...connecting your business

LANCOM 821+
LANCOM 1711+ VPN
LANCOM 1721 VPN

- Handbuch
- Manual

LANCOM
Systems

LANCOM 821+
LANCOM 1711+ VPN
LANCOM 1721 VPN

LANCOM
Systems

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.

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

Trademarks

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

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

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

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

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

This product includes the LZMA SDK written by Igor Pavlov.

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

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Wuerselen
Germany
www.lancom.de
Wuerselen, January 2009

110642/0109

Preface

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

With the LANCOM Router you have chosen a powerful router that possesses integrated DSL respectively ADSL and ISDN interfaces by default as well as an integrated 4-port switch. With this router you can simply and comfortably connect individual PCs or whole local networks to the high-speed Internet.

Model variants

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

- LANCOM 821+
- LANCOM 1721 VPN
- LANCOM 1711+ VPN

Model restriction

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

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

Security settings

To maximize the security available from your product, we recommend that you undertake all of the security settings (e.g. firewall, encryption, access protection) 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.de for the latest information about your product and technical developments, and also to download our latest software versions.

User manual and reference manual

The documentation of your device consists of the following parts:

- Installation guide
- User manual
- Reference manual

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

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

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

This documentation was created by …

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

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

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

contact addresses of LANCOM support, please see the enclosed leaflet or the LANCOM Systems website.

Information symbols	
⚡	Very important instructions. Failure to observe this may result in damage.
❗	Important instruction that should be observed.
ℹ	Additional information that may be helpful but which is not required.

Contents

1 Introduction

The models LANCOM 821+, LANCOM 1721 VPN and LANCOM 1711+ VPN are fully-featured routers that therefore also can be used in combination with the integrated firewall for providing secure Internet access to a complete local network (LAN).

The VPN option, which is either integrated already or can be activated subsquently, enables the LANCOM 1721 VPN and LANCOM 1711+ VPN to act as powerful Dynamic VPN gateways for external offices or mobile users.

The LANCOM Router models offer each a DSL or ADSL connector and also an ISDN connector. The ISDN line can be used as back-up for the DSL connection, for remote management of the router, as basis for the office communication via LANCAPI or for establishing VPN connections to remote sites with dynamic IP addresses.

By using the Voice over IP function, these devices can transfer voice data over broadband Internet connections as well.

1.1 How do ADSL and ADSL 2+ work?

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

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

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

Parallel to data transfer, ADSL also provides full and unlimited support for the classic applications in telephony (telephone, fax, answering machine, PBX).

This is facilitated by splitters which separate the voice frequencies from the data frequencies.

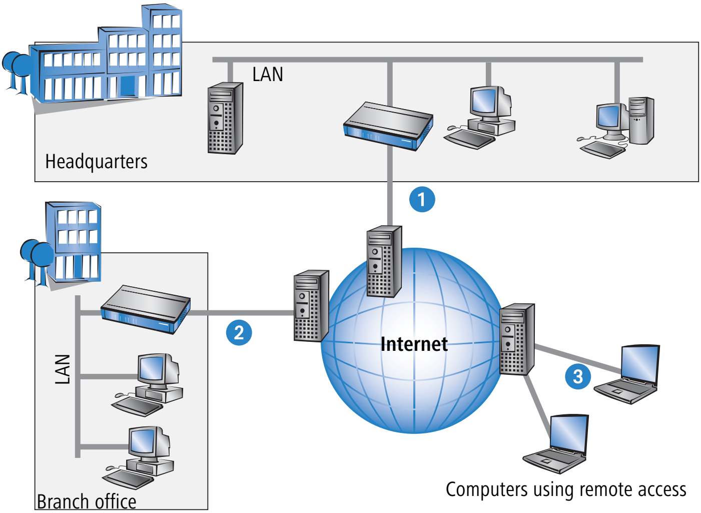
1.2 What does VPN offer?

For LANCOM 1711+ VPN and LANCOM 1721 VPN only

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

The models LANCOM 1721 VPN and LANCOM 1711+ VPN are factory equipped to support VPN with 5 active tunnels. With the additional LANCOM VPN Option, VPN support can be extended to 25 active tunnels (incl. activated hardware accelerator).

The following structure results when using the Internet instead of direct connections:



All participants have fixed or dial-up connections to the Internet. Expensive dedicated lines are no longer needed.

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

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

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

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

The physical connection no longer exists directly between two participants; instead, the participants rely on their connection to the Internet. The access technology used is not relevant in this case: Broadband technology such as DSL (Digital Subscriber Line) is ideal. A conventional ISDN line can be used, too.

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

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

1.3 What can your LANCOM Router do?

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

	LANCOM 821+	LANCOM 1711+ VPN	LANCOM 1721 VPN
Applications			
Internet access	✓	✓	✓
LAN to LAN coupling via VPN		✓	✓
LAN to LAN coupling via ISDN	✓	✓	✓
RAS server (via VPN)		✓	✓
RAS server (via ISDN)	✓	✓	✓
IP router	✓	✓	✓
IPX router (via ISDN), e.g. for coupling of Novell networks or dialling into Novell networks	✓		✓
NetBIOS proxy for coupling of Microsoft peer-to-peer networks via ISDN	✓	✓	✓
DHCP and DNS server (for LAN and WAN)	✓	✓	✓
N:N mapping for coupling networks using the same IP address ranges	✓	✓	✓

	LANCOM 821+	LANCOM 1711+ VPN	LANCOM 1721 VPN
Bridge function for coupling networks via ISDN connection	✓	✓	✓
Port-Mapping to set up LAN ports as additional WAN ports		✓	✓
Policy-based routing for policy-based selection of target routes	✓	✓	✓
Load-balancing for bundling of multiple DSL channels	2 channels	4 channels	4 channels
Backup solutions and load balancing with VRRP	✓	✓	✓
NAT Traversal (NAT-T)	✓	✓	✓
DMZ with configurable IDS checks	✓	✓	✓
PPPoE-Server	✓	✓	✓
WAN-RIP	✓	✓	✓
Spanning Tree Protocol	✓	✓	✓
Layer-2-QoS-Tagging	✓	✓	✓
ISDN leased lines	✓	✓	✓
LANCAPI server for the operating with office applications as fax or answering machine via ISDN interface	✓	✓	✓
WAN connection			
Connection for DSL or cable modem	✓	✓	✓
Integrated ADSL modem (ADSL2+ ready)	✓		✓
ISDN S_0 bus in multi device-mode or in point-to-point mode with automatic D-channel protocol identification. Supports static and dynamic channel bundling per MLPPP and BACP as well as Stac data compression (Hi/fn)	✓	✓	✓
Port for external modem, analogue or GSM (requires LANCOM modem adapter kit; from LCOS 5.0)	✓	✓	✓
LAN connection			
4 individual Fast Ethernet LAN ports, switchable separately, e.g. as LAN switch or separate DMZ ports, auto crossover.	✓	✓	✓
USB connector			
USB 2.0 host port (full speed: 12 Mbps) for connecting a USB printer and for future extensions		✓	✓
Security functions			
IPSec encryption in external software (VPN client)		✓	✓
5 integrated VPN tunnels for protection of network connections		✓	✓
IPSec encryption in hardware (optional; activated with the VPN-25 option)		✓	✓

