

**LANCOM 1811 Wireless DSL –
LANCOM 1821+ Wireless ADSL**

© 2007 LANCOM Systems GmbH, Wuersele (Germany). All rights reserved.

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

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

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

Trademarks

Windows®, Windows XP® and Microsoft® are registered trademarks of Microsoft, Corp.

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

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

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

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

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

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuersele

Germany

www.lancom.eu

Wuersele, March 2007

Preface

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

With the LANCOM Router 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 Router 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.

Model variants

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

- 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 Router.

Security settings

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

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

User manual and reference manual

The documentation of your device consists of three parts: The installation guide, the user manual and the reference manual.

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

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

- The system design of the operating system LCOS
- Configuration
- Management
- Diagnosis
- Security
- Routing and WAN functions
- Firewall
- Quality of Service (QoS)
- Virtual Private Networks (VPN)
- Virtual Local Networks (VLAN)
- Wireless networks (WLAN)
- Voice communication in computer networks with Voice over IP (VoIP)
- Backup solutions
- LANCAPI
- Further server services (DHCP, DNS, charge management)

This documentation was created by ...

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

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

info@lancom.eu



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

In addition, LANCOM support is available. For telephone numbers and contact addresses of LANCOM support, please see the enclosed leaflet or the LANCOM Systems website.

Information symbols



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



Important instruction that should be observed.



Additional information that may be helpful but which is not required.

Contents

1 Introduction	10
1.1 How do ADSL and ADSL 2+ work?	10
1.2 What does VPN offer?	12
1.3 What is a Wireless LAN?	14
1.3.1 Which hardware to use?	14
1.3.2 Operation modes of Wireless LANs and base stations	14
1.4 What can your LANCOM Wireless Router do?	15
2 Installation	19
2.1 Package contents	19
2.2 System requirements	19
2.3 Introducing LANCOM Router	20
2.3.1 Status displays	20
2.3.2 The back of the unit	25
2.4 Hardware installation	27
2.5 Software installation	29
2.5.1 Starting LANCOM setup	29
2.5.2 Which software should you install?	29
3 Basic configuration	31
3.1 Which information is necessary?	31
3.1.1 TCP/IP settings	31
3.1.2 Configuration protection	33
3.1.3 Settings for the Wireless LAN	33
3.1.4 Settings for the ISDN connection	34
3.1.5 Connect charge protection	35
3.2 Instructions for LANconfig	35
3.3 Instructions for WEBconfig	37
3.4 TCP/IP settings to workstation PCs	40
4 Setting up Internet access	42
4.1 Instructions for LANconfig	43
4.2 Instructions for WEBconfig	44

5 Linking two networks	45
5.1 What information is necessary?	46
5.1.1 General information	46
5.1.2 Settings for the TCP/IP router	48
5.1.3 Settings for the IPX router	49
5.1.4 Settings for NetBIOS routing	50
5.2 Instructions for LANconfig	51
5.3 Instructions for WEBconfig	52
6 Providing dial-in access	53
6.1 Which information is required?	53
6.1.1 General information	54
6.1.2 Settings for TCP/IP	55
6.1.3 Settings for IPX	56
6.1.4 Settings for NetBIOS routing	56
6.2 Settings for the dial-in computer	57
6.2.1 Dial-up via VPN	57
6.2.2 Dial-up via ISDN	57
6.3 Instructions for LANconfig	58
6.4 Instructions for WEBconfig	59
7 Sending faxes with LANCAPI	60
7.1 Installation of the LANCOM CAPI Faxmodem	61
7.2 Installation of the MS Windows fax service	62
7.3 Sending a fax	62
7.3.1 Send a fax with any given office application	62
7.3.2 Send a fax with the MS Windows fax service	63

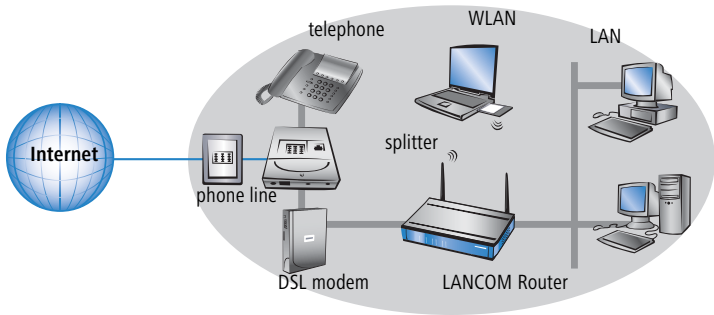
8 Security settings	64
8.1 Security for the Wireless LAN	64
8.1.1 Closed network	64
8.1.2 Access control via MAC address	65
8.1.3 LANCOM Enhanced Passphrase Security	65
8.1.4 Encryption of the data transfer	66
8.1.5 802.1x / EAP	67
8.1.6 IPSec over WLAN	68
8.2 Tips for handling keys	68
8.3 The security settings wizard	69
8.3.1 Wizard for LANconfig	69
8.3.2 Wizard for WEBconfig	70
8.4 The firewall wizard	70
8.4.1 Wizard for LANconfig	71
8.4.2 Configuration under WEBconfig	71
8.5 The security checklist	71
9 Options and accessories	76
9.1 Optional LANCOM Wireless Router antennas	76
9.1.1 Antenna Diversity	76
9.1.2 Installation of AirLancer Extender antennas	77
9.2 LANCOM Public Spot Option	77
9.3 LANCOM VoIP Basic Option and LANCOM VoIP Advanced Option	78
9.3.1 Advantages of VoIP solutions	79
9.4 LANCOM VPN Option	79
10 Troubleshooting	81
10.1 No DSL connection is established	81
10.2 DSL data transfer is slow	81
10.3 Unwanted connections under Windows XP	82
10.4 Cable testing	82

11 Appendix	84
11.1 Performance data and specifications	84
11.2 Contact assignment	86
11.2.1 ADSL interface	86
11.2.2 DSL interface	86
11.2.3 ISDN-S ₀ interface	87
11.2.4 Ethernet interfaces 10/100Base-T	87
11.2.5 Configuration interface (Outband)	88
11.3 CE declaration of conformity	88

1 Introduction

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

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



1.1 How do ADSL and ADSL 2+ work?

ADSL (Asymmetric Digital Subscriber Line) is currently the most common technology for broadband Internet connections. Standard and almost ubiquitous telephone lines (analog or DSL) are the basis for DSL data transfer to the nearest telephone exchange. From here, the data is passed directly on to the Internet over high-speed connections.

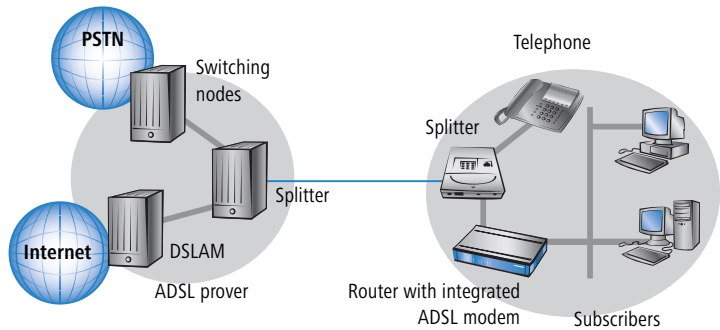
The asymmetric DSL variant ADSL was developed for applications where users receive large amounts of data but transmit only small amounts, such as when surfing in the WWW. ADSL subscribers can receive data at up to 8 Mbps ("downstream") and transmit at up to 800 kbps ("upstream"). ADSL providers are able to reduce these maximum rates as they please.

To satisfy the strongly increasing demand for higher bandwidths, the standards ADSL 2 and ADSL 2+ provide higher data rates as a basis for applications such as video streaming or high-definition TV (HDTV) over the Internet. Depending on the Internet provider, ADSL 2 devices support downstream data rates of up to 12 Mbps, and ADSL 2+ devices support up to 24 Mbps. Hands-

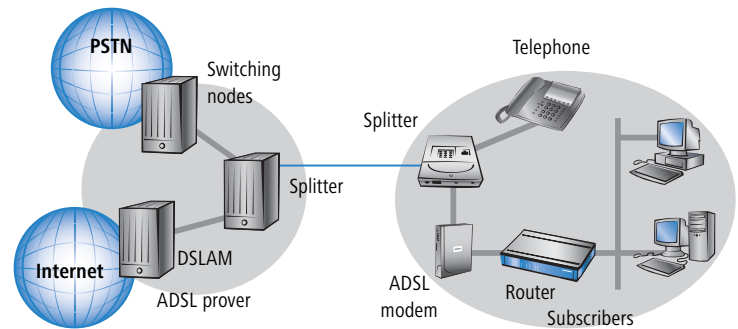
hake routines during connection establishment ensure that the standards ADSL, ADSL 2 and ADSL 2+ are interoperable.

Parallel to data transfer, ADSL also provides full and unlimited support for the classic applications in telephony (telephone, fax, answering machine, PBX). This is facilitated by splitters which separate the voice frequencies from the data frequencies.

Some models feature an integrated modem for ADSL/ADSL 2+. It can be directly connected to the splitter with the supplied cable.



If the device does not feature an integrated ADSL modem, then the router is connected to a separate ADSL modem, which in turn is connected to the splitter.



