



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

LANCOM 1811n Wireless LANCOM 1821n Wireless

- Handbuch
- Manual

LANCOM
Systems

LANCOM 1811n Wireless
LANCOM 1821n Wireless

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

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

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

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

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

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

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

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

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

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

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom.eu

Wuerselen, März 2010

Preface

Thank you for your confidence in us!

With LANCOM 1811n Wireless and LANCOM 1821n Wireless you have chosen a powerful wireless router that possesses integrated DSL respectively ADSL and ISDN interfaces by default as well as an integrated 4-port switch. LANCOM wireless routers provide the comprehensive functions of an access point, professional firewall and high-quality VPN gateway in a single, compact device. They thus combine most important functions as a reliable solution for small and mid-sized enterprises, home and branch offices.

The wireless routers operate either in the 2.4 GHz or in the 5 GHz frequency band. The 5 GHz band is ideal as the backbone for cost-effective, high-bandwidth transmission that is free of interference and highly secure. The LANCOM Wireless Router series models can operate in stand-alone mode, in managed mode or in client mode. The access point can be used in managed mode with a LANCOM WLAN Controller without any additional software upgrades.

The LANCOM 1811n Wireless and LANCOM 1821n Wireless provide a maximum wireless LAN performance of up to 300 Mbps thanks to the support of the IEEE 802.11n standard. The 802.11n standard includes many new mechanisms—such as the use of MIMO, 40-MHz channels, packet aggregation and block acknowledgement—in order to increase the bandwidth available for user applications significantly. This allows a more than fivefold increase in speed over 802.11a/g networks with physical data rates of up to 300 Mbps.

MIMO (multiple input multiple output) technology allows the LANCOM Wireless Router to transfer several data streams in parallel and thus significantly improve data throughput. MIMO uses several transmit/receive units for both the transmitter and the receiver. The separate data streams are identified by unique characteristics that result from the different paths that the data take. By processing multiple data streams MIMO achieves not just higher data throughput but also better coverage (fewer "radio black spots") and better stability. These are the most important arguments for 802.11n for commercial customers in particular.

Model variants

This documentation is intended for LANCOM Wireless Router users. The following models are available:

Model
restrictions

- LANCOM 1811n Wireless
- LANCOM 1821n Wireless

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 Wireless Router 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 Private Networks (VPN)
- Virtual Local Networks (VLAN)
- Wireless networks (WLAN)
- Voice communication in computer networks with Voice over IP (VoIP)
- Backup solutions
- LANCAPI
- Further server services (DHCP, DNS, charge management)

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

This documentation was created by ...

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

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

info@lancom.eu



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

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

Information symbols



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



Important instruction that should be observed.



Additional information that may be helpful but is not essential.

Contents

1 Introduction	10
1.1 What is a wireless LAN?	10
1.1.1 Modes of operation of wireless LANs and access points	11
1.2 Wireless LANs in accordance with 802.11n	11
1.2.1 Advantages of 802.11n	12
1.2.2 Compatibility with other standards	13
1.2.3 The physical layer	13
1.2.4 The MAC layer	19
1.3 What can your LANCOM Wireless Router do?	21
2 Installation	25
2.1 Package contents	25
2.2 System requirements	26
2.2.1 Configuring the LANCOM devices	26
2.2.2 Operating access points in managed mode	26
2.3 Status displays and interfaces	26
2.3.1 Device connectors	33
2.4 Hardware installation	35
2.5 Software installation	37
2.5.1 Starting the software setup	37
2.5.2 Which software should I install?	38
3 Basic configuration	39
3.1 Details you will need	39
3.1.1 TCP/IP settings	39
3.1.2 Configuration protection	41
3.1.3 Settings for the wireless LAN	42
3.1.4 Settings for the ISDN Connection	43
3.1.5 Charge protection	43
3.2 Instructions for LANconfig	43
3.3 Instructions for WEBconfig	45
3.4 TCP/IP settings for PC workstations	49

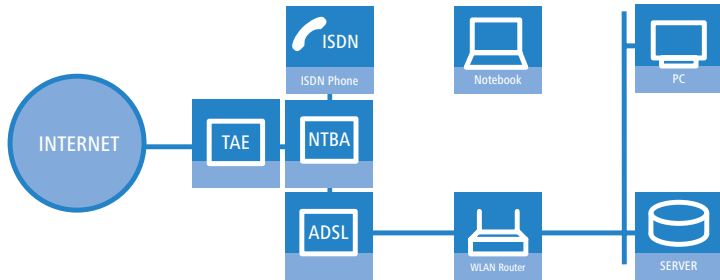
4	Setting up Internet access	50
4.1	The Internet Connection Wizard	52
4.1.1	Instructions for LANconfig	52
4.1.2	Instructions for WEBconfig	53
5	Connecting two networks	54
5.1	Which details are necessary?	55
5.1.1	General information	55
5.1.2	Settings for the TCP/IP router	57
5.1.3	Settings for NetBIOS routing	58
5.2	Instructions for LANconfig	59
5.3	1-Click-VPN for networks (site-to-site)	60
5.4	Instructions for WEBconfig	61
6	Providing dial-in access	62
6.1	Which details are necessary?	62
6.1.1	General information	63
6.1.2	Settings for TCP/IP	64
6.1.3	Settings for NetBIOS routing	65
6.2	Settings on the dial-in computer	65
6.2.1	Dialing-in via VPN	65
6.2.2	Dialing-in via ISDN	65
6.3	Instructions for LANconfig	66
6.4	1-Click-VPN for LANCOM Advanced VPN Client	66
6.5	Instructions for WEBconfig	68
7	Sending faxes with LANCAPI	69
7.1	Installation of the LANCOM CAPI Faxmodem	70
7.2	Installation of the MS Windows fax service	71
7.3	Sending a fax	72
7.3.1	Send a fax with any given office application	72
7.3.2	Send a fax with the MS Windows fax service	72

8 Security settings	74
8.1 Security in the wireless LAN	74
8.1.1 Encrypted data transfer	74
8.1.2 802.1x / EAP	77
8.1.3 LANCOM Enhanced Passphrase Security	77
8.1.4 Access control by MAC address	78
8.1.5 IPSec over WLAN	78
8.2 Tips for the proper treatment of keys and passphrases	78
8.3 Security settings Wizard	79
8.3.1 LANconfig Wizard	79
8.3.2 WEBconfig Wizard	80
8.4 The security checklist	80
9 Options and accessories	85
9.1 Optional AirLancer Extender antennas	85
9.1.1 Antenna diversity	86
9.1.2 Polarization diversity	86
9.1.3 MIMO	86
9.1.4 Installing the AirLancer Extender antennas	86
9.2 LANCOM Public Spot Option	88
10 Advice & assistance	90
10.1 No WAN connection can be established	90
10.2 Slow DSL transmission	90
10.3 Unwanted connections under Windows XP	91
10.4 Cable testing	91
11 Appendix	93
11.1 Performance data and specifications	93
11.2 Connector wiring	95
11.2.1 Ethernet interface 10/100Base-TX	95
11.2.2 ADSL interface	95
11.2.3 DSL interface	96
11.2.4 ISDN-S ₀ interface	96
11.2.5 Configuration interface (outband)	97
11.3 CE declaration of conformity	97
12 Index	98

1 Introduction

The models of the LANCOM Router series offer each a DSL or ADSL connector and also an ISDN connector. The ISDN line can be used as back-up for the DSL connection, for remote management of the router or as basis for the office communication via LANCAPI.

In addition to their function as routers between LAN and the Internet, all models of the LANCOM Router series operate also as base stations for wireless networks. With the base station you link wireless PCs and notebooks to a network, connect these devices to the existing wired LAN and enable also the wireless devices to access the Internet.



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)
- Central administration using a LANCOM WLAN Controller

1.2 Wireless LANs in accordance with 802.11n

The new wireless LAN standard IEEE 802.11n—ratified as „WLAN Enhancements for Higher Throughput“ in september 2009—features a number of

technical developments that promise up to six-times the performance in wireless LANs.

Some of the improvements refer to the physical layer (PHY), which describes the transmission of individual bits over the physical medium—in this case the air represents the physical medium. Other additions are concerned with the MAC (medium access control) that among other things governs access to the transmission medium. The two areas are treated separately below.



You can find additional information on this subject in the LCOS reference manual or in the technical papers relating to this topic.

1.2.1 Advantages of 802.11n

The new technology includes the following advantages:

■ Higher effective data throughput

The 802.11n standard includes a number of new mechanisms to significantly increase available bandwidth. Current wireless LAN standards based on 802.11a/g enable physical data rates (gross data rates) of up to 54 Mbps, which turn out to be approx. 22 Mbps net. Networks based on 802.11n **currently** achieve a gross data throughput of up to 300 Mbps (in reality approx. 120 to 130 Mbps net) – theoretically the standard defines up to 600 Mbps with four data streams. For the first time, maximum speeds exceed the 100 Mbps of cable-based Fast Ethernet networks, which are currently standard in most workplaces.

■ Improved and more reliable wireless coverage

The new 802.11n technologies do not just increase data throughput but bring about improvements in the range and reduce the wireless dead spots in existing a/b/g installations.

This results in better signal coverage and improved stability for significantly better utilization of wireless networks, in particular for users in professional environments.

■ Greater range

Data throughput generally decreases when the distance between receiver and transmitter increases. The overall improved data throughput allows wireless LANs based on 802.11n to achieve greater ranges, as a significantly stronger wireless signal is received by the Access Point over a given distance than in 802.11a/b/g networks.

1.2.2 Compatibility with other standards

The 802.11n standard is backwardly compatible to previous standards (IEEE 802.11a/b/g). However, some of the advantages of the new technology are only available when, in addition to the access points, the wireless LAN clients are also compatible with 802.11n.

In order to allow the co-existence of wireless LAN clients based on 802.11a/b/g (called "legacy clients") 802.11n access points offer special mechanisms for mixed operation, where performance increases over 802.11a/b/g are not as high. Only in all-802.11n environments is the "greenfield mode" used, which can exploit all the advantages of the new technology. In greenfield mode both access points and wireless LAN clients support the 802.11n standard, and access points reject connections with legacy clients.

1.2.3 The physical layer

The physical layers describes how data must be transformed in order for them to be transmitted as individual bits over the physical medium. In this process the following steps are performed in a wireless LAN device:

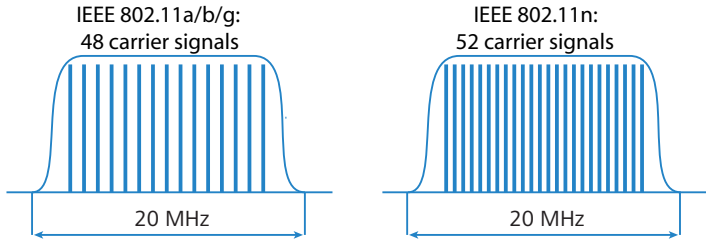
- Modulation of digital data into analog carrier signals
- Modulation of the carrier signal into a radio signal in the selected frequency band, which for a wireless LAN is either 2.4 or 5 GHz.

The second modulation step in IEEE 802.11n occurs in the same way as in conventional wireless LAN standards and is therefore not covered here. However, there are a number of changes in the way digital data are modulated into analog signals in 802.11n.

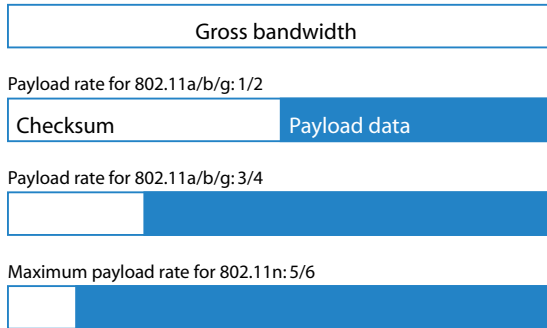
Improved OFDM modulation (MIMO-OFDM)

Like 802.11a/g, 802.11n uses the OFDM scheme (Orthogonal Frequency Division Multiplex) as its method of modulation. This modulates the data signal not on just one carrier signal but in parallel over several. The data throughput that can be achieved with OFDM modulation depends on the following parameters, among other things:

- Number of carrier signals: Whereas 802.11a/g uses 48 carrier signals, 802.11n can use a maximum of 52.



- Payload data rate: Airborne data transmission is fundamentally unreliable. Even small glitches in the WLAN system can result in errors in data transmission. Check sums are used to compensate for these errors, but these take up a part of the available bandwidth. The payload data rate indicates the ratio between theoretically available bandwidth and actual payload. 802.11a/g can operate at payload rates of 1/2 or 3/4 while 802.11n can use up to 5/6 of the theoretically available bandwidth for payload data.

