



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

## LANCOM 9100 VPN

- Handbuch
- Manual

# LANCOM 9100 VPN

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

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

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

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

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

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

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

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

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

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

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

[www.lancom.eu](http://www.lancom.eu)

Wuerselen, April 2009

# Preface

## Thank you for your confidence in us!

You have decided on a high quality product from LANCOM. The LANCOM 9100 VPN is a high performance central site VPN gateway that provides connectivity for up to 1000 sites. The following functions are characteristics of the LANCOM 9100 VPN:

- Provides 200 VPN channels, upgradable to 1000 remote sites
- VRRP and load balancing
- Advanced Routing and Forwarding with 256 VLAN / IP contexts
- Status and error display
- 4 x Gigabit Ethernet + ISDN BRI

## Security settings

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

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

## Components of the documentation

The documentation of your device consists of the following parts:

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

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

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

- The system design of the operating system LCOS
- Configuration
- Management
- Diagnosis
- Security
- Routing and WAN functions
- Firewall
- Quality of Service (QoS)
- Virtual Private Networks (VPN)
- Virtual Local Networks (VLAN)
- Backup solutions
- LANCAPI
- Further server services (DHCP, DNS, charge management)

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

### **An der Erstellung dieser Dokumentation ...**

... haben mehrere Mitarbeiter/innen aus verschiedenen Teilen des Unternehmens mitgewirkt, um Ihnen die bestmögliche Unterstützung bei der Nutzung Ihres LANCOM-Produktes anzubieten.

Sollten Sie einen Fehler finden oder einfach nur Kritik oder Anregung zu dieser Dokumentation äußern wollen, senden Sie bitte eine E-Mail direkt an: [info@lancom.eu](mailto:info@lancom.eu)

# Content

|  |           |
|--|-----------|
| <b>1 Introduction</b>                    | <b>8</b>  |
| 1.1 What does VPN offer?                 | 9         |
| 1.2 Just what can your LANCOM Router do? | 10        |
| <b>2 Installation</b>                    | <b>13</b> |
| 2.1 Package content                      | 13        |
| 2.2 System requirements                  | 13        |
| 2.3 Status displays and interfaces       | 14        |
| 2.3.1 Front                              | 14        |
| 2.3.2 Rear panel                         | 20        |
| 2.4 Hardware installation                | 20        |
| 2.5 Software installation                | 21        |
| 2.5.1 Starting the software setup        | 21        |
| 2.5.2 Which software should I install?   | 22        |
| <b>3 Basic configuration</b>             | <b>23</b> |
| 3.1 What details are necessary?          | 23        |
| 3.1.1 TCP/IP settings                    | 23        |
| 3.1.2 Configuration protection           | 25        |
| 3.1.3 Charge protection                  | 25        |
| 3.2 Instructions for LANconfig           | 26        |
| 3.3 Instructions for WEBconfig           | 27        |
| 3.4 TCP/IP settings for PC workstations  | 31        |
| <b>4 Setting up Internet access</b>      | <b>32</b> |
| 4.1 The Internet Connection Wizard       | 34        |
| 4.1.1 Instructions for LANconfig         | 34        |
| 4.1.2 Instructions for WEBconfig         | 35        |

|          |   |           |
|----------|---|-----------|
| <b>5</b> | <b>Connecting two networks</b>                        | <b>36</b> |
| 5.1      | Which details are necessary?                          | 37        |
| 5.1.1    | General information                                   | 37        |
| 5.1.2    | Settings for the TCP/IP router                        | 39        |
| 5.1.3    | Settings for NetBIOS routing                          | 40        |
| 5.2      | Instructions for LANconfig                            | 41        |
| 5.3      | 1-Click-VPN for networks (site-to-site)               | 42        |
| 5.4      | Instructions for WEBconfig                            | 43        |
| <b>6</b> | <b>Providing dial-in access</b>                       | <b>45</b> |
| 6.1      | Which details are necessary?                          | 45        |
| 6.1.1    | General information                                   | 46        |
| 6.1.2    | Settings for TCP/IP                                   | 47        |
| 6.1.3    | Settings for NetBIOS routing                          | 47        |
| 6.2      | Settings on the dial-in computer                      | 48        |
| 6.2.1    | Dialing-in via VPN                                    | 48        |
| 6.2.2    | Dialing-in via ISDN                                   | 48        |
| 6.3      | Instructions for LANconfig                            | 49        |
| 6.4      | 1-Click-VPN for LANCOM Advanced VPN Client            | 49        |
| 6.5      | Instructions for WEBconfig                            | 50        |
| <b>7</b> | <b>Fax transmission with LANCAPI</b>                  | <b>51</b> |
| 7.1      | Installing the LANCOM CAPI Faxmodem                   | 52        |
| 7.2      | Installing the MS Windows Fax Service                 | 53        |
| 7.3      | Sending a fax   | 54        |
| 7.3.1    | Sending faxes from an office application              | 54        |
| 7.3.2    | Sending faxes with the Windows Fax Service            | 54        |
| <b>8</b> | <b>Security settings</b>                              | <b>56</b> |
| 8.1      | Tips for the proper treatment of keys and passphrases | 56        |
| 8.2      | Security settings Wizard                              | 56        |
| 8.2.1    | LANconfig Wizard                                      | 57        |
| 8.2.2    | WEBconfig Wizard                                      | 57        |
| 8.3      | The security checklist                                | 58        |

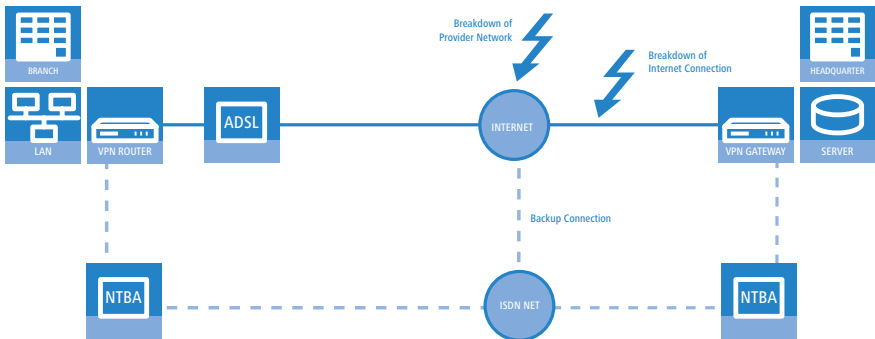
|  |           |
|--|-----------|
| <b>9 Advice &amp; assistance</b>                           | <b>61</b> |
| 9.1 No WAN connection can be established                   | 61        |
| 9.2 Slow DSL transmission                                  | 61        |
| 9.3 Unwanted connections under Windows XP                  | 62        |
| <b>10 Appendix</b>   | <b>63</b> |
| 10.1 Performance and characteristics                       | 63        |
| 10.2 Connector wiring                                      | 64        |
| 10.2.1 LAN/WAN interface 10/100/1000Base-TX, DSL interface | 64        |
| 10.2.2 ISDN-S <sub>0</sub> interface                       | 64        |
| 10.2.3 Configuration interface (outband)                   | 65        |
| 10.3 Declaration of conformity                             | 65        |
| <b>11 Index</b>  | <b>66</b> |



# 1 Introduction

The LANCOM 9100 VPN is a high-performance central-site VPN gateway that supports 200 VPN connections. With the LANCOM VPN Option, it provides VPN connections for up to 1000 sites. Quality-of-Service, dynamic bandwidth management and the four Gigabit-Ethernet slots ensure that data is correctly prioritized in the network and that speeds are maximized. Various connection possibilities including ISDN, WAN and the USB 2.0 host port facilitate its integration into the network. Practical: Various information on the device is permanently displayed, including temperature, CPU load, and active VPNs. The fan's function is permanently monitored by LED and, additionally, an acoustic signal is emitted should the CPU overheat.

The integrated firewall with security functions such as stateful inspection, intrusion detection and denial-of-service protection is supplemented by dynamic bandwidth management and comprehensive backup, high-availability and redundancy functions over ISDN and VRRP.



IPSec-based VPN provides optimal security for connecting branch offices and home offices thanks to the high-security 3-DES or AES encryption, integrated hardware acceleration, and support of digital certificates.