LANCOM 1811 Wireless DSLs can also be used for Internet access via other broadband connections (e.g. cable modems) as long as they

have a 10/100Base-Tx Ethernet connector via PPPeE, PPTP or simple Ethernet (with or without DHCP).

LANCOM 1821+ Wireless ADSL models can use this option as well by configuring the first LAN port as a WAN interface.

ADSL can operate over both ISDN- and analog telephone lines (POTS – **P**lain **O**ld **T**elephone **S**ervice). Devices with an integrated modem are supplied in two versions. Information about the supported telephone system is to be found on the type designation on the underside of the device. The device name is marked on the label along with a suffix which indicates the supported telephone system:

Suffix	Supported telephone system
'Annex A'	ADSL-over-POTS
'Annex A'	ADSL-over-ISDN

Annex A-type devices are exclusively to be operated at ADSL-over-POTS connections. Annex B-type devices are exclusively to be operated at ADSL-over-ISDN connections. Your network operator will be able to inform you of the version you need. These devices cannot be altered or upgraded to a system other than that for which it is equipped.

There are even ADSL-over-ISDN connections which are not combined with an ISDN connection, but with a standard analog telephone connection instead. In Germany, for instance, all T-DSL connections from Deutsche Telekom AG are implemented as ADSL-over-ISDN connections.

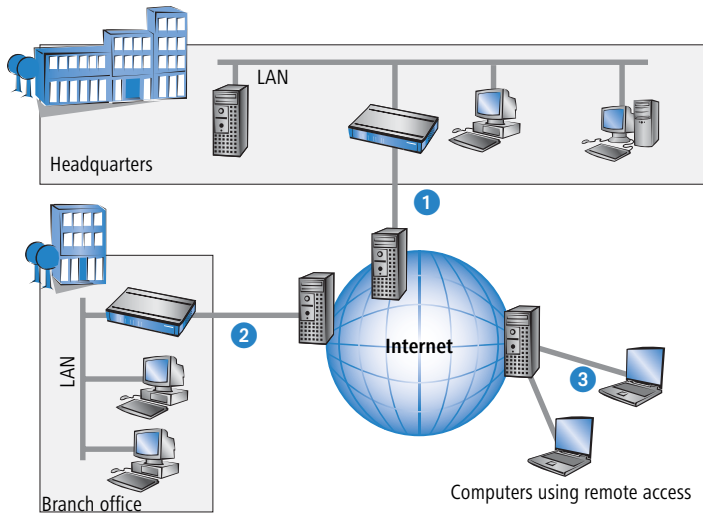
1.2 What does VPN offer?

A VPN (**V**irtual **P**rivate **N**etwork) can be used to set up secure data communications over the Internet.



The models LANCOM 1811 Wireless DSL and LANCOM 1821+ Wireless ADSL are factory equipped to support VPN with 5 active tunnels. With the additional LANCOM VPN Option, VPN support can be extended to 25 active tunnels (incl. activated hardware accelerator).

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.

- ① 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.
- ② The subsidiary also has its own connection to the Internet.
- ③ 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: Broadband technology such as DSL (Digital Subscriber Line) is ideal. A conventional ISDN line can be used, too.

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 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 Router do?' → Page 15.

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.

1.3.1 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.

1.3.2 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)


1.4 What can your LANCOM Wireless Router do?

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

	LANCOM 1811 Wireless DSL	LANCOM 1821+ Wireless ADSL
Applications		
Internet access	✓	✓
LAN-LAN coupling over VPN	✓	✓
LAN-LAN coupling over ISDN	✓	✓
RAS server (over VPN)	✓	✓
RAS server (over ISDN)	✓	✓
IP router	✓	✓
IPX router (over ISDN), for example for coupling Novell networks or for dialing in to Novell networks	✓	✓
NetBIOS proxy for coupling Microsoft peer-to-peer networks over ISDN	✓	✓
DHCP- and DNS server (for LAN and DMZ)	✓	✓
N:N mapping for routing networks with the same IP-address ranges over VPN	✓	✓
Configuring LAN ports as additional WAN ports	✓	✓
Policy-based routing	✓	✓
Load balancing for bundling multiple DSL channels	4 channels	4 channels
Backup solutions and load balancing with VRRP	✓	✓
NAT Traversal (NAT-T)	✓	✓

■ Chapter 1: Introduction

	LANCOM 1811 Wireless DSL	LANCOM 1821+ Wireless ADSL
DMZ with configurable IDS checks	✓	✓
PPPoE-Server	✓	✓
WAN-RIP	✓	✓
Spanning-Tree-Protokoll	✓	✓
Layer-2-QoS-Tagging	✓	✓
ISDN leased lines	✓	✓
LANCAPI server to provide office applications such as fax or answering machine via the ISDN interface.	✓	✓
WLAN		
Wireless transmission compliant with IEEE 802.11g and IEEE 802.11b	✓	✓
Wireless transmission compliant with IEEE 802.11a and IEEE 802.11b	✓	✓
Point-to-point mode (six P2P paths can be defined per WLAN interface)	✓	✓
Relay function to link two P2P connections	✓	✓
Turbo mode: Double the bandwidth at 2.4 GHz and 5 GHz.	✓	✓
Super AG incl. hardware compression and bursting	✓	✓
Multi SSID	✓	✓
Roaming function	✓	✓
802.11i / WPA with hardware AES encryption	✓	✓
WEP encryption (up to 128-bit key lengths, WEP152)	✓	✓
IEEE 802.1x/EAP	✓	✓
MAC address filter (ACL)	✓	✓
Individual passphrases per MAC address (LEPS)	✓	✓
Closed-network function	✓	✓
Integrated RADIUS server	✓	✓
VLAN	✓	✓

	LANCOM 1811 Wireless DSL	LANCOM 1821+ Wireless ADSL
Traffic-lock function	✓	✓
QoS für WLAN (IEEE 802.11e, WMM/WME)	✓	✓
VoIP functions 		
SIP users	4/32 ¹⁾	4/32 ¹⁾
ISDN users	4/32 ¹⁾	4/32 ¹⁾
Lines to SIP providers	16 ¹⁾	16 ¹⁾
Lines to SIP PBX	4 ¹⁾	4 ¹⁾
external ISDN busses for VoIP	1 ¹⁾	1 ¹⁾
¹⁾ depending on VoIP option (Basic/Advanced)		
WAN connections		
Connection for DSL or cable modem	✓	✓
Integrated ADSL modem (ADSL2+ ready)		✓
ISDN S ₀ bus in multi device-mode or in point-to-point mode with automatic D-channel protocol identification. Supports static and dynamic channel bundling per MLPPP and BACP as well as Stac data compression (Hi/fn)	✓	✓
LAN connection		
Separate FastEthernet LAN ports, individually switchable, e.g. as LAN switch or separate DMZ ports; auto crossover. Alternatively switchable as a WAN interface for connecting SDSL modems.	4	4
USB connector		
USB 2.0 host port (full speed: 12 Mbps) for connecting a USB printer and for future extensions		✓
Security functions		
IPSec encryption via external software (VPN client)	✓	✓
5 integrated VPN tunnels for secure network connections	✓	✓
IPSec encryption in hardware (optional; activated with the VPN-25 option)	✓	✓

■ Chapter 1: Introduction

	LANCOM 1811 Wireless DSL	LANCOM 1821+ Wireless ADSL
IP masquerading (NAT, PAT) to conceal individual LAN workstations behind a single public IP address.	✓	✓
Stateful-inspection firewall	✓	✓
Firewall filter for blocking individual IP addresses, protocols and ports	✓	✓
MAC address filter regulates, for example, LAN-workstation access to the IP routing function	✓	✓
Protection of the configuration from brute-force attacks.	✓	✓
Configuration		
Configuration with LANconfig or via web browser; additional terminal mode for Telnet or equivalent terminal programs; SNMP interface and TFTP server function.	✓	✓
Remote configuration via ISDN (with ISDN PPP connections, e.g. via Windows Dial-Up Networking).	✓	✓
Serial configuration interface	✓	✓
Call-back function with PPP authentication mechanisms allowing only predefined ISDN call numbers	✓	✓
FirmSafe for no-risk firmware updates	✓	✓
Optional software extensions		
LANCOM VPN Option with 25 active tunnels for protection of network couplings and hardware acceleration	✓	✓
LANCOM Public Spot Option	✓	✓
LANCOM VoIP Basic Option	✓	✓
LANCOM VoIP Advanced Option	✓	✓

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

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

2.2 System requirements

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

■ Chapter 2: Installation

- Operating system that supports TCP/IP, e.g. Windows Vista™, Windows XP, Millennium Edition (Me), Windows 2000, Windows 98, Linux, BSD Unix, Apple Mac OS, OS/2.
- Access to the LAN via the TCP/IP protocol.
- Wireless LAN adapter or LAN access (if the access point is to be connected to the LAN).



The LANtools also require a Windows operating system. A web browser under any operating system provides access to WEBconfig.