	LANCOM 821+	LANCOM 1711+ VPN	LANCOM 1721 VPN
IP masquerading (NAT, PAT) to conceal individual LAN workstations behind a single public IP address.	✔	✔	✔
Stateful Inspection Firewall	✔	✔	✔
Firewall filter for blocking individual IP addresses, protocols and ports	✔	✔	✔
MAC address filter regulates, for example, LAN-workstation access to the IP routing function	✔	✔	✔
Protection of the configuration from brute-force attacks.	✔	✔	✔
Configuration			
Configuration with LANconfig or with web browser, additionally terminal mode for Telnet or other terminal programs, SNMP interface and TFTP server function.	✔	✔	✔
Remote configuration via ISDN (with ISDN-PPP connections e.g. via Windows network and dial-up connections)	✔	✔	✔
Serial configuration interface	✔	✔	✔
Callback function with PPP authentication mechanisms for restriction to fixed ISDN telephone numbers	✔	✔	✔
FirmSafe with firmware versions for absolutely secure software upgrades	✔	✔	✔
Optional software extensions			
LANCOM VPN Option with 25 active tunnels for protection of network couplings		✔	✔
Optional hardware extensions			
LANCOM Modem Adapter Kit for connection of analog or GSM modems to the serial interface	✔	✔	✔

2 Installation

This chapter will assist you to quickly install hardware and software. First, check the package contents and system requirements. The device can be installed and configured quickly and easily if all prerequisites are fulfilled.

2.1 Package contents

Please check the package contents for completeness before starting the installation. In addition to the device itself, the package should contain the following accessories:

	LANCOM 821+	LANCOM 1721 VPN	LANCOM 1711+ VPN
Power adapter	✓	✓	✓
LAN connector cable (green plugs)	✓	✓	✓
WAN connector cable (dark blue plugs)		✓	
ADSL connector cable (transparent plugs)	✓		✓
ISDN connector cable (light blue plugs)	✓	✓	✓
Connector cable for the configuration interface	✓	✓	✓
LANCOM CD	✓	✓	✓
Printed documentation	✓	✓	✓

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

2.2 System requirements

Computers that connect to a LANCOM 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, interfaces and hardware installation

2.3.1 Status displays

Meanings of the LEDs

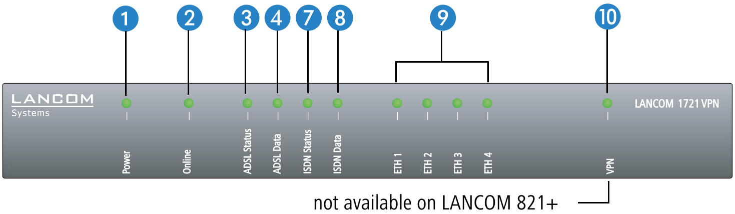
In the following sections we will use different terms to describe the behaviour of the LEDs:

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

Front side

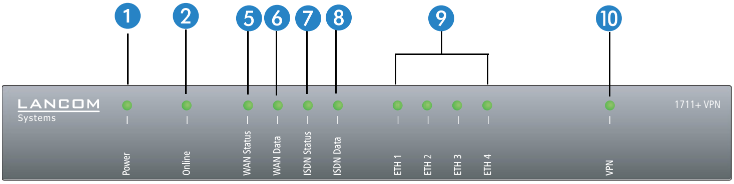
The various LANCOM Router models have different numbers of indicators on the front panel depending on their functionality.

LANCOM 821+and LANCOM 1721 VPN



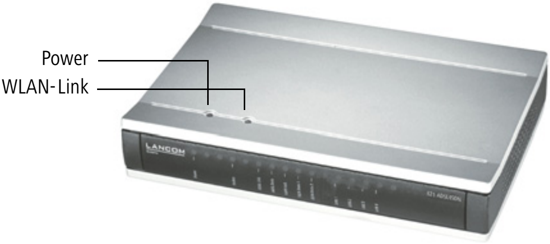
not available on LANCOM 821+

LANCOM 1711+ VPN



Top

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



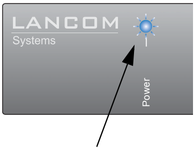
1 Power

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

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

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

Flashing Power LED but no connection?



Signal for reached time or connect-charge limit

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

- Reset connect charge protection.
- Increase the limit that has been reached.
- Completely deactivate the lock that has been triggered (set limit to '0').

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

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

2 Online

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

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

3 ADSL status (LANCOM 821+ and LANCOM 1721 VPN only)

Information on connection status at the ADSL connector:

Off		Interface deactivated
Green	Blinking/flashing	Handshake/training
Green	Permanently	Synchronization successful

Red	Flickering	Error (CRC error, framing error, etc.)
Red	On (permanently)	No synchronization, searching for remote station
Red/ orange	Blinking	Hardware error

4 ADSL data (LANCOM 821+ and LANCOM 1721 VPN only)

Information on data traffic at the ADSL connector:

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

5 WAN Status (only LANCOM 1711+ VPN)

Connection status of the WAN connection:

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

6 WAN Data (only LANCOM 1711+ VPN)

Data traffic via the WAN connection:

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

7 ISDN status

Information on connection status at the ISDN S_0 connector:

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

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

8 ISDN Data

Status display for both ISDN B channels:

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

9 ETH

LAN connector status in the integrated switch:

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

10 VPN

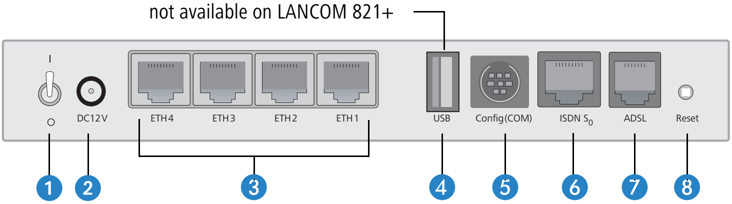
Status of a VPN connection.

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

2.3.2 Device connectors

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

LANCOM 821+ and LANCOM 1721 VPN



1 Voltage switch

2 Connection for the included power adapter

3 Switch with four 10/100Base-Tx connections

4 USB connection

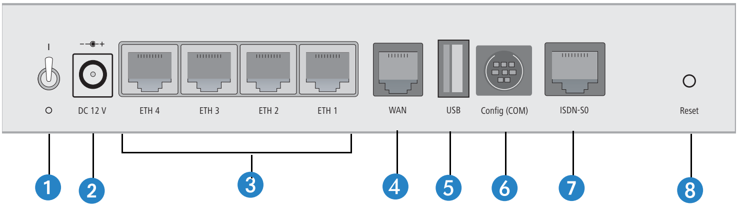
5 Serial configuration port

6 ISDN/S_0 port

7 ADSL port

8 Reset switch

LANCOM 1711+ VPN



1 Voltage switch

2 Connection for the included power adapter

3 Switch with four 10/100Base-Tx connections

4 WAN port

5 USB connection

6 ISDN/S_0 port

7 Serial configuration port

8 Reset switch

The reset switch has two different functions depending on the length of time that it is pressed:

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

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.

Some devices simply cannot be installed under lock and key. There is consequently a risk that the configuration will be deleted by mistake of 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.

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.

