LANCOM Wireless DSL Series – LANCOM Wireless ADSL Series

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Wuerselen
Germany
www.lancom.de

Wuerselen, January 2005

110320/0105

Preface

Thank you for placing your trust in this LANCOM product.

With the LANCOM Wireless DSL 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. With this router you can simply and comfortably connect individual PCs or whole local networks to the high-speed Internet.

As a base station, the LANCOM Wireless DSL provides numerous central functions and services to the participants of wireless networks and it convinces by a simple configuration and a reliable continuous operation. With high-effective technologies, it ensures data security within the whole wireless network.

Security settings

For a carefree use of your device, we recommend to carry out all security settings (e.g. Firewall, encryption, access protection, charge lock), which are not already activated at the time of purchase of your device. The LANconfig wizard 'Check Security Settings' will support you accomplishing this. Further information regarding this topic can be found in chapter 'Security settings' →page 69.

We ask you additionally to inform you about technical developments and actual hints to your product on our Web page www.lancom.de, and to download new software versions if necessary.

User manual and reference manual

The documentation of your device consists of two parts: the user manual and the reference manual.

You are now reading the user manual. It contains all information you need to start your LANCOM Wireless DSL. It also contains the most important technical specification for the device.

The reference manual can be found on the CD as an Acrobat (PDF) document. It is designed as a supplement to the user manual and goes into detail on topics that apply to a variety of devices. These include for example:

▶ Systems design of the LCOS operating system

▶ Configuration

▶ Management

▶ Diagnosis

EN

- ▶ Security
- ▶ Routing and WAN functions
- ▶ Firewall
- ▶ Quality of Service (QoS)
- ▶ Virtual Private Networks (VPN)
- ▶ Virtual Local Networks (VLAN)
- ▶ LANCAPI
- ▶ Further server services (DHCP, DNS, charge management)

Model variants

This user manual applies to the following models of the LANCOM Wireless DSL series:

- ▶ LANCOM 1511 Wireless DSL
- ▶ LANCOM 1521 Wireless ADSL
- ▶ LANCOM 1811 Wireless DSL
- ▶ LANCOM 1821 Wireless ADSL

Model restriction

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

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

This documentation was compiled …

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

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

info@lancom.de

Our online services (www.lancom.de) are available to you around the clock should you have any queries regarding the topics discussed in this manual or require any further support. In addition, support from LANCOM Systems is also available to you. Telephone numbers and

contact information for LANCOM Systems support can be found on a separate insert, or at the LANCOM Systems website.

Notes symbols	
	Very important instructions. If not followed, damage may result.
	Important instruction should be followed.
	Additional instructions which can be helpful, but are not required.

Special formatting in body text	
Bold	Menu commands, command buttons, or text boxes
Code	Inputs and outputs for the display mode
<Value>	Placeholder for a specific value

Contents

EN

EN

1   Introduction

DSL technology permits high-speed Internet access via conventional tele-phone lines. DSL features an outstanding price/performance ratio and is very popular among private users as well as small and mid-sized businesses. All of the devices of the LANCOM Wireless DSL series are fully-featured routers that therefore also can be used for providing Internet access to a complete local network (LAN).

The models of the LANCOM Wireless DSL series offer each a DSL or ADSL con-nector 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 Wireless DSL 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.
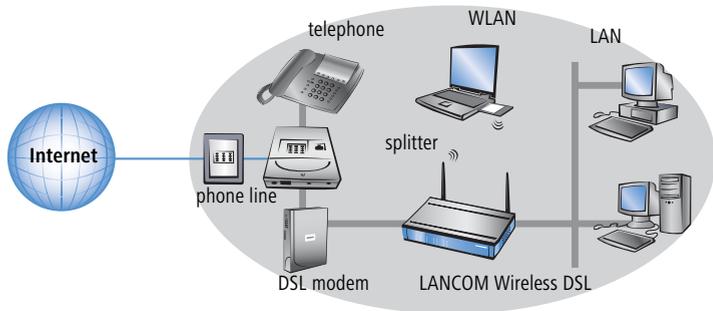
1.1   How does ADSL work?

For LANCOM 1521 Wireless ADSL and LANCOM 1821 Wireless ADSL only

Since the late 1980s, scientists have been working on the idea of using con-ventional telephone lines for video and multimedia applications.

High speed via standard telephone lines

Their approach was based on the use of telephone lines only for the distance between the subscriber and the next local exchange. From the switching center, the data is then transferred via high-speed connections to the desired destination or target network (i.e. the Internet). This minimization of the tel-

EN

ephone line distance used permits considerably higher transfer rates than would be possible when relying solely on the telephone network.
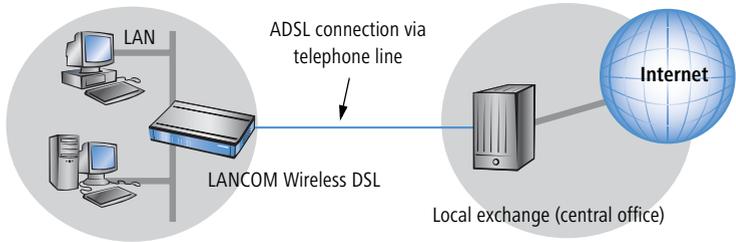
All DSL technologies, of which ADSL is the most common, are based on this concept. Thanks to their high transfer speeds, DSL connections are well-suited for Internet access.

Ideal for Internet surfers

The ADSL version of DSL was designed for applications in which the user receives high volumes of data but only transmits relatively small volumes. A typical example for this would be access to the world wide web (www). Only a few commands (mouse clicks) are required to initiate the download of very large volumes of data such as graphics, texts, audio or video files. The user typically only sends very small amounts of data across the Internet connection.

With an ADSL connection, a user can download at up to 8 Mbps ("downstream") and upload at up to 800 Kbps ("upstream"). These maximum rates can be reduced as required by the ADSL provider. A typical access plan might specify, for example, 768 Kbps download and 128 Kbps upload speed.

All services via a single cable—thanks to the splitter

With ADSL, all traditional telephony applications (telephone, fax, answering machine, PBX) can still be used without restrictions. So-called splitters make this possible. Splitters are devices that separate the telephone line's "voice frequencies" from the "data frequencies" and ensure that the signals are forwarded to the appropriate networks. Voice signals are passed on to the existing telephone network, while data signals are forwarded to their destinations (i.e. Internet providers) via high-bandwidth network connections.

A splitter is also used at the subscriber end to permit ADSL modems/routers and conventional telephone equipment to be used at the same time.
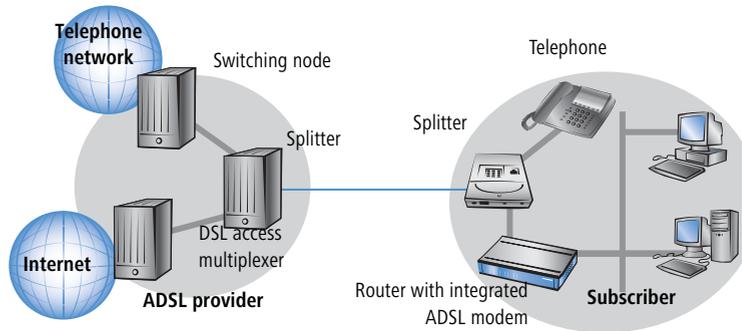
In some models (like in the picture above) the ADSL modem is integrated directly in the router (e.g. LANCOM 1521 Wireless ADSL and LANCOM 1821 Wireless ADSL). Other models like LANCOM 1511 Wireless DSL or LANCOM 1811 Wireless DSL are connected to the splitter using a separate ADSL modem.
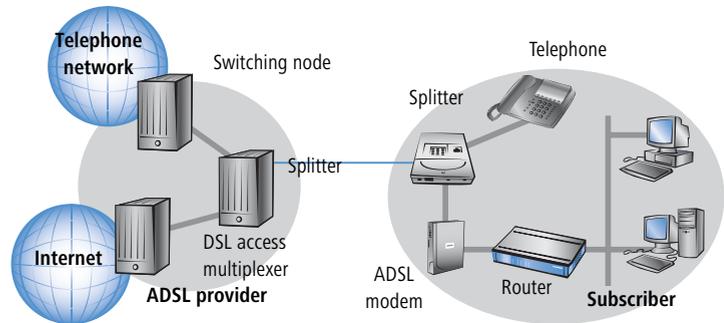
The models LANCOM 1511 Wireless DSL and LANCOM 1811 Wireless DSL can also utilize other broadband connections (e.g. cable modem) that offer a 10/100Base-Tx-Ethernet connector over PPPoE, PPTP or plain Ethernet (with or without DHCP).

The models LANCOM 1521 Wireless ADSL and LANCOM 1821 Wireless ADSL can use this option, if the first LAN ports is configured as WAN interface.

ADSL‑over‑ISDN or ADSL‑over‑POTS?

ADSL can operate over modern ISDN telephone service as well as conventional analog service (POTS – **P**lain **O**ld **T**elephone **S**ervice).

There are, however, different technical specifications for the two telephone systems. For this reason, devices in the LANCOM Wireless DSL series are offered in two different versions: A version for ADSL‑over‑POTS and a version for ADSL‑over‑ISDN.

You can determine which telephone system a device supports by looking at the model description on the bottom of the device. The label containing the device name also contains an additional code which stands for the telephone system the device supports:

Code	Supported telephone system
'Annex A'	ADSL‑over‑POTS
'Annex B'	ADSL‑over‑ISDN

An 'Annex A' type LANCOM Wireless DSL can only be used with ADSL‑over‑POTS service. Similarly, an 'Annex B' device can only be used with ADSL‑over‑ISDN service. Retrofitting a device to function with a different telephone system is not possible.

ADSL‑over‑ISDN connections also exist that do not operate in conjunction with ISDN, but which use a conventional analog telephone connection. A prominent example would be Deutsche Telekom's T‑DSL service.

1.2 Which use does VPN offer?

For LANCOM 1811 Wireless DSL and LANCOM 1821 Wireless ADSL only

A VPN (**V**irtual **P**rivate **N**etwork) can be used to set up cost‑effective, public IP networks, for example via the ultimate network: the Internet.

The models LANCOM 1811 Wireless DSL and LANCOM 1821 Wireless ADSL are equipped with 5 active channels by default. The LANCOM VPN Option. The additional VPN‑25 Option can extend VPN support to 25 tunnels (including hardware acceleration).

While this may sound unspectacular at first, in practice it has profound effects. To illustrate this, let's first look at a typical corporate network without VPN

technology. In the second step, we will see how this network can be optimized by the deployment of VPN.

Conventional network infrastructure

First, let's have a look at a typical network structure that can be found in this form or similar forms in many companies:
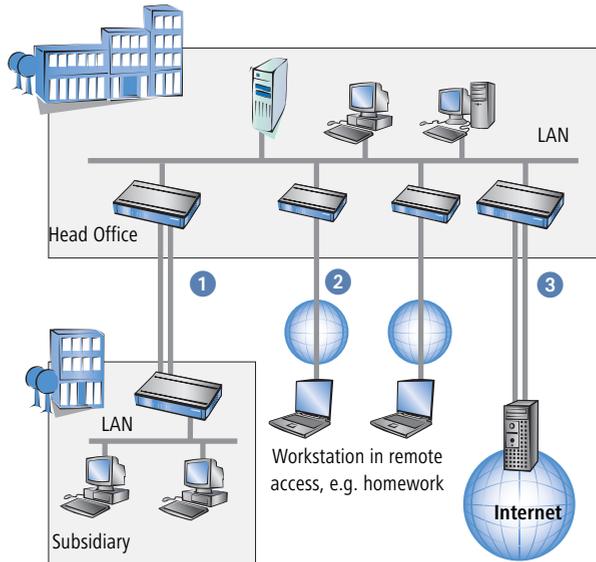
The corporate network is based on the internal network (LAN) in the headquarters. This LAN is connected to the outside world in three ways:

1 A subsidiary is connected to the LAN, typically using a leased line.

2 PCs dial into the central network via modem or ISDN connections (Remote Access Service – RAS).

3 The central LAN has a connection to the Internet so that its users can access the Web, and send and receive e-mail.

All connections to the outside world are based on dedicated lines, i.e. switched or leased lines. Dedicated lines are very reliable and secure. On the other hand, they involve high costs. In general, the costs for dedicated lines are dependent on the distance. Especially in the case of long-distance connections, keeping an eye out of cost-effective alternatives can be worthwhile.

The appropriate hardware must be available in the headquarters for every type of required connection (analog dial‑up, ISDN, leased lines). In addition to the original investment costs, ongoing costs are also incurred for the administration and maintenance of this equipment.