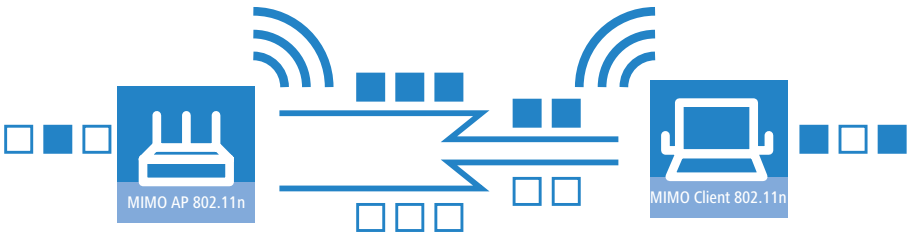


These two features increase the maximum useable bandwidth of 54 Mbps for 802.11a/g to 65 Mbps for 802.11n. This increase is not exactly spectacular, but it can be further improved by using the following features:

MIMO technology

MIMO (multiple input multiple output) is the most important new technology contained in 802.11n. MIMO uses several transmitters and several receivers to transmit up to four parallel data streams on the same transmission channel (currently only two parallel data streams have been implemented). The result is an increase in data throughput and improved wireless coverage.

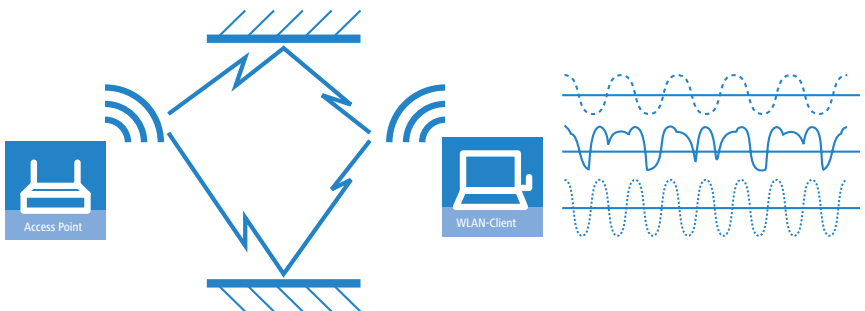
For example, the Access Point splits the data into two groups which are then sent simultaneously via separate antennas to the WLAN client. Data throughput can therefore be doubled using two transmitting and receiving antennas.



EN

But how can several signals be transmitted on a single channel simultaneously? This was considered impossible with previous WLAN applications.

Let us consider how data is transmitted in "normal" wireless LAN networks: Depending on antenna type, an Access Point's antenna broadcasts data in several directions simultaneously. These electromagnetic waves are reflected by the surrounding surfaces causing a broadcast signal to reach the WLAN client's antenna over many different paths; this is also referred to as "multipath propagation". Each of these paths has a different length meaning that individual signals reach the client with a different time delay.

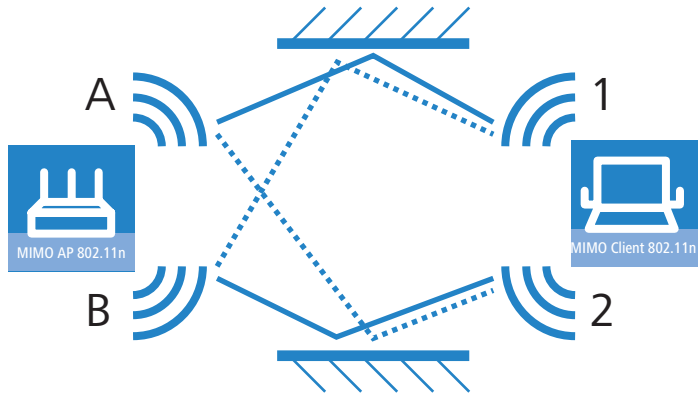


These time-delayed signals interfere with each other at the WLAN client and significantly weaken the original signal. For this reason, conventional WLAN networks should always have a direct line of sight (LOS) between transmitter and receiver in order to reduce the influence of reflections.

MIMO technology transforms this weakness in WLAN transmission into a strength that allows an enormous increase in data throughput. As mentioned

above, it is virtually impossible to transmit different signals on the same channel simultaneously as the receiver cannot distinguish between them. MIMO uses the reflection of electromagnetic waves and the associated spatial aspect to obtain a third criterion for identifying the signals.

A signal sent by transmitter A and received by receiver 1 follows a different path than a signal from transmitter B to receiver 2. Due to the different reflections and changes in polarization that both signals experience along their paths, each of these paths takes on its own characteristics. When data transmission starts, a training phase records the characteristics of the path by transmitting standardized data. Subsequently, the data received here is used to calculate which data stream the signals belong to. The receiver decides for itself which of the incoming signals is to be processed, thus avoiding loss from interference.



MIMO thus allows the simultaneous transmission of several signals over one shared medium, such as the air. Individual transmitters and receivers must be positioned a minimum distance apart from one another, although this is just a few centimeters. This separation results in differing reflections and signal paths that can be used to separate the signals.

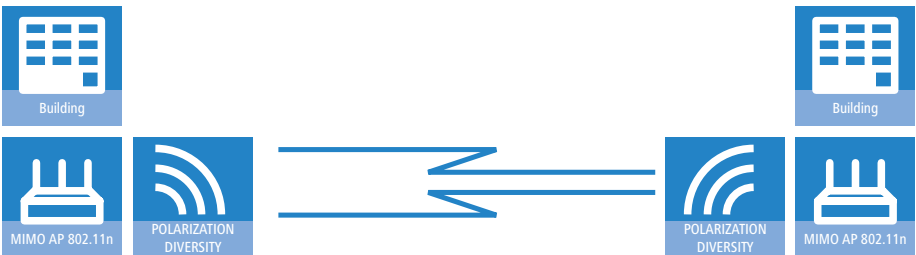
Generally speaking, MIMO can provide up to four parallel data streams, which are also called "spatial streams". However, the current generation of chips can only implement two parallel data streams as the separation of data streams based on characteristic path information demands high levels of computing power, which consumes both time and electricity. The latter tends to be undesirable particularly for WLAN systems, where attempts are often made to achieve independence from power sockets at the WLAN client or when using PoE as the electricity supply for the Access Point.

Even if the aim of four spatial streams has not yet been achieved, the use of two separate data connections results in a doubling of data throughput, which represents a true technological leap in the area of WLAN systems. Combined with the improvements in OFDM modulation, the data throughput that can be attained increases to 130 Mbps.

The short description "transmitter x receiver" expresses the actual number of transmitting and receiving antennas. 2x2 MIMO describes two transmitting and two receiving antennas.

MIMO in outdoor use

Outdoor 802.11n applications cannot use natural reflections since signal transmission usually takes place over the direct path between directional antennas. In order to transmit two data streams in parallel, special antennas are employed that use polarization channels turned through 90° to each other. These so-called "dual-slant" antennas are really two antennas in one housing. Since a third signal does not offer additional reliability, outdoor applications generally use as many antennas (or polarization channels) as there are data streams for transmission.

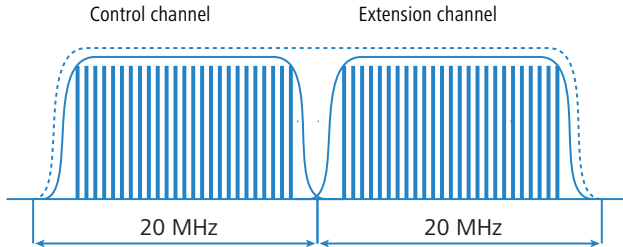


40 MHz channels

As the above explanation of OFDM modulation states, data throughput rises with an increasing number of carrier signals because this allows several signals to be transmitted simultaneously. If a channel with a bandwidth of 20 MHz supports no more than 48 (802.11a/g) or 52 (802.11n) carrier signals, the obvious choice would be to use a second channel with additional carrier signals.

This method was used in the past by a number of manufacturers (including LANCOM Systems) and was referred to as "turbo mode", allowing data rates of up to 108 Mbps. Turbo mode does not form part of the official IEEE stan-

standard but is frequently employed on point-to-point connections, for example, because compatibility to other manufacturers tends to play a secondary role. However, the success of the underlying technology has led to its incorporation into 802.11n. IEEE 802.11n uses the second transmission channel in a way that maintains compatibility to IEEE 802.11a/g devices. 802.11n transmits data over two contiguous channels. One of these assumes the task of a control channel that, among other things, handles the administration of data transmission. Concentrating these basic tasks into the control channel means that devices supporting a transmission at 20 MHz only can also be connected. The second channel is an extension that only comes into effect if the remote client also supports data transmission at 40 MHz. The use of the second channel remains optional throughout, with transmitter and receiver deciding dynamically whether one or two channels should be employed.



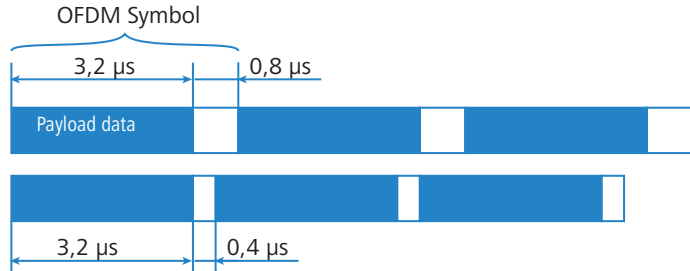
As the implementation of 40 MHz with separate control and extension channels is more efficient in the 802.11n standard than in the conventional turbo mode, more than double the amount of carrier signals can be obtained (108 in total). The maximum data throughput when using improved OFDM modulation and two parallel data streams thus rises to 270 Mbps.

Short guard interval

The final improvement of the 802.11n standard is the improvement in the chronological sequence of data transmission. A signal that is to be transmitted in a WLAN system is not broadcast at a distinct point in time but is "held up" for a certain, constant transmission period. In order to prevent interference at the receiving end, a short break is made following the transmission period before the transmission of the next signal commences. The entire duration of transmission period and break are referred to in WLAN terminology as "symbol length" and the break itself is known as the "guard interval".

IEEE 802.11a/g uses a symbol length of 4 μ s: the information transmitted on the carrier signal changes following transmission of 3.2 μ s and a break of

0.8 μs . 802.11n reduces the break between transmissions to the so-called "short guard interval" of only 0.4 μs .



Transmitting data in shorter intervals thus increases the maximum data throughput when using improved OFDM modulation, two parallel data streams and transmission at 40 MHz to 300 Mbps.

1.2.4 The MAC layer

Frame aggregation

The improvements in the physical layer brought about by the new 802.11n initially describe only the theoretical data throughput of the physical medium. However, the share of this theoretical bandwidth that is actually available for payload data is limited by two factors:

- in addition to the actual payload data, each data packet in a wireless LAN system contains additional information such as a preamble and MAC address information.
- Time is lost to the management events that occur when the transmission medium is actually accessed. Thus the transmitter must negotiate access authorization with the other receivers before transmitting each data packet (frame); further delays are caused by data packet collisions and other events.

This loss, referred to as "overhead", can be reduced by combining several data packets together to form one large frame and transmitting them together. In this process, information such as the preamble are only transmitted once for all the combined data packets and delays due to negotiating access to the transmission medium only occur at longer intervals.

The use of this method, known as frame aggregation, is subject to certain restrictions:

- As information such as MAC address only needs to be transmitted once for the aggregated frame, only those data packets intended for the same address can be combined.
- All data packets that are to be combined into a single large frame must be available at the sender at the time of aggregation—as a consequence some data packets may have to wait until enough data packets for the same destination are available with which they can be combined. This aspect may represent a significant limitation for time-critical transmissions such as voice over IP.

Block acknowledgement

Each data packet directed to a specific address (i.e. not broadcast or multicast packets) is acknowledged immediately after receipt. In this way, the transmitter is informed that the packet was received correctly and does not need to be repeated. This principle also applies to aggregated frames in 802.11n.

Two different methods are used for frame aggregation. These are not explained in detail here, but they differ in the way aggregated frames are acknowledged.

- Mac Service Data Units Aggregation (MSDUA) combines several Ethernet packets together to form one common wireless LAN packet. This packet is acknowledged only once and the acknowledgment is valid for all aggregated packets. If there is no acknowledgement the whole block is resent.
- Mac Protocol Data Units Aggregation (MPDUA) combines individual wireless LAN packets together to form one large common wireless LAN packet. In this case, each wireless LAN packet is acknowledged and the acknowledgements are combined and transmitted as a block. In contrast to MSDUA, the sender receives information about the receipt status of every single WLAN packet and can, if necessary, resend only those specific packets that were not successful.

