Setup** ▶ **Interfaces** ▶ **WLAN interpoint settings**



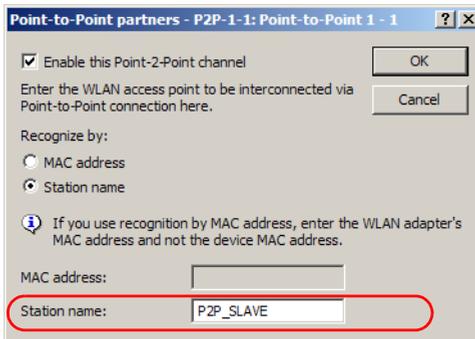
For models with multiple WLAN modules, the station name can be entered separately for each physical WLAN interface.



In the point-to-point configuration, select the identification by station name and enter the name of the corresponding station.

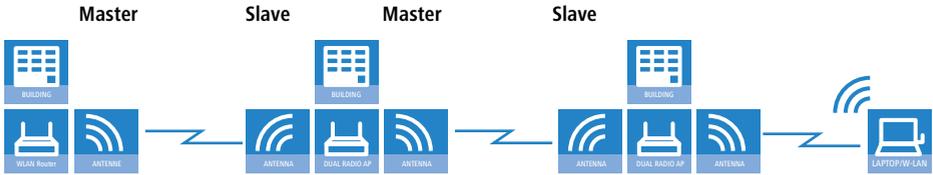
■ LANconfig: **Wireless LAN ▶ General ▶ Point to point partners**

■ WEBconfig: **Setup ▶ Interfaces ▶ WLAN interpoint peers**



5.2.6 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.

5.2.7 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 module for the P2P connection, WLAN-2 if you are using the second module, e.g. as with an access point with two WLAN modules).

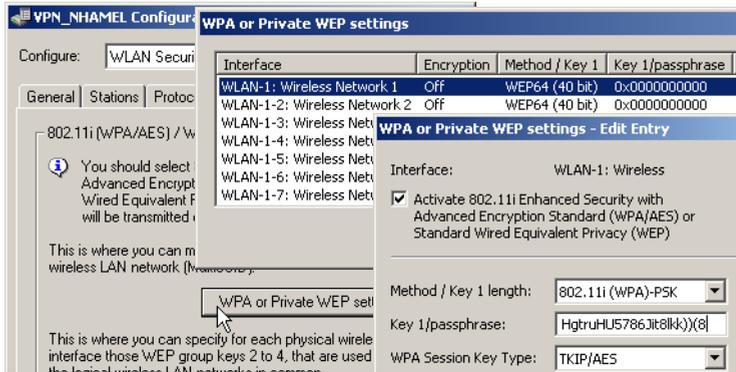
- Activate the 802.11i encryption.
- Select the method '802.11i (WPA)-PSK'.
- Enter the passphrase to be used.



The passphrases should consist of a random string 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.

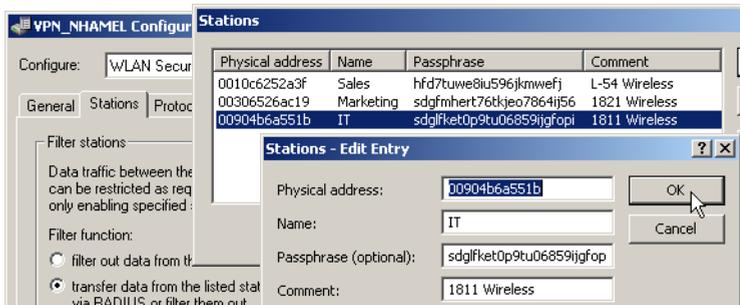


LEPS for P2P connections

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.