Networking via the Internet

The following structure results when using the Internet instead of direct connections :
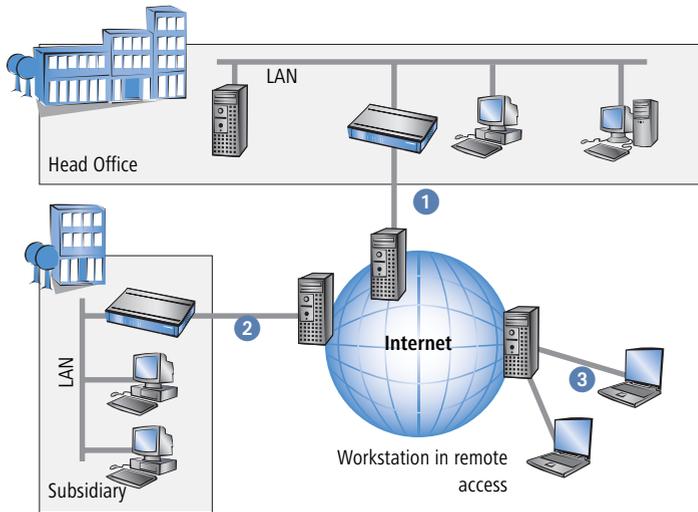
All participants have fixed or dial‑up connections to the Internet. Expensive dedicated lines are no longer needed.

❶ All that is required is the Internet connection of the LAN in the headquarters. Special switching devices or routers for dedicated lines to individual participants are superfluous.

❷ The subsidiary also has its own connection to the Internet.

❸ The RAS PCs connect to the headquarters LAN via the Internet.

The Internet is available virtually everywhere and typically has low access costs. Significant savings can thus be achieved in relation to switched or dedicated connections, especially over long distances.

The physical connection no longer exists directly between two participants; instead, the participants rely on their connection to the Internet. The access

technology used is not relevant in this case: ideally is the use of broadband technologies such as DSL (Digital Subscriber Line) or G.703 (2-Mbit leased lines). But also a conventional ISDN line can be used.

The technologies of the individual participants do not have to be compatible to one another, as would be the case for conventional direct connections. A single Internet access can be used to establish multiple simultaneous logical connections to a variety of remote stations.

The resulting savings and high flexibility makes the Internet (or any other IP network) an outstanding backbone for a corporate network.

1.3   What does a router do?

ⓘ   The following sections describe the functionality of routers in general. The functions supported by your device are listed in the table 'What can your LANCOM Wireless DSL do?' →page 18.

Routers connect LANs at different locations and individual PCs to form a Wide Area Network (WAN). With the appropriate rights, any computer in this WAN can access other computers and services of the complete WAN (as with 'PC 1' accessing 'Server A' in the remote LAN in the diagram).
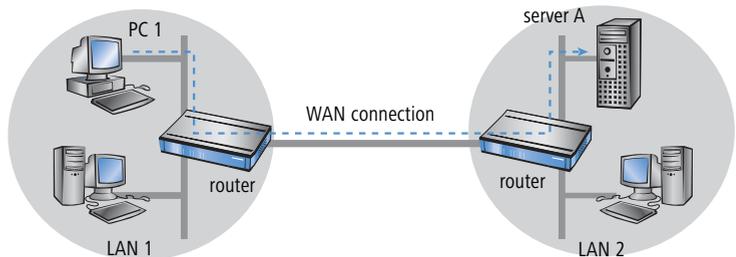
Connecting a LAN to the Internet does not technically differ from coupling two LANs. The only difference is that it is not just a handful of computers behind the Internet provider's router. Instead, it is the net of the networks - the public Internet.

1.3.1   Bridgehead to the WAN

All routers have at least two connections:

▶   at least one for the LAN

EN

> ▶ at least one for WAN connections

In addition to LAN connectivity (10/100 Mbps Ethernet), several models also offer an integrated switch. For the connecting to the WAN, the routers use ISDN, xDSL/cable or ADSL connectors. Several devices contain additionally a wireless network card and can thus integrate also stations of WLANs (Wireless LANs) into the routing.

The router's task is to transfer data from the local network to the target network via a suitable WAN connection. Data is also transferred from the WAN to the desired recipients in the LAN.

1.3.2 Areas of deployment for routers

Routers are mainly used for the following applications:

▶ Internet access for a LAN (e.g. via DSL or ISDN)

The Internet consists of countless large and small networks that are interconnected into the world's largest WAN via routers. The router links all the workstation computers on your local area network to the global Internet. Security functions such as IP masquerading protect your LAN against unauthorized access from outside.

▶ LAN to LAN coupling (via VPN or ISDN)

LAN to LAN coupling links individual LANs to form one large network, even if this means crossing continents. A typical example: A branch office is to be connected to the LAN of the headquarters. In principle, you can connect LANs in two ways:

Not possible with all LANCOM devices.

▷ High-speed coupling via VPN

The fastest and most economical LAN to LAN links are possible with VPN (**V**irtual **P**rivate **N**etwork) technology, as VPN uses the Internet as the basis for its communications. The fast xDSL connection of the router comes into its own here. The precondition: a VPN gateway with access to the Internet is required on either side of the network interconnection.

VPN tunnel via the Internet

VPN gateways

▷ Conventional via ISDN
Without VPN, a LAN to LAN interconnection can alternatively be realized via ISDN. In this case, an intelligent line management and sophisticated filter mechanisms keeps connection costs low.

▶ Remote access to the company network (via VPN or ISDN)

The work of many office workers in modern organizations is less and less dependent on any definite location—the most important factor here is unimpaired access to shared and freely available information.

Remote Access Service (RAS) is the magic word here. Employees working from home or field staff can dial into the company network via VPN or ISDN. When working with remote access via ISDN, the router protects the company network: the call back function only grants access to known and registered users.

1.4 What is a Wireless LAN?

The following sections describe the functionality of wireless networks in general. The functions supported by your device are listed in the table 'What can your LANCOM Wireless DSL do?' →page 18.

A Wireless LAN connects single terminals (e.g. PCs or notebooks) to a local network (also LAN – **L**ocal **A**rea **N**etwork). In contrast to a conventional LAN, communication takes place via radio links rather than via network cables. This is the reason why a Wireless LAN is also called a **W**ireless **L**ocal **A**rea **N**etwork (WLAN).

All functions of a cable-bound network are also available in a Wireless LAN: access to files, servers, printers etc. is as possible as the connection of individual stations to an internal mail system or to the Internet access.

The advantages of Wireless LANs are obvious: notebooks and PCs can be set up just where they are needed. Due to Wireless LANs, problems with missing connections or structural alterations belong to the past.

1.4.1 Which hardware to use?

Each station of the Wireless LAN needs access to the Wireless LAN in the form of a wireless interface. Devices which have no built-in wireless interface can be upgraded with a supplement card or an adapter.

ⓘ LANCOM Systems offers wireless adapters by its AirLancer product line. An AirLancer wireless adapter enables a device (e.g. PC or notebook) for access to the Wireless LAN.

1.4.2 Operation modes of Wireless LANs and base stations

Wireless LAN technology and base stations in Wireless LANs are used in the following operation modes:

▶ Simple direct connections between terminals without base station (ad-hoc mode)

▶ Larger Wireless LANs, connection to LANs with one or more base stations (infrastructure network)

▶ Passing‑through of VPN‑encrypted connections with VPN pass‑through

▶ Setting‑up of an Internet access

▶ Connecting two LANs via a direct radio link (point‑to‑point mode)

▶ Connecting of devices with Ethernet interface via base stations (client mode)

▶ Extending an existing Ethernet network with WLAN (bridge mode)

1.5 What can your LANCOM Wireless DSL do?

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

	LANCOM 1511 Wireless DSL	LANCOM 1811 Wireless DSL	LANCOM 1521 Wireless ADSL	LANCOM 1821 Wireless ADSL
Applications				
Internet access	✓	✓	✓	✓
LAN to LAN coupling via VPN with 5 active tunnels (dynamic VPN)		✓		✓
LAN to LAN coupling via ISDN	✓	✓	✓	✓
RAS server (via VPN)		✓		✓
RAS server (via ISDN)	✓	✓	✓	✓

	LANCOM 1511 Wireless DSL	LANCOM 1811 Wireless DSL	LANCOM 1521 Wireless ADSL	LANCOM 1821 Wireless ADSL
IP router	✓	✓	✓	✓
IPX router (via ISDN), e.g. for coupling of Novell networks or dialling into Novell networks	✓	✓	✓	✓
NetBIOS proxy for coupling of Microsoft peer-to-peer networks via ISDN	✓	✓	✓	✓
DHCP and DNS server (for LAN and WAN)	✓	✓	✓	✓
LANCAPI server for the operating with office applications as fax or answering machine via ISDN interface	✓	✓	✓	✓
Wireless LAN				
Wireless transmission by IEEE 802.11g and IEEE 802.11b	✓	✓	✓	✓
Wireless transmission by IEEE 802.11a		✓		✓
Roaming function	✓	✓	✓	✓
WEP encryption: WEP64, WEP128, WEP152 (up to 128 Bit key length)	✓	✓	✓	✓
IEEE 802.1x/EAP	✓	✓	✓	✓
Multi SSID	✓	✓	✓	✓
Individuelle Passphrases pro MAC-Adresse (LEPS)	✓	✓	✓	✓
WPA – TKIP	✓	✓	✓	✓
802.11i with hardware acceleration	✓	✓	✓	✓
MAC address filter (ACL)	✓	✓	✓	✓
Access to RADIUS server	✓	✓	✓	✓
Closed network function	✓	✓	✓	✓
Traffic lock function	✓	✓	✓	✓
VLAN	✓	✓	✓	✓

EN

▶ *Chapter 1: Introduction*

	LANCOM 1511 Wireless DSL	LANCOM 1811 Wireless DSL	LANCOM 1521 Wireless ADSL	LANCOM 1821 Wireless ADSL
WAN connection				
Connection for DSL or cable modem	✓	✓	✓ [1]	✓ [1]
ADSL Connection			✓	✓
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)	✓	✓	✓	✓

[1] First LAN port can be configured as Ethernet WAN interface

	LANCOM 1511 Wireless DSL	LANCOM 1811 Wireless DSL	LANCOM 1521 Wireless ADSL	LANCOM 1821 Wireless ADSL
LAN connection				
Integrated 4-port auto-mode-switch (10/100 Mbps) to connect terminals (workstations etc.) or subordinated switches or hubs.	✓	✓	✓	✓
Support of data packets with VLAN resp. QoS marking for an intelligent data traffic control within the switch		✓		✓
Security functions				
IP masquerading (NAT, PAT) to hide all workstations of the LAN behind one common public IP address.	✓	✓	✓	✓
Stateful Inspection Firewall	✓	✓	✓	✓
Firewall filters for a selective locking of IP addresses, protocols and ports	✓	✓	✓	✓
MAC address filter control e.g. the access of LAN workstations to IP routing functions	✓	✓	✓	✓
Configuration protection to block "brute force attacks"	✓	✓	✓	✓

	LANCOM 1511 Wireless DSL	LANCOM 1811 Wireless DSL	LANCOM 1521 Wireless ADSL	LANCOM 1821 Wireless ADSL
Configuration				
Configuration with LANconfig or with web browser, additionally terminal mode for Telnet or other terminal programs, SNMP interface and TFTP server function.	✓	✓	✓	✓
Remote configuration via ISDN (with ISDN-PPP connections e.g. via Windows network and dial-up connections)	✓	✓	✓	✓
Serial configuration interface	✓	✓	✓	✓
Callback function with PPP authentication mechanisms for restriction to fixed ISDN telephone numbers	✓	✓	✓	✓
FirmSafe with firmware versions for absolutely secure software upgrades	✓	✓	✓	✓
Optional software extensions				
ISDN leased line option	✓	✓	✓	✓
LANCOM VPN Option with 25 active tunnels (hardware accelerated) for IPSec-over-WLAN or for protection of network couplings and direct radio link		✓		✓
LANCOM Public Spot Option for installation of public accessible WLAN base stations (Wireless Public Hot Spot)	✓	✓	✓	✓

EN

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 1511 Wireless DSL	LANCOM 1811 Wireless DSL	LANCOM 1521 Wireless ADSL	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	✓		✓	
2 external screw-on dualband antennas 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 preconditions

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

▶ Operating system that supports TCP/IP, e.g. Windows XP, Windows Mil-
lennium Edition (Me), Windows 2000, Windows 98, Windows 95, Win-
dows NT, Linux, BSD Unix, Apple Mac OS, OS/2, BeOS.