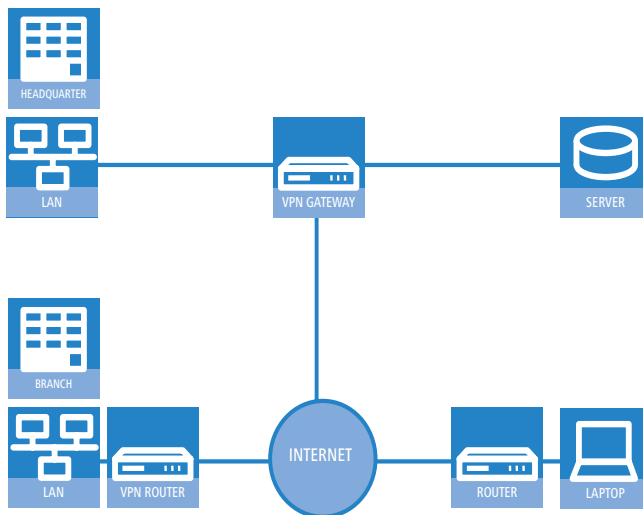
The versatile functions for address translation and routing allow different networks to be connected over common infrastructure. The LANCOM Advanced Routing and Forwarding concept ensures that professional network virtualization is no longer a problem: Existing networks at partner companies, branch offices, or home-office workstations can be integrated into the VPN without problem.

The management systems LANconfig and LANmonitor are included and offer not only cost-effective remote maintenance of entire installations along with highly convenient setup wizards, but also full real-time monitoring and logging. Service providers benefit from the broad range of scripting methods and professional access with individual access rights for administrators via SSH, HTTPS, TFTP and ISDN dial-in.

## 1.1 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 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 sites.

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

## 1.2 Just what can your LANCOM Router do?

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

| LANCOM 9100 VPN   |   |
|---|---|
| Applications  |   |
| Internet access   | ✓ |
| LAN-LAN connectivity over VPN   | ✓ |
| LAN-LAN connectivity over ISDN  | ✓ |
| RAS server (over VPN)   | ✓ |
| RAS server (over ISDN)  | ✓ |
| IP router with stateful inspection firewall                               | ✓ |
| NetBIOS proxy for connectivity Microsoft peer-to-peer networks            | ✓ |
| DHCP and DNS server (for LAN and WLAN)                                    | ✓ |
| N:N mapping for routing networks with the same IP-address ranges over VPN | ✓ |
| Configuring LAN ports as additional WAN ports                             | ✓ |
| Policy-based routing  | ✓ |

| LANCOM 9100 VPN   |            |
|---|------------|
| Load balancing for bundling multiple DSL channels   | 4 channels |
| Backup solutions and load balancing with VRRP   | ✓          |
| NAT Traversal (NAT-T)   | ✓          |
| DMZ with configurable IDS checks  | ✓          |
| PPPoE servers   | ✓          |
| WAN RIP   | ✓          |
| Spanning Tree Protocol  | ✓          |
| Layer 2 QoS tagging   | ✓          |
| ISDN leased lines   | ✓          |
| LANCAPI server to provide office applications such as fax or answering machine via the ISDN interface.            | ✓          |
| <b>WAN connections</b>  |            |
| Connector for DSL or cable mode (via LAN ports)   | ✓          |
| ISDN-S <sub>0</sub> connector for establishing Dynamic VPN connections to remote sites with dynamic IP addresses  | ✓          |
| <b>LAN connection</b>   |            |
| Individual Gigabit Ethernet LAN ports.<br>Alternatively switchable as a WAN interface for connecting SDSL modems. | 4          |
| <b>USB connector</b>  |            |
| USB 2.0 host port (high speed: 12 Mbps) for connecting a USB printer and for future extensions                    | ✓          |
| <b>Security functions</b>   |            |
| IPsec encryption via external software (VPN client)   | ✓          |
| 200 integrated VPN tunnels for secure network connections   | ✓          |
| IPsec encryption in hardware  | ✓          |
| 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                      | ✓          |

| LANCOM 9100 VPN  |   |
|--|---|
| Protection of the configuration from brute-force attacks.  | ✓ |
| <b>Configuration</b>   |   |
| 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  | ✓ |
| <b>Optional software extensions</b>  |   |
| LANCOM VPN Option with 500 active tunnels for secure network connectivity  | ✓ |
| LANCOM VPN Option with 1000 active tunnels for secure network connectivity   | ✓ |
| LANCOM Service 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 content

Before beginning with the installation, please check that nothing is missing from your package. Along with the device itself, the box should contain the following accessories:

| LANCOM 9100<br>VPN                              |   |
|---|---|
| IEC cable                                       | ✓ |
| LAN connector cable (green connectors)          | ✓ |
| WAN connector cable (dark-blue connectors)      | ✓ |
| ISDN connector cable (light-blue connectors)    | ✓ |
| Connector cable for the configuration interface | ✓ |
| Mounting brackets for 19" cabinets              | ✓ |
| Rubber feet                                     | ✓ |
| LANCOM CD                                       | ✓ |
| Printed documentation                           | ✓ |

Should anything be missing, please take up immediate contact to your dealer or to the address on the delivery note supplied with your device.

### 2.2 System requirements

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

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



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

## 2.3 Status displays and interfaces

### Meanings of the LEDs

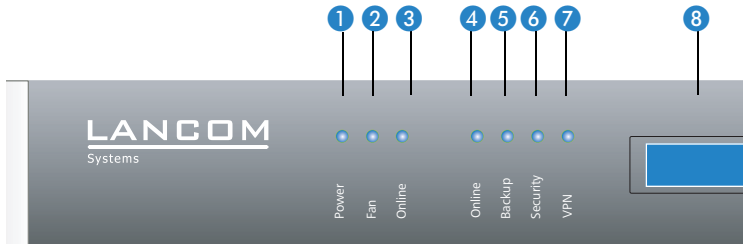
In the following sections we will use different terms to describe the behaviour of the LEDs:

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

### 2.3.1 Front

The LANCOM 9100 VPN is equipped with the following status displays on the front panel:

LANCOM 9100 VPN



#### 1 Power

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

|       |          |                          |
|-------|----------|--------------------------|
| Off   |          | Device switched off      |
| Green | blinking | Self-test after power-up |

|           |                      |   |
|-----------|----------------------|---|
| Green     | On (permanently)     | Device operational  |
| Red/green | Blinking alternately | Device insecure: Configuration password not set             |
| Red       | blinking             | Time or charge limit on online connections has been reached |



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

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

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

There are three ways to remove the lock:

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

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

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



Signal that a charge or time limit has been reached



## ■ Chapter 2: Installation

### 2 Fan

The Fan LED displays the fan's status:

|        |                  |  |
|--------|------------------|--|
| Green  | On (permanently) | CPU temperature OK   |
| Orange | On (permanently) | CPU temperature > 55°  |
| Red    | blinking         | Hardware failure of the fan or CPU temperature > 60°; additional acoustic signal |

To prevent damage to the hardware, this LED is complemented by an acoustic signal. If the fan is blocked or the CPU temperature exceeds 60°, a pulsed acoustic signal is emitted.

### 3 COM

Connection status of the serial configuration interface

|        |                  |  |
|--------|------------------|--|
| Off    |                  | No session logged on                               |
| Green  | On (permanently) | Serial configuration session logged on             |
| Orange | Flickering       | Data transmission during the configuration session |

### 4 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 |

### 5 Backup

Displays the backup status:

|     |                  |   |
|-----|------------------|---|
| Off |                  | None of the WAN connections or virtual routers is in the backup state         |
| Red | On (permanently) | At least one of the WAN connections or virtual routers is in the backup state |

## 6 Standby

Displays the standby status:

|       |                  |   |
|-------|------------------|---|
| Off   |                  | <ul style="list-style-type: none"> <li>■ No VRRP active</li> <li>or</li> <li>■ VRRP active an one virtual router defined in the device is in the Master state.</li> </ul>   |
| Red   | On (permanently) | <p><b>All</b> virtual routers defined in the device are deactivated. A virtual router is deactivated in the following situations:</p> <ul style="list-style-type: none"> <li>■ the link is broken,</li> <li>■ the virtual router is already in backup state and the backup connection is broken,</li> <li>■ the main connections fails and no backup priority is defined for the virtual router.</li> </ul> |
| Green | On (permanently) | <b>All</b> virtual routers defined in the device are in Standby state.  |

## 7 VPN

Status of a VPN connection.