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

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

2.4 Hardware installation

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

① **LAN** – connect the LANCOM Router to your LAN or to an individual PC. For that purpose, plug the included network cable (green plugs) into the LAN connector of the device ❸ and the other end into a free network connecting socket of your local network, into a free socket of a hub/switch or into the network socket of an individual PC.

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

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

821+/1721 only

② **ADSL** – connect the ADSL interface ❼ to the splitter using the supplied ADSL connector cable (transparent plugs).

1711+ only

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

④ **ISDN** – to connect the LANCOM Router to the ISDN, plug one end of the supplied ISDN connector cable (light blue plugs) in the ISDN/S_0 port ❻ (LANCOM 821+ and LANCOM 1721 VPN) or ❺ (LANCOM 1711+ VPN) of the router and the other end into an ISDN/S_0 multi-device mode or point-to-point mode connection.

⑤ **Configuration port** – you may optionally connect the router directly to the serial port (RS-232, V.24) of a PC. Use the cable supplied for this purpose. Connect the configuration port of the LANCOM ❺ (LANCOM 821+ and LANCOM 1721 VPN) or ❻ (LANCOM 1711+ VPN) with a free serial port of the PC.

⑥ Alternatively you may connect an external modem (analogue or GSM) to the serial port using the LANCOM modem adapter kit, if you would like to make use of an additional WAN line for remote maintenance, backup connections or dynamic VPN.

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

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

⑧ **Operational?** – After a short device self-test the Power LED will be permanently lit. Green LAN LEDs indicate the LAN sockets that have functioning connections.

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

2.5 Software installation

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

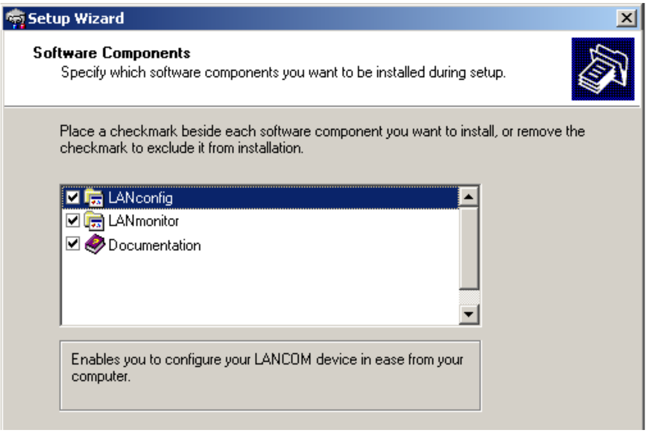
ⓘ You may skip this section if you use your LANCOM VPN Router exclusively with computers running operating systems other than Windows.

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:



Software Components

Specify which software components you want to be installed during setup.

Place a checkmark beside each software component you want to install, or remove the checkmark to exclude it from installation.

☑ LANconfig
☑ LANmonitor
☑ Documentation

Enables you to configure your LANCOM device in ease from your computer.

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.
- With **Documentation** you copy the documentation files onto your PC.

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

3 Basic configuration

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

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

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

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

3.1 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 Wwizard 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 Wwizard 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 Settings for the DSL connection

It may be necessary to enter the transmission protocol used for the DSL connection. The wizard will enter the correct setting for the most important DSL providers on its own. Only when the wizard does not list your provider must the transmission protocol used by your DSL provider be entered.

The wizard will offer you a universal 'multimode' protocol that works with all common types of DSL connection.

3.1.4 Settings for the ISDN Connection

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

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

3.1.5 Charge protection

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

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

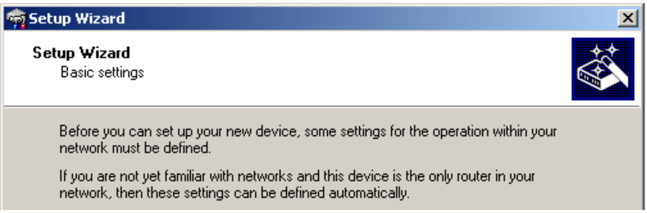
The budget can be completely deactivated by entering a value of '0'.

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

3.2 Instructions for LANconfig

① Start up LANconfig by clicking **Start** ▶ **Programs** ▶ **LANCOM** ▶ **LANconfig**. LANconfig automatically detects the new LANCOM devices in the TCP/IP network.

② If an unconfigured device is being found during searching, the setup wizard starts that will help you make the basic settings of the device or will even do all the work for you (provided a suitable network environment exists).



Setup Wizard
Basic settings

Before you can set up your new device, some settings for the operation within your network must be defined.

If you are not yet familiar with networks and this device is the only router in your network, then these settings can be defined automatically.

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

If you have chosen automatic TCP/IP configuration, please continue with Step ⑤.

③ If you would like to configure the TCP/IP settings manually, assign an available address from a suitable address range to the LANCOM. Confirm your choice with **Next**.

④ Specify whether or not the router should act as a DHCP server. Make your selection and confirm with **Next**.

⑤ In the following window, specify the password for configuration access. Note that the password is case-sensitive and ensure that it is sufficiently long (at least 6 characters).

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

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

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

⑦ Connect charge protection can limit the cost of DSL connections to a predetermined amount if desired. Confirm your choice with **Next**.

⑧ Complete the configuration with **Finish**.

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

3.3 Instructions for WEBconfig

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.

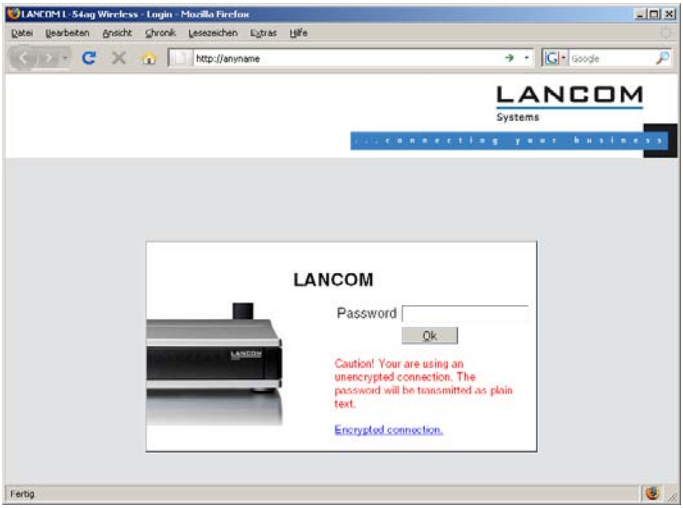
To carry out a configuration with WEBconfig, you need to know how to contact the device. Device behavior and accessibility for configuration via a Web browser depend on whether the DHCP server and DNS server are active in the LAN already, and whether these two server processes share the assignment in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

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 set up an unconfigured LANCOM by entering any name into a Web browser.



http://anyname

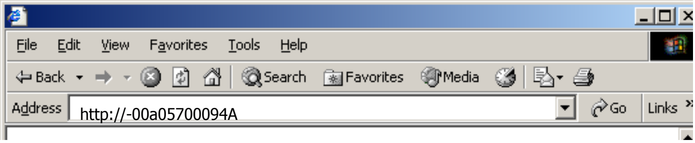
Caution! Your are using an unencrypted connection. The password will be transmitted as plain text.