▶ Access to the LAN via the TCP/IP protocol.

The LANtools and the LANCAPI functions also require a Windows
operating system. A web browser is required for access to WEBconfig.

2.3 Introducing LANCOM Wireless DSL

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

While the information in this section is useful for the installation of the
device, it is not absolutely essential. You may therefore skip this sec-
tion for the time being and go straight forward to the installation on
page 34.

2.3.1 Status displays

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

Front side

The various LANCOM Wireless DSL models have different numbers of indica-
tors on the front panel depending on their functionality (picture: LANCOM
1811 Wireless DSL).

not available on LANCOM 1511 Wireless DSL
and LANCOM 1521 Wireless ADSL

Top panel

The two LEDs on the top panel provide a convenient overview of the most
important status information, especially when the device is installed vertically.

EN

Power
Online

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.

Power

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

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

EN

The power LED flashes red/green in alternation until a configuration password has been specified. Without a configuration password, the configuration data of the LANCOM is insecure. Under normal circumstances, you would assign a configuration password during the basic configuration (see instructions in the following chapter). For information about a later assignment of the configuration password see the section 'Security settings' →page 69.

Flashing Power LED but no connection?

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

Signal for reached time or connect-charge limit

▶ Reset connect charge protection.

▶ Increase the limit that has been reached.

▶ Completely deactivate the lock that has been triggered (set limit to '0').

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

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

Online   The Online LED indicates the overall status of all WAN ports:

off		No active connection
green	flashing	Establishing first connection
green	inverse flashing	Establishing further connection
green	constantly on	At least one connection established
red	constantly on	Error establishing the previous connection

EN

DSL status
(LANCOM 1511
Wireless DSL and
LANCOM 1811
Wireless DSL only)

Connection status of the DSL connection:

off		not connected
green	blinking	Establishing connection
green	flashing	Protocol negotioation
green	constantly on	Connection established

DSL data
(LANCOM 1511
Wireless DSL and
LANCOM 1811
Wireless DSL only)

Data traffic via the DSL connection:

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

ADSL Status
(LANCOM 1521
Wireless ADSL and
LANCOM 1821
Wireless ADSL only)

Connection status of the ADSL connection:

off		not connected
green	flashing	Initialization
green	constantly on	Synchronization successful
red	flickering	Error (e.g. CRC error or framing error
red	constantly on	Synchronization aborted

ADSL Data
(LANCOM 1521
Wireless ADSL and
LANCOM 1821
Wireless ADSL only)

Data traffic via the ADSL connection:

off		No connection
green	flashing	Establishing connection
green	invers flashing	Establishing further connections
green	constantly on	At least one connection estahblished
green	flickering	Data traffic (send or receive)

ISDN status

Status of ISDN S_0 connection:

off		Not connected or no S_0 voltage (no error message)
green	blinking	Initializing D-channel (establishing contact with the connection point)
green	constantly on	D channel ready for use
red	blinking	Error (CRC error, framing error, etc.)
red	constantly on	Activation of D-channel failed

If the ISDN status LED goes out automatically, this does not indicate an S_0 bus error. Many ISDN connections and PBXs put the S_0 bus into a power-save mode after a certain time. The S_0 bus is automatically reactivated as required, and the ISDN status LED will once again light up green.

ISDN data

Separate status display for both ISDN B channels:

off		No connection established
green	blinking	Dialling
green	flashing	Establishing first connection
green	flashing	Establishing further connection
green	constantly on	Connection established via B channel
green	flickering	Data traffic (send or receive)

LAN 1
LAN 2
LAN 3
LAN 4

Status of the four LAN ports in the integrated switch:

off		No network device connected
green	constantly on	Connection to network device operational, no data traffic
green	flickering	Data traffic
red	flickering	Collision of packets

WLAN link

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

The WLAN link display can assume three states:

off		No wireless LAN adapter found
green	constantly on	Wireless LAN adapter ready for use
green	flickering	Activity in wireless LAN (blinking frequency indicates the number of registered stations)

EN

WLAN data

Gives information about the data traffic in the wireless LAN access.

The WLAN data display can assume three states:

off		No data traffic
green	flickering	Data traffic
green	flashing	Error in the wireless LAN (e.g. sending error because of bad connection quality)

VPN

Status of a VPN connection. Only active with LANCOM VPN Option installed.

off		No VPN tunnel established
green	blinking	Negotiating VPN connection
green	flashing	Establishing first connection
green	inverse flashing	Establishing further connection
green	constantly on	VPN connection established

Security

Status of the firewall. Indicates the status of the security settings and averted attacks to the protected network.

green	constantly on	Security settings ok. Packet filter rules are set.
red/ green	blinking	Insecure configuration
red	flickering	Security alert: data packet filtered by firewall rules

2.3.2   **The back of the unit**

The connections and switches of the router are located on the back panel (example: LANCOM 1811 Wireless DSL):

EN
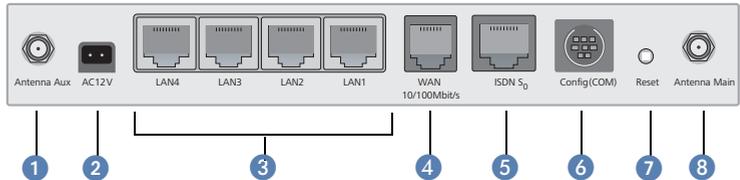
1 Connection for diversity antenna

2 Connection for the included power adapter

3 Switch with four 10/100Base-Tx connections

4 WAN port for LANCOM 1511 Wireless DSL and LANCOM 1811 Wireless DSL respectively ADSL port for LANCOM 1521 Wireless ADSL and LANCOM 1821 Wireless ADSL

5 ISDN/S_0 port

6 Serial configuration port

7 Reset switch

8 Connector for main antenna (use this connector to connect additional AirLancer Extender antennas)

The function of the reset button

The reset button has two different functions depending on how long it is pressed:

▶ **Restarting the device** (soft reset) – push the button for less than five seconds. The device will restart.

▶ **Resetting the configuration** (hard reset) – push the button for more than five seconds. All the device's LEDs will light up green and stay on. As soon as the reset switch is released, the device will restart with factory settings.

EN

(i) Note that resetting the device leads to a loss on the WLAN encryption settings within the device and that the default WEP key is active again ('Standard WEP encryption' →page 72).

2.4   Hardware installation

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

① **Antennas** – Screw on the both included diversity antennas at the back of the LANCOM Wireless DSL base station.

② **LAN** – First connect the LANCOM Wireless DSL 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 ❸ 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.

(i) You should never have more than one unconfigured LANCOM Wireless DSL in a network segment at any given time. All unconfigured LANCOM Wireless DSL 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 Wireless DSL devices one at a time, immediately assigning each device a unique IP address (one that does not end with '254').

1511/1811 only

③ **DSL** – connect the WAN interface ❹ to the DSL modem socket using the supplied DSL connector cable (dark blue plugs).
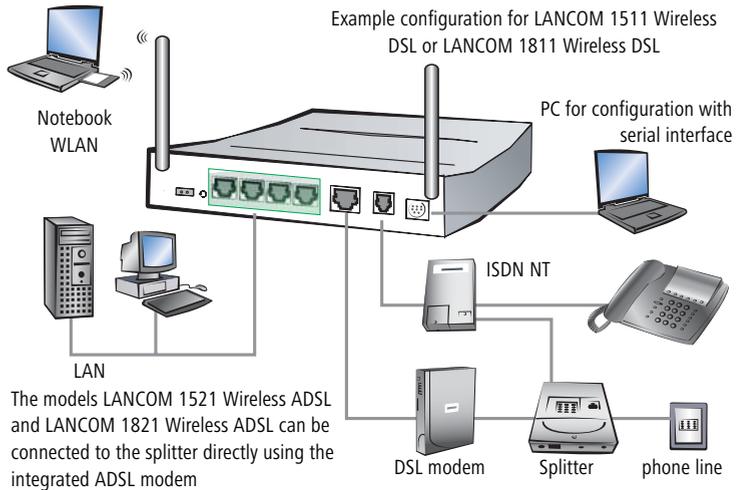
1521/1821 only

④ **ADSL** – connect the ADSL interface ❹ to the splitter using the supplied ADSL connector cable (transparent plugs).

⑤ **ISDN** – to connect the LANCOM Wireless DSL to the ISDN, plug one end of the supplied ISDN connector cable (light blue plugs) in the ISDN/S$_0$ port ❺ of the router and the other end into an ISDN/S$_0$ multi-device mode or point-to-point mode connection.

⑥ **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 ❻ with a free serial port of the PC.

⑦ **Connect to power** – Connect socket ❶ of the unit to a power supply using the included power adapter.

EN

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

⑧ **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.

Example configuration for LANCOM 1511 Wireless DSL or LANCOM 1811 Wireless DSL

Notebook WLAN

PC for configuration with serial interface

ISDN NT

LAN

The models LANCOM 1521 Wireless ADSL and LANCOM 1821 Wireless ADSL can be connected to the splitter directly using the integrated ADSL modem

DSL modem   Splitter   phone line

⚡ Devices with integrated ADSL modem could become quite warm during their operation. Concerning these models, please pay attention to the ambient air temperature range of max. 35°C. Make sure that the ventilation is sufficient. Do not stack the devices and do not expose them to direct insolation!

2.5   Software installation

This section covers the installation of the included system software LANtools for Windows.

> ⓘ   You may skip this section if you use your LANCOM Wireless DSL exclusively with computers running operating systems other than Windows.
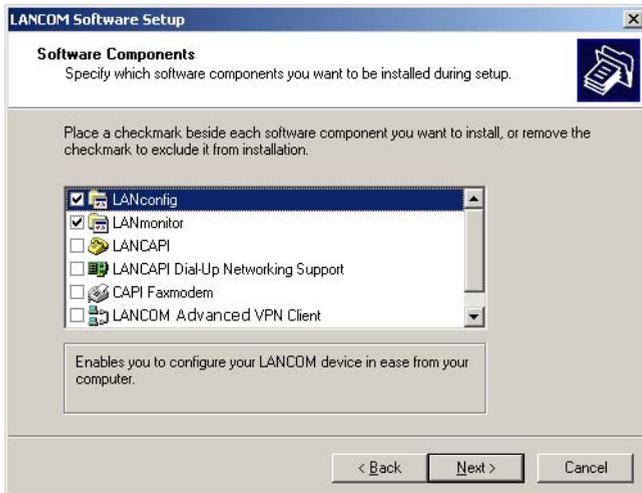
2.5.1   Starting LANCOM setup

Place the LANCOM CD in your CD drive. The LANCOM setup program will start automatically.

> ⓘ   If the setup program does not start automatically, run AUTORUN.EXE in the root folder of the LANCOM CD.

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

32

2.5.2 Which software should you install?

▶ **LANconfig** is the configuration program for all LANCOM routers and LANCOM Wireless DSL base stations. WEBconfig can be used alternatively or in addition via a web browser.

▶ **LANmonitor** lets you monitor on a Windows PC all LANCOM routers and LANCOM Wireless DSL base stations.

▶ **LANCAPI** is a special form of the CAPI-2.0 interface that all workstations of the LAN need to get access to office communication functions as fax or EuroFile transfer. With **LANCAPI Dial-Up Networking Support**, single workstations can realize dial-up connections to an Internet provider via LANCAPI. The **CAPI fax modem** makes you available a first class fax driver.

▶ The **LANCOM VPN Client** enables a setting of VPN connections from a remote workstation via Internet to a router with LANCOM VPN Option.

▶ With **LANCOM Online Documentation,** you can copy the documentation files on your PC.

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

EN

3 Basic configuration

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

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

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

At the end of this chapter we will show you the settings that are needed for the LAN's workstations to ensure trouble-free access to the router ('TCP/IP settings to workstation PCs' →page 44).

3.1 Which information is necessary?

The basic configuration wizard will take care of the basic TCP/IP configuration of the router, protect the device with a configuration password, and will set up the ISDN connection if required. The following descriptions of the information required by the wizard are grouped in these three configuration sections:

▶ TCP/IP settings

▶ protection of the configuration

▶ information related to the Wireless LAN

▶ information on DSL connection

▶ information on ISDN connection

▶ configuring connect charge protection

3.1.1 TCP/IP settings

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

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

New LAN—fully automatic configuration possible

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

▶ a single PC is connected to the router

▶ setup of a new network

Fully automatic TCP/IP configuration will not be available when integrating the LANCOM Wireless DSL in an existing TCP/IP LAN. In this case, continue with the section 'Information required for manual TCP/IP configuration' →page 35.