2.3 Introducing LANCOM Router

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



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

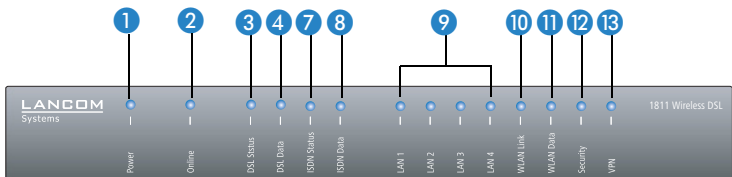
2.3.1 Status displays

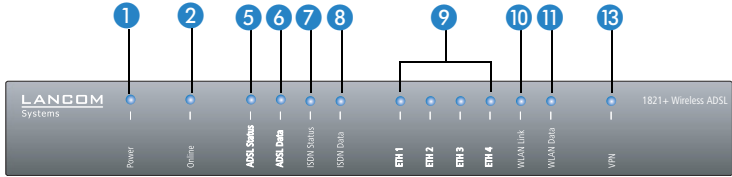
The front and the rear panels of the unit feature a series of light emitting diodes (LEDs) that provide information on the status of the device.

Front side

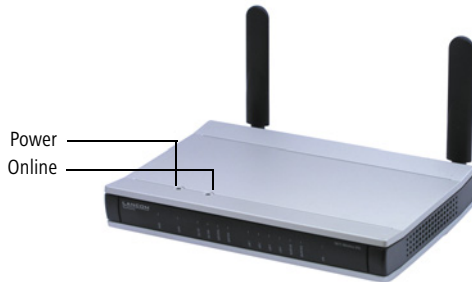
The various LANCOM Router models have different numbers of indicators on the front panel depending on their functionality (picture: LANCOM 1811 Wireless DSL).

LANCOM 1811
Wireless DSL



LANCOM 1821+
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.

**1** Power

This LED provides information on the device's operating state. After being switched on, it blinks green during the self-test. The LED then shines constantly to indicate operational readiness, unless an error is detected as indicated by a code blinked in red.

Off		Device switched off
Green	Blinking	Self-test after power-up
Green	On (permanently)	Device operational
Red/green	Blinking alternately	Device insecure: Configuration password not set
Red	Blinking	Charge or time limit reached



The power LED blinks alternately in red/green until a configuration password has been set. Without a configuration password, the configuration data in the LANCOM are unprotected. Normally you would set a configuration password during the basic configuration (instruc-

tions in the following chapter). Information about setting a configuration password at a later time is available in the section 'The Security Wizard'.

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

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



Signal that a charge or time limit has been reached

There are three ways to remove the lock:

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

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

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

2 Online

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

Off		No active connection
Green	Flashing	Opening the first connection
Green	Inverse flashing	Opening an additional connection
Green	On (permanently)	At least one connection is established
Red	On (permanently)	Error establishing the last connection

- 3 DSL status
(LANCOM
1811 Wireless
DSL only)

Connection status of the DSL connection:

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

- 4 DSL data
(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

- 5 ADSL Status
(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
Red/ orange	Blinking	Hardware error

- 6 ADSL Data
(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 established
green	flickering	Data traffic (send or receive)
Red/ orange	Blinking	Hardware error

Chapter 2: Installation

7 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.

8 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)

9 LAN 1 to LAN 4 (1811) ETH 1 to ETH 4 (1821+)

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

10 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)

11 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)

12 Security
(LANCOM
1811 Wireless
DSL only)

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

13 VPN

Status of a VPN connection.

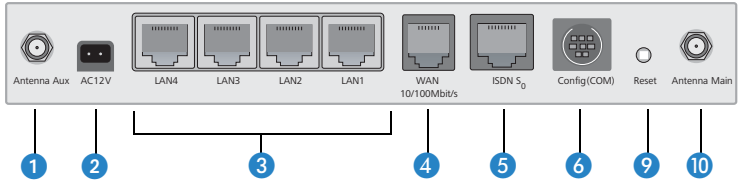
off		No VPN tunnel established
green	blinking	Negotiating VPN connection
green	flashing	Establishing first connection
green	inverse flashing	Establishing further connection
green	constantly on	VPN connection established

2.3.2 The back of the unit

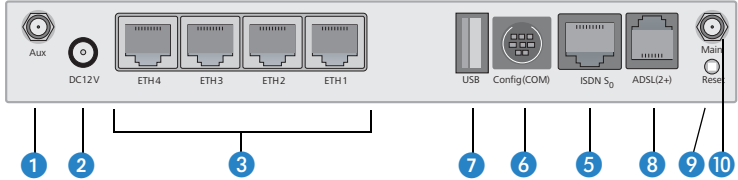
The connections and switches of the router are located on the back panel:

■ Chapter 2: Installation

LANCOM 1811 Wireless DSL



LANCOM 1821+ Wireless ADSL



- 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 1811 Wireless DSL
- 5 ISDN/S₀ port
- 6 Serial configuration port
- 7 USB connector (USB host)
- 8 ADSL port for LANCOM 1821+ Wireless ADSL
- 9 Reset switch
- 10 Connector for main antenna (use this connector to connect additional LANCOM Wireless Router 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.



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 67).

2.4 Hardware installation

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

- ① **Antennas** – Screw on the both included diversity antennas at the back of the LANCOM Router base station.
- ② **LAN** – First connect the LANCOM Router base station to your LAN or to an individual PC. For that purpose, plug the included network cable (green plugs) into the LAN connector of the device ③ and the other end into a free network connecting socket of your local network, into a free socket of a hub/switch or into the network socket of an individual PC.

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



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

1811 only

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

1821+ only

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

1821+ only

- ⑥ **USB port** – you may optionally connect printers with USB connector to the LANCOM and make them available to the entire network. The

LANCOM provides a print server to manage the printing jobs from the network. Supported protocols are RawIP and LPR/LPD.

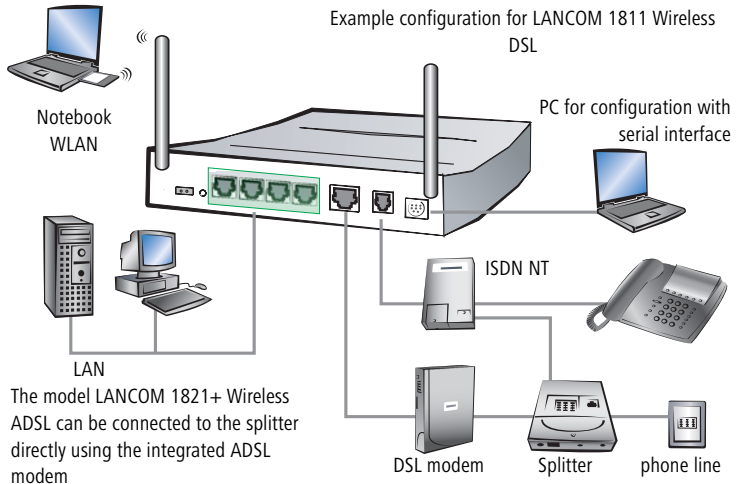
i Further information about configuration of the print server can be found in the LCOS reference manual.

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

8 Connect to power – Connect socket **1** of the unit to a power supply using the included power adapter.

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

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



⚡ Devices with integrated ADSL 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 Router exclusively with computers running operating systems other than Windows.

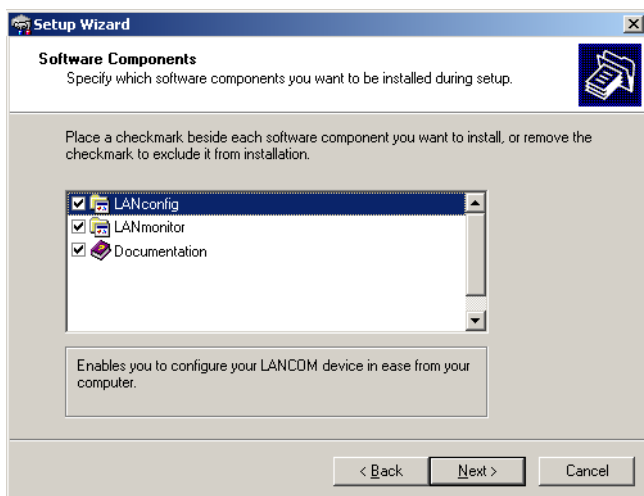
2.5.1 Starting LANCOM setup

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:



2.5.2 Which software should you install?

- **LANconfig** is the configuration program for all LANCOM routers and LANCOM Router 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 Router base stations.

■ *Chapter 2: Installation*

- **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.
- 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.

3 Basic configuration

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

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

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

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

3.1 Which information is necessary?

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

- TCP/IP settings
- protection of the configuration
- information related to the Wireless LAN
- information on DSL connection
- configuring connect charge protection
- security settings

3.1.1 TCP/IP settings

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

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

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 Router in an existing TCP/IP LAN. In this case, continue with the section 'Information required for manual TCP/IP configuration'.

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

Configure manually nevertheless?

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

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

Information required for manual TCP/IP configuration

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

■ IP address and netmask for the LANCOM Router

Assign a free IP address from the address range of your LAN to the LANCOM Router and specify the netmask.

3.1.2 Configuration protection

The password for configuration access to the LANCOM Router 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.



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

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 **I**dentifier). 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.



As standard, WEP128 encryption is activated for every unconfigured device as standard. Further information can be found in the LCOS reference manual under "Standard WEP encryption".

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/h 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 Router base station itself adjust the best channel via TPC and DSF.

3.1.4 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 provider. 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 Router for connect-charge budgets and the accounting function.