1.3 What can your LANCOM Wireless Router do?

The following table contains a direct comparison of the properties and functions of your devices with other models

	LANCOM 1811n Wireless	LANCOM 1821n Wireless
Applications		
Expansion of the LAN through WLAN (infrastructure mode)	✓	✓
WLAN via point-to-point	✓	✓
Internet access	✓	✓
LAN-LAN coupling over VPN	✓	✓
LAN-LAN coupling over ISDN	✓	✓
RAS server (over VPN)	✓	✓
RAS server (over ISDN)	✓	✓
IP router	✓	✓
NetBIOS proxy for coupling Microsoft peer-to-peer networks over ISDN	✓	✓
DHCP- and DNS server (for LAN and DMZ)	✓	✓
N:N mapping for routing networks with the same IP-address ranges over VPN	✓	✓
Configuring LAN ports as additional WAN ports	✓	✓
Policy-based routing	✓	✓
Load balancing for bundling multiple DSL channels	4 Channels	4 Channels
Backup solutions and load balancing with VRRP	✓	✓
NAT Traversal (NAT-T)	✓	✓
DMZ with configurable IDS checks	✓	✓
PPPoE-Server	✓	✓
WAN-RIP	✓	✓
Spanning Tree Protocol	✓	✓

■ Chapter 1: Introduction

	LANCOM 1811n Wireless	LANCOM 1821n Wireless
Layer-2-QoS-Tagging	✓	✓
ISDN leased lines	✓	✓
LANCAPI server to provide office applications such as fax or answering machine via the ISDN interface.	✓	✓
WLAN		
Wireless transmission compliant with IEEE 802.11g and IEEE 802.11b	✓	✓
Wireless transmission compliant with IEEE 802.11a and IEEE 802.11h	✓	✓
Wireless transmission by IEEE 802.11n (including 40 MHz channels, packet aggregation, block acknowledgement, short guard interval)	✓	✓
Internal antennas	1	1
External antennas and connectors for AirLancer Extender antennas	2	2
Access point mode	✓	✓
Client mode	✓	✓
Managed mode for central configuration of WLAN modules by a WLAN Controller	✓	✓
Point-to-point mode (six P2P paths can be defined per WLAN interface)	✓	✓
Turbo mode: Double the bandwidth at 2.4 GHz and 5 GHz.	✓	✓
Super AG incl. hardware compression and bursting	✓	✓
Multi SSID	✓	✓
Roaming function	✓	✓
802.11i / WPA with hardware AES encryption	✓	✓
WEP encryption (up to 128-bit key lengths, WEP152)	✓	✓
IEEE 802.1x/EAP	✓	✓
MAC address filter (ACL)	✓	✓
Individual passphrases per MAC address (LEPS)	✓	✓
Closed-network function	✓	✓

	LANCOM 1811n Wireless	LANCOM 1821n Wireless
Integrated RADIUS server	✓	✓
VLAN	✓	✓
QoS für WLAN (IEEE 802.11e, WMM/WME)	✓	✓
WAN connections		
Connection for DSL or cable modem	✓	✓
Integrated ADSL modem (ADSL2+ ready)		✓
ISDN S ₀ bus in multi device-mode or in point-to-point mode with automatic D-channel protocol identification. Supports static and dynamic channel bundling per MLPPP and BACP as well as Stac data compression (Hi/fn)	✓	✓
LAN connection		
Separate FastEthernet LAN ports, individually switchable, e.g. as LAN switch or separate DMZ ports; auto crossover. Alternatively switchable as a WAN interface for connecting SDSL modems.	4	4
USB connector		
USB 2.0 host port (full speed: 12 Mbps) for connecting a USB printer and for future extensions	✓	✓
Security functions		
IPSec encryption via external software (VPN client)	✓	✓
5 integrated VPN tunnels for secure network connections	✓	✓
IPSec encryption in hardware (optional; activated with the VPN-25 option)	✓	✓
IP masquerading (NAT, PAT) to conceal individual LAN workstations behind a single public IP address.	✓	✓
Stateful-inspection firewall	✓	✓
Firewall filter for blocking individual IP addresses, protocols and ports	✓	✓
MAC address filter regulates, for example, LAN-workstation access to the IP routing function	✓	✓
Protection of the configuration from brute-force attacks.	✓	✓
Configuration		

■ Chapter 1: Introduction

	LANCOM 1811n Wireless	LANCOM 1821n Wireless
Configuration with LANconfig or via web browser; additional terminal mode for Telnet or equivalent terminal programs; SNMP interface and TFTP server function.	✓	✓
Remote configuration via ISDN (with ISDN PPP connections, e.g. via Windows Dial-Up Networking).	✓	✓
Serial configuration interface	✓	✓
Call-back function with PPP authentication mechanisms allowing only predefined ISDN call numbers	✓	✓
FirmSafe for no-risk firmware updates	✓	✓
Optional software extensions		
LANCOM VPN Option with 25 active tunnels for protection of network couplings and hardware acceleration	✓	✓
LANCOM Public Spot Option	✓	✓
LANCOM Next Business Day Service Extension CPE, item no. 61411	✓	✓
LANCOM 2-Year Warranty Extension CPE, item no.. 61414	✓	✓

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 1811n Wireless DSL	LANCOM 1821+ Wireless ADSL
Power adapter	✓	✓
LAN connector cable (green plugs)	✓	✓
WAN connector cable (dark blue plugs)	✓	
ADSL connector cable (transparent plugs)		✓
ISDN connector cable (light blue plugs)	✓	✓
2 external screw-on single band antennas (2,4 GHz) with reverse SMA connection	✓	✓
Connector cable for the configuration interface	✓	✓
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").

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

2.3 Status displays and interfaces

Meanings of the LEDs

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

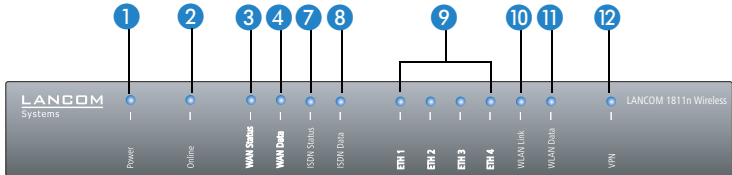
- **Blinking** means, that the LED is switched on or off at regular intervals in the respective indicated colour.
- **Flashing** means, that the LED lights up very briefly in the respective colour and stay then clearly longer (approximately 10x longer) switched off.
- **Inverse flashing** means the opposite.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

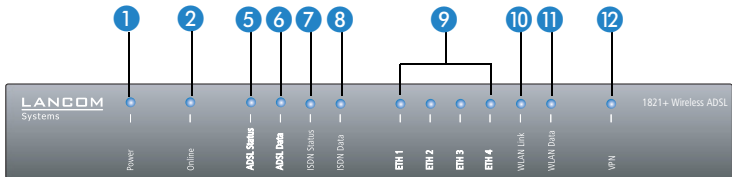
Front side

The LANCOM Wireless Routers have status displays on the front panel.

LANCOM 1811n
Wireless



LANCOM 1821n
Wireless



Top

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



■ Chapter 2: Installation

1 Power

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

Off		Device switched off
Green	blinking	Self-test after power-up
Green	On (permanently)	Device operational
Red/green	Blinking alternately	Device insecure: Configuration password not set
Orange/green	In the housing cover; blinking alternately with the online LED	At least one WLAN module is in managed mode and has not found a WLAN Controller yet. The corresponding WLAN module(s) is/are switched off until a WLAN Controller is found to supply a configuration, or until being switched manually into another operating mode.
Orange /red	In the housing cover; blinking alternately with the online LED	At least one WLAN module is in managed mode and has found a WLAN Controller. However, the WLAN Controller cannot assign a configuration because the firmware and/or the device's loader version is not compatible with the WLAN Controller.
Red	blinking	Time or charge limit on online connections has been reached



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

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

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

There are three ways to remove the lock:

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

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

With WEBconfig, charge protection and all parameters are to be found under **LCOS menu tree ▶ Setup ▶ Charges ▶ Reset budgets**.



Signal that a charge or time limit has been reached

2 Online

The online LED displays the general status of all WAN interfaces:

Off		No active connection
Green	Flashing	Opening the first connection
Green	Inverse flashing	Opening an additional connection
Green	On (permanently)	At least one connection is established
Red	On (permanently)	Error establishing the last connection
Orange/ green	In the housing cover; blinking alternately with the power LED	At least one WLAN module is in managed mode and has not found a WLAN Controller yet. The corresponding WLAN module(s) is/are switched off until a WLAN Controller is found to supply a configuration, or until being switched manually into another operating mode.
Orange / red	In the housing cover; blinking alternately with the power LED	At least one WLAN module is in managed mode and has found a WLAN Controller. However, the WLAN Controller cannot assign a configuration because the firmware and/or the device's loader version is not compatible with the WLAN Controller.

■ Chapter 2: Installation

- 3** WAN Status
(only LANCOM
1811n
Wireless)

Connection status of the WAN connection:

off		not connected
green	blinking	Establishing first connection
green	invers flashing	Establishing further connection
green	constantly on	At least one connection established
red	constantly on	Error while establishing connection

- 4** WAN Data
(only LANCOM
1811n
Wireless)

Data traffic via the WAN connection:

off		No network device connected
green	constantly on	Connection to network device operational, no data traffic
green	flickering	Data traffic (send or receive)

- 5** ADSL status

Information on connection status at the ADSL connector:

Off		Interface deactivated
Green	Blinking/flashing	Handshake/training
Green	Permanently	Synchronization successful
Red	Flickering	Error (CRC error, framing error, etc.)
Red	On (permanently)	No synchronization, searching for remote station
Red/ orange	Blinking	Hardware error

- 6** ADSL data

Information on data traffic at the ADSL connector:

Off		No logical connection
Green	Blinking	Opening the first connection
Green	Inverse flashing	Opening an additional connection
Green	Permanently	At least one logical connection is established
Green	Inverse flickering	Data traffic (send or receive)

7 ISDN status

Information on connection status at the ISDN S_0 connector:

Off		Not connected or no S_0 voltage (no error message)
Green	Blinking	D-channel initialization (establishing contact to provider)
Green	On (permanently)	D-channel operational
Red	Flickering	D-channel error
Red	On (permanently)	D-channel activation failed



If the ISDN status LED goes off automatically, this does not indicate an error at the S_0 bus. It is in fact because several ISDN connections and PBXs switch the S_0 bus into power-saving mode after a certain period of inactivity. When needed, the S_0 bus automatically reactivates and the ISDN status LED illuminates in green.

8 ISDN Data

Status display for both ISDN B channels:

off		No connection established
green	Blinking	Dialling
green	Flashing	Establishing first connection
green	Inverse flashing	Establishing further connection
green	Constantly on	Connection established via B channel
green	Flickering	Data traffic (send or receive)

9 ETH

LAN connector status in the integrated switch: LAN connector status:

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

10 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.
Red	Blinking	Hardware error in the WLAN module

11 WLAN Data

Provides information about the data traffic at the internal WLAN module.

The following can be displayed for WLAN data:

Green	Flickering	TX data traffic.
Red	Flickering	Error in wireless LAN (TX error, e.g. transmission error due to a poor connection)
Red	Blinking	Hardware error in the WLAN module

12 VPN

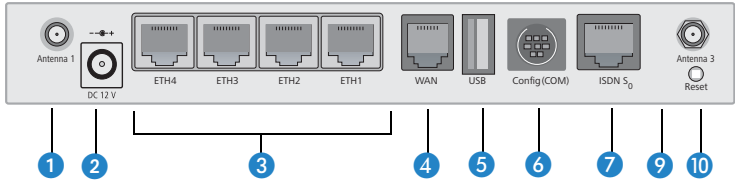
Status of a VPN connection.

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

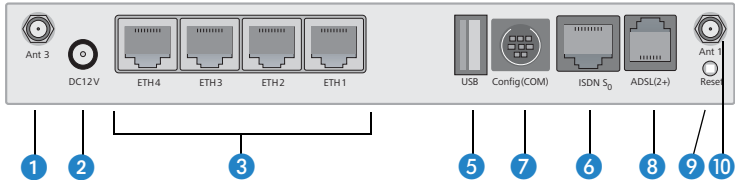
2.3.1 Device connectors

The connections and switches of the router are located on the back panel:

LANCOM 1811n
Wireless




LANCOM 1821n
Wireless



1 Connector for antenna 1 (LANCOM 1811n Wireless) respectively antenna 3 (LANCOM 1821n Wireless) in MIMO mode.

2 Connection for the included power adapter

 Antenna 2 is an internal antenna that does not have an external connector.