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

Configure manually nevertheless?

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

▶ Choose automatic configuration if you are **not** familiar with networks and IP addresses.

▶ Select manual TCP/IP configuration if you are familiar with networks and IP addresses, and one of the following conditions is applicable:

▷ You have not yet used IP addresses in your network but would like to do so now. You would like to specify the IP address for your router, selecting it from the address range reserved for private use, e.g. '10.0.0.1' with the netmask '255.255.255.0'. At the same time you will set the address range that the DHCP server uses for the other devices in the network (provided that the DHCP server is switched on).

▷ You have previously used IP addresses for the computers in your LAN.

Information required for manual TCP/IP configuration

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

35

EN

▶ **IP address and netmask for the LANCOM Wireless DSL**
Assign a free IP address from the address range of your LAN to the LANCOM Wireless DSL and specify the netmask.

▶ **Enable DHCP server?**
Disable the DHCP server function in the LANCOM Wireless DSL if you would like to have a different DHCP server assign the IP addresses in your LAN.

3.1.2 Configuration protection

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

The setup wizard for the basic configuration automatically disables remote configuration access via ISDN, thus protecting your configuration against tampering. ISDN remote configuration access can be enabled at any time using the security wizard (see 'Have you permitted remote configuration?' →page 77).

3.1.3 Settings for the Wireless LAN

The network name (SSID)

The basic configuration wizard asks for the network name of the base station (often designated as SSID – **S**ervice **S**et **Id**entifier). The network name will be registered in the base stations of the Wireless LAN. You can choose any name. Several base stations with the same network name form a common Wireless LAN.

Open or closed Wireless LAN?

Mobile radio stations dial‐in the wanted Wireless LAN by declaration of the network name. The specification of the network name is facilitated by two technologies:

▶ Mobile radio stations can search for Wireless LANs in the environs („scan") and offer for selection the found Wireless LANs in a list.

▶ By using the network name 'ANY', the mobile radio station will enrol in the next available Wireless LAN.

The Wireless LAN can be „closed" to prevent this procedure. In this case, no enrolment with the network name 'ANY' will be accepted.

For standard, LANCOM base stations are responsive under the network name 'LANCOM'. The wireless basic configuration of a base station takes therefore place via this network name. If another network name is set during the basic configuration, also the Wireless LAN access of the configuring mobile base station must be changed to this new network name after closing the basic configuration.

Selection of a radio channel

The base station operates in a certain radio channel. The radio channel will be selected from a list of up to 11 channels in the 2,4 GHz frequency range or up to 19 channels in the 5 GHz frequency range. (in various countries some radio channels are restricted, see appendix).

The used channel and frequency range define the operating of the common radio standard, in doing so the 5 GHz frequency range correspond to the IEEE 802.11a standard and the 2,4 GHz frequency range to the IEEE 802.11g and IEEE 802.11b standard.

If no further base stations operate in reach of the base station, any radio channel can be adjusted. Otherwise, the channels in the 2,4 GHz band must be chosen in the way that they preferably do not overlap one another or have a distance as great as possible respectively. The automatic setting is normally enough in the 5 GHz band, in which the LANCOM Wireless DSL base station itself adjust the best channel via TPC and DSF.

3.1.4   Settings for the DSL connection

For the DSL connection it may be necessary to enter the transfer protocol being used. The wizard will automatically enter the correct settings for major DSL providers. You only need to enter the protocol used by your DSL provider if the wizard does not list your provider.

3.1.5   Settings for the ISDN connection

Set up the basic configuration of your ISDN connection if required. You will need the following data:

▶ One or more ISDN MSNs on which the router will accept calls. MSNs are ISDN subscriber numbers that are assigned to you by your telephone pro-

EN

vider. They are normally entered without an area code. These numbers are only relevant for the router functions (LAN to LAN coupling, RAS), not for remote configuration and LANCOM VPN Option.

▶ A dialing prefix for access to the public telephone network. This is normally required only when using an ISDN PBX. '0' is the usual prefix. It is used for all outgoing calls.

▶ Finally, you should know whether your telephone provider transmits an ISDN connect-charge pulse. This signal can be used LANCOM Wireless DSL for connect-charge budgets and the accounting function.

3.1.6   Connect charge protection

Connect charge protection blocks connections that go beyond a previously set amount, protecting you from unexpectedly high connection costs.

In LANCOM Wireless DSL, there are three independent budgets: For DSL access, you can set a maximum connection time in minutes. In addition to this time budget, there is also a budget for limiting ISDN connection charges.

In order for the limitations according to connect charge rates to function properly, it is necessary to enter the information for connect charge rates through ISDN.

Any budget can be deactivated by entering the value '0'.

It is possible to completely turn off connect charge protection

In basic settings the charge protection is defined to maximum 600 minutes within seven days. Adapt this setting to your personal needs or deactivate the charge protection if you have arranged a flatrate with your provider.

3.2   Instructions for LANconfig

① Start up LANconfig by clicking **Start ▶ Programs ▶ LANCOM ▶ LANconfig**

LANconfig automatically detects the new LANCOM Wireless DSL in the TCP/IP network. Then the setup wizard starts that will help you make the basic settings of the device or will even do all the work for you (provided a suitable network environment exists).
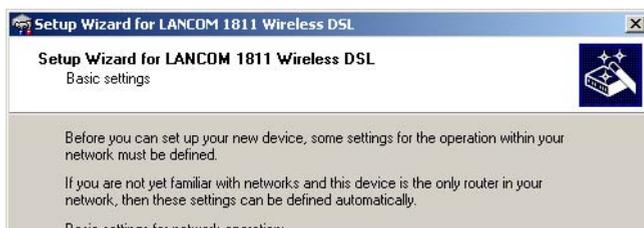
> If the setup wizard does not start automatically, start a manual search for new devices on all ports (if the LANCOM Wireless DSL is connected via a serial port) or in the network (**Device ► Find**).

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

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

② If you would like to configure the TCP/IP settings manually, assign an available address from a suitable address range to the LANCOM Wireless DSL. Confirm your choice with **Next**.

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

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

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

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

EN

⑤ Enter the wireless parameters. Select a network name (SSID) and a radio channel. Turn on if necessary the function for 'closed network'. Confirm your choice with **Next**.

⑥ In the next window, select your DSL provider from the list that is displayed. If you select 'My provider is not listed here,' you must enter the transfer protocol used by your DSL provider manually. Confirm your choice with **Next**.

⑦ Enter the ISDN subscriber numbers (as MSNs, i.e. without area code) on which the router will accept calls. Multiple numbers are separated by semicolons. If you do not specify any MSNs, the router will answer all incoming calls on the ISDN connection.

In addition, you can enter a trunk code for dialling into ISDN. Finally, you should specify whether or not the tariff information is to be transmitted at your ISDN connection. Confirm your choice with **Next**.

⑧ Connect charge protection can limit the cost of DSL and ISDN connections to a predetermined amount if desired. Confirm your choice with **Next**.

⑨ Complete the configuration with **Finish**.

> Section 'TCP/IP settings to workstation PCs' on page 44 will describe the settings required for the individual workstations in the LAN.

3.3   Instructions for WEBconfig

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

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

Network without DHCP server

In a network without DHCP server, unconfigured LANCOM devices activate their own DHCP server service after starting, and assign appropriate IP addresses and gateway information to the other workstations within the LAN, provided that the workstations are set to obtain their IP address automatically (auto-DHCP). In this constellation, the device can be accessed with any web browser from each PC with activated auto-DHCP function through the name **LANCOM** or by its IP address **172.23.56.254**.

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

Network with DHCP server

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

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

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

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

  ▷ Figure out the DHCP‑assigned IP address of the LANCOM by suitable tools and contact the device directly with this IP address.

  ▷ Use LANconfig.

  ▷ Connect a PC with a terminal program via the serial configuration interface to the device.

Starting the wizards in WEBconfig

① Start your web browser (e.g. Internet Explorer, Netscape Navigator, Opera) and call the LANCOM Wireless DSL there:

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

 (or with a name as discribed above)

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

The WEBconfig main menu will be displayed:

Setup Wizards

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

🔧 **Basic Settings**

🔧 **Security Settings**

🔧 **Setup Internet Access**

🔧 **Selection of Internet Provider**

🔧 **Setup a RAS Account**

🔧 **Connect Two Local Area Networks**

Device Configuration and Status

These menu options enable you to access the device's entire configuration:

📟 **Expert Configuration**

💾 **Save Configuration**

📂 **Load Configuration**

Firmware Handling

💾 **Perform a Firmware Upload**

Extras

🔍 **Show/Search Other Devices**

💾 **Get Device SNMP MIB**

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

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

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

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

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

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

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

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

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

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

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

3.4 TCP/IP settings to workstation PCs

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

Entering the password in the web browser

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

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

Entering the configuration password

▶ Default gateway – receives all packets that are not addressed to computers within the local network.

▶ DNS server – translates network names (www.**lancom.de**) or names of computers (**www**.lancom.de) to actual IP addresses.

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

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

▶ **IP address assignment via the LANCOM Wireless DSL (default)**

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

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

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

▶ **Manual IP address assignment**

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

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

EN

4 Setting up Internet access

All computers in the LAN can take advantage of the central Internet access of the LANCOM Wireless DSL. The connection to the Internet provider can be established via any WAN connection, i.e. not only via DSL, but also via the ISDN port (if present). Internet access via ISDN can be used as a backup connection for DSL, for example.
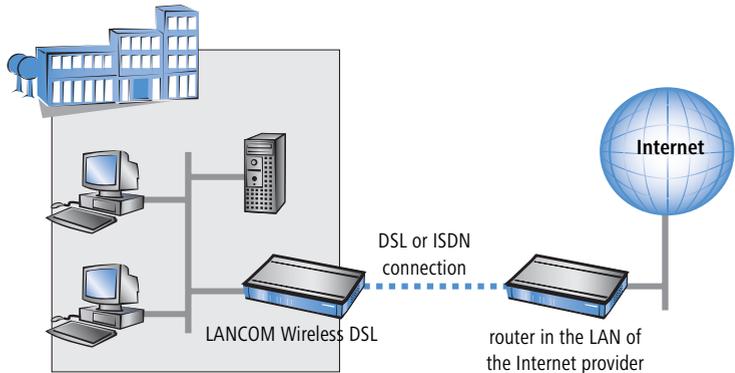
Does the setup wizard know your Internet provider?

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

Additional information for unknown Internet providers

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

▶ **DSL**

▷ Protocol: PPPoE, PPTP or Plain Ethernet (IPoE)

▷ Additionally for Plain Ethernet: own public IP address with netmask (not to be confused with the private LAN IP address), default gateway and DNS server. These values can be received automatically from providers that support DHCP.

    ▷ User name and password

▶ **ISDN** – dial-in number

    ▷ User name and password

Additional connection options

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

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

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

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

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

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

▶ Dynamic channel bundling (ISDN only)

    ▷ if required, the second ISDN B-channel will automatically be bundled to the connection. This doubles the available bandwidth; it may also double your connect charges as well, however. What's more, your ISDN connection will be busy in this case, with all other incoming and outgoing calls being rejected.

▶ Data compression (ISDN only)

    ▷ this permits an additional increase in data throughput.

EN

4.1   Instructions for LANconfig

① Highlight the LANCOM Wireless DSL in the selection window. From the menu bar, select **Tools** ► **Setup Wizard**.
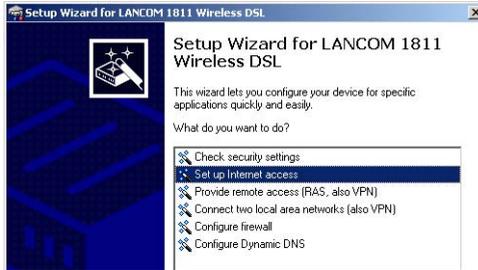
② From the menu, select the **Setup Internet access** wizard and click **Next**.

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

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

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

LANconfig:
Quick access to the setup wizards

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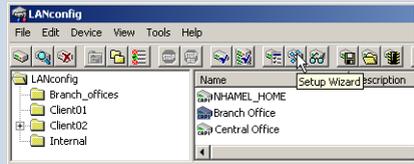
4.2   Instructions for WEBconfig

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

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

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

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

5 Linking two networks

With the network interconnection (also known as LAN to LAN coupling) of the LANCOM Wireless DSL, two local networks are linked. The LAN to LAN coupling can be realized in principle in two different ways:

Only LANCOM 1811 Wireless DSL and LANCOM 1821 Wireless ADSL

EN

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

▶ **ISDN**: For coupling via ISDN, a direct connection between both LANs is established over an ISDN connection. A router with ISDN interface is required in both LANs.