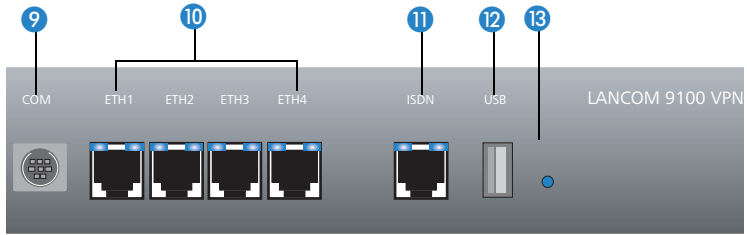
|       |                  |                             |
|-------|------------------|-----------------------------|
| Off   |                  | No VPN tunnel established   |
| Green | Blinking         | Connection establishment    |
| Green | Flashing         | First connection            |
| Green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

## 8 LCD display

The LC display has two lines of 16 characters each to display the following information in rotation:

- ▶ Device name
- ▶ Firmware version
- ▶ Device temperature
- ▶ Date and time
- ▶ CPU load
- ▶ Memory load
- ▶ Number of VPN tunnels
- ▶ Data transfer in reception direction
- ▶ Data transfer in transmission direction

The LANCOM 9100 VPN is equipped with the following interfaces on the front panel:



### 9 COM

Connector for the serial configuration cable.

### 10 ETH 1 to 4

Ethernet sockets ( 10/100/1000Base-Tx) for connection to the LAN. 10 Mbit, 100 Mbit or 1000 Mbit connections are supported. The available transfer rate is detected automatically (autosensing).

Each Ethernet socket has two LEDs (green and yellow).

|        |                  |  |
|--------|------------------|--|
| Green  | Off              | No networking device attached                              |
| Green  | On (permanently) | Connection to network device operational, not data traffic |
| Green  | Flickering       | Data traffic   |
| Yellow | Off              | 1000 Mbps  |
| Yellow | On (permanently) | 10/100 Mbps  |

### 11 ISDN

ISDN-S<sub>0</sub> connector. Each ISDN/S<sub>0</sub> socket has two LEDs (green and orange):

|                  |                  |  |
|------------------|------------------|--|
| Green            | Orange           |  |
| blinking         | blinking         | Hardware error                               |
| On (permanently) | blinking         | D channel connected, B channel not connected |
| On (permanently) | Flashing         | ISDN protocol negotiation (B channel)        |
| On (permanently) | On (permanently) | B channel connected                          |
| blinking         | Off              | Layer-1 being established                    |
| Off              | Off              | Layer-1 deactivated                          |
| On (permanently) | Off              | TEI or Layer-2 activation available          |

### 12 USB

USB connector (USB host)

## 13 Reset

Reset button (see 'Reset button functions')

### Reset button functions

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

It is not always possible to install a device under lock and key. There is consequently a risk that the configuration will be deleted by mistake if a co-worker presses the reset button too long. With the suitable setting, the behavior of the reset button can be controlled.

| Configuration tool | Call                                  |
|--------------------|---------------------------------------|
| WEBconfig, Telnet  | Expert configuration > Setup > Config |

### ■ Reset button

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

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



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

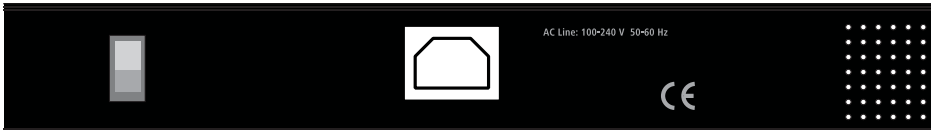
- Reset-or-boot (standard setting): Press the button briefly to re-start the device. Pressing the button for 5 seconds or longer restarts the device and resets the configuration to its factory settings.  
All green LEDs on the device light up continuously.  
Once the switch is released the device will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



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

### 2.3.2 Rear panel

The following connectors are located on the rear of the device.



14

14 On/  
off switch

Switch to separate the device from the mains supply.

15

15 IEC power  
socket

Connector for IEC power cable for power supply.



#### Please observe the following notice:


The device can only be completely separated from the mains power supply by unplugging the (IEC) power cable.

## 2.4 Hardware installation

Installing the LANCOM Router involves the following steps:


- ① **Mounting** – The device is designed for mounting in an available 19" unit in a server cabinet. If necessary fix the rubber pads to the underside of the device to prevent any scratching to other equipment.
- ② **LAN** – first of all connect your LANCOM Router to the LAN or to an individual PC. Plug one end of the supplied network cable (green connectors) into an Ethernet port on the device ⑩, and the other end into an available network connector socket in your local network, a free socket on a switch or hub, or the networking connector of an individual PC.

The Ethernet ports use autosensing to recognize the data rate (10/100/1000 Mbit) and the type (node/hub) of attached network devices. It is possible to connect devices of different speeds and types in parallel.

-  Avoid having multiple unconfigured LANCOMs at once within a single network segment. Any unconfigured LANCOM takes on the same IP address (ending in '254'), and so address conflicts could arise. To avoid problems, multiple LANCOMs should be configured one after the other with the respective device being assigned with a new and unique IP address (not ending in '254') each time.
- ③ **WAN** – You can operate up to three Ethernet ports as WAN interfaces. In the device configuration, set the necessary Ethernet port to "DSL-1" to "DSL-4" and activate the corresponding DSL interface. Use the supplied cable (dark-blue connectors) to connect the Ethernet port ⑩ to the Ethernet socket on, for example, a DSL modem or cable modem.
- ④ **ISDN** – To connect the LANCOM Router to the ISDN, plug in one end of the supplied ISDN cable (light-blue connectors) to the ISDN S<sub>0</sub> interface ⑪ on the router and the other end to an ISDN S<sub>0</sub> point-to-point or point-to-multipoint connection.
- ⑤ **Configuration interface** – optionally, the router can be connected directly to the serial interface (RS-232, V.24) of a PC. Use the connection cable supplied for this. Connect the LANCOM configuration interface ⑧ to an available serial interface on the PC.
- ⑥ **Supply power and switch on** – Using the IEC cable ⑮, supply power to the device and switch it on using the switch ⑭ located on the rear panel.


## 2.5 Software installation

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

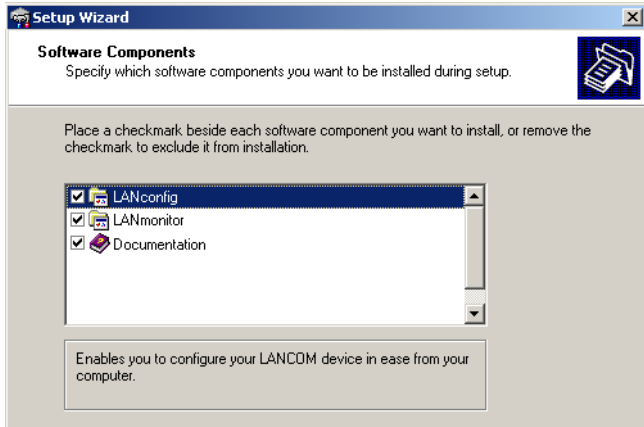
-  You may skip this section if you use your LANCOM VPN Router exclusively with computers running operating systems other than Windows.

### 2.5.1 Starting the software setup

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

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

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



## 2.5.2 Which software should I install?

- **LANconfig** is the Windows configuration program for all LANCOM routers and LANCOM access points. WEBconfig can be used alternatively or in addition via a web browser.
- With **LANmonitor** you can use a Windows computer to monitor all of your LANCOM routers and LANCOM access points.

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

## 3 Basic configuration

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

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

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

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

### 3.1 What details are necessary?

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

- TCP/IP settings
- Protecting the configuration
- Configuring toll protection
- Security settings

#### 3.1.1 TCP/IP settings

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

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



### New LAN – fully automatic configuration possible

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

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

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

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

### Should you still configure manually?

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

- Select automatic configuration if you are **not** familiar with networks and IP addresses.
- Select manual TCP/IP configuration if you are familiar with networks and IP addresses and one of the following statements is true:
  - You have not yet used any IP addresses in your network but would like to now; You would like to specify the IP address for the router yourself and would like to assign it a user-defined address from one of the address ranges reserved for private use, for example '10.0.0.1' with a network mask of '255.255.255.0'. If you do this you simultaneously specify the address range that the DHCP server will subsequently use for the other devices in the network (provided the DHCP server is activated).
  - You have so far also used IP addresses on the computers in the LAN.