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, 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 "-<MAC address>", e.g. “-00a057xxxxxx”.



http://-00a05700094A

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

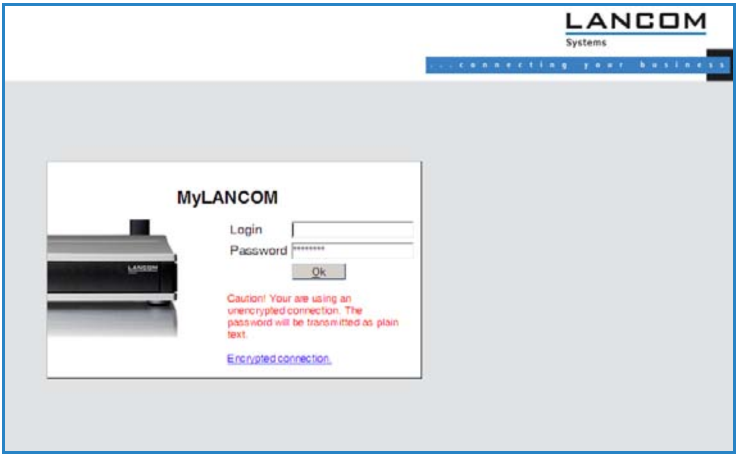
- If there is no DNS server in the LAN, or if it is not coupled to the DHCP server, the device cannot be reached via the name. In this case the following options remain:
  - □ Use LANconfig's "Find Device" function, or perform WEBconfig's "Device Search" from another yet accessible LANCOM.
  - □ Use 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.



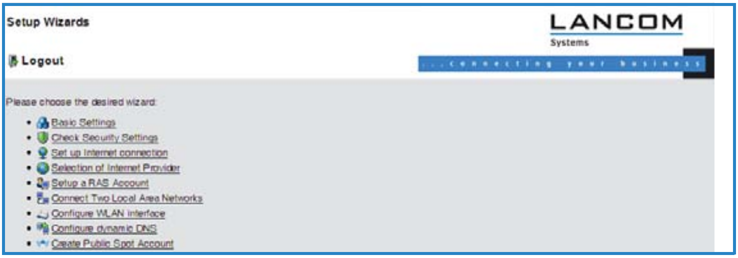
Login

Password ********

Caution! Your are using an unencrypted connection. The password will be transmitted as plain text.

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.



Setup Wizards

Logout

Please choose the desired wizard:

- Basic Settings
- Check Security Settings
- Set up Internet connection
- Selection of Internet Provider
- Setup a RAS Account
- Connect Two Local Area Networks
- Configure WLAN interface
- Configure dynamic DNS
- Create Public Spot Account

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

3.4 TCP/IP settings to workstation PCs

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

- Default gateway – receives all packets that are not addressed to computers within the local network.
- DNS server – translates network names (www.**lancom.de**) or names of computers (**www**.lancom.de) to actual IP addresses.

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

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

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

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

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

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

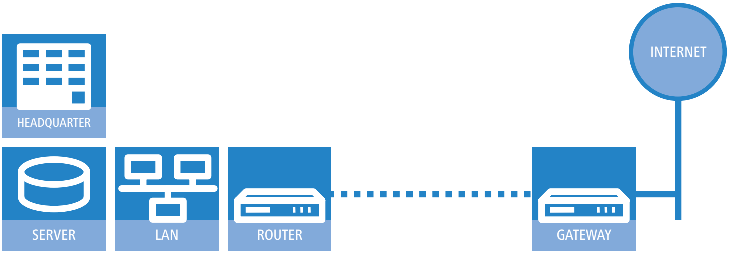
- **Manual IP address assignment**

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

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

4 Setting up Internet access

The LANCOM provides a central point of Internet access for all of the computers in the LAN.



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 ADLS 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 stations 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 station.

    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

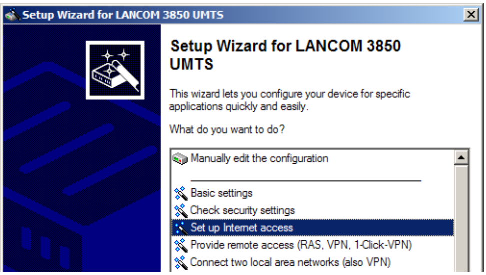
The most common utilization of the backup solution is to provide an auxiliary Internet connection. When setting up an Internet connection, an the additional option is to create a second connection to the Internet via an alternative WAN interface. If the primary Internet access is set up to operate via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



Setup Wizard for LANCOM 3850 UMTS

Setup Wizard for LANCOM 3850 UMTS

This wizard lets you configure your device for specific applications quickly and easily.

What do you want to do?

Manually edit the configuration
Basic settings
Check security settings
Set up Internet access
Provide remote access (RAS, VPN, 1-Click-VPN)
Connect two local area networks (also VPN)

② In the selection menu, select the Setup Wizard, **Set up Internet connection** and confirm the selection with **Next**.

③ In the following windows you select your country, your Internet provider if possible, and you enter your access data.

④ Depending on availability the Wizard provides further options for your Internet connection.

⑤ After entering all of the necessary data the Wizard then offers you the option of setting up a backup connection. Select the corresponding WAN interface to be used for the backup connection and enter the relevant access data for the Internet connection.

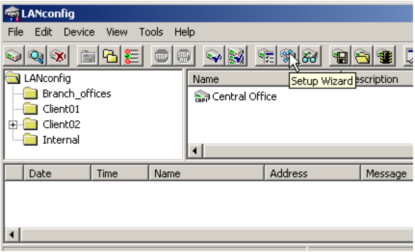
The Wizard then sets up the alternative Internet access and at the same time creates the necessary entries into the backup table and also in the PPP table for checking the Internet connection.

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

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

LANconfig: Fast activation of the Setup Wizards

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



4.1.2 Instructions for WEBconfig

① Select the entry **Set up Internet connection** from the main menu.

② In the following windows you select your country, your Internet provider if possible, and you enter your access data.

③ Depending on availability the Wizard provides further options for your Internet connection.

④ The wizard will inform you as soon as the entries are complete. Close the configuration with **Finish**.

4.2 The Firewall Wizard

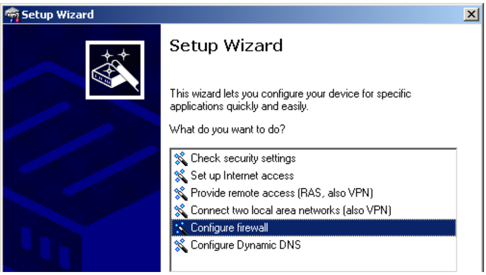
Your LANCOM features a stateful inspection firewall and firewall filter that provides effective protection from the Internet for your LAN. The core concept of the stateful inspection firewall is that the only data transfers that are considered to be valid are those implemented by the protected device itself. All access attepts that were not requested from within the local network are invalid.

The Firewall Wizard assists you to generate new rules for the firewall quickly and conveniently.

More information on your LANCOM's firewall and its configuration are available in the reference manual.

4.2.1 LANconfig Wizard

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



Setup Wizard

This wizard lets you configure your device for specific applications quickly and easily.

What do you want to do?