Always configure both sides

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

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

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

Security aspects

You must, of course, protect your LAN against unauthorized access. A LANCOM Wireless DSL therefore offers a whole range of security mechanisms that can provide an outstanding level of protection:

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

▶ **ISDN**: For network couplings via ISDN, the connection password, the checking of the ISDN number and the callback function ensure the security of the connection.

> The ISDN call back function cannot be configured using the wizard. It can only be set up in the expert configuration. For details, please see the reference manual.

5.1 What information is necessary?

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

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

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

5.1.1 General information

The following details are required for the installation of LAN to LAN couplings. The first column indicates, whether the information is required for network couplings over VPN (standard method using "preshared keys") and/or ISDN.

> Further details to network couplings via VPN using enhanced methods can be found in the LCOS reference manual.

Coupling	Entry	Gateway 1		Gateway 2
VPN	ISDN connection available?	yes/no		yes/no
VPN	Type of the local IP address	static/dynamic	⤬	static/dynamic
VPN	Type of the remote IP address	static/dynamic		static/dynamic
VPN + ISDN	Name of the local device	'HEAD'	⤬	'BRANCH'
VPN + ISDN	Name of the remote station	'BRANCH'		'HEAD'
VPN + ISDN	Remote ISDN calling number	(0123) 123456	⤬	(0789) 654321
VPN + ISDN	Remote ISDN caller ID	(0789) 654321		(0123) 123456
VPN + ISDN	Password for secure transmission of the IP address	'Password'	⟷	'Password'
VPN	Shared secret for encryption	'Secret'	⟷	'Secret'

Coupling	Entry	Gateway 1		Gateway 2
VPN	IP address of remote station	'10.0.2.100'		'10.0.1.100'
VPN	IP network address of the remote network	'10.0.2.0'		'10.0.1.0'
VPN	Netmask of the remote network	255.255.255.0		255.255.255.0
VPN	Domain name of the remote network	'head'		'branch'
VPN	Hide local stations for access to remote network (Extranet VPN)?	yes/no		yes/no
ISDN	TCP/IP routing for access to remote network	yes/no		yes/no
ISDN	IPX routing for access to remote network	yes/no		yes/no
VPN + ISDN	NetBIOS routing for access to remote network?	yes/no		yes/no
VPN + ISDN	Name of remote workgroup (NetBIOS only)	'workgroup1'		'workgroup2'
ISDN	Data compression	on/off	◀▶	on/off
ISDN	Channel bundling	on/off	◀▶	on/off

▶ In case your device has an **ISDN connection**, the wizard asks whether the remote site has ISDN as well.

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

Thanks to Dynamic VPN, connections can be enabled not only between gateways with fixed, static IP addresses, but even between gateways with dynamic IP addresses. The active initiation of VPN connections towards remote sites with dynamic IP addresses requires ISDN.

▶ If you haven't already named your LANCOM Wireless DSL, the wizard will ask you for a new, **unique device name.** With this entry, you will rename your LANCOM Wireless DSL. Be sure to give the two devices different names.

▶ The **name of the remote station** is needed for its identification.

▶ Enter the subscriber number of the remote station in the **ISDN subscriber number** field. The complete subscriber number including all necessary area and country codes is required.

▶ The stated **ISDN caller ID** is used to identify and authenticate callers. When a LANCOM Wireless DSL receives a call, it compares the ISDN caller ID entered for the remote station with the actual caller ID transferred via
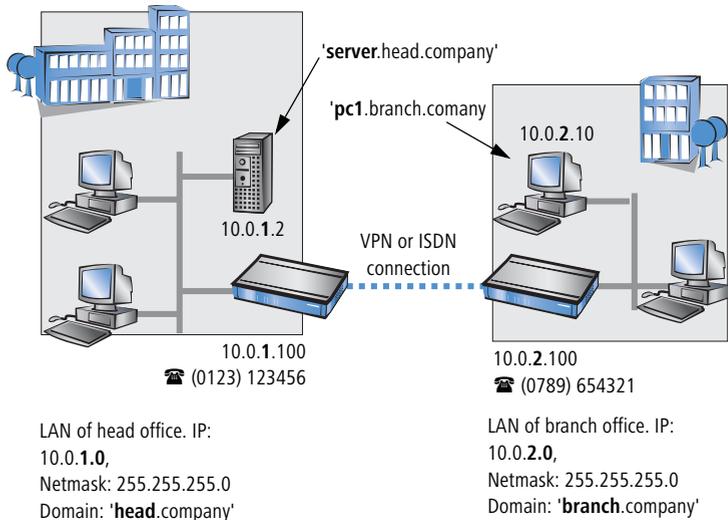
the D channel. An ISDN caller ID generally consists of an area code and an MSN.

► The **password for the ISDN connection** is an alternative to the use of the ISDN caller ID. It is always used to authenticate callers that do not send an ISDN caller ID. The exact same password must be entered on both sides. It is used for calls in both directions.

► The **Shared Secret** is the central password for security within the VPN. The exact same password has to be entered on both sides

► Data compression increases the transfer speed of the connection at no additional cost. This is completely unlike the bundling of two ISDN- channels with MLPPP (**Multi Link PPP**): The transfer rate will be doubled but there will also be additional telephone costs for two connections.

5.1.2 Settings for the TCP/IP router

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

'**server**.head.company'

'**pc1**.branch.comany'

10.0.**2**.10

10.0.**1**.2

VPN or ISDN
connection

10.0.**1**.100
☎ (0123) 123456

10.0.**2**.100
☎ (0789) 654321

LAN of head office. IP:
10.0.**1.0**,
Netmask: 255.255.255.0
Domain: '**head**.company'

LAN of branch office. IP:
10.0.**2.0**,
Netmask: 255.255.255.0
Domain: '**branch**.company'

Unlike when accessing the Internet, all of the IP addresses in the involved networks are visible on the remote side when coupling networks, not just those of the router. The computer with the IP address 10.0.2.10 in the branch office

EN

LAN sees the server 10.0.1.2 in the headquarters and can access it (assuming it has the appropriate rights), and vice versa.

DNS access to the remote LAN

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

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

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

Extranet VPN

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

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

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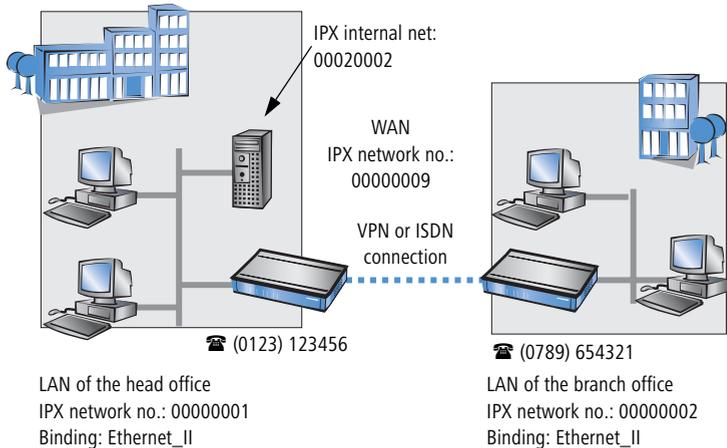
5.1.3 Settings for the IPX router

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

Coupling two typical IPX networks to form a WAN requires three IPX network numbers:

▶ for the LAN of the head office

▶ for the LAN of the branch office

▶ for the higher-level WAN

The IPX network numbers in the head and branch offices are specified to the respective remote sides.

IPX internal net:
00020002

WAN
IPX network no.:
00000009

VPN or ISDN
connection

☎ (0123) 123456

☎ (0789) 654321

LAN of the head office
IPX network no.: 00000001
Binding: Ethernet_II

LAN of the branch office
IPX network no.: 00000002
Binding: Ethernet_II

The three required network numbers are designated as "External Network Numbers" by the IPX conventions. Like IP network addresses, the apply to an entire LAN segment. On the other hand, internal IPX numbers are used to address specific Novell servers in the LAN. All three specified network numbers must be distinct from one another and from all used internal IPX network numbers.

In addition, it may be necessary to enter the frame type ("binding").

Specifying the IPX network number and binding used is not necessary if the remote network also contains a Novell server. It is only necessary to enter the network number for the WAN manually in this case.

5.1.4   Settings for NetBIOS routing

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

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

5.2   Instructions for LANconfig

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

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

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

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

5.3   Instructions for WEBconfig

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

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

EN

① From the main menu, launch the 'Connect two local area networks' wizard. Follow the wizard's instructions and enter the required information.

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

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

Ping – quick testing for TCP/IP connections

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

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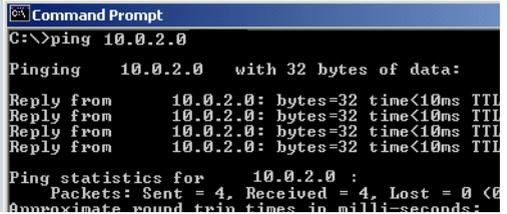

```
Command Prompt
C:\>ping 10.0.2.0

Pinging    10.0.2.0    with 32 bytes of data:

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

Ping statistics for    10.0.2.0 :
    Packets: Sent = 4, Received = 4, Lost = 0 (0
Approximate round trip times in milli-seconds:
```

---

6   Providing dial-up access

Your LANCOM Wireless DSL supports dial-up connections to permit individual computers full access to your network. This service is also known as RAS (Remote Access Service). In principle, the RAS access can be realized in two different ways:

Only LANCOM 1811 Wireless DSL and LANCOM 1821 Wireless ADSL

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

▶ **ISDN**: For a RAS access via ISDN, a direct connection between the LAN and the dial-in PC is established over an ISDN dial-up connection. The router in the LAN requires an ISDN interface, the dial-up PC an ISDN adapter or an ISDN modem. The data transfer protocol is PPP. Therefore, the support of all usual devices and operating systems is ensured.

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

Security aspects

You must, of course, protect your LAN against unauthorized access. An LANCOM Wireless DSL therefore offers a whole range of security mechanisms that can provide an outstanding level of protection:

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

▶ **ISDN**: For network couplings via ISDN, the connection password, the checking of the ISDN number and the callback function ensure the security of the connection.

ⓘ   The ISDN call back function cannot be configured using the wizard. It can only be set up in the expert configuration. For details, please see the reference manual.

6.1   Which information is required?

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

6.1.1 General information

The following entries are required to set up a RAS connection. The first column indicates whether the information is required for a connection via VPN (standard method using "preshared keys") and/or ISDN .

> **ⓘ** Further details to RAS connections via VPN using enhanced methods can be found in the LCOS reference manual.

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

Notes to the individual values:

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

▶ **Incoming number**: The LANCOM Wireless DSL uses the optional ISDN caller ID as an additional user authentication. This security function should not be used when users dial in from differing locations.

> **ⓘ** Please refer to chapter 'Zwei Netzwerke verbinden' auf Seite 50 for advice about the other values required for the installation of a RAS access.

The ISDN calling line identity (CLI)

The ISDN caller ID—also known as CLI (**C**alling **L**ine **I**dentity)—this is the telephone number of the caller which is transmitted to the participant receiving the call. As a rule, it consists of the country and area codes and an MSN.

The CLI is well- suited for authentication purposes for two reasons: it is very difficult to manipulate, and the number is transferred free of charge via the ISDN control channel (D- channel).

6.1.2 Settings for TCP/IP

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

LAN of the head office.
IP: 10.0.**1**.0

Remote workstation
IP: 10.0.**1**.101

VPN or ISDN connection

ISDN adapter

10.0.**1**.100
☎ (0123) 123456

User: 'SAMPLE'
☎ (0123) 777888
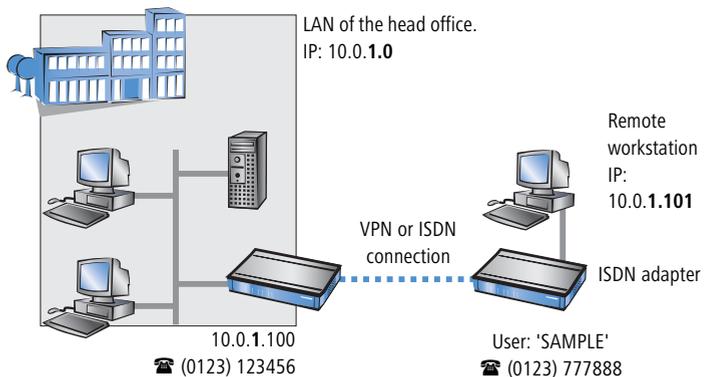
This IP address can be permanently assigned when setting up a user. However, it is simpler to let the LANCOM Wireless DSL automatically assign free IP addresses to users when they dial in. In this case you only need to specify the IP address range that the LANCOM Wireless DSL should use for RAS users.