3 Second Ethernet socket (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).

LANCOM 1811n
Wireless

4 WAN connector

5 USB connector (USB host)

6 ISDN/S₀ port

7 Serial configuration port

LANCOM 1821n
Wireless

8 ADSL port

9 Reset switch

10 Connector for antenna 3 (LANCOM 1811n Wireless) respectively antenna 1 (LANCOM 1821n Wireless) in MIMO mode.

Reset button functions

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

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

■ Reset button

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

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



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

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

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



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



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

2.4 Hardware installation

The installation of the LANCOM Router base station takes place in the following steps:

- ① **Antennas** – screw the antennas supplied to the back of the LANCOM Wireless Router. Depending on how the antennas are to be used, the 'Antenna Grouping' parameter may need to be configured in order to provide the desired MIMO behavior (→'Advanced Wireless LAN Configuration').



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



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

- ② **LAN** – First connect the LANCOM Router base station to your LAN or to an individual PC. For that purpose, plug the included network cable (green plugs) into the LAN connector of the device ③ and the other end into a free network connecting socket of your local network, into a free socket of a hub/switch or into the network socket of an individual PC.

The LAN connector identifies automatically the transfer rate (10/100 Mbps) of the connected network device (autosensing). A parallel connection of devices with different speeds and types is possible.



You should never have more than one unconfigured LANCOM Router in a network segment at any given time. All unconfigured LANCOM Router devices use the same IP address (with the final digits '254'), which would result in an address conflict. To avoid problems, always configure multiple LANCOM Router devices one at a time, immediately assigning each device a unique IP address (one that does not end with '254').

- ③ **DSL** – connect the WAN interface ④ to the DSL modem socket using the supplied DSL connector cable (dark blue plugs).


 ■ Chapter 2: Installation

1821+ only


- ④ **ADSL** – connect the ADSL interface ④ to the splitter using the supplied ADSL connector cable (transparent plugs).
- ⑤ **ISDN** – to connect the LANCOM Router to the ISDN, plug one end of the supplied ISDN connector cable (light blue plugs) in the ISDN/S₀ port ⑤ of the router and the other end into an ISDN/S₀ multi-device mode or point-to-point mode connection.

1821+ only


- ⑥ **USB port** – you may optionally connect printers with USB connector to the LANCOM and make them available to the entire network. The LANCOM provides a print server to manage the printing jobs from the network. Supported protocols are RawIP and LPR/LPD.

 Further information about configuration of the print server can be found in the LCOS reference manual.

- ⑦ **Configuration port** – you may optionally connect the router directly to the serial port (RS-232, V.24) of a PC. Use the cable supplied for this purpose. Connect the configuration port of the LANCOM ⑥ with a free serial port of the PC.
- ⑧ **Connect to power** – Connect socket ① of the unit to a power supply using the included power adapter.

 Use the supplied power supply unit only! Using an unsuitable power supply unit may cause damage or injury.

- ⑨ **Operational?** – After a short device self-test the Power LED will be permanently lit. Green LAN LEDs indicate the LAN sockets that have functioning connections.

 Devices with integrated ADSL modems can become very warm during operation. For these models, environmental temperatures are not to exceed 35°C. Sufficient ventilation is of vital importance. Do not stack the devices and do not expose them to direct sunlight.

2.5 Software installation

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



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

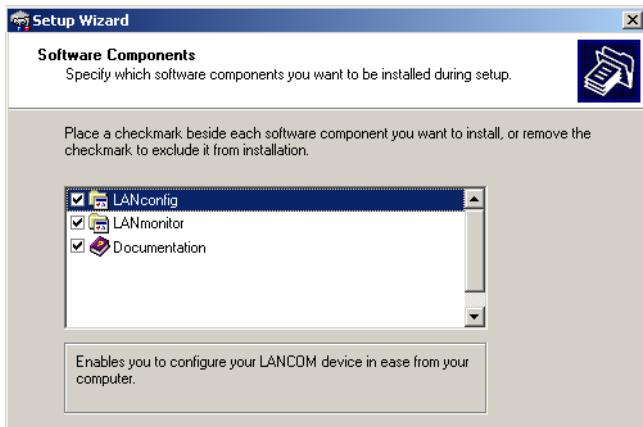
2.5.1 Starting the software setup

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



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

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



2.5.2 Which software should I install?

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

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

3 Basic configuration

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

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

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

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

3.1 Details you will need

The Basic Settings Wizard is used to set the LANCOM Wireless Routers 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
- DSL connection details
- Configuring toll protection
- 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 Wireless Router
- Setting up a new network

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

Should you still configure manually?

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

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

Required information for manual TCP/IP configuration

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

- **DHCP mode of operation**
 - Off: The IP addresses required must be entered manually.

- Server: The LANCOM Wireless Router operates as DHCP server in the network; as a minimum its own IP address and the network mask must be assigned.
- Client: The LANCOM Wireless Router obtains its address information from another DHCP server; no address information is required.
- **IP address and network mask for the LANCOM Wireless Router**
Assign the LANCOM Wireless Router 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 Wireless Router'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 Wireless Router. 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.

3.1.4 Settings for the ISDN Connection

If you wish to use the ISDN connection you can make the following settings:

- One or more ISDN MSNs on which the router should answer calls. MSNs are ISDN call numbers that your telephone company allocates to you. They are usually specified without a prefix. The numbers specified are only important for router functions (LAN-LAN coupling, RAS), but not for the remote configuration and LANCOM VPN Option.
- A prefix to access the public telephone network. It is normally only required when connecting via an ISDN PBX. Usually this is a '0'. This prefix is used for all outgoing calls.
- Finally you should know whether the telephone company transmits an ISDN metering pulse. This can be evaluated by the LANCOM Router for cost budgets and the accounting function.

3.1.5 Charge protection

Charge protection prevents DSL connections being established above and beyond a predefined amount and therefore protects you from unexpectedly high connection charges.

If you operate the LANCOM Router on a DSL link that is charged on a time basis you can set the maximum connection time in minutes.

The budget can be completely deactivated by entering a value of '0'.

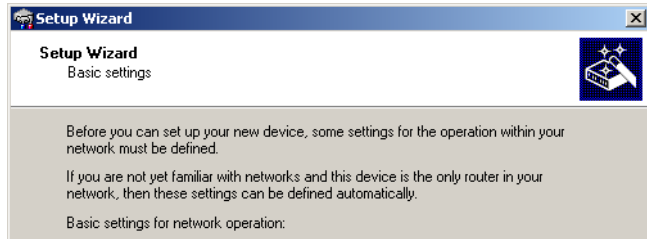



In the basic settings, charge protection is set to a maximum value of 600 minutes in any seven day period. Please adjust this parameter to match your own requirements, or deactivate charge protection if you have agreed a tariff for unlimited traffic with your provider.


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 manually search for new devices at all interfaces (if the LANCOM Wireless Router is connected via the serial configuration interface) or in the network (**File ► Find devices**).

 If you cannot access an unconfigured LANCOM Wireless Router, 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 .

-  Give the LANCOM an address from the applicable IP address range. Confirm with **Next**.
-  In the window that follows, you first set the password to the configuration. Entries are case sensitive and should be at least 6 characters long.
You also define whether the device can be configured from the local network only, or if remote configuration via WAN (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.

-  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**.
-  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.

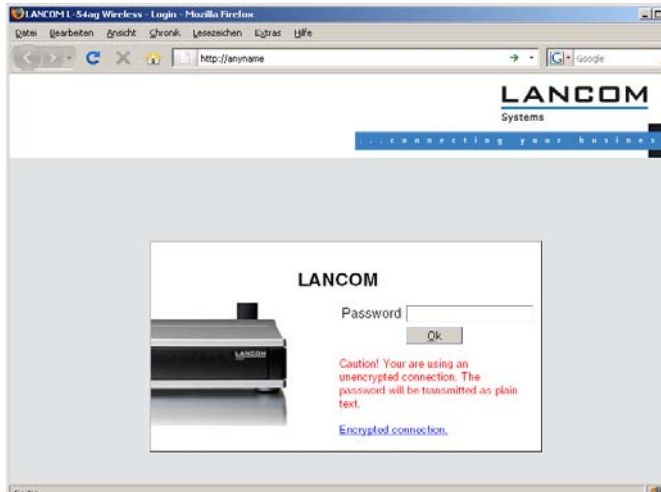
Not for centrally managed LANCOM Wireless Routers or LANCOM Access Points

Network without a DHCP server

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



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

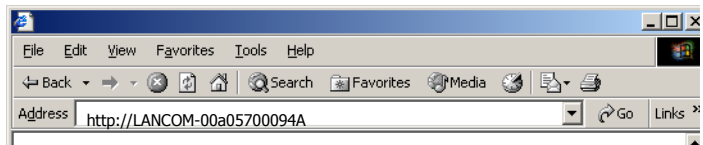


If the configuration computer does not retrieve its IP address from the LANCOM DHCP server, it determines the current IP address of the computer (with **Start ▶ Run ▶ cmd** and command **ipconfig** at the prompt under Windows 2000 or Windows XP or Windows Vista, with **Start ▶ Run ▶ cmd** and command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

Network with DHCP server

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

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



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

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

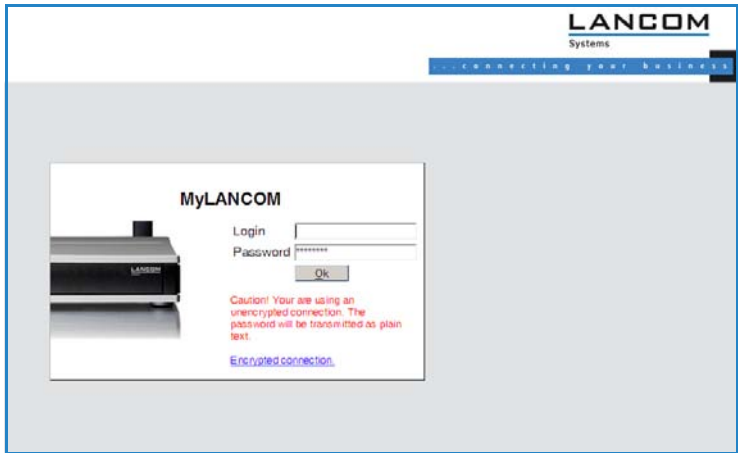
Login

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

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

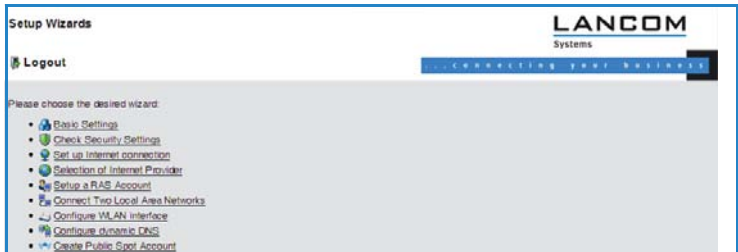


As an alternative, the login dialog provides a link for an encrypted connection over HTTPS. Always use the HTTPS connection for increased security whenever possible.



Setup Wizards

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



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

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 Wireless Router 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

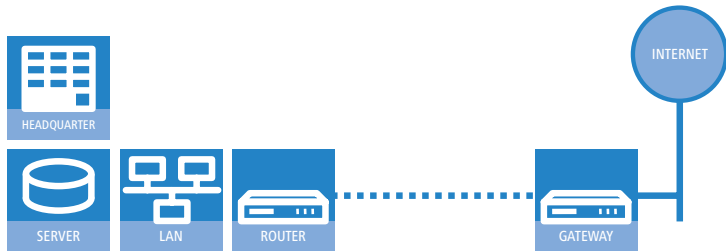
If IP addresses in a network are statically assigned, then the IP address of the LANCOM is to be set as the standard gateway and DNS server in the TCP/IP configuration of each PC in the LAN.



Further information and help on the TCP/IP settings for your LANCOM Wireless Router 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 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 any WAN connector, i.e. via DSL or ISDN (where available). Internet access via ISDN can be used to backup a DSL connection.



Which WAN interface?

Setting up the Internet access is carried out with the help of a convenient Wizard. In the first step you select the WAN interface that is to be used for establishing the Internet connection.

To establish an Internet connection via the DSL interface, an external ADSL modem first has to be connected to one of the device's ETH ports. When setting up the Internet access, you define which ETH port the ADSL modem has been connected to.

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.