### Required information for manual TCP/IP configuration

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

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

- Server: The LANCOM VPN Router operates as DHCP server in the network; as a minimum its own IP address and the network mask must be assigned.
- Client: The LANCOM VPN Router obtains its address information from another DHCP server; no address information is required.
- **IP address and network mask for the LANCOM VPN Router**  
Assign the LANCOM VPN Router a free IP address from your LAN's address range and enter the network mask.
- **Gateway address**  
Enter the gateway's IP address if you have selected 'Off' as the DHCP mode of operation or if another network device is assuming the role of gateway in the 'Server' mode of operation.
- **DNS server**  
Enter the IP address of a DNS server to resolve domain names if you have selected 'Off' as the DHCP mode of operation or if another network device is assuming the role of DNS server in the 'Server' mode of operation.

### 3.1.2 Configuration protection

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



Multiple administrators can be set up in the configuration of the LANCOM, each with differing access rights. Up to 16 different administrators can be set up for a LANCOM VPN Router. Further information can be found in the LCOS reference manual under "Managing rights for different administrators".

### 3.1.3 Charge protection

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

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

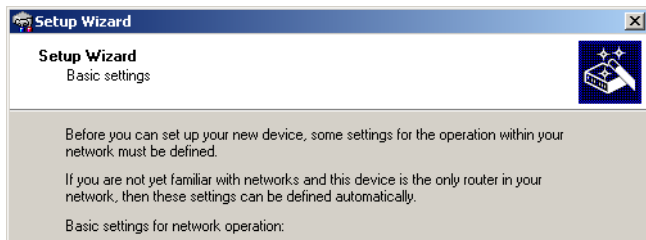
The budget can be completely deactivated by entering a value of '0'.



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

## 3.2 Instructions for LANconfig

- ① Start LANconfig with **Start ▶ Programs ▶ LANCOM ▶ LANconfig**. LANconfig automatically detects new LANCOM devices in the TCP/IP network.
- ② If the search detects an unconfigured device, the Setup Wizard launches to help you with its basic settings, or indeed to handle the entire process on your behalf (assuming that the appropriate networking environment exists).



If the Setup Wizard does not start automatically, you can manually search for new devices at all interfaces (if the LANCOM VPN Router is connected via the serial configuration interface) or in the network (**File ▶ Find devices**).




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


If you choose automatic TCP/IP configuration, you can continue with step ⑤.

- ③ Give the LANCOM an address from the applicable IP address range. Confirm with **Next**.
- ④ In the window that follows, you first set the password to the configuration. Entries are case sensitive and should be at least 6 characters long.

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

- 
-  Be aware that releasing this option also allows remote configuration over the Internet. Whichever option you select, make sure that configuration access is password protected.
  - ⑤ Charge protection is a function which can place a limit on the costs from WAN connections. Accept your entries with **Next**.
  - ⑥ Close the configuration with **Finish**.

---

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

### 3.3 Instructions for WEBconfig


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

#### Secure with HTTPS

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

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

---

 Always use the latest version of your browser to ensure maximum security. For Windows, LANCOM Systems GmbH recommends the latest version of the Internet Explorer.

#### Accessing the device with WEBconfig

To carry out a configuration with WEBconfig, you need to know how to contact the device. Device behavior and accessibility for configuration via a Web browser depend on whether the DHCP server and DNS server are active in the LAN already, and whether these two server processes share the assignment in the LAN of IP addresses to symbolic names. WEBconfig accesses the LANCOM

either via its IP address, the device name (if configured), or by means of any name if the device has not yet been configured.

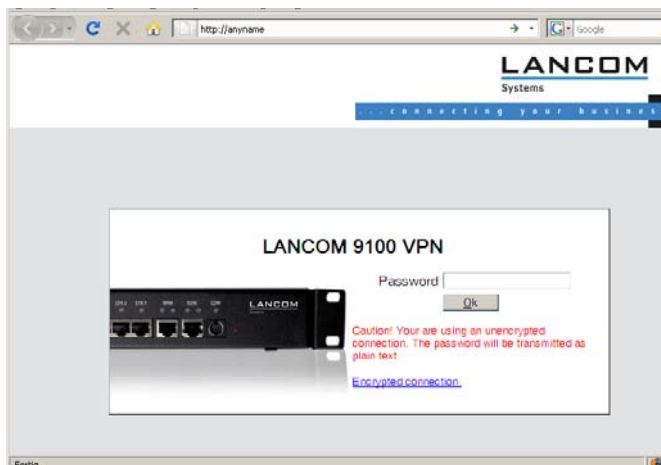
Following power-on, unconfigured LANCOM devices first check whether a DHCP server is already active in the LAN. Depending on the situation, the device can either enable its own DHCP server or enable DHCP client mode. In the second operating mode, the device can retrieve an IP address for itself from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

### Network without a DHCP server

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



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



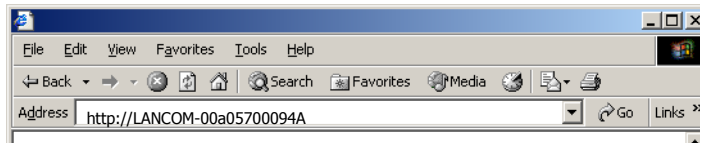
If the configuration computer does not retrieve its IP address from the LANCOM DHCP server, it determines the current IP address of the computer (with **Start ▶ Run ▶ cmd** and command **ipconfig** at the prompt under Windows 2000 or Windows XP or Windows Vista, with **Start ▶ Run ▶ cmd** and


command **winipcfg** at the prompt under Windows Me or Windows 9x, or with command **ifconfig** in the console under Linux). In this case, the LANCOM can be accessed with address **x.x.x.254** (the "x"s stand for the first three blocks in the IP address of the configuration computer).

### Network with DHCP server

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

- If the LAN also has a DNS server for name resolution and this communicates the IP address/name assignment to the DHCP server, the device can be reached under name "LANCOM-<MAC address>", e.g. "LANCOM-00a057xxxxxx".



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

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

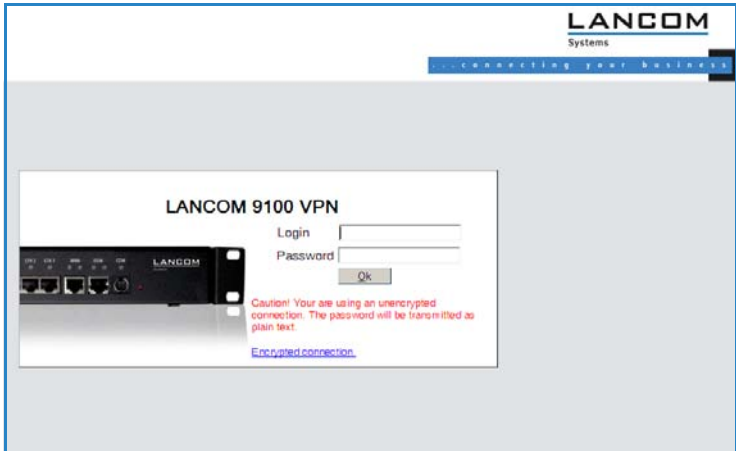
### Login

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

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

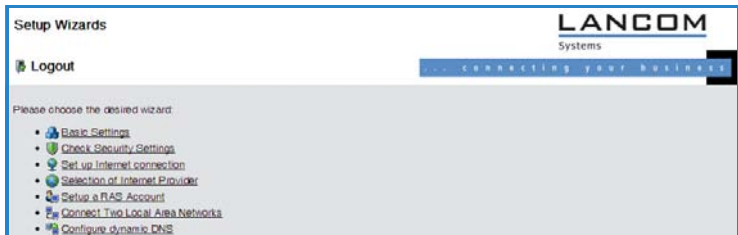


As an alternative, the login dialog provides a link for an encrypted connection over HTTPS. Always use the HTTPS connection for increased security whenever possible.



## Setup Wizards

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



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

## 3.4 TCP/IP settings for PC workstations

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

- Standard gateway – receives all packets which are not addressed to computers in the local network
- DNS server – translates network and computer names into their actual IP addresses.

The LANCOM VPN Router can fulfill the functions of a standard gateway and also of a DNS server. It can also operate as a DHCP server, which automatically assigns IP addresses to all of the computers in the LAN.