3.1.5 Connect charge protection

Connect charge protection blocks DSL connections that go beyond a previously set limit, thus protecting you from unexpectedly high connection charges.

If you run the LANCOM Router via DSL access with a flat-rate tariff, you can set the maximum connecting-time in minutes.

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

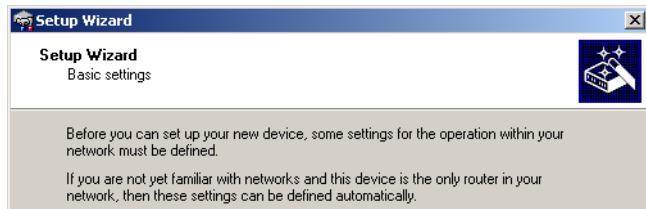


In basic settings the charge protection is defined to maximum 600 minutes within seven days. Adapt this setting to your personal needs or deactivate the charge protection if you have arranged a flatrate with your provider.

3.2 Instructions for LANconfig

- ① Start up LANconfig by clicking **Start** ► **Programs** ► **LANCOM** ► **LANconfig**

LANconfig automatically detects the new LANCOM Router 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 Router is connected via a serial port) or in the network (**Device** ► **Find**).




If you cannot access an unconfigured LANCOM Router, the problem may be due to the netmask of the LAN: with less than 254 possible

hosts (netmask > '255.255.255.0'), please ensure that the IP address 'x.x.x.254' is located in your own subnet.


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 Router. 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.

- 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 Connect charge protection can limit the cost of DSL connections to a pre-determined amount if desired. Confirm your choice with **Next**.
- ⑧ Complete the configuration with **Finish**.

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

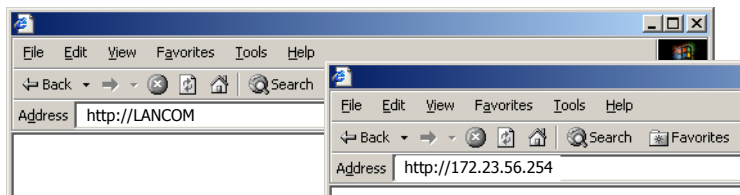
3.3 Instructions for WEBconfig

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

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

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**.

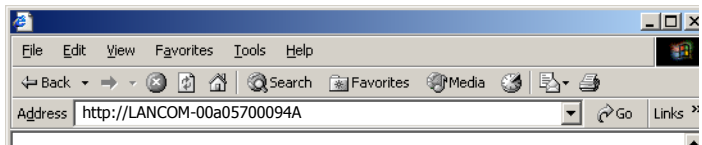



If the configuration PC does not obtain its IP address from the LANCOM DHCP server, figure out the current IP address of this PC (with **Start ▶ Execute ▶ cmd** and command **ipconfig** at the prompt under Windows 2000 or Windows XP, with **Start ▶ Execute ▶ cmd** and the command **windowsipcfg** at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

Network with DHCP server

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

- If there is a DNS server for name resolution in the LAN, which interchanges the assignment of IP addresses to names with the DHCP server, then the device can be accessed by the name “LANCOM <MAC address>” (e.g. “LANCOM-00a057xxxxx”).



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


- If there is no DNS server in the LAN, or it is not linked to the DHCP server, then the device can not be reached by the name. The following options remain in this case:
 - Figure out the DHCP-assigned IP address of the LANCOM by suitable tools and contact the device directly with this IP address.
 - Use LANconfig.
 - Connect a PC with a terminal program via the serial configuration interface to the device.

Starting the wizards in WEBconfig

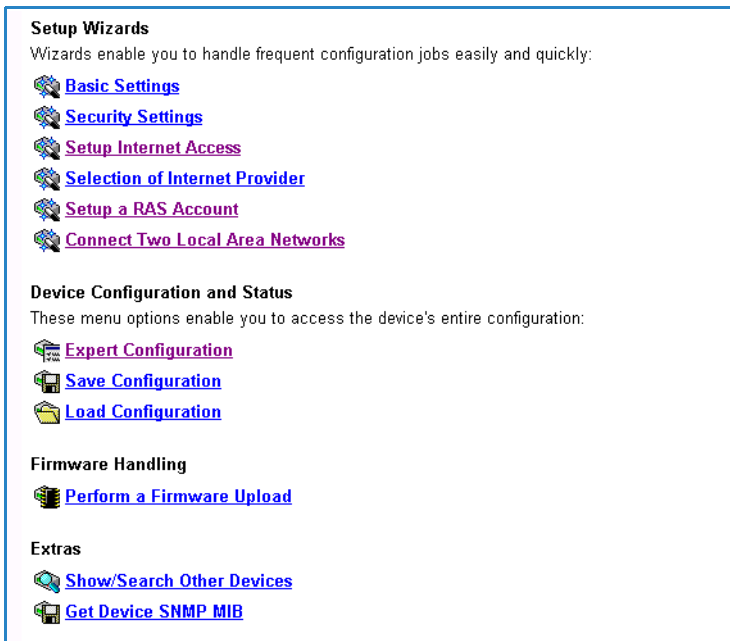
- ① Start your web browser (e.g. Internet Explorer, Netscape Navigator, Opera) and call the LANCOM Router there:

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







(or with a name as described above)

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




The WEBconfig main menu will be displayed:




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 Router. As a result, your device may offer different wizards than those shown here.

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

- ② If you would like to configure the TCP/IP settings manually, assign an available address from a suitable address range to the LANCOM Router. Also set whether or not it is to operate as a DHCP server. Confirm your entry with **Apply**.
- ③ Enter the wireless parameters. Select a network name (SSID) and a radio channel. Turn on if necessary the function for 'closed network'. Confirm your choice with **Next**.
- ④ In the following 'Security settings' window, specify a password for configuration access. Note that the password is case-sensitive and ensure that it is sufficiently long (at least 6 characters).

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

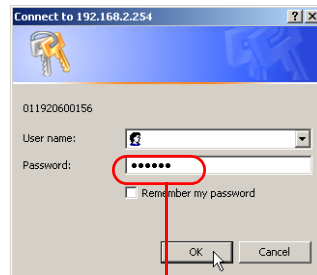


Please note that enabling this will also permit remote configuration via the Internet. You should always make sure that the configuration access is suitably protected, e.g. with a password.

Entering the password in the web browser

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

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



Entering the configuration password

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

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

- ⑥ Connect charge protection can limit the cost of DSL connections to a pre-determined amount if desired. Confirm your choice with **Apply**.
- ⑦ The basic setup wizard reports that all the necessary information has been provided. You can end the wizard with **Go on**.

3.4 TCP/IP settings to workstation PCs

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

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

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

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

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

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

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

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

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

- **Manual IP address assignment**

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



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

4 Setting up Internet access

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

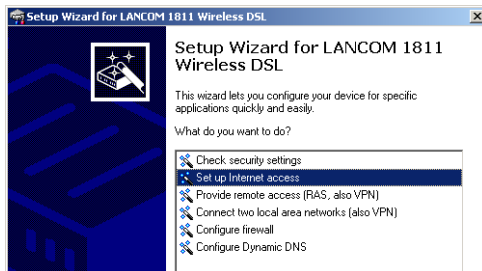
You may also enable or disable further options in the wizard, depending on whether or not they are supported by your Internet provider:

- 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 Router to automatically close existing connections if no data has been transferred within a specified time (the so-called idle time).
In addition, you can activate a line monitor that identifies inactive remote stations faster and therefore can close the connection before the idle time has elapsed.
- Active line monitoring can also be used with flat rate billing to continuously check the function of the remote station.
You also have the option of keeping flat rate connections alive if required. Dropped connections are then automatically re-established.
- 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.

4.1 Instructions for LANconfig

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



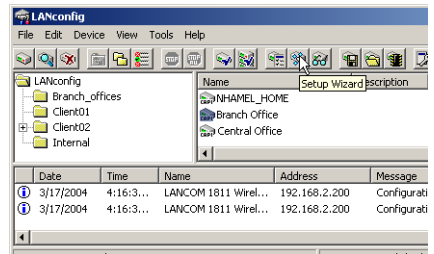
- ② From the menu, select the **Setup Internet access** wizard and click **Next**.
- ③ In the following window select your country and your Internet provider if possible, and enter your access information.
- ④ Depending on their availability, the wizard will display additional options for your Internet connection.

■ Chapter 4: Setting up Internet access

- 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 Router, two local networks are linked. The LAN to LAN coupling can be realized in principle in two different ways:

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

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

Security aspects

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

- **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 (e.g. digital certificates) 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'
VPN	IP address of remote station	'10.0.2.100'		'10.0.1.100'

Coupling	Entry	Gateway 1	Gateway 2
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.