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

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

EN

6.1.3   Settings for IPX

Two IPX network numbers must be provided for remote access to an IPX net-work:

▶ the IPX network number of the head office

▶ an additional IPX network number for the higher-level WAN

IPX internal net:
00020002

WAN
IPX network no.:
00000009

Remote
workstation

VPN or ISDN
connection

ISDN adapter

☎ (0123) 123456

User: 'SAMPLE'
☎ (0123) 777888

LAN of the head office
IPX network no.: 00000001, Binding: Ethernet_II
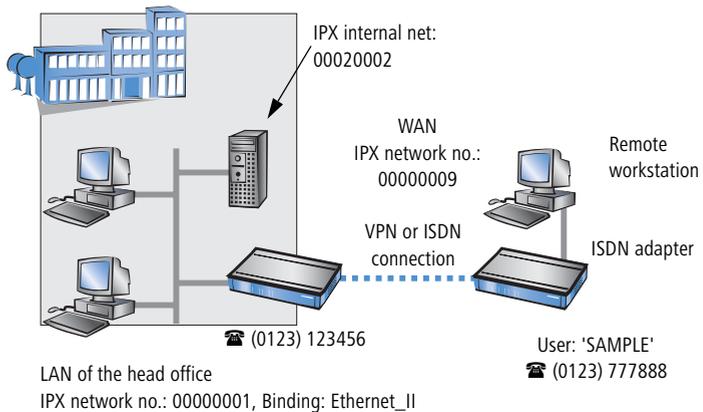
The required network numbers are designated as "External Network Num-bers". Like IP network addresses, they apply to an entire LAN segment. On the other hand, internal IPX numbers are used to address specific Novell servers in the LAN. All three specified network numbers must be distinct from one another and from all used internal IPX network numbers.

In addition, it may be necessary to enter the frame type ("binding").

Specifying the IPX network number and binding used is not necessary if the remote network also contains a Novell server. A network number for the WAN must also be entered manually in this case, however.

6.1.4   Settings for NetBIOS routing

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

The connection is not established automatically. The RAS user must manually establish a connection to the LANCOM Wireless DSL via Dial-Up Networking first. When connected, they can search for and

access computers in the remote network (via **Find** ▶ **Computer**s, not through the Network   Neighbourhood).

6.2 Settings for the dial-in computer

6.2.1 Dial-up via VPN

For dialing into a network via VPN a workstation requires:

▶ an Internet access

▶ a VPN client

LANCOM Systems offers the LANCOM VPN Client on the LANCOM CD. It can be run under Windows 2000 and Windows XP. A detailed description of the LANCOM VPN Client and a description of its installation can also be found on the CD.

For configuring a new profile, select the option 'Configure VPN Remote Access (IPSec over PPTP)' in the LANCOM VPN Client configuration wizard.
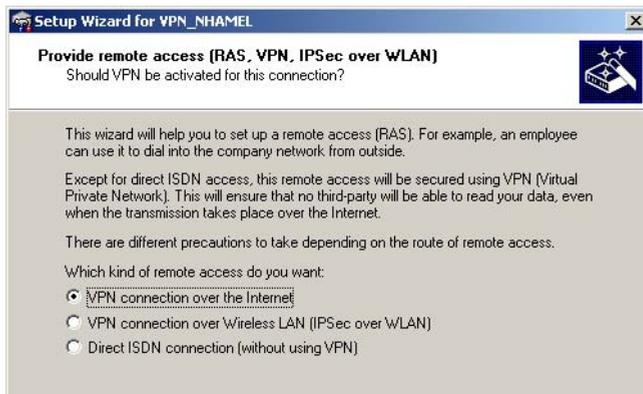
The wizard asks then for the values that have been defined during the installation of the RAS access in the LANCOM Wireless DSL.

EN

Please notice the following relationship between the names of the entries of the LANCOM VPN Client and the LANconfig wizard:

LANCOM VPN Client	LANconfig
Preshared Key	Shared Secret
PPTP User name	Name
PPTP password	Password

6.2.2 Dial-up via ISDN

A number of settings must be configured on the dial-in computer. These are briefly listed here, based on a Windows computer:

▶ Dial-Up Networking (or another PPP client) must be correctly configured

▶ Network protocol (TCP/IP, IPX) installed and bound to the dial-up adapter

▶ New connection in Dial-Up Networking with the call number of the router

▶ Terminal adapter or ISDN card set to PPPHDLC

▶ PPP selected as the Dial-Up server type, 'Enable software compression' and 'Require data encryption' unchecked

▶ Select desired network protocols (TCP/IP, IPX)

▶ Additional TCP/IP settings:

　▷ Assignment of IP address and name server address enabled

　▷ 'IP header compression' disabled

These settings will permit a PC to dial into a remote LAN via ISDN and access its resources in the usual manner.

6.3 Instructions for LANconfig

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

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

③ Configure Dial-Up Networking access on the dial-in PC as described. Next, test the connection (see box 'Ping – quick testing for TCP/IP connections' →page 56).

6.4   Instructions for WEBconfig

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

④ From the main menu, launch the 'Connect two local networks' wizard. Follow the wizard's instructions and enter the required information.

⑤ Configure Dial-Up Networking access on the dial-in PC as described. Next, test the connection (see box 'Ping – quick testing for TCP/IP connections' →page 56).

EN

7   Sending faxes with LANCAPI

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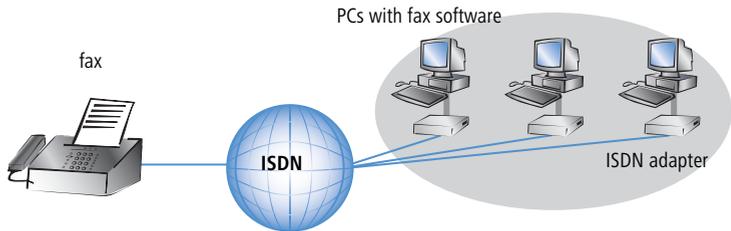
With LANCAPI by LANCOM it is possible to send faxes comfortably from your workstation PC, without having connected a fax device. To do so, you need to install several components:

▶ the **LANCAPI client**. It provides the connection between your workstation PC and the LANCAPI server.

▶ the **CAPI fax modem**. 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 fax modem** and MS Windows fax service.

7.1   Installation of the LANCOM CAPI fax modem

① Select the entry **Install LANCOM software** in the setup program of your LANCOM CD**.**

② Highlight the option **CAPI fax modem**, click **Next** and follow the instructions of the installation routine**.**

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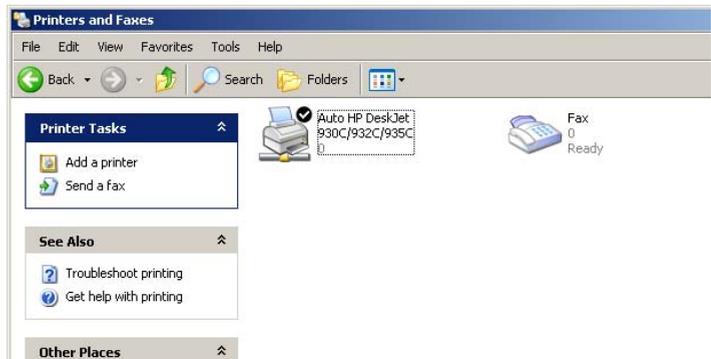
For checking the installation, click with the right mouse button on the fax-icon and select **Properties**. The LANCOM **CAPI fax modem should now be entered into register** 'devices'.

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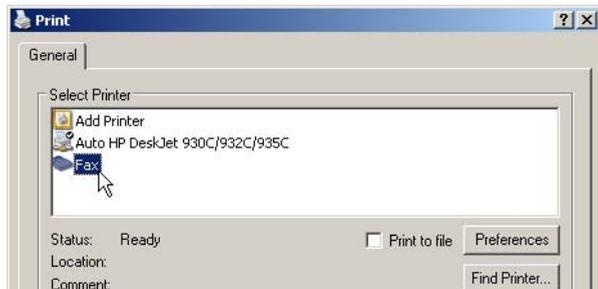
③ Click on OK. A wizard appears, that will guide you through the remaining sending process.

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.
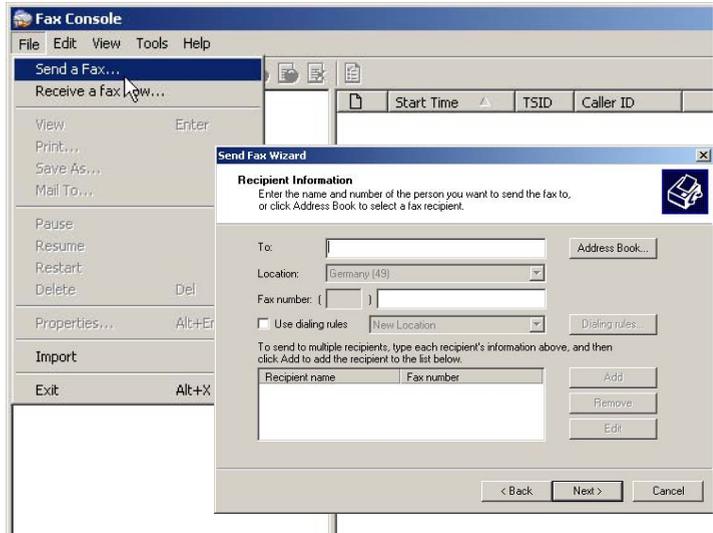
8 Security settings

Your LANCOM Wireless DSL has numerous security functions. You find in this chapter all information you need for an optimal protection.

8.1 Security for the Wireless LAN

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

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

▶ Closed network

▶ Access Control (via MAC‑addresses)

▶ LANCOM Enhanced Passphrase Security

▶ Encryption of data transfer (802.11i/WPA or WEP)

▶ 802.1x / EAP

▶ optional IPSec over WLAN (VPN), in combination with external VPN gateway

8.1.1 Closed network

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

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

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

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

EN

8.1.2 Access control via MAC address

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

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

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

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

8.1.3 LANCOM Enhanced Passphrase Security

With LEPS (**L**ANCOM **E**nhanced **P**assphrase **S**ecurity) LANCOM Systems has developed an efficient method which uses the simple configuration of IEEE 802.11i with passphrase and yet which avoids the potential error sources of passphrase sharing. LEPS uses an additional column in the ACL to assign an individual passphrase consisting of any 4 to 64 ASCII characters to each MAC address. The connection to the access point and the subsequent encryption with IEEE 802.11i or WPA is only possible with the right combination of passphrase and MAC address.

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

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

8.1.4 Encryption of the data transfer

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

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

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

▶ Regularly change the WEP keys in your access points. The passphrases for 802.11i or WPA do not have to be changed regularly as new keys are generated for each connection anyway. This is not the only reason that the encryption with 802.11i/AES or WPA/TKIP is so much more secure than the now aged WEP method.

▶ If the data is of a high security nature, you can further improve the encryption by additionally authenticating the client with the 802.1x method ('802.1x / EAP' →page 72) or activate an additional encryption of the WLAN connection as used for VPN tunnels ('IPSec over WLAN' →page 73). In special cases, a combination of these two mechanisms is possible.

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

Please take note of the information in the box "Standard WEP encryption".

EN

Standard WEP encryption

As of LCOS version 4.0, WEP128 encryption is activated for every uncon-figured device as standard.

The key 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 "00A0570FB9BF" thus has a standard WEP key of "L00A0570FB9BF". This key is entered into the 'Private WEP settings' of the device for each logical WLAN network as 'Key 1'.

To use a WLAN adapter to establish a connection to a new LANCOM access point, the WEP128 encryption must be activated for the WLAN adapter and the standard 13-character WEP key entered.

Note that a reset also causes the WLAN key settings to be lost from the device and the standard WEP key comes into effect again. WLAN access can only work after a reset if the standard WEP key is programmed into the WLAN adapter as well.

8.1.5 802.1x / EAP

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

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

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

8.1.6 IPSec over WLAN

By means of IPSec over WLAN a radio network can be optimally secured in addition to the already introduced securing mechanisms.