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

### ■ IP address allocation by a LANCOM

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

### ■ IP address allocation by a separate DHCP server

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

### ■ Manual IP address assignment

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

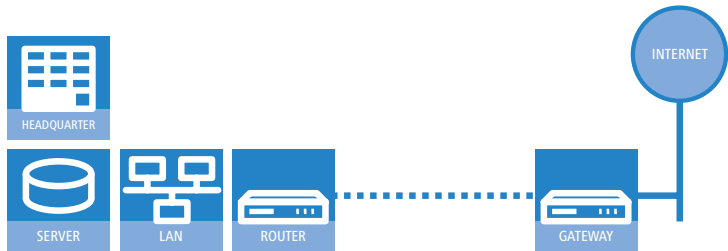


Further information and help on the TCP/IP settings for your LANCOM VPN Router is available in the Reference Manual. For information on the network configuration of workstation PCs, refer to the documentation for the installed operating system.



## 4 Setting up Internet access

The LANCOM provides a central point of Internet access for all of the computers in the LAN. The connection to the Internet provider can be established via any WAN connector, i.e. via DSL or ISDN (where available). Internet access via ISDN can be used to backup a DSL connection.



### Which WAN interface?

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

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

### Does the Setup Wizard know your Internet provider?

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

### Internet provider unknown

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

### Other connection options

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

- Billing by time or flatrate – select the method by which you are billed by your Internet provider.
  - In case of billing by time, you can set the LANCOM to cut connections automatically if no data flows for a certain time (the hold time).  
You can also set up line polling that detects inactive remote sites very quickly and, in such cases, can close the connection before the hold time expires.
  - In case of flatrate billing you can also set up line polling to monitor the function of the remote site.  
Apart from that you can opt to keep flatrate connections permanently active ("keep-alive"). In case a connection should fail, it is re-established automatically.

### Creating a backup connection to the Internet

The most common utilization of the backup solution is to provide an auxiliary Internet connection. When setting up an Internet connection, an additional option is to create a second connection to the Internet via an alternative WAN interface. If the primary Internet access is set up to operate via the ADSL interface, you can set up your backup connection to operate via UMTS or ISDN.



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

## 4.1 The Internet Connection Wizard


### 4.1.1 Instructions for LANconfig

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



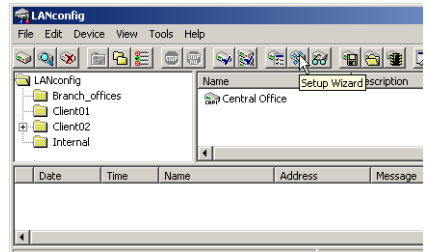
- 2 In the selection menu, select the Setup Wizard, **Set up Internet connection** and confirm the selection with **Next**.
- 3 In the following windows you select your country, your Internet provider if possible, and you enter your access data.
- 4 Depending on availability the Wizard provides further options for your Internet connection.
- 5 After entering all of the necessary data the Wizard then offers you the option of setting up a backup connection. Select the corresponding WAN interface to be used for the backup connection and enter the relevant access data for the Internet connection.

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

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

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

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



#### 4.1.2 Instructions for WEBconfig

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

## 5 Connecting two networks

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

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

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

### Always configure both ends

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



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

### Security aspects

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

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



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

## 5.1 Which details are necessary?

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

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






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

### 5.1.1 General information

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



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

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

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

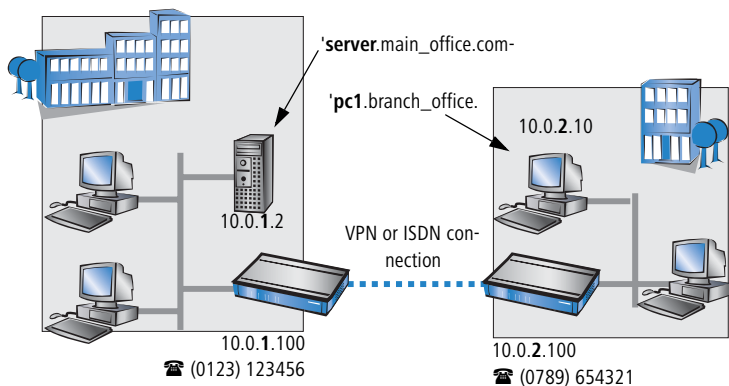
Notes on the different settings:

- If your own device features an **ISDN connection**, the Wizard will ask you whether the remote site also has one.
- For VPN connections over the Internet, the type of IP address at each end must be specified. There are two **types of IP address**. Static and dynamic. The differences between these two IP address types are explained in the Reference Manual.  
The Dynamic VPN function makes it possible to establish VPN connections between gateways with dynamic IP addresses, and not only between gateways with static (fixed) IP addresses. An ISDN connection is required to actively establish VPN connections to remote sites that use dynamic IP addresses.
- If you have not yet given a name to your LANCOM, the Wizard will ask you to enter a new **name for your device**. Entering a name will cause your LANCOM to be renamed. Ensure that you give different names to the two remote devices.
- The **name of the remote site** is required for identifying the devices.
- In the field **ISDN number** the telephone number of the remote ISDN site is specified. Enter the full telephone number for the remote site, including all necessary prefixes (e.g. area codes).

- The **ISDN calling line ID** specified is used to identify and authenticate the caller. If a LANCOM Router is called, it compares the ISDN calling line ID entered for the remote site to the ID that is actually received over the D channel from the caller. An ISDN ID generally consists of the country code and an MSN.
- The **password for the ISDN connection** is an alternative to the ISDN calling line ID. This is used to authenticate the caller if no ISDN calling line ID is received. The password must be entered identically at both ends. It is used for calls in both directions.
- The **shared secret** is the central password for the VPN connection's security. It must be entered identically at both ends.
- Data compression improves transmission speeds without incurring extra costs. This is completely different to the bundling of two ISDN channels by MLPPP (**M**ulti**L**ink-**P**PP): This doubles the bandwidth, although this generally doubles the connection costs as well.

### 5.1.2 Settings for the TCP/IP router

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



LAN at the main office. IP:  
10.0.1.0,  
Netmask: 255.255.255.0

Branch office LAN. IP: 10.0.2.0,  
Netmask: 255.255.255.0  
Domain: 'branch\_office.com-

Unlike with Internet access, network connectivity makes all of IP addresses visible in all participating networks, including those in the remote LAN, and



not just that of the router. The computer with the IP address 10.0.2.10 in the branch-office LAN sees the server 10.0.1.2 at the main office and, with the appropriate rights, has access to it. The same applies in the other direction.

### DNS access to the remote LAN

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

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



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

### VPN extranet

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

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

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

### 5.1.3 Settings for NetBIOS routing

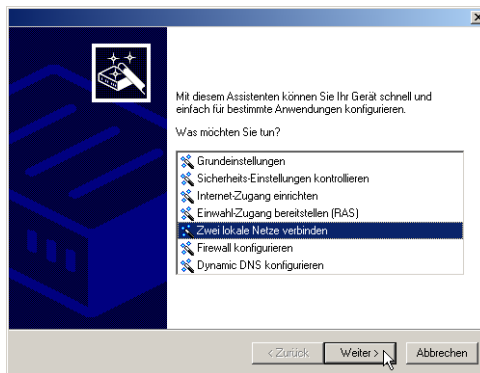
NetBIOS routing is quick to set up: In addition to the specifying the TCP/IP protocol being used, the only other information required is the name of a Windows workgroup in the LAN used by the router.

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

## 5.2 Instructions for LANconfig

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

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



- ② The Wizard will inform you when the required information is complete. You can then close the Wizard with **Finish**.
- ③ Once you have completed the set-up of both routers, you can start testing the network connection. Try to communicate with a computer in the

remote LAN (e.g. with ping). The LANCOM Router should automatically connect to the remote site and make contact to the requested computer.