■ DSL

- Protocol: PPPoE, PPTP or Plain Ethernet (IPoE or IPoEoA)

- Additional to Plain Ethernet: Your own public IP address with net mask (not to be confused with the private LAN IP address), default gateway and DNS server. If the provider supports DHCP you can automatically retrieve these IP parameters.
- User name and password
- **ISDN**
 - Dial-in telephone number
 - User name and password

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.
- Dynamic channel bundling (ISDN only)
 - If required, the second ISDN B-channel can be activated and added to the connection. The result is that bandwidth is doubled. However, under certain circumstances the connection fees may double as well. Furthermore your ISDN connection would be engaged, so preventing any other incoming or outgoing telephone calls from being made.
- Data compression (ISDN only)
 - This enables data transfer rates to be increased even further.

Creating a backup connection to the Internet

The most common utilization of the backup solution is to provide an auxiliary Internet connection. When setting up an Internet connection, an additional option is to create a second connection to the Internet via an alternative

WAN interface. If the primary Internet access is set up to operate via the ADSL interface, you can set up your backup connection to operate via UMTS or ISDN.

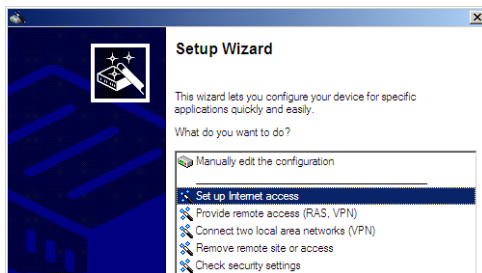


When configuring the backup connection you can set up an alternative provider, if available. This allows you not only to overcome problems with the physical line, but also problems in your provider's own network as well.

4.1 The Internet Connection Wizard

4.1.1 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 After entering all of the necessary data the Wizard then offers you the option of setting up a backup connection. Select the corresponding WAN interface to be used for the backup connection and enter the relevant access data for the Internet connection.

The Wizard then sets up the alternative Internet access and at the same time creates the necessary entries into the backup table and also in the PPP table for checking the Internet connection.

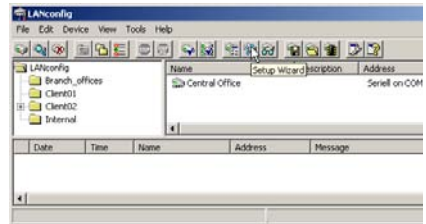


Please be aware that in the case of backup via UMTS, some of the services provided over the main Internet connection may not be available. Some UMTS service providers either prevent the use of VPN tunnels or VoIP applications or only allow them after payment of additional fees. Other providers assign IP addresses from an internal address range, so preventing applications that rely on public IP addresses from working. Please ask your UMTS provider for information on limitations that may apply.

- ⑥ The Wizard will inform you as soon as the entries are complete. Close the configuration with **Finish**.

LANconfig: Fast starting of the Setup Wizards

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



4.1.2 Instructions for WEBconfig

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

5 Connecting two networks

Network connectivity, also known as LAN-LAN connectivity, with the LANCOM Router is used for interconnecting two local area networks. LAN-LAN connectivity can be implemented in two basic ways:

- **VPN:** Connecting LANs over VPN ensures that the Internet-based connection between the two LANs has high-security protection. Each LAN must be equipped with a VPN-capable router.
- **ISDN:** Connectivity based on ISDN uses a direct connection between the two LANs via an ISDN connection. Each LAN must be equipped with a router with an ISDN interface.

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

Always configure both ends

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



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

Security aspects

Of course your LAN has to be protected from unauthorized access. For this reason, a LANCOM provides a range of security mechanisms that offer an outstanding level of protection.

- **VPN:** VPN-based connectivity relies on IPsec for transferring data. The encryption methods employed are 3-DES, AES or Blowfish
- **ISDN:** Security for ISDN-based connectivity relies on password protection, a check of the ISDN number, and the call-back function.



The ISDN call-back function cannot be set up by Wizard, but in the manual configuration only. Refer to the reference manual for information on this.

5.1 Which details are necessary?

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

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

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

5.1.1 General information

The following information is required for setting up LAN-LAN connectivity. The first column shows whether the information for network connectivity is required via VPN (simple method with pre-shared keys) and/or via ISDN.



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

Connectivity	Entry	Gateway 1		Gateway 2
VPN	Does the remote site have an ISDN connection?	Yes/No		Yes/No
VPN	Type of local IP address	Static/dynamic		Static/dynamic
VPN	Type of remote IP address	Static/dynamic		Static/dynamic
VPN + ISDN	Name of the local device	'MAIN OFFICE'		'BRANCH OFFICE'
VPN + ISDN	Name of the remote device	'BRANCH OFFICE'		'MAIN OFFICE'
VPN + ISDN	ISDN-calling number of the remote device	(0123) 123456		(0789) 654321
VPN + ISDN	ISDN calling line ID of the remote device	(0789) 654321		(0123) 123456
VPN	Password for the secure transmission of the IP address	'Secret'		'Secret'
VPN	Shared Secret for encryption	'Secret'		'Secret'
VPN	IP address of remote device	'10.0.2.100'		'10.0.1.100'
VPN + ISDN	IP-network address of the remote network	'10.0.2.0'		'10.0.1.0'
VPN + ISDN	Netmask of the remote network	'255.255.255.0'		'255.255.255.0'

Connectivity	Entry	Gateway 1	Gateway 2
VPN + ISDN	Domain descriptor in the remote network	'branch_office.com-pany'	'main_office.com-pany'
VPN	Hide own stations when accessing remote network (extranet VPN)?	Yes/No	Yes/No
ISDN	TCP/IP routing for accessing the remote network?	Yes/No	Yes/No
VPN + ISDN	NetBIOS routing for accessing the remote network?	Yes/No	Yes/No
VPN + ISDN	Name of a local workgroup (for NetBIOS only)	'workgroup1'	'workgroup2'
ISDN	Data compression	On/off	↔ On/off
ISDN	Channel bundling	On/off	↔ On/off

Notes on the different settings:

- If you own device features an **ISDN connection**, the Wizard will ask you whether the remote site also has one.
- For VPN connections over the Internet, the type of IP address at each end must be specified. There are two **types of IP address**. Static and dynamic. The differences between these two IP address types are explained in the Reference Manual.

The Dynamic VPN function makes it possible to establish VPN connections between gateways with dynamic IP addresses, and not only between gateways with static (fixed) IP addresses. An ISDN connection is required to actively establish VPN connections to remote sites that use dynamic IP addresses.

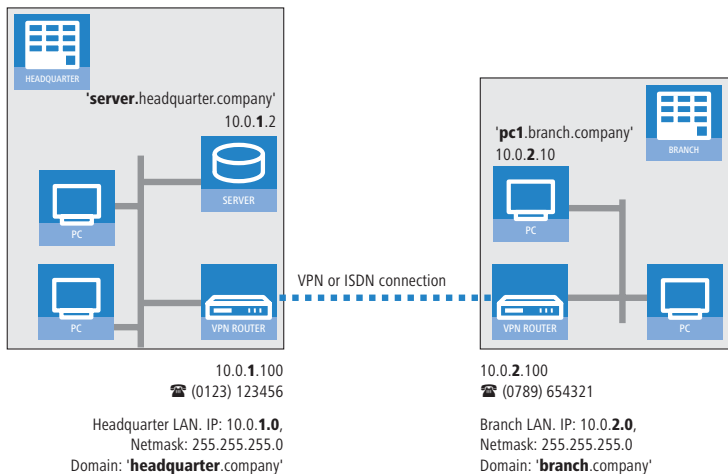
- If you have not yet given a name to your LANCOM, the Wizard will ask you to enter a new **name for your device**. Entering a name will cause your LANCOM to be renamed. Ensure that you give different names to the two remote devices.
- The **name of the remote site** is required for identifying the devices.
- In the field **ISDN number** the telephone number of the remote ISDN site is specified. Enter the full telephone number for the remote site, including all necessary prefixes (e.g. area codes).
- The **ISDN calling line ID** specified is used to identify and authenticate the caller. If a LANCOM Router is called, it compares the ISDN calling line ID entered for the remote site to the ID that is actually received over the D

channel from the caller. An ISDN ID generally consists of the country code and an MSN.

- The **password for the ISDN connection** is an alternative to the ISDN calling line ID. This is used to authenticate the caller if no ISDN calling line ID is received. The password must be entered identically at both ends. It is used for calls in both directions.
- The **shared secret** is the central password for the VPN connection's security. It must be entered identically at both ends.
- Data compression improves transmission speeds without incurring extra costs. This is completely different to the bundling of two ISDN channels by MLPPP (**M**ulti**L**ink-**P**PP): This doubles the bandwidth, although this generally doubles the connection costs as well.

5.1.2 Settings for the TCP/IP router

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



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

DNS access to the remote LAN

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

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



The domain can only be specified in the LANconfig Wizard. With WEBconfig, the necessary changes are made later in the manual configuration. Refer to the LANCOM Router reference manual for more detailed information.

VPN extranet

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

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

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

5.1.3 Settings for NetBIOS routing

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

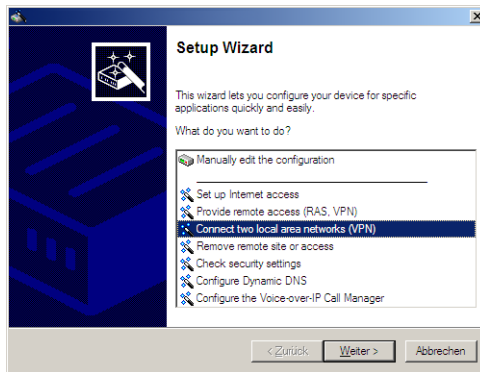


Remote Windows workgroups do not appear in the Windows network environment, but they can be contacted directly (e.g. by searching for a computer of known name).

5.2 Instructions for LANconfig

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

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



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

Ping – the quick test of a TCP/IP connection

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

IPX connections can be tested by searching for a remote Novell server. NetBIOS connections can be tested by searching a computer in the remote Windows workgroup.

```

C:\>ping 10.0.2.0

Pinging 10.0.2.0 with 32 bytes of data:

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

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

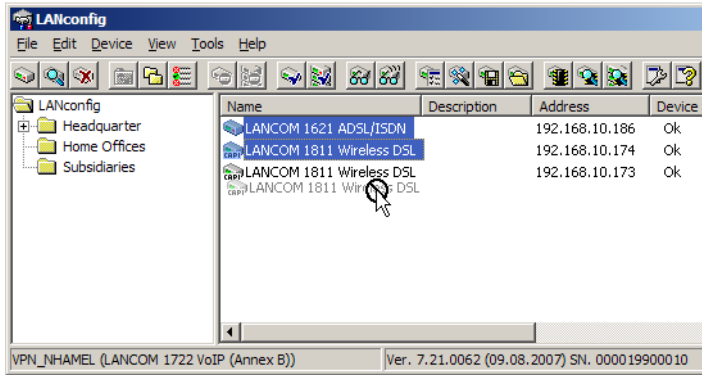
C:\>

```

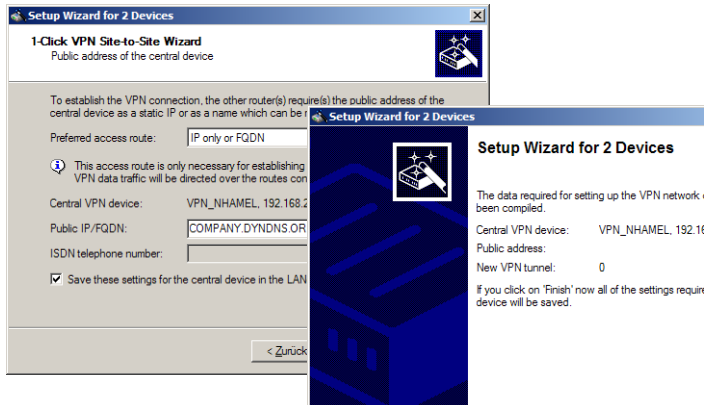
5.3 1-Click-VPN for networks (site-to-site)

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


- ① In LANconfig, mark the routers at branch offices which are to be coupled to a central router via VPN.
- ② Use drag&drop by mouse to place the devices onto the entry for the central router.




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



- ④ Select whether connection establishment is to take place via the name or IP address of the central router, or via an ISDN connection. Enter the address or name of the central router, or its ISDN number.
- ⑤ The final step is to define how the networks are to intercommunicate:
 - The INTRANET at headquarters only is to be provided to the branch offices.
 - All private networks at the branch offices can also be connected to one another via headquarters.