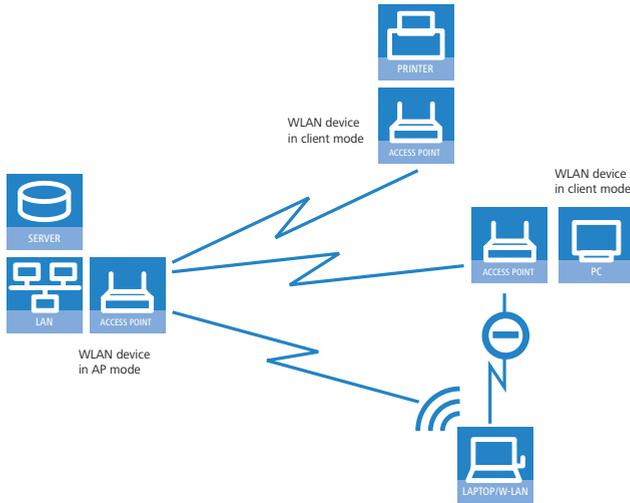
When using LANconfig for the configuration, you enter the passphrases of the stations approved for the WLAN in the configuration area 'Wireless LAN' on the 'Stations' tab under the button **Stations**.



5.3 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.



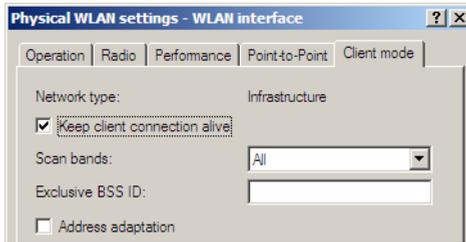
Multiple WLAN clients can register with a WLAN device in AP mode, which is not the case for a WLAN device in client mode.

5.3.1 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.

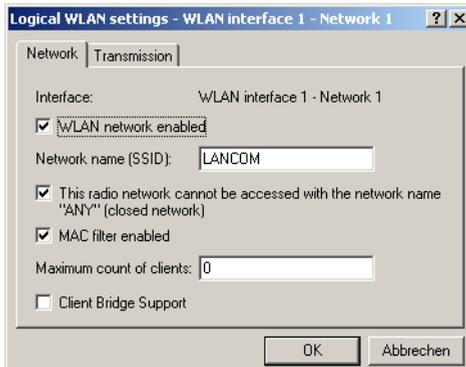


- ① To edit the settings for client mode in LANconfig, go to the 'Client mode' tab under the physical WLAN settings for the desired WLAN interface.
- ② In 'Scan bands', define whether the client station scans just the 2.4 GHz, just the 5 GHz, or all of the available bands to locate an access point.

5.3.2 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.

5.3.3 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.

The screenshot shows a dialog box titled "WPA or Private WEP settings - Edit Entry". It contains the following fields and options:

- Interface: Wireless Network 1
- Encryption activated:
- Method / Key 1 length: WEP128 (104 bit)
- Key 1/passphrase: L00A0570FB9BF
- WPA Session Key Type: TKIP/AES
- WPA version: WPA1
- Authentication: Open system (recom)
- Default key: Key 1
- Client EAP method: TLS

- 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.

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.

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

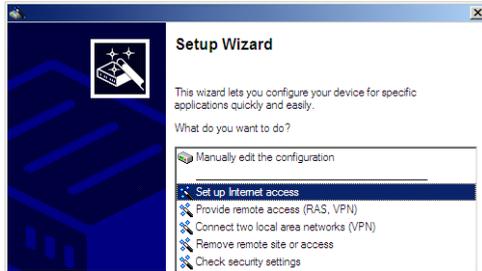
In addition you can use the Wizard to activate or deactivate additional options (if supported by your Internet provider):

- 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 sites 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 site.
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

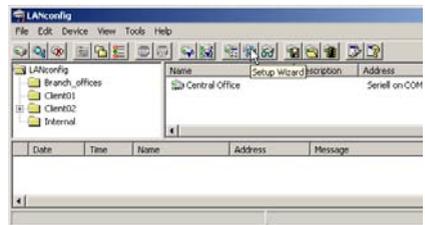
6.1.1 Instructions for LANconfig

- 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**.

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.