② In the selection menu, select the Setup Wizard, **Configure firewall** and confirm the selection with **Continue**.

③ In the windows that follow you select the services/protocols that the rule is to relate to. In the next step you define the source and destination stations that the rule applies to, and the actions that are to be carried out by the rule on a data packet.

④ Finally the new rule is given a name, it is activated, and you define whether further rules are to be considered when the rule acts on a data packet.

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

4.2.2 Configuration under WEBconfig

WEBconfig provides the option of checking and altering the parameters for Internet access under **Configuration ▶ Firewall / QoS ▶ Rules ▶ Rule table**.

5 Linking two networks

With the network interconnection (also known as LAN to LAN coupling) of the LANCOM Router, two local networks are linked.

The LAN to LAN coupling can be realized in principle in two different ways:

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

Always configure both sides

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

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

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

Security aspects

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

- **VPN**: Network couplings via VPN transmit data by IPSec. The data are encrypted by AES, 3-DES, Blowfish or CAST encryption algorithms.
- **ISDN**: For network couplings via ISDN, the connection password, the checking of the ISDN number and the callback function ensure the security of the connection.

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

5.1 What information is necessary?

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

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

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

5.1.1 General information

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

Further details to network couplings via VPN using enhanced methods (e.g. digital certificates) can be found in the LCOS reference manual.

Coupling	Entry	Gateway 1		Gateway 2
VPN	ISDN connection available?	yes/no		yes/no
VPN	Type of the local IP address	static/dynamic	⤨	static/dynamic
VPN	Type of the remote IP address	static/dynamic		static/dynamic
VPN + ISDN	Name of the local device	'HEAD'	⤨	'BRANCH'
VPN + ISDN	Name of the remote station	'BRANCH'		'HEAD'
VPN + ISDN	Remote ISDN calling number	(0123) 123456	⤨	(0789) 654321
VPN + ISDN	Remote ISDN caller ID	(0789) 654321		(0123) 123456
VPN + ISDN	Password for secure transmission of the IP address	'Password'	↔	'Password'
VPN	Shared secret for encryption	'Secret'	↔	'Secret'
VPN	IP address of remote station	'10.0.2.100'		'10.0.1.100'

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

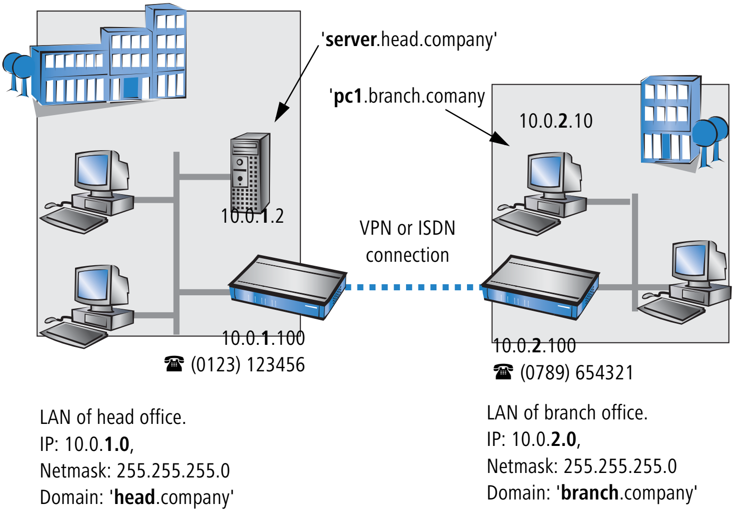
- In case your device has an **ISDN connection**, the wizard asks whether the remote site has ISDN as well.
- The type of IP address must be stated for both sides for VPN connections via the Internet. There are two types of IP addresses: static and dynamic. An explanation of the two **IP address types** can be found in the reference manual.

  Thanks to Dynamic VPN, connections can be enabled not only between gateways with fixed, static IP addresses, but even between gateways with dynamic IP addresses. The active initiation of VPN connections towards remote sites with dynamic IP addresses requires ISDN.
- If you haven't already named your LANCOM Router, the wizard will ask you for a new, **unique device name.** With this entry, you will rename your LANCOM Router. Be sure to give the two devices different names.
- The **name of the remote station** is needed for its identification.
- Enter the subscriber number of the remote station in the **ISDN subscriber number** field. The complete subscriber number including all necessary area and country codes is required.
- The stated **ISDN caller ID** is used to identify and authenticate callers. When a LANCOM Router receives a call, it compares the ISDN caller ID entered for the remote station with the actual caller ID transferred via the D channel. An ISDN caller ID generally consists of an area code and an MSN.

- The **password for the ISDN connection** is an alternative to the use of the ISDN caller ID. It is always used to authenticate callers that do not send an ISDN caller ID. The exact same password must be entered on both sides. It is used for calls in both directions.
- The **Shared Secret** is the central password for security within the VPN. The exact same password has to be entered on both sides
- Data compression increases the transfer speed of the connection at no additional cost. This is completely unlike the bundling of two ISDN- channels with MLPPP (**Multi Link PPP**): The transfer rate will be doubled but there will also be additional telephone costs for two connections.

5.1.2 Settings for the TCP/IP router

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



Unlike when accessing the Internet, all of the IP addresses in the involved networks are visible on the remote side when coupling networks, not just those of the router. The computer with the IP address 10.0.2.10 in the branch office LAN sees the server 10.0.1.2 in the headquarters and can access it (assuming it has the appropriate rights), and vice versa.

DNS access to the remote LAN

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

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

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

Extranet VPN

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

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

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

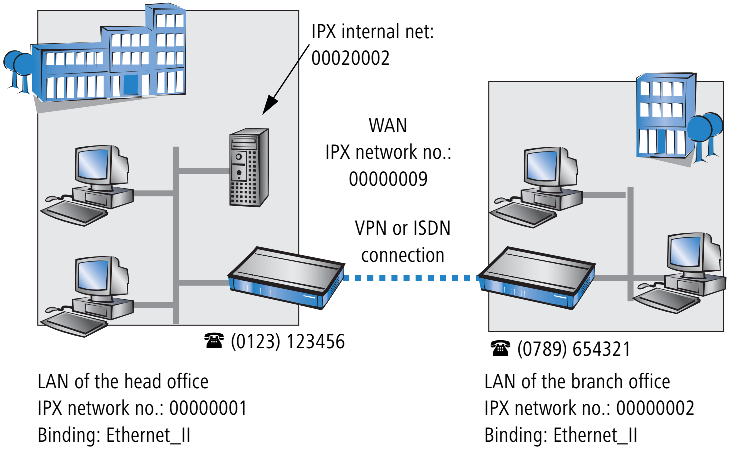
5.1.3 Settings for the IPX router

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

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

- for the LAN of the head office
- for the LAN of the branch office
- for the higher-level WAN

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



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

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

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

5.1.4 Settings for NetBIOS routing

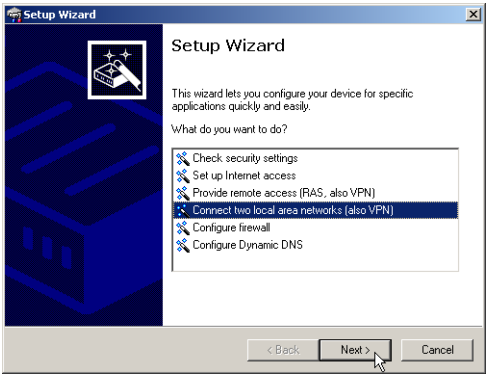
NetBIOS routing can be set up quickly: All that is required in addition to the information for the TCP/IP protocol used is the name of a Windows workgroup from in the router's own LAN.