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

5.4 Instructions for WEBconfig

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

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

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

6 Providing dial-in access

Your LANCOM can be set up with dial-in access accounts enabling individual computers to dial-in to your LAN and fully participate in the network for the duration of the connection. This service is called RAS (**R**emote **A**ccess **S**ervice). RAS access can be implemented in two basic ways:

- **VPN:** RAS access via VPN provides a highly secure Internet-based connection between the LAN and the dial-in computer. The router in the LAN must support VPN; the dial-in computer needs any form of Internet access and a VPN client.
- **ISDN:** RAS access via ISDN provides a direct connection between the LAN and the dial-in computer over an ISDN phone line. The router in the LAN needs an ISDN interface. The dial-in computer needs an ISDN adapter or an ISDN modem. The protocol of data transfer is PPP. This ensures that all normal devices and operating systems are supported.

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

Security aspects

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

For this reason, a LANCOM provides a range of security mechanisms that offer an outstanding level of protection.

- **VPN:** VPN-based connectivity relies on IPsec for transferring data. The encryption methods employed are 3-DES, AES or Blowfish
- **ISDN:** Security for ISDN-based connectivity relies on password protection, a check of the ISDN number, and the call-back function.



The ISDN call-back function cannot be set up by Wizard, but in the manual configuration only. Refer to the reference manual for information on this.

6.1 Which details are necessary?

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

6.1.1 General information

The following information is required for setting up RAS access. The first column shows whether the information for RAS access is required via VPN (simple method with pre-shared keys) and/or via ISDN.



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

Connectivity	Entry
VPN + ISDN	User name
VPN + ISDN	Password
VPN	Shared Secret for encryption
VPN	Hide own stations when accessing remote network (extranet VPN)?
ISDN	Incoming caller ID number of the dial-in computer
ISDN	TCP/IP routing for accessing the remote network?
VPN + ISDN	IP address(es) for one or more dial-in computer(s): Fixed or dynamic from the IP address pool
VPN + ISDN	NetBIOS routing for accessing the remote network?
VPN + ISDN	Name of a local workgroup (for NetBIOS only)

Notes on the different settings:

- **User name and password:** This access data serves to identify the user when dialing in.
- **Incoming number:** The optional ISDN calling line ID is used by the LANCOM Router for additional user authentication. This security function should not be employed if the user will be dialing-in from various ISDN connections.



You will find information on the other parameters required for RAS access in the chapter 'Connecting two networks'.

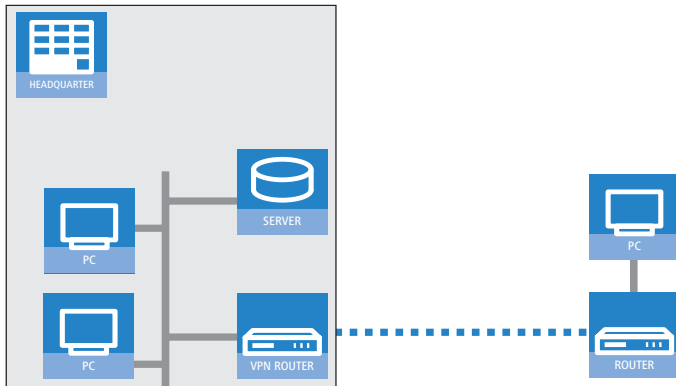
The ISDN calling line ID (CLI)

The ISDN Calling Line Identity (CLI) is the phone number of the calling party as transmitted to the called party. This is a number generally made up of the national dial code and an MSN.

The CLI is ideal for authentication for two reasons: It is difficult to manipulate. It is transmitted free of charge via the ISDN D-channel.

6.1.2 Settings for TCP/IP

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



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

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

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

6.1.3 Settings for NetBIOS routing

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



The connection is not established automatically. The RAS user first has to manually establish a connection to the LANCOM Router with the help of Dial-Up Networking. Once the connection has been established, the computer can access and search the other network (click on **Search ► Computer**, do not use the Network Neighborhood).

6.2 Settings on the dial-in computer

6.2.1 Dialing-in via VPN

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

- Internet access
- A VPN client

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

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

6.2.2 Dialing-in via ISDN

A number of settings are required by the dial-in computer. This example is based on a Windows computer.

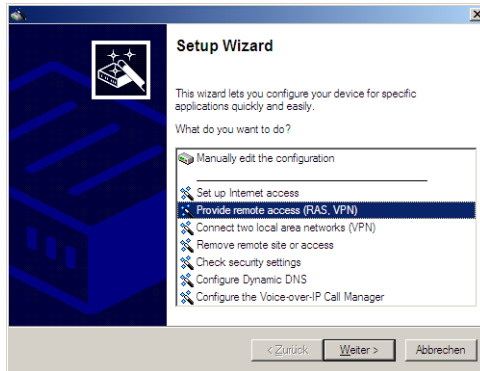
- Dial-Up Networking (or any other PPP client) installed correctly.
- Network protocol (TCP/IP, IPX) installed and associated with the dial-up adapter
- New connection in Dial-Up Networking with the phone number of the router
- Terminal adapter or ISDN card set up for PPPHDLC
- PPP selected and the dial-up server type, 'Activate compression in software' and 'Request encrypted password' switched off.
- Select the required network protocols (TCP/IP)
- Additional TCP/IP settings
 - Assignment of IP address and name server address activated

- 'IP header compression' deactivated

With these settings, a PC can dial-in to the remote LAN and access the network resource in the usual manner.

6.3 Instructions for LANconfig

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



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

6.4 1-Click-VPN for LANCOM Advanced VPN Client

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

- ① Use LANconfig to start the 'Set up a RAS Account' wizard and select the 'VPN connection'.

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



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

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

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

- Gateway: If defined in the LANCOM VPN Router, a DynDNS name is used here, or alternatively the IP address
- FQDN: Combination of the name of the connection, a sequential number and the internal domain in the LANCOM VPN Router.
- Domain: If defined in the LANCOM VPN Router, the internal domain is used here, or alternatively a DynDNS name or IP address
- VPN IP networks: All IP networks defined in the device as type 'Intranet'.
- Preshared key: Randomly generated key 16 ASCII characters long.
- Connection medium: The LAN is used to establish connections.
- VoIP prioritization: VoIP prioritization is activated as standard.
- Exchange mode: The exchange mode to be used is 'Aggressive Mode'.
- IKE config mode: The IKE config mode is activated, the IP address information for the LANCOM Advanced VPN Client is automatically assigned by the LANCOM VPN Router.

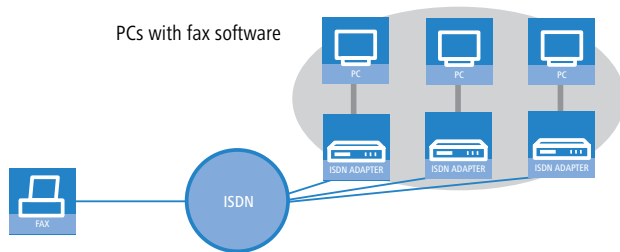
6.5 Instructions for WEBconfig

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

7 Sending faxes with LANCAPI

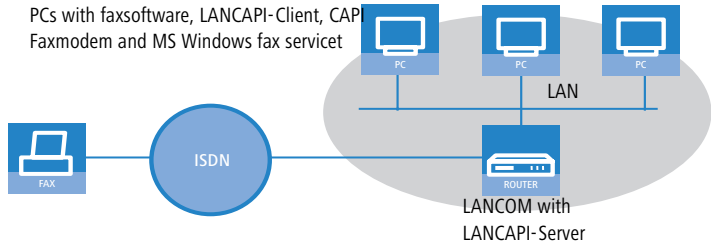
LANCAPI from LANCOM Systems is a special version of the popular CAPI interface. CAPI (Common ISDN Application Programming Interface) establishes the connection between ISDN adapters and communications programs. For their part, these programs provide the computers with office communications functions such as a fax machine or answering machine.

The main advantages of using LANCAPI are economic. LANCAPI provides all Windows workstations integrated in the LAN (local-area network) with unlimited access to office communications functions such as fax machines, answering machines, online banking and eurofile transfer. All functions are supplied via the network without the necessity of additional hardware at each individual workstation, thus eliminating the costs of equipping the workstations with ISDN adapters or modems. All you need do is install the office communications software on the individual workstations.



With LANCAPI by LANCOM it is possible to send faxes comfortably from your workstation PC, without having connected a fax device. To do so, you need to install several components:

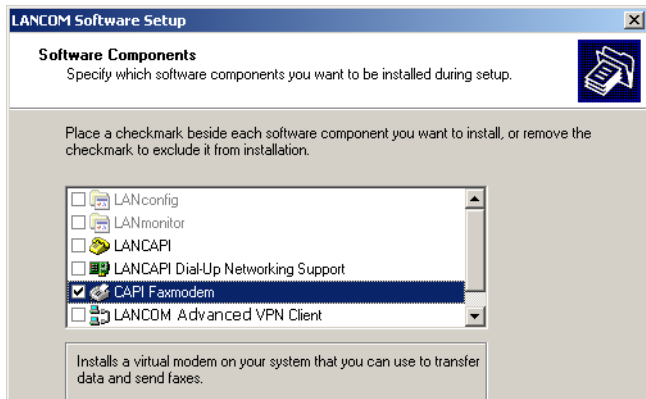
- the **LANCAPI client**. It provides the connection between your workstation PC and the LANCAPI server.
- the **CAPI Faxmodem**. This tool simulates a fax device on your workstation PC.
- the **MS Windows fax service**. This is the interface between the fax applications and the virtual fax.



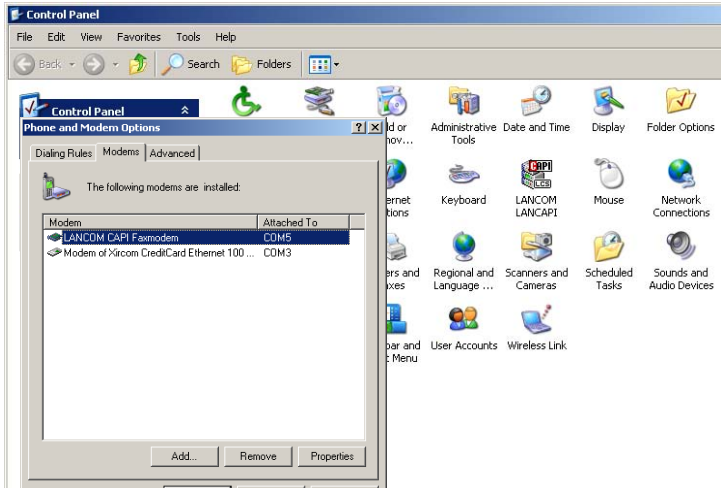
The installation of the LANCAPI client is described in the reference manual. This chapter shows the installation of LANCOM CAPI Faxmodem and MS Windows fax service.

7.1 Installation of the LANCOM CAPI Faxmodem

- ① Select the entry **Install LANCOM software** in the setup program of your LANCOM CD.
- ② Highlight the option **CAPI Faxmodem**, click **Next** and follow the instructions of the installation routine.

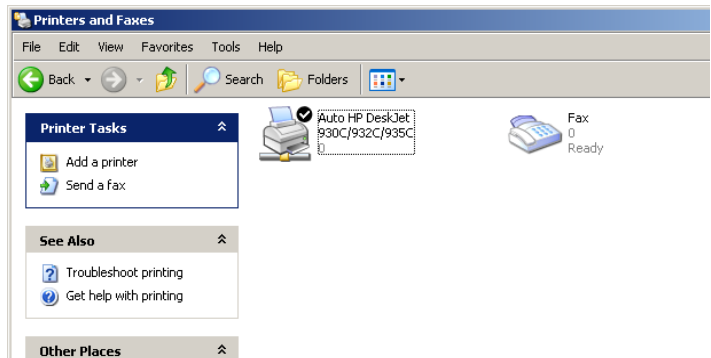


When the installation was successful, the LANCOM CAPI Faxmodem is entered into the **Phone and Modem Options** of the control panel.



7.2 Installation of the MS Windows fax service

- ① Select the option **Printers and Faxes** from the control panel.
- ② Select the option **Set up faxing** from the window 'Printers and Fax'. Follow, if necessary, the instructions of the installation tool. Into the recent window, an icon will appear for the newly installed fax printer.