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

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

```

Command Prompt
C:\>ping 10.0.2.0

Pinging 10.0.2.0 with 32 bytes of data:

Reply from 10.0.2.0: bytes=32 time<10ms TTL=64
Reply from 10.0.2.0: bytes=32 time<10ms TTL=64
Reply from 10.0.2.0: bytes=32 time<10ms TTL=64
Reply from 10.0.2.0: bytes=32 time<10ms TTL=64

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

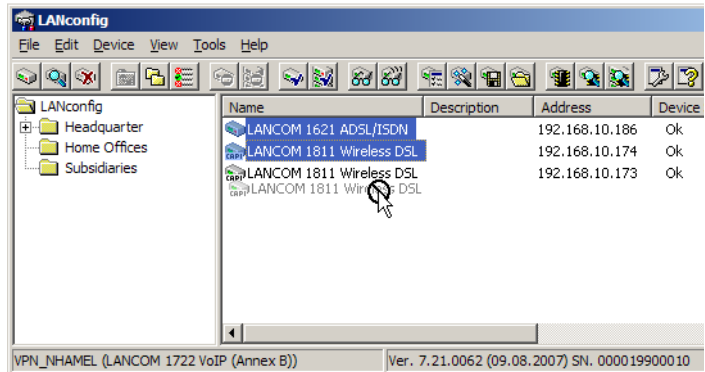
C:\>

```

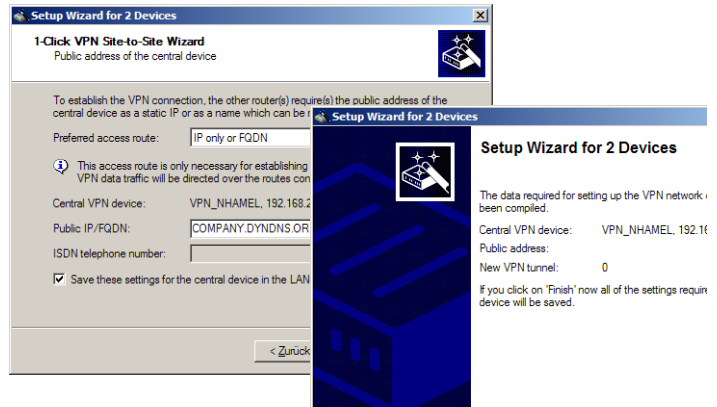
### 5.3 1-Click-VPN for networks (site-to-site)

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


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




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



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

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

## 5.4 Instructions for WEBconfig

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

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

- ① In the main menu, launch the Wizard 'Connect two local area networks'. Follow the Wizard's instructions and enter the necessary data.

■ *Chapter 5: Connecting two networks*

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

## 6 Providing dial-in access

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

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

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

### Security aspects

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

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

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



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

### 6.1 Which details are necessary?

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

### 6.1.1 General information

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



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

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

Notes on the different settings:

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



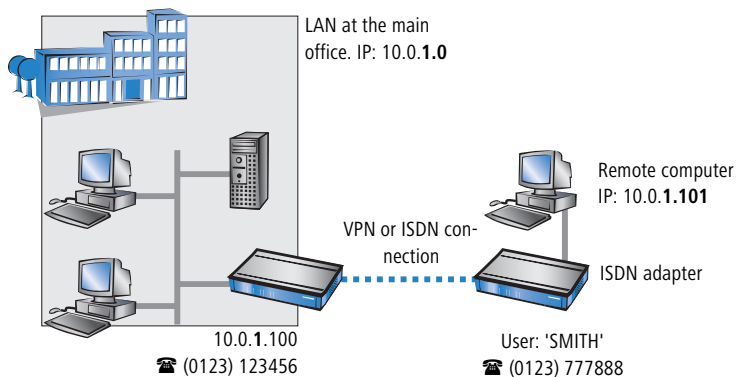
You will find information on the other parameters required for RAS access in the chapter 'Connecting two networks'.

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

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

### 6.1.2 Settings for TCP/IP

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



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

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

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

### 6.1.3 Settings for NetBIOS routing

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





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

## 6.2 Settings on the dial-in computer

### 6.2.1 Dialing-in via VPN

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

- Internet access
- A VPN client

### 6.2.2 Dialing-in via ISDN

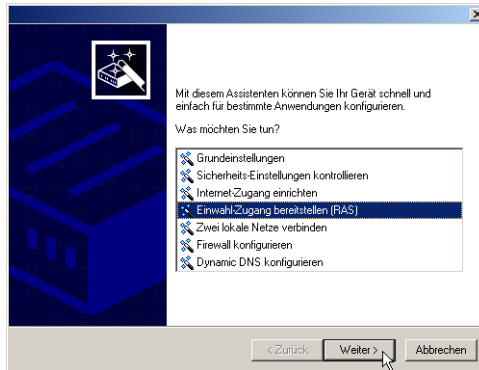
A number of settings are required by the dial-in computer. This example is based on a Windows computer.

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

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

## 6.3 Instructions for LANconfig

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



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

## 6.4 1-Click-VPN for LANCOM Advanced VPN Client

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

- 1 Use LANconfig to start the 'Set up a RAS Account' wizard and select the 'VPN connection'.
- 2 Activate the options 'LANCOM Advanced VPN Client' and 'Speed up configuration with 1-Click-VPN'.
- 3 Enter a name for this access and select the address under which the router is accessible from the Internet.
- 4 In the final step you can select how the access data is to be entered:

- Save profile as an import file for the LANCOM Advanced VPN Client
- Send profile via e-mail
- Print out profile



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

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

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

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

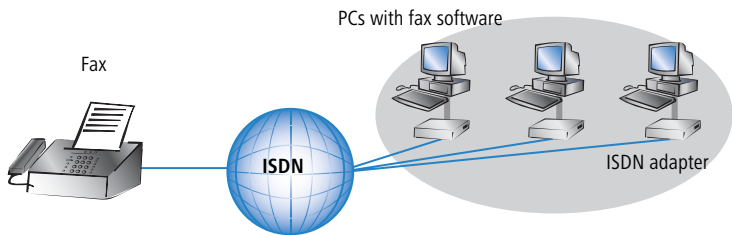
## 6.5 Instructions for WEBconfig

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

## 7 Fax transmission with LANCAPI

LANCAPI from LANCOM Systems is a specialized version of the widespread ISDN CAPI interface. CAPI stands for Common ISDN Application Programming Interface and it links ISDN adapters and communications software. This software in turn provides the computer with office-communications functions such as a fax or answering machine.

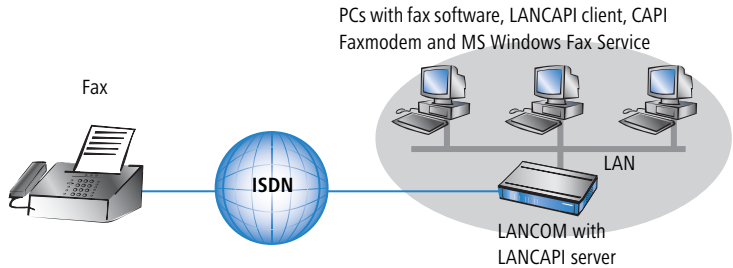
The chief benefit from using LANCAPI is economical. LANCAPI provides all of the Windows workstations in a LAN with unlimited access to ISDN office-communication functions such as fax, answering machine, online banking, and Eurofile transfer. Without any additional hardware, every workstation can make use of the full range of ISDN functions provided via the network. This completely dispenses with the need to equip workstations with expensive equipment such as ISDN adapters or modems. The sole requirement is to install the office-communication software on each workstation.



LANCAPI from LANCOM equips workstation PCs with a convenient fax transmission facility without having a fax machine connected to it. A number of components must be installed on the computer to support this:

- The **LANCAPI client**. This sets up the connection between your workstation PC and the LANCAPI server.
- The **LANCOM CAPI Faxmodem**. This tool simulates a fax machine on your computer.

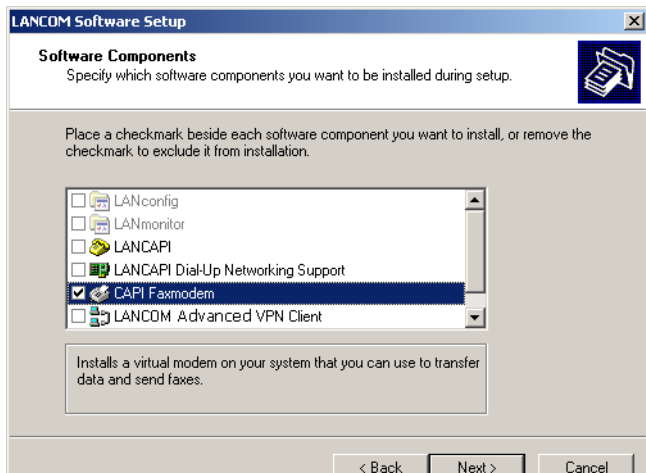
- The **MS Windows Fax Service**. This is the interface between the fax applications and the virtual fax.