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

5.2 Instructions for LANconfig

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

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



Setup Wizard

This wizard lets you configure your device for specific applications quickly and easily.

What do you want to do?

- Check security settings
- Set up Internet access
- Provide remote access (RAS, also VPN)
- Connect two local area networks (also VPN)
- Configure firewall
- Configure Dynamic DNS

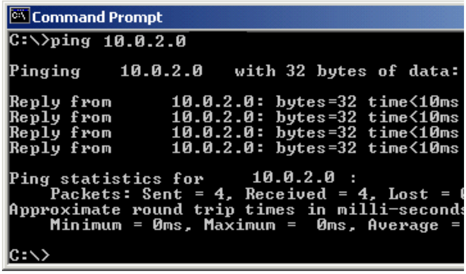
② The wizard will return a message to indicate that it has all the information it needs. Close the wizard with **Finish**.

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

Ping – quick testing for TCP/IP connections

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

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



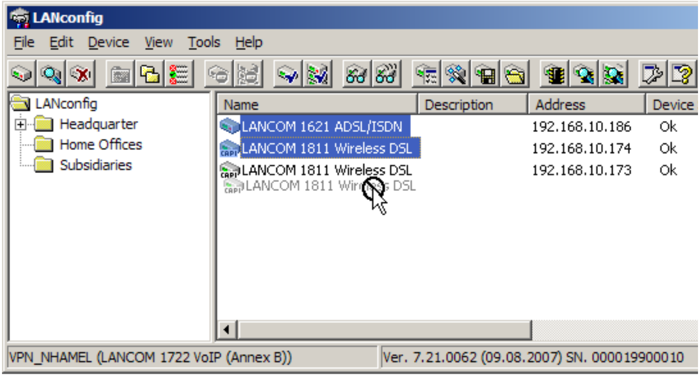
```
C:\>ping 10.0.2.0

Pinging    10.0.2.0   with 32 bytes of data:

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

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

C:\>
```

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

The site-to-site coupling 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.

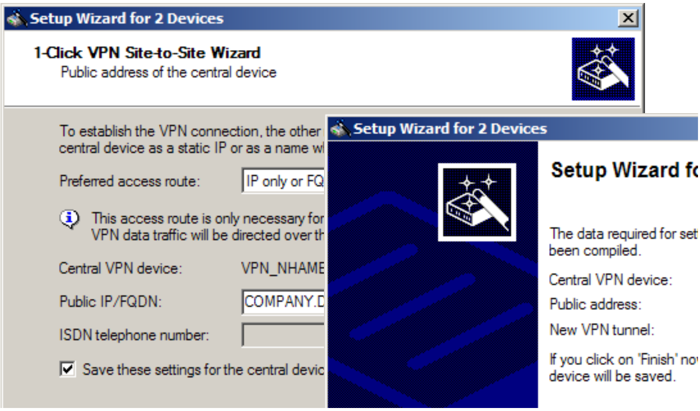
② Use drag&drop by mouse to place the devices onto the entry for the central router.



Name	Description	Address	Device
LANCOM 1621 ADSL/ISDN		192.168.10.186	Ok
LANCOM 1811 Wireless DSL		192.168.10.174	Ok
LANCOM 1811 Wireless DSL		192.168.10.173	Ok

VPN_NHAMEL (LANCOM 1722 VoIP (Annex B)) | Ver. 7.21.0062 (09.08.2007) SN. 000019900010

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.



1-Click VPN Site-to-Site Wizard
Public address of the central device

To establish the VPN connection, the other
central device as a static IP or as a name wi

Preferred access route: IP only or FQ

This access route is only necessary for
VPN data traffic will be directed over th

Central VPN device: VPN_NHAME

Public IP/FQDN: COMPANY.D

ISDN telephone number:

☑ Save these settings for the central devic

Setup Wizard fo

The data required for set
been compiled.

Central VPN device:

Public address:

New VPN tunnel:

If you click on 'Finish' no
device will be saved.

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

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

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

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

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

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

6 Providing dial-in access

Your LANCOM Router supports dial-in connections to permit individual computers full access to your network. This service is also known as RAS (Remote Access Service).

In principle, the RAS access can be realized in two different ways:

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

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

Security aspects

You must, of course, protect your LAN against unauthorized access.

A LANCOM Router therefore offers a whole range of security mechanisms that can provide an outstanding level of protection:

- **VPN**: Network couplings via VPN transmit data by IPSec. The data are encrypted by AES, 3-DES, Blowfish or CAST encryption algorithms.
- **ISDN**: For network couplings via ISDN, the connection password, the checking of the ISDN number and the callback function ensure the security of the connection.

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

6.1 Which information is required?

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

6.1.1 General information

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

Further details to network couplings via VPN using enhanced methods (e.g. digital certificates) can be found in the LCOS reference manual.

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

Notes to the individual values:

- **User name and password**: Users authenticate themselves with this information when dialling in.
- **Incoming number**: The LANCOM Router uses the optional ISDN caller ID as an additional user authentication. This security function should not be used when users dial in from differing locations.

Please refer to chapter "Linking two networks" on page 39 for advice about the other values required for the installation of a RAS access.

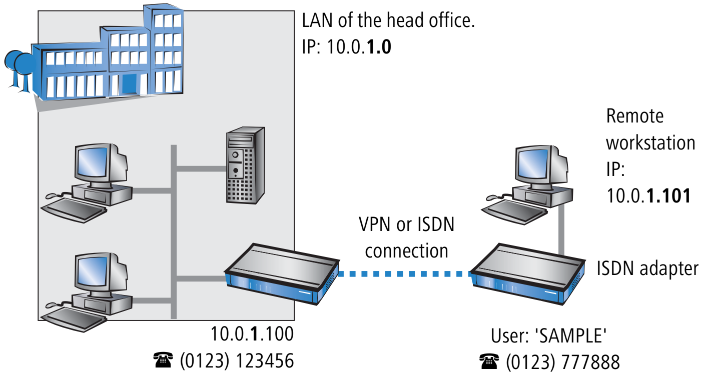
The ISDN calling line identity (CLI)

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

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

6.1.2 Settings for TCP/IP

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



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

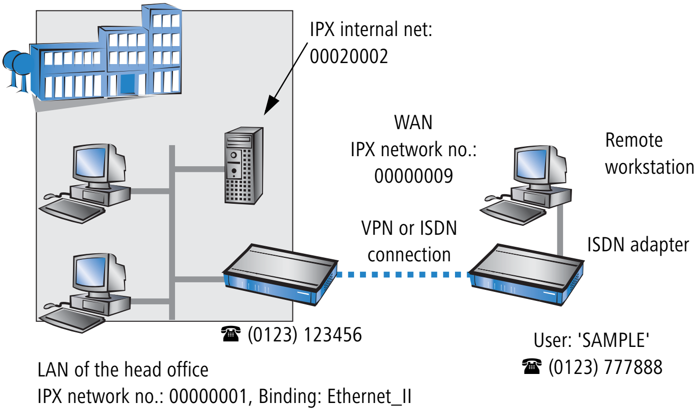
During both manual and automatic IP address assignment, please ensure that only free addresses from the address range of your local network are used. In our example, the IP address '10.0.1.101' will be assigned to the PC when connecting.