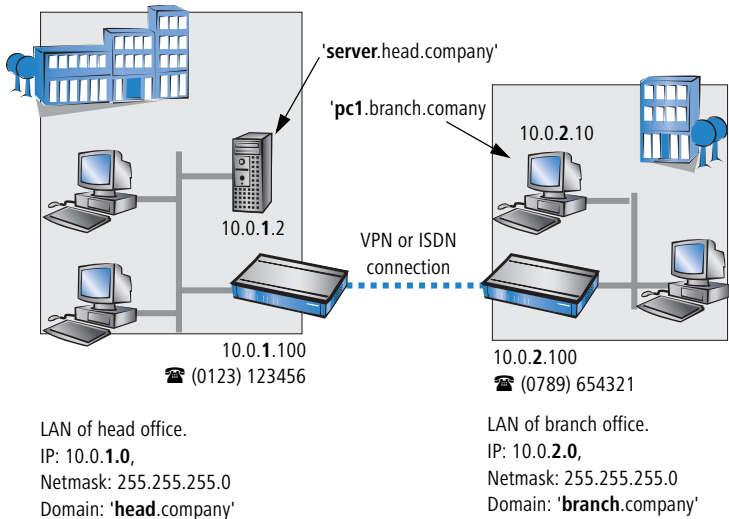
- If you haven't already named your LANCOM Router, the wizard will ask you for a new, **unique device name**. With this entry, you will rename your LANCOM Router. Be sure to give the two devices different names.
- The **name of the remote station** is needed for its identification.
- Enter the subscriber 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 Router 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.



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

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

DNS access to the remote LAN

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

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



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

Extranet VPN

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

Therefore, the stations within the remote LAN cannot access IP stations in the other LAN directly. For example, if a headquarters LAN in 'Extranet VPN' mode is hidden behind its gateway's address '10.10.2.100', and one 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 deem to be 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



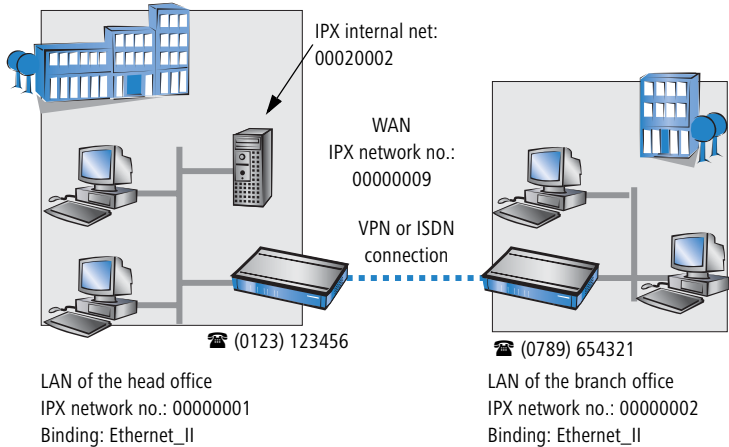
The coupling of IPX networks via VPN cannot be configured using the wizard. It can only be set up in the expert configuration. For details, please see the reference manual.

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

■ Chapter 5: Linking two networks

- 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.




The three required network numbers are designated as “External Network Numbers” by the IPX conventions. 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. It is only necessary to enter the network number for the WAN manually in this case.

5.1.4 Settings for NetBIOS routing

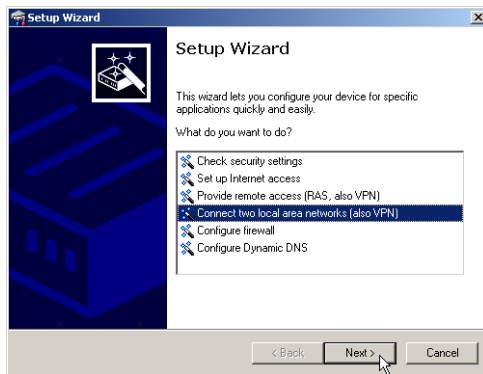
NetBIOS routing can be set up quickly: All that is required in addition to the information for the TCP/IP protocol used is the name of a Windows workgroup from in the router's own LAN.

-  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 Router should automatically set up a connection to the remote station and contact the required computer.

Ping – quick testing for TCP/IP connections

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

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

```

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
Reply from 10.0.2.0: bytes=32 time<10ms
Reply from 10.0.2.0: bytes=32 time<10ms
Reply from 10.0.2.0: bytes=32 time<10ms
Ping statistics for 10.0.2.0 :
    Packets: Sent = 4, Received = 4, Lost = 0
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average =
C:\>

```

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.

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

6 Providing dial-in access

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

- **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-in connection in the usual convenient manner.

Security aspects

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

- **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 VPN (standard method using “preshared keys”) and/or an ISDN connection.



Further details to network couplings via VPN using enhanced methods (e.g. digital certificates) 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 Router 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 'Linking two networks' → Page 39 for advice about the other values required for the installation of a RAS access.

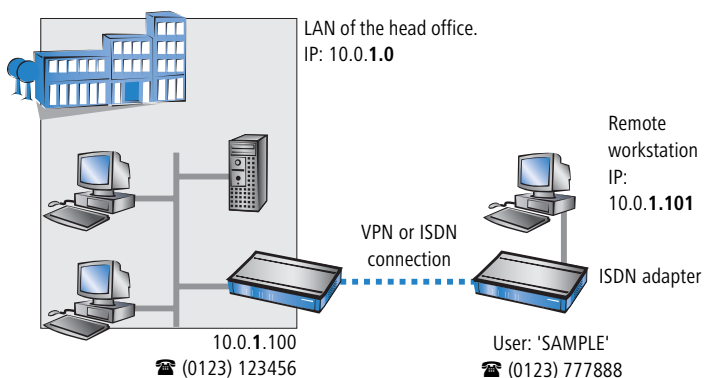
The ISDN calling line identity (CLI)

The ISDN caller ID—also known as CLI (Calling Line Identity)—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.



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

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

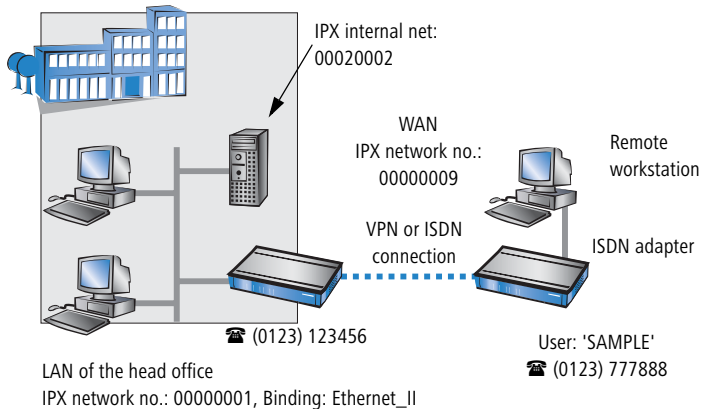
This IP address makes the computer a fully-fledged member of the LAN: with the appropriate rights, it can access all of the other devices in the LAN. The

same applies in the other direction as well: computers in the LAN will also be able to access the remote machine.

6.1.3 Settings for IPX

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

- the IPX network number of the head office
- an additional IPX network number for the higher-level WAN



The required network numbers are designated as “External Network Numbers”. 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 Router via Dial-Up

Networking first. When connected, they can search for and access computers in the remote network (via **Find ► Computers**, not through the Network Neighbourhood).

6.2 Settings for the dial-in computer

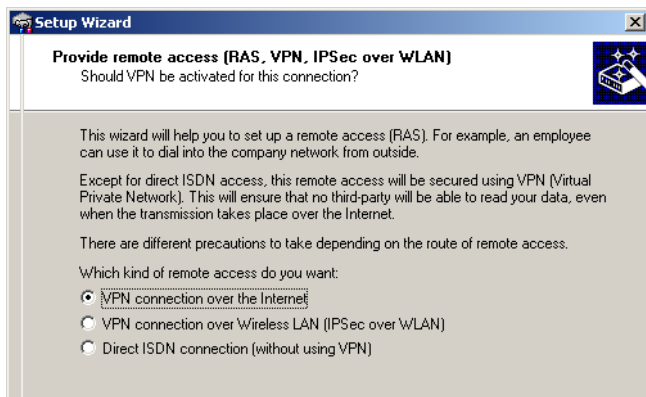
6.2.1 Dial-up via VPN

For dialing into a network via VPN a workstation requires:

- an Internet access
- a VPN client

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

For configuring a new profile, select the option 'LANCOM Advanced VPN Client' in the configuration wizard.



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

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

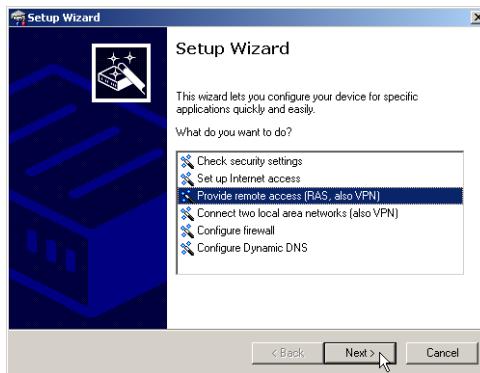
■ Chapter 6: Providing dial-in access

- Terminal adapter or ISDN card set to PPPHDL
- 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 46).

6.4 Instructions for WEBconfig



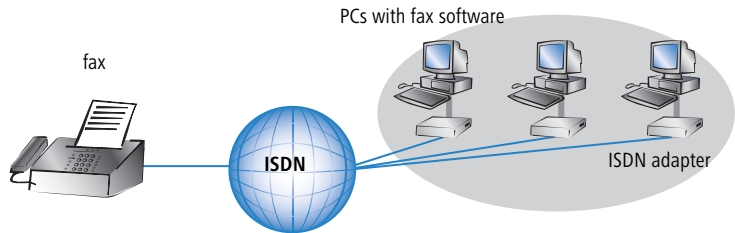
RAS access via VPN cannot be configured using the wizard under WEBconfig yet. It can only be set up in the expert configuration. For details, please refer to the reference manual.