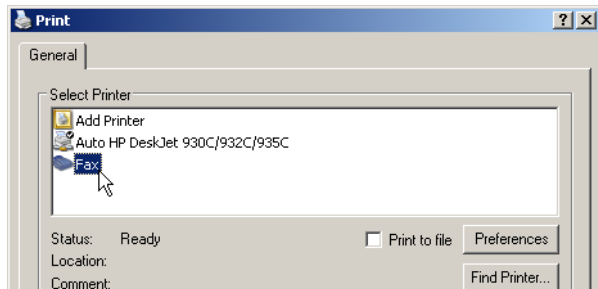
For checking the installation, click with the right mouse button on the fax-icon and select **Properties**. The LANCOM CAPI Faxmodem should now be entered into register 'devices'.

7.3 Sending a fax

After installing all required components, you have several possibilities to send a fax from your workstation PC. If you have already an existing data file, you can send it directly from your respective application. If you only want to send a short message, select the MS Windows fax service. You can use of course any other fax software alternatively.

7.3.1 Send a fax with any given office application

- ① Open as usual a document in your office application and select the menu item **File/Print**.
- ② Adjust the fax device as printer.

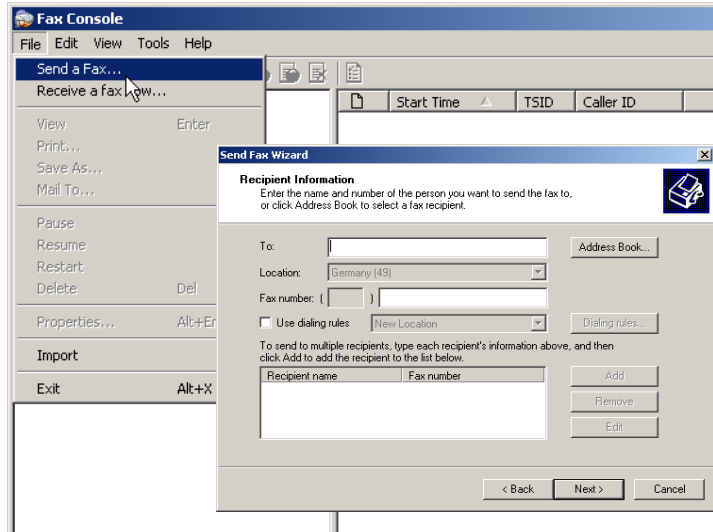


- ③ Click on OK. A wizard appears, that will guide you through the remaining sending process.

7.3.2 Send a fax with the MS Windows fax service

- ① Open the window 'Printers and Faxes' from the control panel.
- ② Double click with the left mouse button the icon of the fax device.

- ③ The fax client console will open. Select the menu item **Send a Fax**. A wizard will assist you through the remaining sending process.



8 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.

8.1 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 with WPA2 and AES encryption
- 802.1x / EAP
- LANCOM Enhanced Passphrase Security (LEPS)
- Access control by MAC address
- Optional IPSec-over-WLAN VPN

8.1.1 Encrypted data transfer

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



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

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

- The passphrases for 802.11i or WPA do not have to be changed quite so regularly as new keys are generated for each connection anyway. This is not the only reason that the encryption with 802.11i/AES or WPA/TKIP is so much more secure than the now obsolete WEP method. If you use WEP encryption to maintain compatibility with older WLAN clients, regularly change the WEP key in your access point.
- If the data is of a high security nature, further improvements include additionally authenticating the client with the 802.1x method ('802.1x / EAP' →page 77) or activate an additional encryption of the WLAN connection as used for VPN tunnels ('IPSec over WLAN' →page 78). 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.



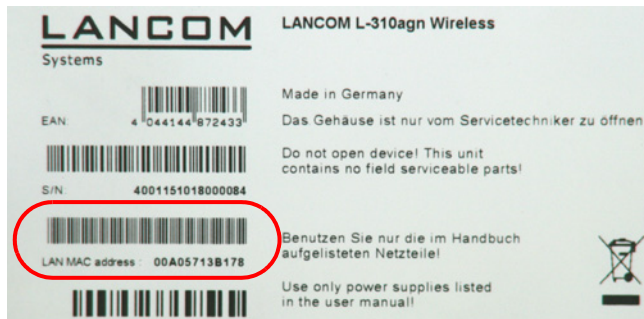
Please also observe the information in the "Standard WEP encryption" box.

Standard encryption with WPA-PSK

The factory settings (or those after resetting the device) are different in LANCOM Access Points than in LANCOM Wireless Routers.

- Unconfigured Access Points with standard factory settings cannot be commissioned by means of the WLAN interface. The WLAN modules are switched off and the devices search the LAN for a LANCOM WLAN Controller which will supply a configuration profile.
- Unconfigured Wireless Routers with standard factory settings cannot be commissioned by means of the WLAN interface. Furthermore, encryption with WPA-PSK as described here is used as standard.

The preshared key (PSK) for the standard WPA encryption consists of the first letter “L” followed by the LAN MAC address of the access point in ASCII characters. The LAN MAC addresses of the LANCOM devices always begin with the character string “00A057”. You will find the LAN MAC address on a sticker on the base of the device. **Only** use the number labeled as “MAC address” that starts with “00A057”. The other numbers that may be found are **not** the LAN MAC address.



A device with the LAN MAC address “00A05713B178” thus has a preshared key of “L00A05713B178”. This key is entered into the ‘WPA or private WEP settings’ of the device for each logical WLAN network as ‘Key 1/Passphrase’.

To use a WLAN adapter to establish a connection to a LANCOM Wireless Router that has factory settings, the WPA encryption must be activated for the WLAN adapter and the standard 13-character preshared key.



After registering for the first time, change the WPA preshared key to ensure that you have a secure connection.

8.1.2 802.1x / 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 Wireless Router 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.

8.1.3 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.

8.1.4 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.

8.1.5 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.

8.2 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.

8.3 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.

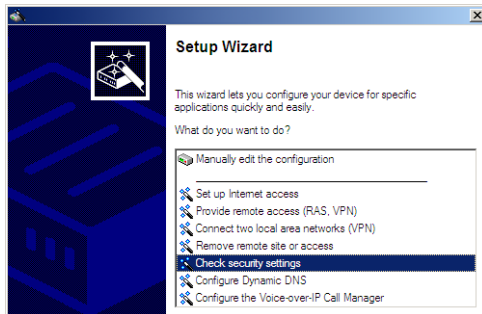
Your LANCOM offers password-protected access to its configuration. This is activated during the initial basic configuration simply by entering a password.

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).

8.3.1 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**.

8.3.2 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

8.4 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.



Ex-factory, WPA encryption is activated for every unconfigured device as standard. This WPA encryption in WLAN devices being managed by a LANCOM WLAN Controller is overwritten by the central encryption settings in the profiles of the WLAN-Controller.

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 your 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 you 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 rou-

ter 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.

With the ISDN location verification, the device can only be operated at one particular ISDN connection. After being switched on, the device calls itself at the corresponding telephone number to check that it is still connected to the "correct" ISDN connection (for further information see the reference manual).

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

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

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

9 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.

9.1 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 device in the LANCOM Antenna Calculator, which can be downloaded from our Web site at 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!

9.1.1 Antenna diversity

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.

9.1.2 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.

9.1.3 MIMO

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

9.1.4 Installing the AirLancer Extender antennas

The following diversity antennas are available as accessories for the LANCOM Wireless Routers:

- 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

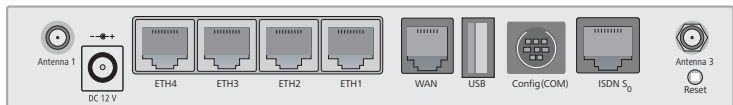
To install an optional AirLancer antenna, switch the device off by unplugging the power cable. Now carefully unplug the diversity antennas from the back by unscrewing them. Connect the AirLancer antennas to the antenna connectors marked 'ANT 1' and 'ANT 3' (external antennas cannot be connected to Antenna 2).



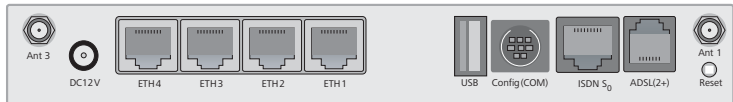
Please note the following when connecting antennas:

The configuration of the device software must agree with the actual antenna connections.

LANCOM 1811n Wireless



LANCOM 1821n Wireless



9.2 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).



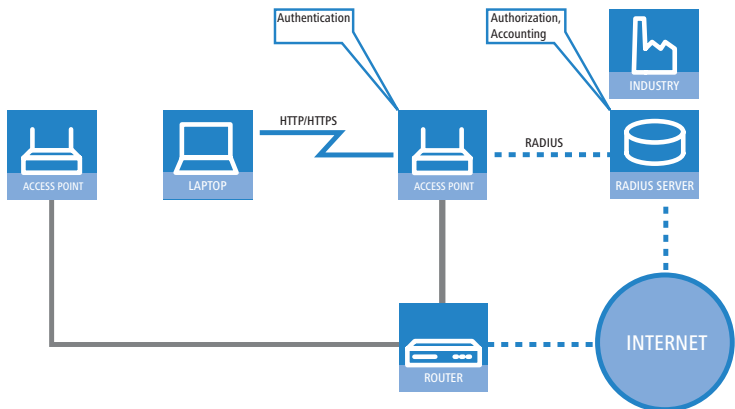
Please note that operating a LANCOM Wireless Router with the LANCOM Public Spot Option (also referred to as a HotSpot) can be subject to legal regulation in your country. Before installing a LANCOM Wireless Router, please inform yourself about any applicable regulations.

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.

Authentication and billing for individual users is implemented with user-friendly Web pages, enabling client PCs with a WiFi-certified wireless card (e.g. AirLancer) and standard Internet browser to go directly online.

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.

10 Advice & assistance

See this chapter for first-aid assistance if some of the typical problems should occur.

10.1 No WAN connection can be established

After starting, the router attempts automatically to connect to the Internet provider. If successful, this LED switches to constant green. This is generally due to one of the following causes:

Problems with the cabling?

For the DSL connection, use only the connector cable supplied. This cable must be connected to the Ethernet connector of the DSL modem

Is the correct transmission protocol selected?

The transmission protocol is defined with the basic settings. The Basic Settings Wizard actually sets the correct protocol for a wide variety of DSL providers. If your DSL provider is unknown to the Wizard you have to set the protocol yourself. The protocol specified by your DSL provider should work without problem.

You can check and adjust your protocol settings under:

LANconfig: Communication ► General ► Communication layers

WEBconfig: LCOS Menu Tree ► Setup ► WAN module ► Layer list

10.2 Slow DSL transmission

The speed of data transmission over an (Internet) DSL connection depends on a number of factors, most of which are beyond the influence of normal users. Along with bandwidth of your provider's connection, of decisive importance is the provider's Internet connection and the load on the target Web page. Several other factors in the Internet itself can also influence the transmission speeds.

Increasing the TCP/IP window size under Windows

If the actual transmission speed over a DSL connection is significantly lower than the maximum specified by the DSL provider, there are very few potential error sources with your own equipment.

A typical problem arises when a Windows PC simultaneously sends and receives large quantities of data over an asynchronous connection. This situation can severely impact download speeds. The cause of this is the RCP/IP receive windows size as defined in the Windows operating system. The default value is too small for asynchronous connections.

Instructions for increasing the windows size are available in the Knowledge-Base in the Support area of the LANCOM Systems Web site (www.lancom.eu).

10.3 Unwanted connections under Windows XP

When booting, Windows XP computers attempt to update the time by accessing a time server in the Internet. For this reason, Windows XP computers booting in the WLAN cause the LANCOM to connect to the Internet.

To prevent Windows XP computers from automatically synchronising the time, **right-click on the time** ► **Change time/date** ► **Internet time** off.

10.4 Cable testing

A cabling defect might have occurred, if no data is transmitted over LAN or WAN connection, although the configuration of the devices does not show any discernible errors.

You can test the cabling with the built-in cable tester of your LANCOM. Change under WEBconfig to menu item **LCOS Menu Tree** ► **Status** ► **LAN statistics** ► **Cable test**. Enter here the name of the interface to be tested (e.g. "DSL1" or "LAN-1"). Pay attention to the correct spelling of the interfaces. Start the test for the specified interface by clicking on **Execute**.

Expert Configuration
 Status
 LAN-statistics

Cable-Test


Enter here any additional arguments for the command you are about to execute:


Arguments

Execute Reset

Change then to menu item **LCOS Menu Tree ▶ Status ▶ LAN statistics ▶ Cable test results**. The results of the cable test for the individual interfaces are show up in a list.