■ *Chapter 6: Setting up Internet access*

- ③ Depending on availability the Wizard provides further options for your Internet connection.
- ④ The wizard will inform you as soon as the entries are complete. Close the configuration with **Finish**.

7 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.

EM

7.1 Optional AirLancer Extender antennas

AirLancer Extender antennas are capable of extending the operating range of the devices, or of adapting access point coverage to local conditions. An overview of the supported antennas is available from the LANCOM Web site under www.lancom.eu.



You will also find further information on calculating the best configuration for AirLancer Extender antennas and third-party antennas that you wish to connect to the LANCOM under www.lancom.eu.



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.



For internal lightning protection, the surge adapter AirLancer Extender SA-5L is **always necessary**—the AirLancer Extender SA-5L is mounted between the Access Point and the antenna, as close to the antenna as is possible.



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

Only LANCOM OAP-54-1 Wireless

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).

Each wireless LAN module is equipped with two send/receive units, each of which can be connected to an antenna. In the case of antenna diversity, the WLAN module checks which send/receive unit (antenna) is receiving the strongest signal from a client. Only the stronger signal is used. The Access Point stores the information on which send/receive unit was used to receive data and proceeds to use the same unit for the transmission to the client. Antenna diversity ensures that the various clients associated with the Access Point always use the send/receive unit with the best signal.

7.1.2 Polarization diversity

Other diversity techniques process the two signals and combine them into a single signal. The most common methods are space diversity and polarization diversity. LANCOM Systems supplies various polarization diversity antennas for connection to LANCOM devices. With these models, two orthogonally polarized signals are received at a transmitter/receiver unit and combined to form a single signal which is stronger than the two individual signals. This improvement is the polarization gain. Further information about this technique is available in our "Polarization Diversity" techpaper.

7.1.3 MIMO

MIMO also uses polarization antennas which can process two orthogonally polarized signals. Different to polarization diversity, MIMO uses each of these signals to transport a separate data stream and achieve twice the data throughput.

7.1.4 Installing the AirLancer Extender antennas

The following diversity antennas are available as accessories for the LANCOM OAP/OAC-54-1 Wireless:

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



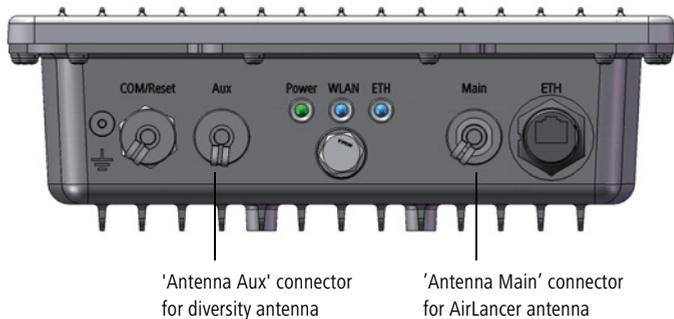
Before mounting external antennas, please observe the information on lightning protection in the LANCOM Outdoor Wireless Guide (supplied or available as a download from www.lancom.eu). Mounting antennas without adequate lightning protection could lead to serious damage to the access point and the network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

LANCOM OAP-54-1
Wireless

The antennas integrated into the LANCOM OAP-54-1 Wireless are primarily designed for establishing point-to-point connections. External antennas are an option if the device is to be operated as an Access Point, to achieve a higher antenna gain, or to use the diversity function.

For installing the enclosed omni-directional antenna or optional AirLancer Extender antennas, switch the LANCOM OAP/OAC-54-1 Wireless off by interrupting the PoE power supply. Then carefully unscrew the terminators. Connect the antenna to the appropriate 'Antenna Main' connector. Connecting an antenna to the Main connector automatically deactivates the internal antennas.

With the LANCOM OAP-54-1 Wireless, you can additionally use the "Tx diversity" function via the Aux connector. Refer to the LCOS reference manual for further information on this.



7.2 LANCOM Public Spot Option

Wireless Public Spots are publicly accessible areas where users can use their own mobile computers to access a wireless network (such as a company network or the Internet).