- 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 46).

7 Sending faxes with LANCAPI

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

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



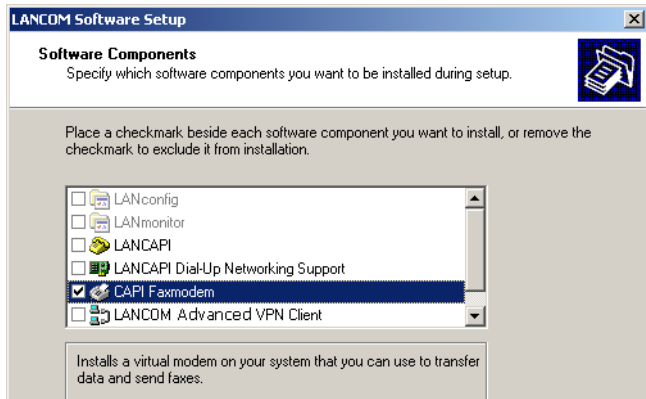
With LANCAPI by LANCOM it is possible to send faxes comfortably from your workstation PC, without having connected a fax device. To do so, you need to install several components:

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

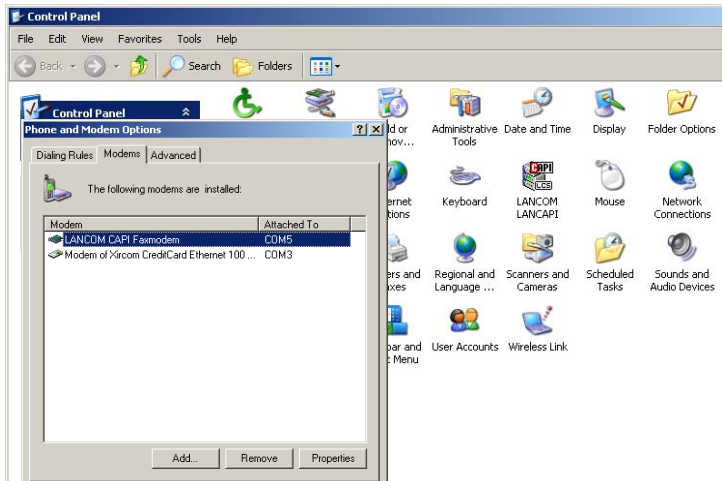
The installation of the LANCAPI client is described in the reference manual. This chapter shows the installation of LANCOM CAPI Faxmodem and MS Windows fax service.

7.1 Installation of the LANCOM CAPI Faxmodem

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

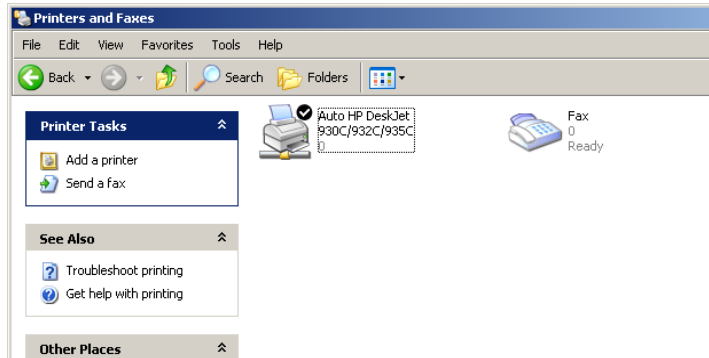


When the installation was successful, the LANCOM CAPI Faxmodem is entered into the **Phone and Modem Options** of the control panel.



7.2 Installation of the MS Windows fax service

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



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

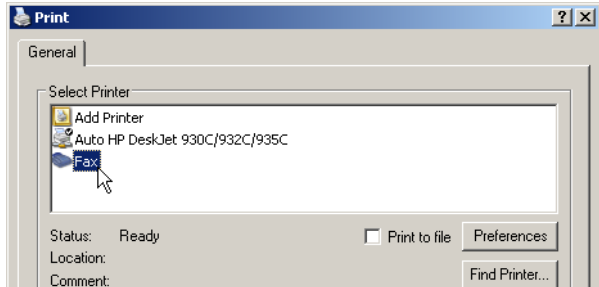
7.3 Sending a fax

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

7.3.1 Send a fax with any given office application

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

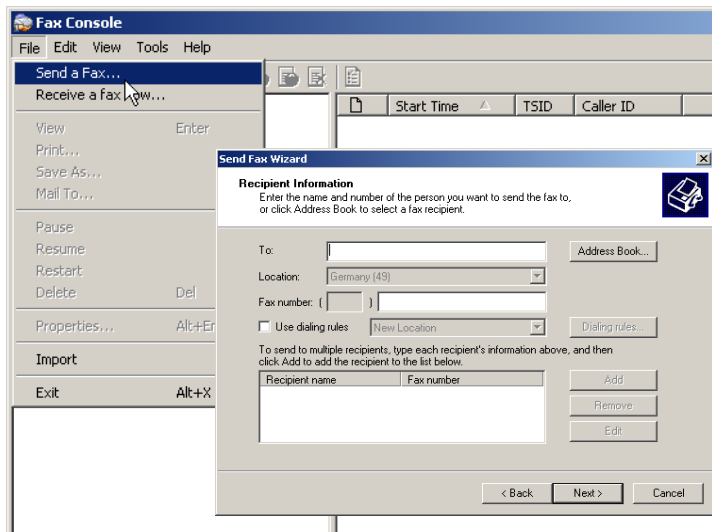
- ② Adjust the fax device as printer.



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

7.3.2 Send a fax with the MS Windows fax service

- ① Open the window 'Printers and Faxes' from the control panel.
- ② Double click with the left mouse button the icon of the fax device.
- ③ The fax client console will open. Select the menu item **Send a Fax**. A wizard will assist you through the remaining sending process.



8 Security settings

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

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 Systems permit the employment of modern security technologies:

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

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.

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 Systems have got a MAC address label on the casing.

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

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

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.



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

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 or activate an additional encryption of the WLAN connection as used for VPN tunnels ('IPSec over WLAN'). In special cases, a combination of these two mechanisms is possible.



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

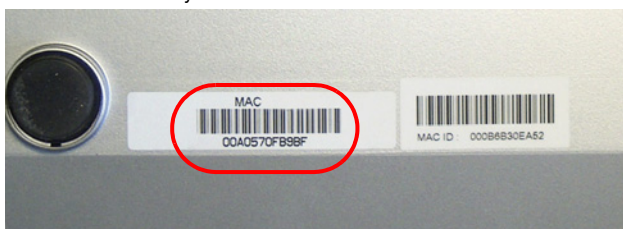


Please take note of the information in the box "Standard WEP encryption".

Standard WEP encryption

As standard, WEP128 encryption is activated for every unconfigured device.

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.



After registering for the first time, change the WEP password to ensure that you have a secure connection.



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 **Extensible Authentication Protocol (EAP)** enables the realization of reliable and secure access controls for base stations. The access data is centrally administered on a RADIUS server then, and can be retrieved by the base station if required.

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

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

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

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.

8.2 Tips for handling keys

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

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

8.3 The security settings wizard

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

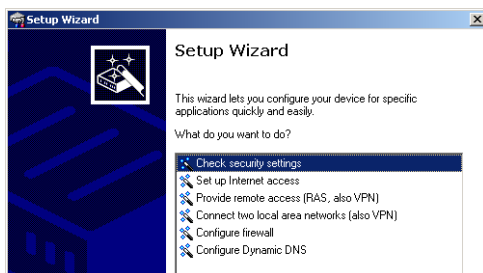
Your LANCOM Router has a password protection for the configuration access. This protection is already activated during the basic configuration by entering a password.

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.

8.3.1 Wizard for LANconfig

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



- ② Select in the selection menu the setup wizard **Control Security Settings** and confirm your choice with **Next**.
- ③ Enter your password in the following windows and select the allowed protocols for the configuration access from local and remote networks.
- ④ In a next step parameters of the configuration lock like number of failed log-in attempts and the duration of the lock can be adjusted.

- ⑤ Now 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**.

8.3.2 Wizard for WEBconfig

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

- password for the device
- allowed protocols for the configuration access of local and remote networks
- parameters of configuration lock (number of failed log-in attempts and duration of the lock)
- security parameters as WLAN name, closed network function, WEP key, ACL list and protocol filters

8.4 The firewall wizard

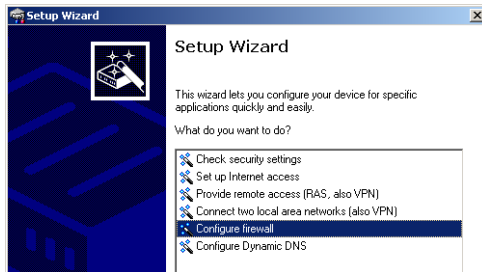
The LANCOM Router incorporates an effective protection of your WLAN when accessing the Internet by its Stateful Inspection firewall and its firewall filters. Basic idea of the Stateful Inspection firewall is that only self-initiated data transfer is considered allowable. All unasked accesses, which were 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 Router and about its configuration in the reference manual.