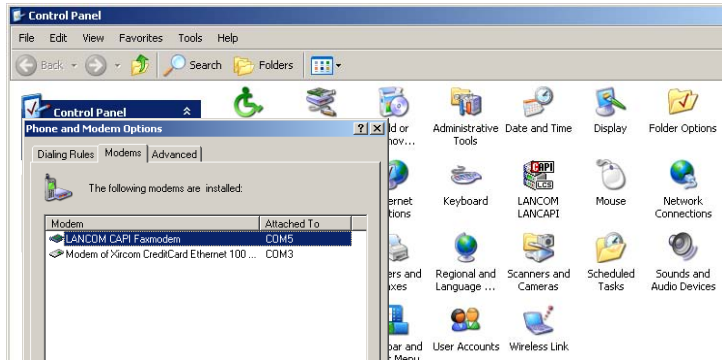
Installing the LANCAPI client is described in the Reference Manual. This chapter deals with installing and configuring the LANCOM CAPI Faxmodem and MS Windows Fax Service.

## 7.1 Installing the LANCOM CAPI Faxmodem

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

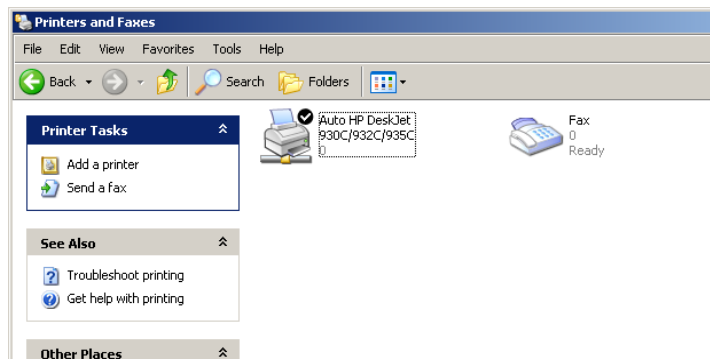


After successful installation, the LANCOM CAPI Fax Modem is entered into the Control Panel under **Phone and modem options**.



## 7.2 Installing the MS Windows Fax Service

- ① Go to the Control Panel and select the option **Printers and faxes**.
- ② In the Printers and faxes window select the option **Install a local fax printer**. Then follow the instructions provided by the installation tool. In the current window, an icon for the new fax printer appears.



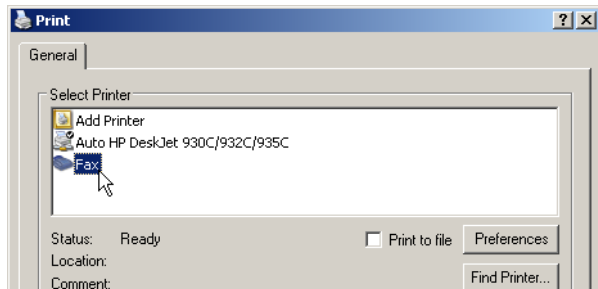
To check the installation, click with the right-hand mouse key on the fax icon and select **Properties**. The LANCOM CAPI Faxmodem should be entered on the 'Devices' tab.

## 7.3 Sending a fax

After installing the necessary components, there are a number of ways to send a fax from your computer. If you have a file ready to send, you can send this straight from its application. On the other hand, if you just want to send a short note, you can use the MS Windows Fax Service itself. Alternatively you can use any fax program.

### 7.3.1 Sending faxes from an office application

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

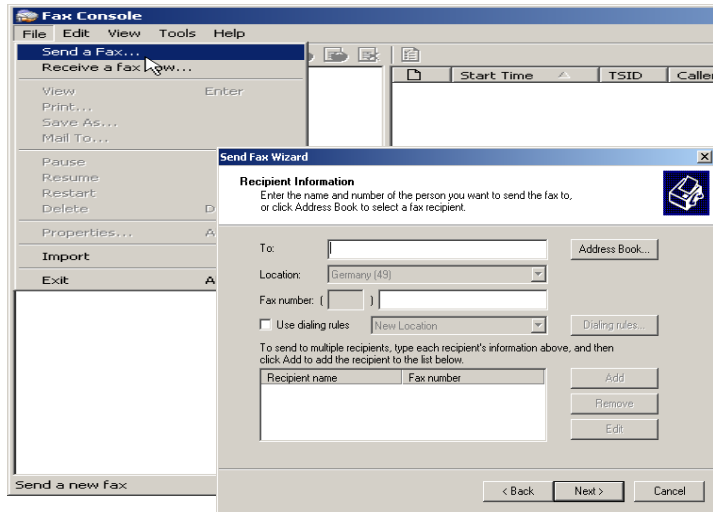


- ③ Click on "OK". A Wizard is displayed that guides you through the rest of the procedure.

### 7.3.2 Sending faxes with the Windows Fax Service

- ① Go to the Control Panel and open the **Printers and faxes** dialog.
- ② Double-click with the left-hand mouse key on the fax-device icon.

- ③ The fax client console opens up. Select the menu item **Send file/fax**. A Wizard guides you through the remaining procedure.





## 8 Security settings

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



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

### 8.1 Tips for the proper treatment of keys and passphrases

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

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

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

- **Choose a random key.**

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

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

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

### 8.2 Security settings Wizard

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

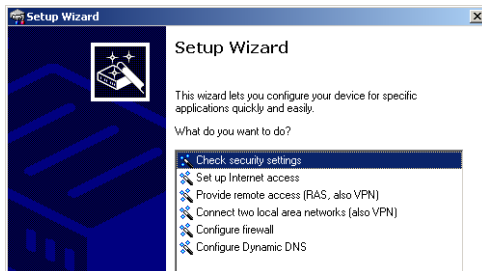
Your LANCOM offers password-protected access to its configuration. This is activated during the initial basic configuration simply by entering a password.

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

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

## 8.2.1 LANconfig Wizard

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



- 2 In the selection menu, select the Setup Wizard, **Check security settings** and confirm the selection with **Next**.
- 3 In the dialogs that follow you can set the password and select the protocols to be available for accessing the configuration from local and remote networks.
- 4 In a subsequent step, you can set parameters for locking the configuration such as the number of incorrect password entries and the duration of the lock.
- 5 For the firewall, you can activate stateful inspection, ping blocking, and the stealth mode.
- 6 The Wizard will inform you as soon as the entries are complete. Close the configuration with **Finish**.

## 8.2.2 WEBconfig Wizard

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

- Device password
- The protocols to be available for accessing the configuration from local and remote networks
- The parameters for locking the configuration (the number of incorrect password entries and the duration of the lock)

## 8.3 The security checklist

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



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

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

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

### ■ Have you permitted remote configuration?

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

### ■ Have your password-protected the SNMP configuration?

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

### ■ Have you activated the firewall?

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



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

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

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

**■ Have you activated IP masquerading?**

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

**■ Have you used filters to close critical ports?**

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

**■ Have you excluded certain stations from accessing the device?**

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

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

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

**■ Have you activated the protection of your WAN access in case the device is stolen?**

After being stolen, the device can theoretically be operated at another location by unauthorized persons. Password-protected device configurations do not stop third parties from operating RAS access, LAN connectivity or VPN connections that are set up in the device: A thief could gain access to a protected network.

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

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

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

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

## 9 Advice & assistance

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

### 9.1 No WAN connection can be established

After starting, the router attempts automatically to connect to the Internet provider. During this phase, the Internet-connection status LED blinks green. If successful, this LED switches to constant green. If contact cannot be made, the LAN LED does not illuminate. This is generally due to one of the following causes:

#### Problems with the cabling?

For the DSL connection, use only the connector cable supplied. This cable must be connected to the Ethernet connector of the DSL modem. The LED for the WAN connection must illuminate in green to show that it is physically connected.