[Expert Configuration](#)

 [Status](#)

 [LAN-statistics](#)

Cable-Test-Results

Port	Rx-Status	Rx-Distance	Tx-Status	Tx-Distance
DSL1	open	0m	open	0m
LAN-1	unknown		unknown	
LAN-2	unknown		unknown	
LAN-3	unknown		unknown	
LAN-4	unknown		unknown	

The following results can occur:

- **OK:** Cable plugged in correctly, line ok.
- **open** with distance **"0m"**: No cable plugged in or interruption within less than 10 meters distance.
- **open** with indication of distance: Cable is plugged in, but defect (short-circuited) at the indicated distance.
- **Impedance error:** The pair of cables is not terminated with the correct impedance at the other end.

11 Appendix

11.1 Performance data and specifications

		LANCOM 1811n Wireless	LANCOM 1821n Wireless
Connections	Ethernet LAN	4x 10/100Base-TX, auto sensing, switch with node/hub auto sensing, cable tester	
	WAN (ADSL)	10/100Base-TX, auto sensing	ADSL over ISDN as per ITU G.992.1 Annex B (compatible to U-R2 connections of the Deutsche Telekom) or ADSL over POTS as per ITU G.992.1 Annex A ADSL over ISDN as per ITU 992.3, ITU G.992.5 Annex B (ADSL2+) or ADSL over POTS naas per ITU G992.3 and ITU G.992.5 Annex A
	ISDN	ISDN S ₀	
	WLAN	Two 3 dBi dipole antennas (in package contents) and one 3 dBi internal dipole antenna. Two reverse SMA connectors for external LANCOM AirLancer Extender antennas or antennas of other manufacturers. Please remember the legal requirements of your country for operating antenna systems. Information about the calculation of conforming antenna configurations under www.lancom.eu .	
	Outband	serial V.24/V.28 port (8 pol. mini DIN)	
	Power supply	12V DC over external power adapter, or PoE compliant with IEEE 802.3af. Permitted power supplies: NEST 12V/1A DC/S Hohlstkr 2.1/5.5mm (RoHS) LANCOM item no. 110524 Type identification on the power supply „Type: 15.22305“	
	Wireless LAN	Frequency band	2400 - 2483,5 MHz (ISM) or 5150 - 5750 MHz
Standards		IEEE 802.11a IEEE 802.11g (compatible to IEEE 802.11b), IEEE 802.11n	
Housing	210 mm x 143 mm x 45 mm (W x H x D), rugged plastic case, provision for wall mounting		
Norms	CE conform according to EN 300 328, EN 301 893, EN 55024, EN 55022, EN 55011, EN 50081, EN 60950, ES 59005, EN 60950		
Licences	Notified in the countries Germany, Belgium, Netherlands, Luxembourg, Austria, Switzerland, Great Britain, Italy. More information about added notifications under www.lancom.eu .		
Environment / temperature range	Temperature range 0°C to +35°C at 80% max. humidity (non condensing)		

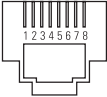
■ Chapter 11: Appendix

		LANCOM 1811n Wireless	LANCOM 1821n Wireless
Package contents		LAN cable (CAT.5, STP, 3 m), WAN cable (CAT.5, STP, 3 m), only LANCOM Wireless DSL series), ADSL cable (RJ45 – RJ11, CAT.5, STP, 3 m, only LANCOM Wireless ADSL series), ISDN cable, external power adapter (12V AC, 1.2 A for LANCOM Wireless DSL series; 12V DC, 1.0 A for LANCOM Wireless ADSL series), printed manual (English, German), software CD	
Options		<ul style="list-style-type: none"> ■ LANCOM Public Spot Option (authentication and accounting software for hotspots) (Art. no. 60642) ■ LANCOM Next Business Day Service Extension CPE, item no. 61411 ■ LANCOM 2-Year Warranty Extension CPE, item no. 61414 ■ LANCOM VPN Option 25 channels (max.25 simultaneous connections, 50 connections configurable) for VPN in WAN or IPsec-over-WLAN (Art. no. 60083) 	
Optional antennas		<ul style="list-style-type: none"> ■ AirLancer Extender I-180 2,4 GHz indoor antenna Art. no. 60914 ■ AirLancer Extender I-60ag Dualband indoor antenna Art. no. 61214 ■ AirLancer Extender O-30 2,4 GHz outdoor antenna Art. no. 60478 ■ AirLancer Extender O-70 2,4 GHz outdoor antenna Art. no. 60469 ■ AirLancer Extender O-D80g 2,4GHz polarizations diversity outdoor antenna Art. no. 61221 ■ AirLancer Extender O-360ag dualband omnidirectional outdoor antenna Art. no. 61223 ■ AirLancer Extender O-18a 5 GHz outdoor antenna Art. no. 61210 ■ AirLancer Extender O-D60a 5GHz polarizations diversity outdoor antenna Art. no. 61222 ■ AirLancer Extender O-9a 5GHz point to point outdoor antenna Art. no. 61220 ■ AirLancer Extender O-9a 5GHz point to point outdoor antenna Art. no. 61224 ■ AirLancer Cable NJ-NP 3m antenna cable elongation Art. no. 61230 ■ AirLancer Cable NJ-NP 6m antenna cable elongation Art. no. 61231 ■ AirLancer Cable NJ-NP 9m antenna cable elongation Art. no. 61232 ■ AirLancer Extender SA-5L surge arrester for antenna cables Art. no. 61553 ■ AirLancer Extender SA-LAN surge arrester for LAN cables Art. no. 61213 ■ LANCOM Modem Adapter Kit for connecting modems (analogue or GSM) to the serial configuration interface Art. no. 110288 	

11.2 Connector wiring

11.2.1 Ethernet interface 10/100Base-TX


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

11.2.2 ADSL interface

Only LANCOM
1821n Wireless

6-pin RJ11 socket

Connector	Pin	IAE
	1	–
	2	–
	3	a
	4	b
	5	–
	6	–

11.2.3 DSL interface

LANCOM 1811n
Wireless only

6-pin RJ45 socket

Connector

Pin

IAE



1

T+

2

T-

3

R+

4

–

5

–

6

R-

11.2.4 ISDN-S₀ interface

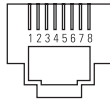
8-pin RJ45 socket (ISO 8877, EN 60603-7)

Connector

Pin

Line

IAE



1

–

–

2

–

–

3

T+

2a

4

R+

1a

5

R-

1b

6

T-

2b

7

–

–


8

–

–

11.2.5 Configuration interface (outband)

8-pin Mini DIN socket

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

EN

11.3 CE declaration of conformity



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

The CE declarations of conformity for your device are available for download on the LANCOM Systems web site (www.lancom.eu).

Index

Numerics

10/100Base-TX	33
100-Mbit network	33
3 DES	54, 62
802.11i	22, 74, 77, 80
802.11i/	75
802.1x	22, 74, 75, 77

A

Access point mode	11, 26
Access-control list	78
Accounting	43
ACL	77, 78
ADSL	

Connector cable	25
-----------------	----

AES	54, 62, 74
-----	------------

Anschlussbelegung	
ADSL-Schnittstelle	97

Antenna	
Connector for main antenna	33

Antenna Calculator	85
--------------------	----

Autosensing	33, 35
-------------	--------

B

Blowfish	54, 62
----------	--------

C

Call-back function	24, 54, 62
--------------------	------------

Calling Line Identity (CLI)	64
-----------------------------	----

CAPI interface	69
----------------	----

Charge limiter	29
----------------	----

Charge protection	43, 44
-------------------	--------

Common ISDN Application Programming Interface (CAPI)	69
---	----

Configuration access	44
----------------------	----

Configuration file	83
--------------------	----

Configuration interface	24
-------------------------	----

Connector cable	25
-----------------	----

Configuration password	81
------------------------	----

Configuration port	33
--------------------	----

Configuration protection	23, 41
--------------------------	--------

Connector wiring	95
------------------	----

ADSL interface	95
----------------	----

Configuration port	97
--------------------	----

DSL interface	96
---------------	----

ISDN S ₀ interface	96
-------------------------------	----

LAN interface	95
---------------	----

Outband	97
---------	----

Cost budget	43
-------------	----

D

Declaration of conformity	97
---------------------------	----

Default gateway	49, 83
-----------------	--------

DHCP	49
------	----

DHCP server	21, 40, 49
-------------	------------

Dial-in access	62
----------------	----

Dial-up adapter	65
-----------------	----

DNS	
-----	--

DNS access to the remote LAN	58
------------------------------	----

DNS server	21, 49
------------	--------

Documentation	25
---------------	----

Domain	58
--------	----

Download	5
----------	---

DSL transmission too slow	90
---------------------------	----

E

EAP	22, 74, 77
-----	------------

Encryption	54, 62
------------	--------

F

Firewall	23, 83
----------	--------

Block stations	83
----------------	----

FirmSafe	24
----------	----

Firmware	5
----------	---

Flatrate	51
----------	----

H

Hardware installation	35
-----------------------	----

HTTPS	45
-------	----

I		
ICMP	83	
Information symbols	6	
Installation	25	
ADSL	36	
Antennas	35	
configuration port	36	
DSL	35	
ISDN	36	
LAN	35	
power adapter	36	
Internet access	21, 50	
Authentication data	50	
Default gateway	51	
DNS server	51	
Flatrate	51	
IP address	51	
Network mask	51	
Protocol	50	
Internet access setup	50	
Internet provider	50	
IP		
Block ports	83	
Filter	83	
IP address	40, 41, 83	
IP address of the LANCOM	35	
IP masquerading	23, 82	
IP router	21	
IPoE	50	
IPoEoA	50	
IPsec	54, 62	
IPSec over WLAN	74	
ISDN		
Connector cable	25	
D channel	64	
Dial-in number	51	
Dynamic channel bundling	51	
MSN	43	
S ₀ port	33	
ISDN calling line ID	56, 63, 64	
ISDN connection		
Basic settings	43	
ISDN data compression	51	
ISDN leased-line option	22	
ISDN modem	62	
ISDN number	56	
ISDN PBX	43	
ISDN S ₀ connection	23	
L		
LAN		
Connector cable	25	
LAN connection	33	
LANCAPi	22, 43	
LANCOM Enhanced Passphrase Security	74	
LANCOM Public Spot Option	88	
LANCOM VPN Option	24	
LANconfig	38, 43	
Starting the Wizards	53	
LAN-LAN connectivity	43, 54	
Required information	55	
LAN-LAN coupling	21	
LANmonitor	38	
LANtools		
System requirements	26	
LEPS	22, 77	
M		
MAC address	76	
MAC address filter	22, 23	
Managed mode	11, 26	
Metering pulse	43	
MSN	64	
Multi SSID	22	
N		
NAT – see IP masquerading		
NetBIOS	58	
NetBIOS proxy	21	
Network connectivity	54	
Security aspects	54, 62	

■ *Index*

Network mask	40, 41, 83	Reset the toll protection	29
Network segment	35	Routing table	83
O			
Optional antennas	85	S	
Options and accessories	85	SDSL modem	23
P			
P2P	77	Security	
Package contents	25	Protecting the configuration	74
Password	41, 44, 54, 62	Security checklist	80
Password for the ISDN connection	57	Security settings	90
PAT – see IP masquerading		self-sufficient	11, 26
Ping	59	SNMP	
Plain Ethernet	50	Configuration protection	82
Plain IP	50	Software installation	37
Point-to-point	77	SSID	42, 44
point-to-point	21	Status display	
Power adapter	25, 33	ETH	31
PPP	62	Power	29
PPP client	65	WLAN data	32
PPPoE	50	WLAN link	32
PPTP	50	Statusanzeigen	27
Prefix for external line	43	Power	27
Printer at the USB port	36	Wireless Link	32
R			
RADIUS	77	Super AG	22
Remote Access Service (RAS)		Support	5
Activate compression in software	65	System requirements	26
Configuring the dial-in computer	65	T	
NetBIOS	65	TCP	83
Server	21	TCP/IP	26, 65
Setup	62	Connect test	59
Specify MSN	43	Settings	39
TCP/IP	64	TCP/IP configuration	
User name	63	Fully automatic	39, 40
Windows workgroup search	65	Manual	39, 40
Remote configuration	44	TCP/IP filter	23, 83
Remote configuration via ISDN	24	TCP/IP router	
Reset switch	33	Settings	57
		TCP/IP windows size	90
		Telnet	83
		TFTP	83
		Transmission protocol	90

Turbo Mode	22	WAN-Anschluss	33
U		WEBconfig	45
UDP	83	HTTPS	45
V		System requirements	26
Virtual Private Networks (VPN)	21	WEP	22, 74, 79, 80
VPN client	65	Windows workgroup search	58
W		Wireless LANs	
WAN		Operating modes	11
Connector cable	25	WPA	22, 74, 77, 80