8.4.1 Wizard for LANconfig

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



- ② Select in the selection menu the setup wizard **Configuring Firewall** and confirm your choice with **Next**.
- ③ In the following windows, select the services/protocols the rule should be related to. Then you define the source and destination stations for this rule and what actions will be executed when the rule will apply to a data packet.
- ④ You finally give a name to the new rule, activate it and define, whether further rules should be observed when the rule will apply to a data packet.
- ⑤ The wizard will inform you as soon as the entries are complete. Complete the configuration with **Finish**.

8.4.2 Configuration under WEBconfig

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

8.5 The security checklist

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



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

■ Have you assigned a password for the configuration?

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

■ Have you permitted remote configuration?

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

■ Have you 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 be allowed by the dedicated Firewall rule then. Thus 'Trojans' and certain E-mail viruses lose their communication way back. The Firewall rules are summarized in LANconfig under 'Firewall/QoS' on the register card 'Rules'. A guidance can be found in the reference manual.

■ Have you activated the IP masquerading?

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

■ Have you closed critical ports with filters?

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

■ Have you excluded certain stations from access to the router?


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

■ Is your saved LANCOM configuration stored in a safe place?


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

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

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

 As standard, WEP128 encryption is activated for every unconfigured device.

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.

 Change the default WEP password immediately after configuring the router for the first time.

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

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

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

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

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

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

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

With the ISDN site verification, the device can only be operated at one particular ISDN connection. After being switched on, the device calls itself at the corresponding telephone number to check that it is still connected to the "proper" ISDN connection.

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

9 Options and accessories

Your LANCOM Router 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 LANCOM Wireless Router series and can be adapted to special conditions of environs.
- With the LANCOM Public Spot Option option it is possible to extend the LANCOM Router for additional billing and accounting functions in order to upgrade it to a Wireless Public Spot.

9.1 Optional LANCOM Wireless Router antennas

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



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



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

9.1.1 Antenna Diversity

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

Transmission quality can be improved with so-called "diversity" methods. The principle of diversity methods relies on the fact that a transmitted signal is often received multiple times (generally twice). With appropriate processing,

these signals can be re-combined into a single signal. The most common methods are space diversity and polarization diversity.

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

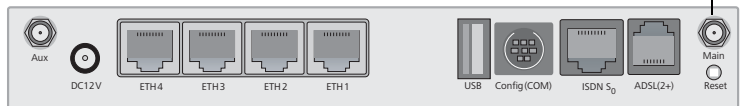
Polarization diversity antennas from LANCOM Systems:

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

9.1.2 Installation of AirLancer Extender antennas

For installation of an optional AirLancer antenna turn off the LANCOM Wireless Router 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 antennas to the antenna connector with the inscription 'Antenna Main'.

'Antenna Main' connector for AirLancer antenna



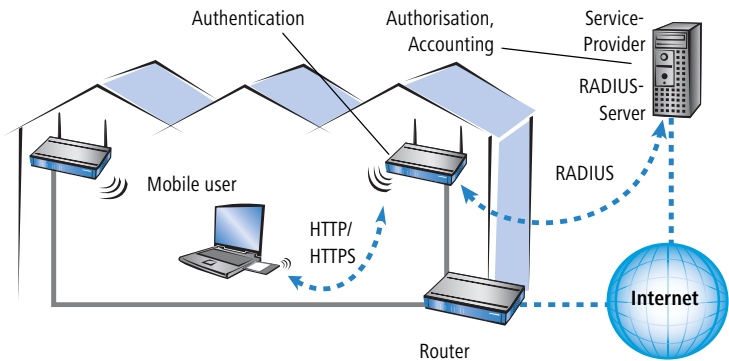
9.2 LANCOM Public Spot Option

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 Router 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 Systems 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.

9.3 LANCOM VoIP Basic Option and LANCOM VoIP Advanced Option



The term Voice over IP (VoIP) refers to voice communications over computer networks based on the Internet protocol (IP). The core idea is to provide the functions of traditional telephony via cost-effective and wide-spread networking structures such as the Internet. VoIP itself is not a standard, rather it is a collective term for the various technologies (equipment, protocols, voice encoding, etc.) which make voice communications in IP networks possible.

9.3.1 Advantages of VoIP solutions

Using Voice over IP offers considerable potential savings in the costs of corporate communication. LANCOM routers with VoIP support enable voice data to be transferred in parallel over existing data connections. LANCOM Systems supports not only networking with new VoIP installations; it also enables the integration of existing telephony equipment.

LANCOM VoIP solutions offer several advantages:

- SIP support for investment protection and flexibility
- Secured transfer of VoIP voice data with IPSec VPN
- Intelligent call routing to SIP providers, proprietary VoIP servers or into the plain old telephone system
- Flexible migration from existing ISDN/analog telephones and PBXs to VoIP
- High-availability VoIP site coupling with backup
- Comprehensive QoS functions with integrated broadband management even with standard Internet connections
- Intelligent and automatic switching between traditional telephony and VoIP for widespread acceptance by users
- High quality and reliability of VoIP components (e.g. fallback, life-line), so that VoIP can replace ISDN equipment

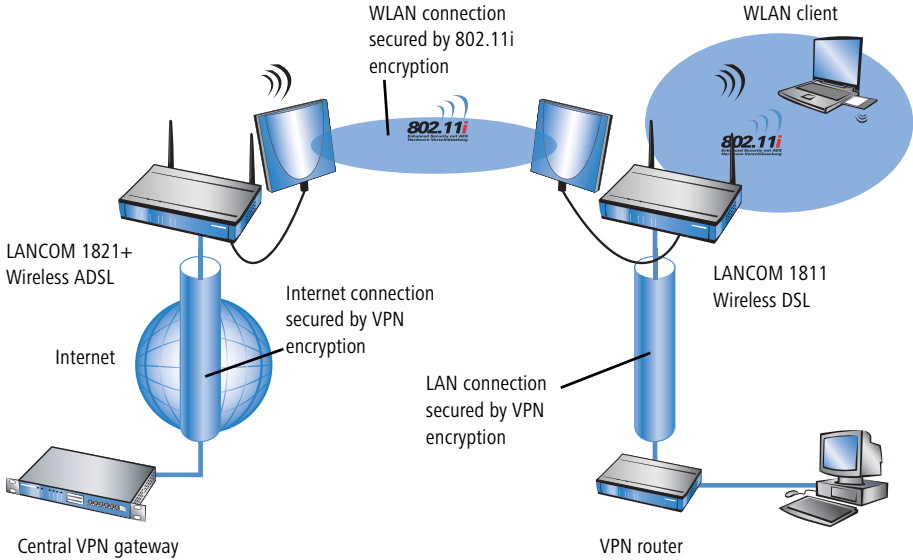
9.4 LANCOM VPN Option

The LANCOM VPN Option is an upgrade which advances your device to a VPN gateway with hardware encryption. In combination with the VPN encryption which is then available, you can offer optimal security for every type of connection.

- VPN encryption for WAN connections, e. g. over the Internet
- VPN encryption for LAN connections too, to protect data even from those eavesdroppers who have physical access to the transmitting medium (e. g. to the LAN cables).
- 802.11i encryption for point-to-point WLAN connections
- 802.11i encryption for connecting mobile WLAN clients

■ Chapter 9: Options and accessories

This function is suitable even for scenarios with high security requirements as the entire data path is secured even over multiple intermediate points.



Further information about VPN functions and their configuration can be found in the documentation for the LANCOM VPN Option and in the LCOS reference manual.

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

Increasing the TCP/IP window size under Windows

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

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

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

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.

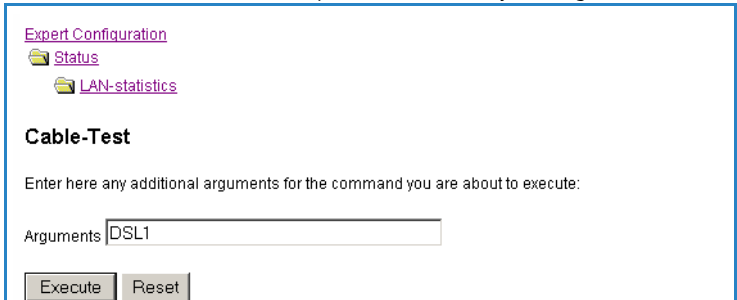
To resolve this issue, you can turn off the automatic time synchronization on the Windows XP computers under **Right mouse click on the time of day ▶ Properties ▶ Internet time**.

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**.