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

6.1.3 Settings for IPX

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

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



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

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

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

6.1.4 Settings for NetBIOS routing

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

The connection is not established automatically. The RAS user must manually establish a connection to the LANCOM Router via Dial-Up

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

6.2 Settings for the dial-in computer

6.2.1 Dial-up via VPN

For dialing into a network via VPN a workstation requires:

- an Internet access
- a VPN client

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

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

6.2.2 Dial-up via ISDN

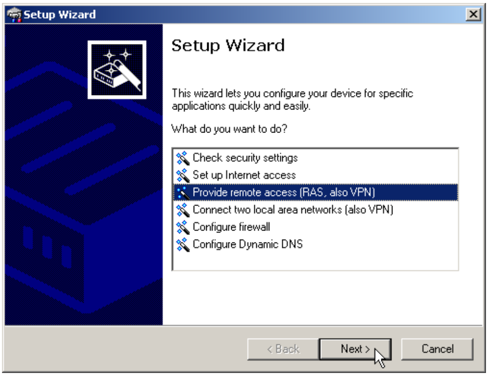
A number of settings must be configured on the dial-in computer. These are briefly listed here, based on a Windows computer:

- Dial-Up Networking (or another PPP client) must be correctly configured
- Network protocol (TCP/IP, IPX) installed and bound to the dial-up adapter
- New connection in Dial-Up Networking with the call number of the router
- Terminal adapter or ISDN card set to PPPHDLC
- PPP selected as the Dial-Up server type, 'Enable software compression' and 'Require data encryption' unchecked
- Select desired network protocols (TCP/IP, IPX)
- Additional TCP/IP settings:
  - Assignment of IP address and name server address enabled
  - 'IP header compression' disabled

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

6.3 Instructions for LANconfig

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



Setup Wizard

This wizard lets you configure your device for specific applications quickly and easily.

What do you want to do?

- Check security settings
- Set up Internet access
- Provide remote access (RAS, also VPN)
- Connect two local area networks (also VPN)
- Configure firewall
- Configure Dynamic DNS

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

③ Configure Dial-Up Networking access on the dial-in PC as described. Next, test the connection (see box “Ping – quick testing for TCP/IP connections” on page 46).

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 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

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

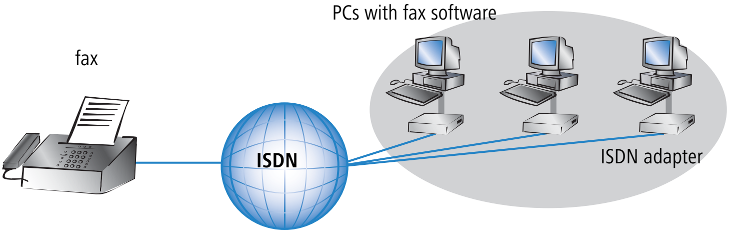
⑤ From the main menu, launch the 'Connect two local networks' wizard. Follow the wizard's instructions and enter the required information.

⑥ Configure Dial-Up Networking access on the dial-in PC as described. Next, test the connection (see box ’Ping – quick testing for TCP/IP connections’).

7 Sending faxes with LANCAPI

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

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



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

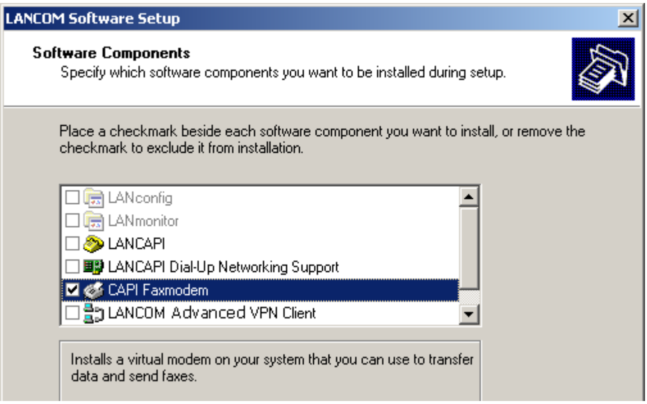
- the **LANCAPI client**. It provides the connection between your workstation PC and the LANCAPI server.
- the **CAPI Faxmodem**. This tool simulates a fax device on your workstation PC.
- the **MS Windows fax service**. This is the interface between the fax applications and the virtual fax.

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

7.1 Installation of the LANCOM CAPI Faxmodem

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

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



LANCOM Software Setup

Software Components

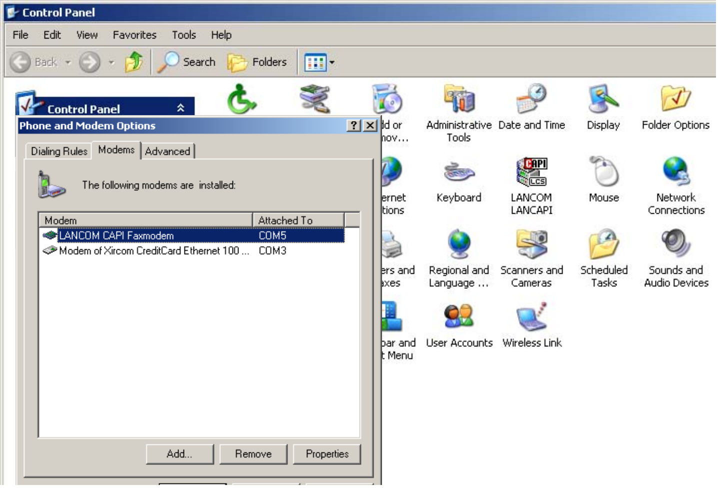
Specify which software components you want to be installed during setup.

Place a checkmark beside each software component you want to install, or remove the checkmark to exclude it from installation.

- □ LANconfig
- □ LANmonitor
- □ LANCAPI
- □ LANCAPI Dial-Up Networking Support
- ☑ CAPI Faxmodem
- □ LANCOM Advanced VPN Client

Installs a virtual modem on your system that you can use to transfer data and send faxes.

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



Phone and Modem Options

Dialing Rules | Modems | Advanced

The following modems are installed:

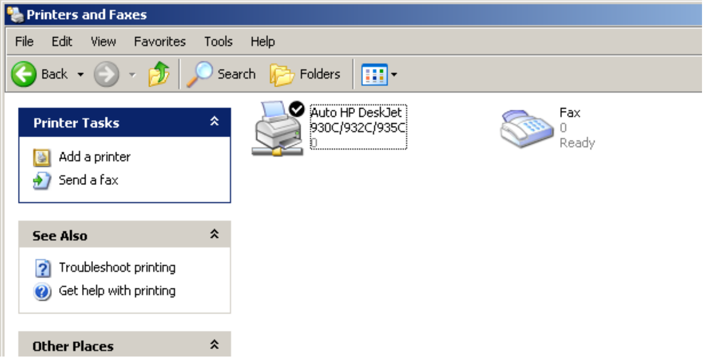
Modem	Attached To
LANCOM CAPI Faxmodem	COM5
Modem of Xircom CreditCard Ethernet 100 ...	COM3

Add... Remove Properties

7.2 Installation of the MS Windows fax service

① Select the option **Printers and Faxes** from the control panel.