#### Is the correct transmission protocol selected?

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

You can check and adjust your protocol settings under:

| Configuration tool | Call   |
|--------------------|--|
| LANconfig          | Communication ► General ► Communication layers         |
| WEBconfig          | Expert configuration ► Setup ► WAN module ► Layer list |

### 9.2 Slow DSL transmission

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

### Increasing the TCP/IP window size under Windows

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

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

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

## 9.3 Unwanted connections under Windows XP

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

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

# 10 Appendix

## 10.1 Performance and characteristics

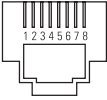
| LANCOM 9100 VPN             |               |  |
|-----------------------------|---------------|--|
| Connections                 | Ethernet LAN  | 10/100/1000Base-TX, autosensing, cable tester  |
|                             | ISDN          | ISDN S <sub>0</sub>  |
|                             | Configuration | Serial V.24/RS-232 outband interface with Mini-DIN8 connector  |
|                             | Power supply  | Internal power supply unit (100-240 V, 50-60 Hz)   |
| Housing                     |               | Robust metal housing, 19" 1 HU, (440 x 44.2 x 265 mm) with removable mounting brackets, network connectors on the front  |
| Conformity                  |               | CE-conformity to EN 300 328, EN 301 893, EN 55024, EN 55022, EN 55011, EN 50081, EN 60950, ES 59005, EN 60950  |
| Approvals                   |               | Notified in Germany, Belgium, Netherlands, Luxembourg, Austria, Switzerland, UK, and Italy. For information on new notifications, see <a href="http://www.lancom.eu">www.lancom.eu</a> .   |
| Environment/<br>Temperature |               | Temperature range 0–40°C; humidity 5–90%; non-condensing   |
| Options                     |               | <ul style="list-style-type: none"> <li>■ LANCOM Service Option (4-year warranty, advance replacement) (item no. 61401)</li> <li>■ LANCOM VPN Option 500 channels (item no. 61402)</li> <li>■ LANCOM VPN Option 1000 channels (item no. 61403)</li> </ul> |



## 10.2 Connector wiring

### 10.2.1 LAN/WAN interface 10/100/1000Base-TX, DSL interface

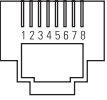
8-pin RJ45 sockets (ISO 8877, EN 60603-7)

| Connector   | Pin | Fast Ethernet | Gigabit Ethernet |
|---|-----|---------------|------------------|
|  | 1   | T+            | BI_DA+*          |
|   | 2   | T-            | BI_DA-           |
|   | 3   | R+            | BI_DB+           |
|   | 4   | PoE/G         | BI_DC+           |
|   | 5   | PoE/G         | BI_DC-           |
|   | 6   | R-            | BI_DB-           |
|   | 7   | PoE/ -48 V    | BI_DD+           |
|   | 8   | PoE/ -48 V    | BI_DD-           |

\*BI\_DA+ stands for "bi-directional pair +A"


### 10.2.2 ISDN-S<sub>0</sub> interface

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

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

### 10.2.3 Configuration interface (outband)

8-pin Mini DIN socket

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

EN

### 10.3 Declaration of conformity



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

The CE declarations of conformity for your device are available in the appropriate product area on the LANCOM Systems web site ([www.lancom.eu](http://www.lancom.eu)).

# Index

## Numerics

|                  |        |
|------------------|--------|
| 10/100Base-TX    | 18     |
| 100-Mbit network | 18     |
| 3 DES            | 36, 45 |

## A

|                    |        |
|--------------------|--------|
| AES                | 36, 45 |
| Anschlussbelegung  |        |
| ADSL-Schnittstelle | 65     |
| Autosensing        | 18, 20 |

## B

|          |        |
|----------|--------|
| Blowfish | 36, 45 |
|----------|--------|

## C

|  |            |
|--|------------|
| Call-back function                                   | 12, 36, 45 |
| Calling Line Identity (CLI)                          | 47         |
| CAPI interface                                       | 51         |
| Charge limiter                                       | 15         |
| Charge protection                                    | 25, 27     |
| Common ISDN Application Programming Interface (CAPI) | 51         |
| Configuration access                                 | 27         |
| Configuration cable                                  | 18         |
| Configuration file                                   | 60         |
| Configuration interface                              | 12         |
| Connector cable                                      | 13         |
| Configuration password                               | 58         |
| Configuration protection                             | 12, 25     |
| Connector wiring                                     | 64         |
| Configuration port                                   | 65         |
| ISDN S <sub>0</sub> interface                        | 64         |
| LAN interface  | 64         |
| Outband  | 65         |
| CPU load   | 17         |

## D

|                 |    |
|-----------------|----|
| Date            | 17 |
| Default gateway | 59 |
| Device name     | 17 |

|                              |            |
|------------------------------|------------|
| DHCP                         | 31         |
| DHCP server                  | 10, 24, 31 |
| Dial-in access               | 45         |
| Dial-up adapter              | 48         |
| DNS                          |            |
| DNS access to the remote LAN | 40         |
| DNS server                   | 10, 31     |
| Documentation                | 13         |
| Domain                       | 40         |
| DSL transmission too slow    | 61         |

## E

|            |        |
|------------|--------|
| Encryption | 36, 45 |
|------------|--------|

## F

|                  |            |
|------------------|------------|
| Firewall         | 10, 11, 59 |
| Block stations   | 59         |
| FirmSafe         | 12         |
| Firmware version | 17         |
| Flatrate         | 33         |

## H

|                       |    |
|-----------------------|----|
| Hardware installation | 20 |
| HTTPS                 | 27 |

## I

|                         |        |
|-------------------------|--------|
| ICMP                    | 59     |
| Installation            | 13     |
| Configuration interface | 21     |
| ISDN                    | 21     |
| LAN                     | 20     |
| LANtools                | 21     |
| WAN                     | 21     |
| Internet access         | 10, 32 |
| Authentication data     | 32     |
| Flatrate                | 33     |
| Internet access setup   | 32     |
| Internet provider       | 32     |
| IP                      |        |
| Block ports             | 59     |

- Filter 59
- IP address 21, 24, 25, 59
- IP masquerading 11, 59
- IP router 10
- IPsec 36, 45
- IPX 48
- ISDN
  - Connector cable 13
  - D channel 47
  - S<sub>0</sub> connector 18
- ISDN calling line ID 39, 46
- ISDN leased-line option 11
- ISDN modem 45
- ISDN number 38
- ISDN S<sub>0</sub> connection 11
- L**
- LAN
  - Connector cable 13
- LAN connection 18
- LANCAPI 11
- LANconfig 22, 26
- LAN-LAN connectivity 36
  - Required information 37
- LAN-LAN coupling 10
- LANmonitor 22
- LANtools
  - System requirements 14
- LCD display 17
- M**
- MAC address filter 11
- Memory load 17
- MSN 47
- N**
- NAT – see IP masquerading
- NetBIOS 40
- NetBIOS proxy 10
- Netmask 24
- Network connectivity 36
  - Security aspects 36, 45
  - Network mask 25, 59
  - Network segment 21
  - Number of VPN tunnels 17
- P**
- Package content 13
- Password 25, 26, 36, 45
- Password for the ISDN connection 39
- PAT – see IP masquerading
- PPP 45
- PPP client 48
- R**
- RAS 9
- Remote Access Service (RAS)
  - Activate compression in software 48
  - Configuring the dial-in computer 48
  - NetBIOS 47
  - Server 10
  - Setup 45
  - TCP/IP 47
  - User name 46
  - Windows workgroup search 47
- Remote configuration 27
- Remote configuration via ISDN 12
- Reset the toll protection 15
- Routing table 59
- S**
- SDSL modem 11
- Security checklist 58
- Security settings 61
- Serial configuration cable 18
- SNMP
  - Configuration protection 58
- Software installation 21
- Standard gateway 31
- Stateful inspection firewall 10
- Status display
  - Power 15

■ *Index*

|                       |        |                                |    |
|-----------------------|--------|--------------------------------|----|
| System requirements   | 13     | <b>U</b>                       |    |
| <b>T</b>              |        | UDP                            | 59 |
| TCP                   | 59     | USB connector                  | 18 |
| TCP/IP                | 13, 48 | <b>V</b>                       |    |
| Settings              | 23     | Virtual Private Network        | 9  |
| TCP/IP configuration  |        | Virtual Private Networks (VPN) | 10 |
| Fully automatic       | 23, 24 | VPN                            | 9  |
| Manual                | 23, 24 | VPN client                     | 48 |
| TCP/IP filter         | 11, 59 | <b>W</b>                       |    |
| TCP/IP router         |        | WAN                            |    |
| Settings              | 39     | Connector cable                | 13 |
| TCP/IP windows size   | 62     | WEBconfig                      | 27 |
| Telnet                | 59     | HTTPS                          | 27 |
| Temperature           | 17     | System requirements            | 14 |
| TFTP                  | 59     | Windows workgroup search       | 41 |
| Time                  | 17     |                                |    |
| Transmission protocol | 61     |                                |    |