In order to run IPSec over WLAN you have to upgrade the base stations of the with the LANCOM VPN option and the LANCOM Advanced VPN Client, which runs under the operating systems Windows 98ME, Windows 2000 and Windows XP. For other operating systems client software from other manufacturers is available. The drivers for the LANCOM AirLancer wireless adapter are already equipped with a 802.1x client.

8.1.7 Tips for handling keys

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

▶ **Keep keys as secret as possible.**
  Never note a key. Popular, but completely unsuitable are for example: notebooks, wallets and text files in PCs. Do not share a key unnecessarily.

▶ **Select a random key.**
  Use randomized keys of character and number sequences. Keys from the general linguistic usage are insecure.

▶ **Change a key immediately in case of suspicion.**
  It is time to change the key of the Wireless LAN if an employee with access to a key leaves your company. The key should also be renewed in case of smallest suspicion of a leak.

8.2 The security settings wizard

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

EN

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

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

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

8.2.1 Wizard for LANconfig

① Mark your LANCOM Wireless DSL in the selection window. Select from the command bar **Extras** ▶ **Setup Wizard**.
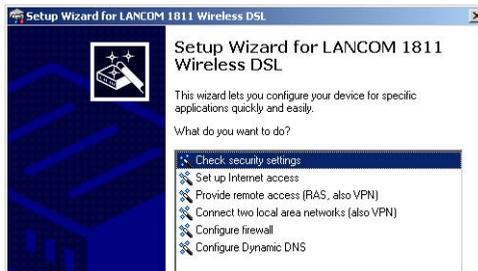
② Select in the selection menu the setup wizard **Control Security Settings** and confirm your choice with **Next**.

③ Enter your password in the following windows and select the allowed protocols for the configuration access from local and remote networks. Additionally, enter the MSN for remote configuration via ISDN.

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

⑤ Now you can set the security settings for the WLAN. These include the name of the wireless network, the closed network function and the WEP encryption. You can type in the parameters for both wireless networks separately on devices with the option of a second WLAN interface.

⑥ Now you specify filter lists for stations (ACL) accessing the WLAN and protocols. Thereby, you restrict data exchange between the wireless network and the local network.

⑦ Now activate Stateful Inspection, ping-blocking and Stealth mode in the the firewall configuration.

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

8.2.2 Wizard for WEBconfig

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

▶ password for the device

▶ allowed protocols for the configuration access of local and remote networks

▶ the MSN for remote configuration via ISDN

▶ parameters of configuration lock (number of failed log-in attempts and duration of the lock)

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

8.3 The firewall wizard

The LANCOM Wireless DSL incorporates an effective protection of your LAN and WLAN when accessing the Internet by its Stateful Inspection firewall and its firewall filters. Basic idea of the Stateful Inspection firewall is that only self-initiated data transfer is considered allowable. All unasked accesses, which were not initiated from the local network, are inadmissible.

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

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

8.3.1 Wizard for LANconfig

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

① Mark your LANCOM Wireless DSL in the selection window. Select from the command bar **Extras** ▶ **Setup Wizard**.
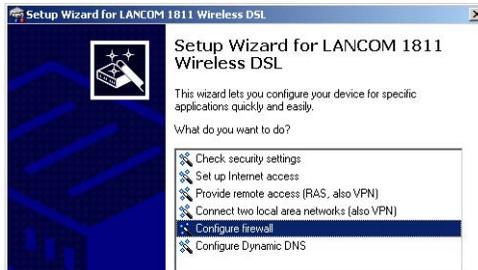
② Select in the selection menu the setup wizard **Configuring Firewall** and confirm your choice with **Next**.

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

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

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

8.3.2 Configuration under WEBconfig

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

8.4 The security checklist

In the following checklist you will find an overview of the most important security functions. That way you can be quite sure not to have overlooked anything important during the security configuration of your LANCOM.

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

The simplest option for the protection of the configuration is the establishment of a password. As long as a password hasn't been set, anyone can change the configuration of the device. The box for entering the password is located in LANconfig in the 'Management' configuration area on

the 'Security' tab. It is particularly advisable to assign a password to the configuration if you want to allow remote configuration.

▶ **Have you permitted remote configuration?**

If you do not require remote configuration, then deactivate it. If you require remote configuration, then be sure to assign a password protection for the configuration (see previous section). The field for deactivating the remote configuration is also contained in LANconfig in the 'Management' configuration area on the 'Security' tab.

▶ **Have you permitted the configuration by the wireless network?**

If you do not require configuration by the wireless network, then deactivate it. The field for deactivating the configuration by the wireless network is also contained in LANconfig in the 'Management' configuration area on the 'Security' tab. Select here under 'Access rights - from Wireless LAN' for all types of configuration the option 'not allowed'.

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

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

▶ **Have you activated the Firewall?**

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

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

For maximum security and control you prevent at first any data transfer through the Firewall. Only those connections, which are explicitly desired have to allowed by the a dedicated Firewall rule then. Thus 'Trojans' and certain E-mail viruses loose their communication way back. The Firewall rules are summarized in LANconfig under 'Firewall/Qos' on the register card 'Rules'. A guidance can be found in the reference manual.

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

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

found in the LANconfig in the 'IP router' configuration section on the 'Routing' tab.

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

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

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

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

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

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

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

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

As of LCOS version 4.0, WEP128 encryption is activated for every unconfigured device as standard ('Standard WEP encryption' →page 72).

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

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

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

▶ **Have you set the 802.1x functions for particularly sensitive data exchange in the wireless network?**

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

EN

9 Options and accessories

Your LANCOM Wireless DSL base station 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 Extender series and can be adapted to special conditions of environs.

▶ With the LANCOM Public Spot Option option it is possible to extend the LANCOM Wireless DSL for additional billing and accounting functions in order to upgrade it to a Wireless Public Spot.

9.1 Optional AirLancer Extender antennas

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

For installation of an optional AirLancer Extender antenna turn off the LANCOM Wireless DSL by pulling out the power supply cable of the device. Remove now carefully the two diversity antennas on the back by screwing them out. Connect the AirLancer Extender antennas to the antenna connector with the inscription 'Antenna Main'.

'Antenna Main' connector for AirLancer Extender antenna

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

EN

9.2 LANCOM Public Spot Option

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

The Wireless LAN technology is ideally suitable to offer wireless Internet services to the public at places such as airports, hotels, stations, restaurants or cafés, so-called Public Hot Spots. The LANCOM Public Spot Option is intended for operators of public wireless networks, and unveils additional functions for authentication and billing of public Internet services for the LANCOM Wireless DSL base station, thus enabling a simple set-up and maintenance of public hot spots.

The authentication and billing of the individual users is realized via user-friendly web sites, so that client PCs with a Wi-Fi certificated radio card (e.g. AirLancer) and a standard Internet browser can directly go online.

The LANCOM Public Spot Option is the optimal solution for public Wireless LANs. Wireless LANs are very suitable for company networks and for wireless networking at home. But for public access services, there is a lack of mechanisms for authentication and billing of single users (AAA - Authentication / Authorisation / Accounting). This lack remedies the LANCOM Open User Authentication (OUA), the main part of the LANCOM Public Spot Option. The OUA procedure realizes the authentication of all wireless clients via user name and password, and checks the authorization of single users via RADIUS. Accounting data (online time and data volume) can be transferred per user and per session to a central RADIUS server. Client PCs need only radio card (e.g. AirLancer), TCP/IP and an Internet browser. Additional software is not needed. Therefore, the public spot option is ideally suitable to install wireless

Internet access services in hotels, restaurants, cafés, airports, stations, exhibition centres or universities.
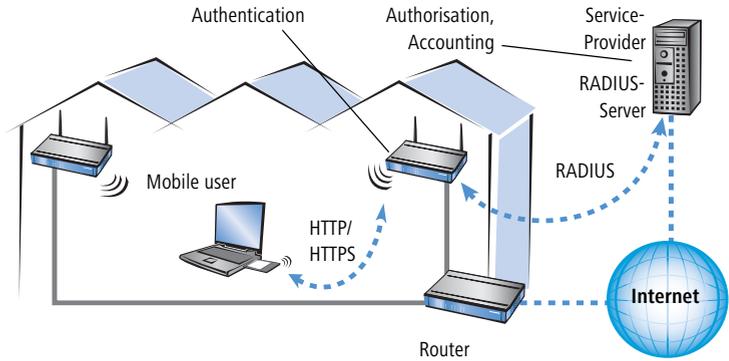
With the LANCOM Public Spot Option you extend a base station additionally with these functions and upgrade it to a Wireless Public Spot.

10   Troubleshooting

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

10.1   No DSL connection is established

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

Problems with the cabling?

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

Has the correct transfer protocol been selected?

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

You can monitor and correct the protocol settings under:

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

10.2   DSL data transfer is slow

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

EN

Numerous other factors involving the Internet itself can also influence the transfer rate.

Increasing the TCP/IP window size under Windows

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

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

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

10.3   Unwanted connections under Windows XP

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

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

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 **Expert configuration** ▶ **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**.

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

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 1511 Wireless DSL	LANCOM 1521 Wireless ADSL	LANCOM 1811 Wireless DSL	LANCOM 1821 Wireless ADSL
Connections	Ethernet LAN	4x 10/100Base-TX, auto sensing, switch with node/hub auto sensing, cable tester			
	WAN (ADSL)	**LANCOM Wireless DSL series:** 10/100Base-TX, auto sensing **LANCOM Wireless ADSL series:** 'Annex A' devices: ADSL over POTS to ITU G.992.5 (ADSL2+), ADSL over POTS to ITU G.992.1 Annex A, ANSI T1.413, ITU G.992.2 (G.Lite), G.994.1 (G.hs); 'Annex B' devices: ADSL over ISDN to ITU G.992.5 (ADSL2+), ADSL over ISDN to ITU G.992.1 Annex B, as well as ADSL over ISDN proprietary (Texas Instruments, ADI, Alcatel), ETSI TS 101 388;			
	ISDN	ISDN S0			
	WLAN	internal wireless module, IEEE 802.11b/g		internal wireless module, IEEE 802.11a switchable to IEEE 802.11b/g	
	Outband	serial V.24/V.28 port (8 pol. mini DIN)			
	Power supply	12V over external power adapter			
Operating modes	Multiprotocol router	IP router, IPX router, NAT/inverse NAT (IP masquerading) DHCP server incl. auto-detection, DHCP client, DHCP relay server, DNS server, PPPoE client, PPTP client, NetBIOS proxy, DynDNS client			
	WLAN client	client mode for the connecting of printers or PCs with Ethernet connection			
	WLAN access point	up to 255 clients			
	WLAN bridge	Point-to-multipoint connection up to 7 Ethernet LANs (mixed operation possible)			
	ISDN gateway	ISDN S0 bus, multi-device mode and point-to-point mode, I.430, (auto sensing), D channel: 1TR6, DSS1 (Euro ISDN); B channel: PPP (asynchronous/synchronous), X.75, HDLC, MLPPP for channel bundling, CAPI 2.0 via LANcapi, Stac data compression			
Protocols	LAN	IP: ARP, Proxy ARP, IP, ICMP, UDP, TCP, TFTP, RIP-1, RIP-2, DHCP, DNS, SNMP, HTTP, HTTPS, BOOTP, NTP, NetBIOS, LANCAPI			
		IPX: RIP, SAP, IPX- and SPX-Watchdogs, NetBIOS Watchdogs			
	WAN	PPPoE, PPPoA, PPTP, IPoA and plain ethernet		PPPoE, PPPoA, PPTP, IPoA and plain ethernet	
Transmitting power (maximum)	LAN	100 Mbps, full-duplex			
	WAN		8 Mbit/s (ADSL)		8 Mbit/s (ADSL)