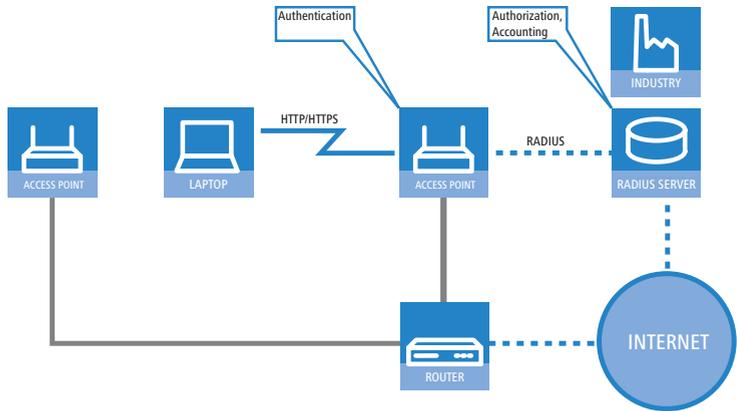


Please note that operating a LANCOM OAP/OAC-54-1 Wireless with the LANCOM Public Spot Option (also referred to as a HotSpot) can be subject to legal regulation in your country. Before installing a LANCOM OAP/OAC-54-1 Wireless, please inform yourself about any applicable regulations. More information on this subject is available in our white paper "Public Spot - Rechte und Pflichten eines Betreibers" available for download from www.lancom.eu.

Wireless LAN technology is ideal for offering wireless Internet services to the public in locations such as airports, railway stations, restaurants or cafes via so-called HotSpots. The LANCOM Public Spot Option is intended for operators of public wireless networks. It enables the easy installation and maintenance of public HotSpots by providing LANCOM Access Points and LANCOM Routers with additional functions for authentication and billing for public Internet services.

The LANCOM Public Spot Option is the ideal solution for public wireless LAN. Wireless LAN are very well suited for company networks and for wireless networking in the home. However, for public access services the standard setup lacks important mechanisms for authentication and billing of individual users (AAA — authentication, authorization, accounting). This is remedied by the LANCOM Systems Open User Authentication (OUA), the core component of the LANCOM Public Spot Option. OUA implements the authentication of all wireless clients by user name and password. It checks the authorization of each user with a RADIUS server. Accounting data (online time, volumes) on a per user and per session basis can be passed on to the central RADIUS server. All the client PC needs is a wireless card (e.g. AirLancer), TCP/IP, and an Internet browser. No further software is required. The Public Spot Option is optimally suited for setting up wireless Internet access services in hotels,

restaurants, cafes, airports, railway stations, exhibition grounds or universities.



The LANCOM Public Spot Option equips an access point with these functions and upgrades 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

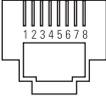
9.1 Performance data and specifications

		LANCOM OAP-54-1 Wireless	LANCOM OAC-54-1 Wireless
Frequency band		WLAN module with 2400 - 2483,5 MHz (ISM) or 5150 - 5725 MHz and 5725 - 5850 (UK only)	
Connections	LAN	10/100Base-TX, Autosensing, Auto Node-Hub	
	WLAN	2x N socket with antenna diversity	
Power supply		Via Power over Ethernet only. One PoE Injector supplied.	
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.eu	
Housing		235 mm x 210 mm x 80 mm (W x H x D), 3.4kg, robust metal housing, IP66 water-jet resistant, ready for wall and pole mounting, 3 LEDs for status display	
Approvals		CE compliant according to ETSI EN 300 328, ETSI EN 301 893 Version 1.3.1 (incl. DFS 2), ETSI EN 301 489-1, ETSI EN 301 489-17, EN 60950-1	
Regulations		Notified in Germany, Belgium, Netherlands, Luxemburg, Austria, Switzerland, United Kingdom, Italy, France, Czechia, Denmark The current list of notifications can be found at www.lancom.eu	
Environment/ Temperature		Temperature range –30 °C bis +70 °C at 95 % max. humidity (non condensing)	
Service		Warranty: 3 years	
Support		Via hotline and Internet	
Accessories		<ul style="list-style-type: none"> ■ LANCOM Next Business Day Service Extension OAP item no 61412 ■ LANCOM 2-Year Warranty Extension OAP item no 61415 	