Expert Configuration
 Status
 LAN-statistics

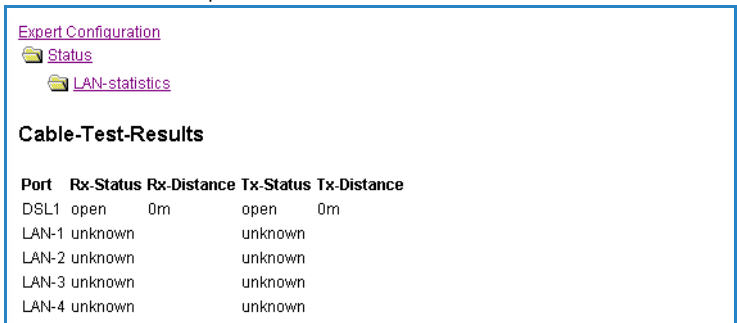
Cable-Test

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

Arguments

Execute Reset

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



Expert Configuration
 Status
 LAN-statistics

Cable-Test-Results

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

The following results can occur:

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

11 Appendix

11.1 Performance data and specifications

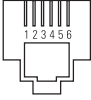
		LANCOM 1811 Wireless DSL	LANCOM 1821+ Wireless ADSL
EN Connections	Ethernet LAN	4x 10/100Base-TX, auto sensing, switch with node/hub auto sensing, cable tester	
	WAN (ADSL)	10/100Base-TX, auto sensing	ADSL over ISDN as per ITU G.992.1 Annex B (compatible to U-R2 connections of the Deutsche Telekom) or ADSL over POTS as per ITU G.992.1 Annex A ADSL over ISDN as per ITU 992.3, ITU G.992.5 Annex B (ADSL2+) or ADSL over POTS naas per ITU G992.3 and ITU G.992.5 Annex A
	ISDN	ISDN S ₀	
	WLAN	two 3 dBi dipole antennas (in package contents). Two reverse SMA connectors for external LANCOM AirLancer Extender antennas or antennas of other manufacturers. Please remember the legal requirements of your country for operating antenna systems. Information about the calculation of conforming antenna configurations under www.lancom.eu .	
	Outband	serial V.24/V.28 port (8 pol. mini DIN)	
	Power supply	12V AC over external power adapter	12V DC over external power adapter
	Wireless LAN	Frequency band	2400 - 2483,5 MHz (ISM) or 5150 - 5750 MHz
Standards		IEEE 802.11a (fully compliant to ETSI standards due to TPC and DFS) or IEEE 802.11g, compatible to IEEE 802.11b	
Housing	210 mm x 143 mm x 45 mm (W x H x D), rugged plastic case, provision for wall mounting		
Norms	CE conform according to EN 300 328, EN 301 893, EN 55024, EN 55022, EN 55011, EN 50081, EN 60950, ES 59005, EN 60950		
Licences	Notified in the countries Germany, Belgium, Netherlands, Luxembourg, Austria, Switzerland, Great Britain, Italy. More information about added notifications under www.lancom.eu .		
Environment / temperature range	Temperature range 0°C to +35°C at 80% max. humidity (non condensing)		

		LANCOM 1811 Wireless DSL	LANCOM 1821+ Wireless ADSL
Package contents		LAN cable (CAT.5, STP, 3 m), WAN cable (CAT.5, STP, 3 m), only LANCOM Wireless DSL series), ADSL cable (RJ45 – RJ11, CAT.5, STP, 3 m, only LANCOM Wireless ADSL series), ISDN cable, external power adapter (12V AC, 1.2 A for LANCOM Wireless DSL series; 12V DC, 1.0 A for LANCOM Wireless ADSL series), printed manual (English, German), software CD	
Options		<ul style="list-style-type: none"> ■ LANCOM VoIP Basic Option (Art. no. 61420) ■ LANCOM VoIP Advanced Option (Art. no. 61421) ■ LANCOM Public Spot Option (authentication 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) 	
Optional antennas		<ul style="list-style-type: none"> ■ AirLancer Extender I-180 2,4 GHz indoor antenna Art. no. 60914 ■ AirLancer Extender I-60ag Dualband indoor antenna Art. no. 61214 ■ AirLancer Extender O-30 2,4 GHz outdoor antenna Art. no. 60478 ■ AirLancer Extender O-70 2,4 GHz outdoor antenna Art. no. 60469 ■ AirLancer Extender O-D80g 2,4GHz polarizations diversity outdoor antenna Art. no. 61221 ■ AirLancer Extender O-360ag dualband omnidirectional outdoor antenna Art. no. 61223 ■ AirLancer Extender O-18a 5 GHz outdoor antenna Art. no. 61210 ■ AirLancer Extender O-D60a 5GHz polarizations diversity outdoor antenna Art. no. 61222 ■ AirLancer Extender O-9a 5GHz point to point outdoor antenna Art. no. 61220 ■ AirLancer 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 arrester for antenna cables Art. no. 61212 ■ AirLancer Extender SA-LAN surge arrester for LAN cables Art. no. 61213 ■ LANCOM Modem Adapter Kit for connecting modems (analogue or GSM) to the serial configuration interface Art. no. 110288 	

11.2 Contact assignment

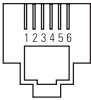
11.2.1 ADSL interface

6-pin RJ45 socket

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

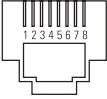
11.2.2 DSL interface

6-pin RJ45 socket

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

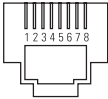
11.2.3 ISDN-S₀ interface

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

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


11.2.4 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+
	4	–
	5	–
	6	R-
	7	–
	8	–

11.2.5 Configuration interface (Outband)

8-pin mini-DIN socket

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

11.3 CE declaration of conformity



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

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

Index

Numerics

10/100Base-TX	26
3-DES	45, 53
802.11i	16, 64, 65, 66, 74
802.1x	16, 64, 66

A

Accounting	35
ACL	65
ADSL	
Connector cable	19
Transfer rates	10
AES	45, 53
Annex A	12
Annex B	12
Answering machine	11
Antenna	
Connector for main antenna	26
Outdoor	76
Autosensing	27

B

Blowfish	45, 53
----------	--------

C

Call routing	79
Call-back function	18
Callback function	45, 53
Calling Line Identity (CLI)	55
CAPI interface	60
CAST	45, 53
Charge limiter	22
Common ISDN Application Programming Interface (CAPI)	60
Configuration access	36, 40
Configuration interface	18
Connector cable	19
Configuration port	26
Configuration protection	18, 33

Connect charge protection	36, 40
Connect-charge budget	35
Connect-charge metering	35
Contact assignment	86
ADSL interface	86
Configuration interface	88
DSL interface	86
Ethernet interface	87
ISDN-S ₀ interface	87
LAN interface	87
Outband	88
WAN interface	87

D

Data frequencies	11
Declaration of conformity	88
Default gateway	40
DHCP	41
DHCP server	15, 32, 36, 39, 41
Dialing prefix	34
Dial-up access	53
Dial-up adapter	57
DNS	
access to the remote LAN	49
DNS server	15, 41
Documentation	19
Domain	49
Download	4
Downstream	10
DSL	
provider	36, 40
transfer protocol	40
DSL connection	
problems establishing the connection	81
DSL transfer protocol	36
E	
EAP	16, 64, 67

■ Index

Encryption	45, 53	IP masquerading	18
F		IP router	15
Fallback	79	IPoE	42
Fax	11	IPSec	45, 53
Firewall	18, 73	IPX	57
Firewall filter	70	Binding	50, 56
FirmSafe	18	External Network Number	50, 56
Firmware	4	Frame type	50
Flat rate	42	Internal-Net-Number	56
H		IPX conventions	50
Hardware installation	27	IPX router	15
I		Settings	49
ICMP	73	ISDN	
Information symbols	5	caller ID	47, 54, 55
Installation	19	connection	28
ADSL	27	Connector cable	19
antennas	27	D channel	55
configuration port	28	data compression	43
DSL	27	Dial-in number	42
ISDN	27	dynamic channel bundling	43
LAN	27	MSN	34
LANtools	29	NTBA	28
power adapter	28	password for connection	48
Interconnection	45	S ₀ port	26
Security aspects	45	ISDN connection	
Internet access	15, 42	Basic settings	34
Authentication data	42	ISDN leased-line option	16
Default gateway	42	ISDN modem	53
DNS server	42	ISDN PBX	34
Flat rate	42	ISDN S ₀ connection	17
IP address	42	L	
Netmask	42	LAN	
Internet provider	42	Connector cable	19
IP		LAN to LAN coupling	34, 45
Filter	73	Required information	46
Lock ports	73	LANCAPI	16, 30
IP address	32, 33, 50	LANCOM Enhanced Passphrase Security	64
IP address of the LANCOM	27	LANCOM setup	29
		LANCOM VPN Option	18

■ Index

SIP	79	fully automatic	31, 32
Software installation	29	manual	31, 32
Splitter	28	TCP/IP filter	18, 73
SSID	33, 36, 39	TCP/IP router	
Stateful Inspection Firewall	70	Settings	48
Status display		T-DSL	12
Power	22	Telephone	11
Status displays	20	Transfer protocol	81
ADSL Data	23	Turbo Mode	16
ADSL Link	23	U	
DSL Data	23	UDP	73
DSL status	23	Upstream	10
ISDN Data	24	V	
ISDN Status	24	Virtual Private Network	12
LAN	24	Virtual Private Networks (VPN)	15
Online	22	Voice communication	78
Power	21	Voice frequencies	11
Security	25	Voice over IP	78
VPN	25	VoIP	78
Wireless Link	25	VPN	12
Super AG	16	VPN client	57
Support	5	W	
Switch	26	WAN	
System requirements	19	Connector cable	19
T		WEBconfig	37
TCP	73	password	40
TCP/IP	20, 57	System requirements	20
check connection	52	WEP	16, 67, 74
Settings	31, 36, 39	Wireless LAN	
Settings to PCs in the LAN	40	operation modes	14
Windows size	82	WPA	16, 64, 65, 66, 74
TCP/IP configuration			
Automatic	39		