		LANCOM 1511 Wireless DSL	LANCOM 1521 Wireless ADSL	LANCOM 1811 Wireless DSL	LANCOM 1821 Wireless ADSL
ATM	Transport		up to 8 ATM AAL-5 PVCs		up to 8 ATM AAL-5 PVCs
	OAM		ATM-F4- and F5-loop-back		ATM-F4- and F5-loop-back
Wireless LAN	Frequency band	2400 - 2483,5 MHz (ISM)		2400 - 2483,5 MHz (ISM) or 5150 - 5750 MHz	
	Standards and transfer rates *	54 Mbps according to IEEE 802.11g (fallback to 48, 36, 24, 18, 12, 11, 9, 6, 5,5, 2, 1 Mbps, automatic rate selection) compatible to IEEE 802.11b		up to 108 Mbps (turbo mode) according to IEEE 802.11a (fallback to 54,48, 36, 24, 18, 12, 9, 6 MBit/s, automatic rate selection), or up to 54 Mbps according to IEEE 802.11g (fallback to 48, 36, 24, 18, 12, 11, 9, 6, 5,5, 2, 1 Mbps, automatic rate selection) compatible to IEEE 802.11b	
	Ranges *	up to 150 m (up to 30 m in buildings)			
	Transmitting power	up to 17 dBm in 2,4 GHz band with manual power setting		up to 17 dBm in 2,4 GHz band, up to 18dBm in 5 GHz band with power control (TPC) and manual power setting	
	Radio channels	11 channels, max. 3 non-overlapping (2,4 GHz band)		up to 17 dBm in 2,4 GHz band, up to 18dBm in 5 GHz band with power control (TPC) and manual power setting	
	Roaming	change between radio cells (seamless handover), IAPP support			
	MultiSSID	8 autonomous wireless netweorks at the same time			
	VLAN	up to 4094 VLAN IDs or WLAN connections, 32 simultaniously, 802.1p/q VLAN support for LAN and WLAN, 32 VLAN segments, 8 priorities			
Security	WLAN	IEEE 802.11i / WPA with passphrase or 802.1x and hardware encrypted AES, closed network, WEP64, WEP128, WEP152, access control lists, RADIUS client,user authentication, 802.1x / EAP, LEPS			
				hardware accelerated IPSec-over-WLAN for optional IPSec encryption of the radio link	
	Router, LAN, ISDN	Intrusion detection (IP spoofing, Log-in attempts, portscans), denial-of-service protection (fragmentation error, SYN flooding, automatic closing of ports/connections). DNS hitlists as well as wildcard filter (URL blocking). High availability by ISDN dial-backup for Internet access. Alerting by email, SNMP traps and SYSLOG. PAP, CHAP and MS-CHAP as PPP authentication mechanisms, password protected configuration access pro interface, access control list (IP, MAC and protocol filter) for configuration access and LANCAPI, ISDN dial up number list. FirmSafe with 2 firmware versions for absolute secure software upgrades.			
Firewall		Stateful Inspection, IP packet filter with port ranges; masking (NAT/PAT) of TCP, UDP, ICMP, FTP, PPTP, H.323,Net meeting, IRC and IPSec; DNS forwarding; inverse masking for IP services out of the intranet as e.g. web server; support of 2 local networks (LAN plus DMZ); DMZ with own IP address range without NAT.			

EN

▶ *Chapter 11: Appendix*

	LANCOM 1511 Wireless DSL	LANCOM 1521 Wireless ADSL	LANCOM 1811 Wireless DSL	LANCOM 1821 Wireless ADSL
Management	LANtools (professional management software for Windows), WEBconfig (HTTP / HTTPS), Telnet, TFTP, SNMP V2 (MIB II, 802.11, 802.1D, 802.3, private MIB), RADIUS, syslog remote maintenance via ISDN, DynDNS ssh configuration access outband interface as command line interface or optional as COM port for connecting external modems			
Antenna connections	two 3 dBi dipole antennas (in package contents). 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.de.			
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 55024, EN 55022, EN 55011, EN 50081, EN 60950, ES 59005, EN 60950		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. More information about added notifications under www.lancom.de.			
Environment / temperature range	Temperature range 0°C to +35°C at 80% max. humidity (non condensing)			
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, 1.2 A for LANCOM Wireless ADSL series), printed manual (English, German), software CD		

EN

		LANCOM 1511 Wireless DSL	LANCOM 1521 Wireless ADSL	LANCOM 1811 Wireless DSL	LANCOM 1821 Wireless ADSL
Options		LANCOM Public Spot Option (authentification and accounting software for hotspots) (Art. no. 60642) LANCOM leased line option (Art.Nr. 00789)		LANCOM Public Spot Option (authentification and accounting software for hotspots) (Art. no. 60642) LANCOM VPN Option 25 channels (max.25 simultaneous connections, 50 connections configurable) for VPN in WAN or IPSec‑over‑WLAN (Art. no.60083) LANCOM eased line option (Art.Nr. 00789)	
Optional antennas		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 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‑5 surge arrestor for antenna cables Art. no. 61212 AirLancer Extender SA‑LAN surge arrestor for LAN cables Art. no. 61213 LANCOM Modem Adapter Kit for connecting modems (analogue or GSM) to the serial configuration interface Art. no. 110288			
				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	

* The effective range and data transfer rate depend on site conditions and possible disturbances.

11.2 Radio channels

11.2.1 Radio channels in the 2,4 GHz frequency band

In the frequency range from 2400 to 2483 MHz are up to 13 channels available. The following overview shows which channels are supported by the dif-

ferent regions (EU/WORLD). The last column shows which channels can be used without overlapping.

Frequency range	2400–2500 MHz		no overlapping with
Channel No.	EU (ETSI)	WORLD (ETSI + FCC)	
1	2412	2412	6, 11
2	2417	2417	7
3	2422	2422	8
4	2427	2427	9
5	2432	2432	10
6	2437	2437	1, 11
7	2442	2442	2
8	2447	2447	3
9	2452	2452	4
10	2457	2457	5
11	**2462**	**2462**	1, 6
12	2467	–	–
13	2472	–	–

Bold values indicate the default setting of the AirLancer radio adapters when utilized in a base station.

11.2.2 Radio channels in the 5 GHz frequency band

In the frequency range from 5,13 to 5,805 GHz up to 19 non-overlapping channels are available in Europe, defined as the sub-bands as follows:

▶ Band 1: 5150 - 5350 MHz (channels 36, 40, 44, 48, 52, 56, 60 and 64)
▶ Band 2: 5470 - 5725 MHz (channels 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 und 140)
▶ Band 3: 5725 - 5875 MHz (channels 147, 151, 155, 167)

Please note that frequency ranges an radio channels in band 3 are reserved for operation in UK only!

EN

The following overview shows which channels are allowed in different regions.

	Channel No.	Frequency	ETSI (EU)	FCC (US)
Band 1	36	5,180 GHz	yes	yes
	40	5,200 GHz	yes	yes
	44	5,220 GHz	yes	yes
	48	5,240 GHz	yes	yes
	52	5,260 GHz	yes	yes
	56	5,280 GHz	yes	yes
	60	5,300 GHz	yes	yes
	64	5,320 GHz	yes	yes
Band 2	100	5,500 GHz	yes	no
	104	5,520 GHz	yes	no
	108	5,540 GHz	yes	no
	112	5,560 GHz	yes	no
	116	5,580 GHz	yes	no
	120	5,600 GHz	yes	no
	124	5,620 GHz	yes	no
	128	5,640 GHz	yes	no
	132	5,660 GHz	yes	no
	136	5,680 GHz	yes	no
	140	5,700 GHz	yes	no
Band 3 (UK only)	147	5,735 GHz	no	yes
	151	5,755 GHz	no	yes
	155	5,775 GHz	no	yes
	167	5,835 GHz	no	yes

11.2.3 Radio channels and frequency ranges for Indoor and Outdoor operating

In several countries specific regulations are valid concerning the use of frequency ranges and radio channels for indoor and outdoor operating. The following table gives information on the permitted application:

Country	Band (GHz)	Sub band	Frequency	Channels	Turbo channels	Emitted power (dBm)	Indoor/ Outdoor
Germany	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	200/23	I
		2	5,470-5,725	100-140	106-130	1000/30	I+O
Austria	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,25	36–44	–	60/17,5	I
Switzerland	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	200/23	I
Netherlands	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	200/23	I+O
		2	5,470-5,725	100-140	106-130	1000/30	I+O
Belgium	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	120/20,8	I
Luxembourg	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	200/23	I
		2	5,470-5,725	100-140	106-130	1000/30	I+O
UK	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	200/23	I
		2	5,470-5,725	100-140	106-130	1000/30	I+O
		3	5,725-5,585	147, 151, 155, 167	–	2000/33,1	(only fixed WLAN outdoor installations!)
Czechia	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	200/23	I
Italy	2,4	1	2,4-2,4835	1-13	6	100/20	I+O

Country	Band (GHz)	Sub band	Frequency	Channels	Turbo channels	Emitted power (dBm)	Indoor/ Outdoor
	5	1	5,15-5,35	36-64	42-58	200/23	I
		2	5,470-5,725	100-140	106-130	1000/30	I+O
France	2,4	1	2,4-2,4835	1-13	6	100/20	I
	2,4	1	2,4-2,454	1-9	6 (up to max. 10 dBm only!)	100/20	O
	2,4	1	2,454-2,4835	10-13		10/10	O
	5	1	5,15-5,35	36-64	42-58	200/23	I
Malta	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	200/23	I
		2	5,470-5,725	100-140	106-130	1000/30	I+O

Further details to the restrictions for the use of wlan adapters within th EU can be found in the internet:

Country	Organisation	Link
Belgium	Institut Belge des Postes et Tele-communications (BIPT)	www.bipt.be
Denmark	National Telecom Agency	www.tst.dk
Finland	Finnish Communications Regula-tory Authority (FICORA)	www.ficora.fi
France	Autorité de Régulation des Télé-communications (ART)	www.art-telecom.fr
Greece	National Telecommunications Commission (EET)	www.eett.gr
Great Britain	Office of Telecommunications (Oftel)	www.oftel.gov.uk
	Postal Services Commission (Post-comm)	www.postcomm.gov.uk/
	Radiocommunications Agency	www.open.gov.uk/radiocom
Ireland	Commission for Communications Regulation (ComReg)	www.comreg.ie
Iceland	Post and Telecom Administration (PTA)	www.pta.is
Italy	L'Autorità per le garanzie nelle communicazioni (AGC)	www.agcom.it

Country	Organisation	Link
Latvia	Telecommunication State Inspection	www.vei.lv
Liechtenstein	Amt für Kommunikation (AK)	www.ak.li
Lithuania	Radio Administration	www.rrt.lt/
Luxembourg	Institut Luxembourgeois des Télé-communications (ILT)	www.etat.lu/ILT
Netherlands	Onafhankelijke Post en Telecom-municatie Autoriteit (OPTA)	www.opta.nl
	Agentschap Telecom	www.agentschap-telecom.nl
	Ministerie Economische Zaken	www.ez.nl
Norway	Norwegian Post and Telecommunications Authority (NPT)	www.npt.no
Austria	Rundfunk und Telekom Regulierungs-GmbH	www.rtr.at
	Bundesministerium für Verkehr, Innovation und Technologie	www.bmvit.gv.at
Poland	Urzad Regulacji Telekomunikacji (URT)	www.urt.gov.pl
Portugal	Autoridad Nacional De Comuni-caçòes (ICP-Anacom)	www.anacom.pt
Sweden	National Post and Telecom Agency	www.pts.se
Switzerland	Bundesamt für Kommunikation	www.bakom.ch
Slowenia	Agencija za telekomunikacije, radi-odifuzijo in pošto	www.atrp.si
Spain	Comision del Mercado de las Tele-comunicaciones (CMT)	www.cmt.es
Tschechien	Czech Telecommunication Office	www.ctu.cz
Ungarn	Communication Authority (HIF)	www.hif.hu

Please inform yourself about the current radio regulations of the country you want to operate a Wireless LAN device.

11.3 Contact assignment

11.3.1 ADSL interface

6-pin RJ45 socket

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

11.3.2 DSL interface

6-pin RJ45 socket

Connector	Pin	IAE
	1	T+
	2	T-
	3	R+
	4	–
	5	–
	6	R-

11.3.3 ISDN-S_0 interface

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

Connector	Pin	Line	IAE
	1	–	–
	2	–	–
	3	T+	2a
1 2 3 4 5 6 7 8	4	R+	1a
	5	R-	1b
	6	T-	2b
	7	–	–
	8	–	–

11.3.4 Ethernet interfaces 10/100Base-T

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

Connector	Pin	Line
	1	T+
	2	T-
	3	R+
1 2 3 4 5 6 7 8	4	–
	5	–
	6	R-
	7	–
	8	–

11.3.5 Configuration interface (Outband)

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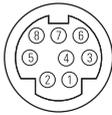
Connector	Pin	Line
	1	CTS
	2	RTS
	3	RxD
	4	RI
	5	TxD
	6	DSR
	7	DCD
	8	DTR
	U	GND

11.4 CE declaration of conformity

This product corresponds to the requirements of the guide line about radio installations and telecommunication sending installations (FTEG) and to the guide line 1999/5/EG (R&TTE).

This product has been notified in the countries of Germany, Great Britain, Belgium, Netherlands, Luxembourg, Austria, Switzerland.

The CE declarations of conformity for LANCOM routers are available for download on the LANCOM web site (www.lancom.de).

12 Index

EN

EN

EN