9.2 Connector wiring

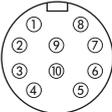
9.2.1 Ethernet interface 10/100Base-TX, DSL interface

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

Connector	Pin	Line
	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)

10-pin Mini DIN socket

Connector	Pin	Line
	1	DSR
	2	RI
	3	DCD
	4	DTR
	5	TXD
	6	RTS
	7	CTS
	8	RXD
	9	RST (Reset)
	10	GND

9.3 CE-declarations 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 can be found on the relevant product page on the LANCOM Web site (www.lancom.eu).

Index

Numerics

100-Mbit network	18
802.11i	11, 38, 39, 42, 43
802.11i/	39
802.1x	12, 38, 39
802.3af- standard	24

A

Access point mode	9, 15
Access-control list	40
ACL	39, 40
AES	38
Antenna Calculator	50
Antenna power	53
Autosensing	18

C

Charge protection	32
Client mode	62, 63
Closed network	12
Configuration access	32
Configuration file	46
Configuration password	44
Configuration protection	29
Connector wiring	77
Configuration port	77
LAN interface	77
Outband	77

D

Declaration of conformity	78
Default gateway	36, 45
DFS	51
DHCP	12, 37
DHCP server	28, 37
DNS	12
DNS server	11, 37
Documentation	14
DSL connection	

problems establishing the connection
74

DSLolL	22
Dynamic Frequency Selection	51
Dynamic frequency selection	51

E

EAP	12, 38, 39
Encryption methods	64

F

Firewall	11, 12, 45
Block stations	46
FirmSafe	13
Flatrate	66
Fresnel zone	52

H

HTTPS	32
-------	----

I

ICMP	45
Installation	14
Internet access	66
Authentication data	66
Flatrate	66
Internet access setup	66
Internet provider	66
Internet-Zugang	11
IP	
Block ports	45
Filter	45
IP address	28, 29, 46
IP masquerading	12, 45
IPSec over WLAN	38

L

LAN	
Connector cable	14
LANCOM Enhanced Passphrase Security	38

■ *Index*

LANCOM Public Spot Option	72	Protecting the configuration	38
LANconfig	26, 31	Security checklist	43
LANmonitor	26	self-sufficient	9, 15
LANtools		SNMP	
System requirements	15	Configuration protection	44
LEDs		Software installation	25
see status displays	16	SSID	30, 32, 64
LEPS	12, 39	Stateful Inspection Firewall	11
M		Status display	
MAC address filter	12	ETH	17
Managed mode	9, 15	WLAN link	17
mount accessories	14	Statusanzeigen	
Multi SSID	11	Power	16
N		Super AG	11
NAT – see IP masquerading		System requirements	15
Network mask	28, 29, 46	T	
O		TCP	45
Optional antennas	69	TCP/IP	15
Options and accessories	69	Settings	28
P		Windows size	75
P2P	40	TCP/IP configuration	
Password	29, 32	Fully automatic	28
PAT – see IP masquerading		Manual	28, 29
PoE Power Injector	14	TCP/IP filter	12, 45
Point-to-point	40, 50	Technische Daten	76
point-to-point	10	Telnet	46
Power-over-Ethernet	24	TFTP	46
Q		Transfer protocol	74
QoS	12	Turbo Modus	11
Quality of Service	12	U	
R		UDP	45
RADIUS	12, 39	W	
Remote configuration	32	WEBconfig	32
Routing table	45	HTTPS	32
S		System requirements	15
Security		WEP	11, 38, 41, 42, 43
		Wireless LANs	
		Operating modes	10

WLAN		Client mode	63
Bands scanned	64	WPA	11, 38, 39, 42, 43