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



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

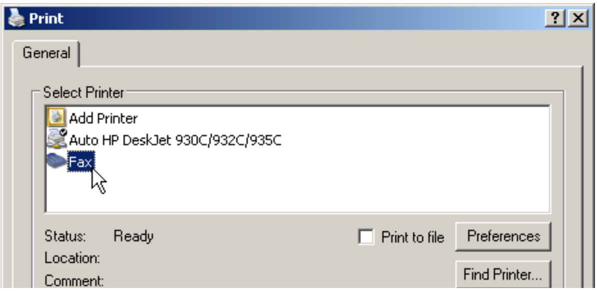
7.3 Sending a fax

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

7.3.1 Send a fax with any given office application

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

② Adjust the fax device as printer.



Status: Ready
Location:
Comment:

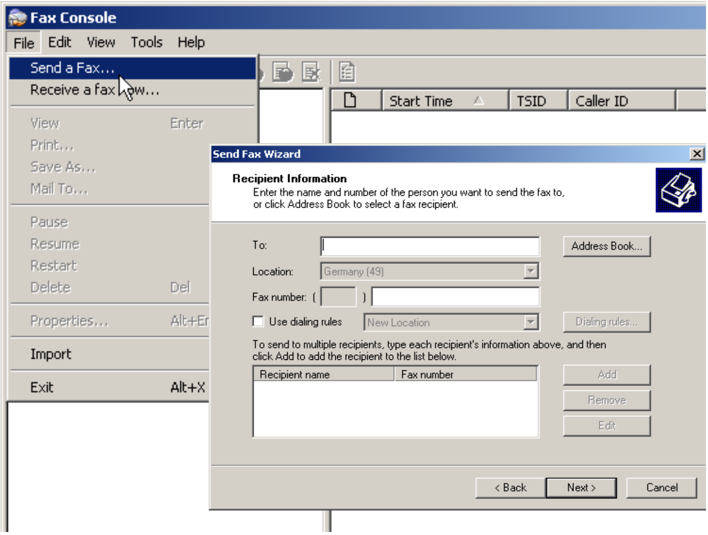
③ Click on OK. A wizard appears, that will guide you through the remaining sending process.

7.3.2 Send a fax with the MS Windows fax service

① Open the window 'Printers and Faxes' from the control panel.

② Double click with the left mouse button the icon of the fax device.

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



Recipient Information

Enter the name and number of the person you want to send the fax to, or click Address Book to select a fax recipient.

To:

Location: Germany (49)

Fax number: ( )

□ Use dialing rules New Location

To send to multiple recipients, type each recipient's information above, and then click Add to add the recipient to the list below.

Recipient name	Fax number

8 Security settings

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

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

8.1 The security settings wizard

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

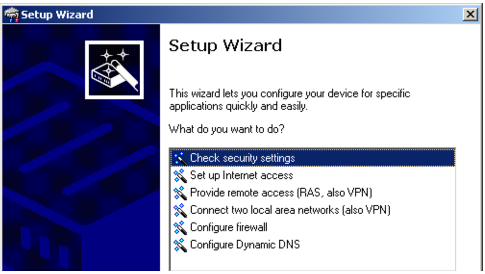
Your LANCOM has a password protection for the configuration access. This protection is already activated during the basic configuration by entering a password.

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

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

8.1.1 Wizard for LANconfig

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



Setup Wizard

This wizard lets you configure your device for specific applications quickly and easily.

What do you want to do?

- Check security settings
- Set up Internet access
- Provide remote access (RAS, also VPN)
- Connect two local area networks (also VPN)
- Configure firewall
- Configure Dynamic DNS

② Select in the selection menu the setup wizard **Control Security Settings** and confirm your choice with **Next**.

③ Enter your password in the following windows and select the allowed protocols for the configuration access from local and remote networks.

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

⑤ Now activate Stateful Inspection, ping-blocking and Stealth mode in the the firewall configuration.

⑥ The wizard will inform you when entries are complete. Complete the configuration with **Finish**.

8.1.2 Wizard for WEBconfig

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

- password for the device
- allowed protocols for the configuration access of local and remote networks
- parameters of configuration lock (number of failed log-in attempts and duration of the lock)

8.2 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 disenabling 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 you local network cannot be attacked from the outside. Activate the firewall in LANconfig under 'Firewall/QoS' on the 'General' tab.

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

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

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

- **Have you activated IP masquerading?**

  IP masquerading refers to the concealment of local computers while they access the Internet. All that is revealed to the Internet is the IP number of the router module of the device. The IP address can be fixed or dynamically assigned by the provider. The computers in the LAN then use the 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.

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

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

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

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

9 Troubleshooting

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

9.1 No WAN connection is established

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

Problems with the cabling?

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

Has the correct transfer protocol been selected?

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

You can monitor and correct the protocol settings under:

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

9.2 DSL data transfer is slow

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

Increasing the TCP/IP window size under Windows

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

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

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

9.3 Unwanted connections under Windows XP

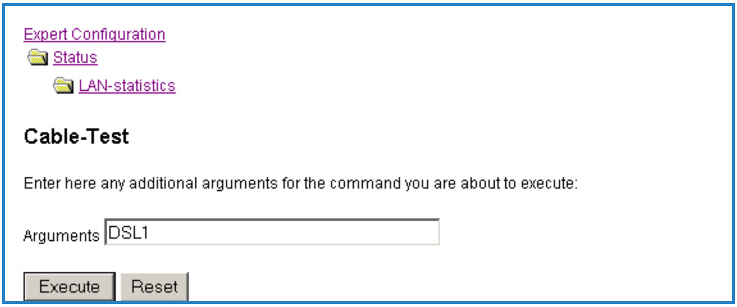
Windows XP computers attempt to compare their clocks with a timeserver on the Internet at start-up. This is why when a Windows XP in the WLAN is started, a connection to the Internet is established by the LANCOM.

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

9.4 Cable testing

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

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

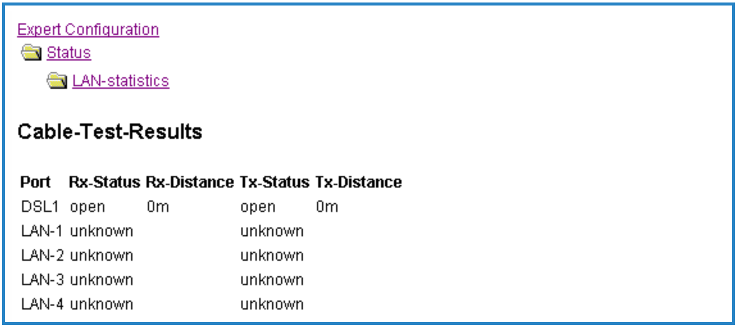


Cable-Test

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

Arguments DSL1

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



Cable-Test-Results

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

The following results can occur:

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

10 Appendix

10.1 Performance data and specifications

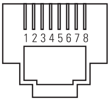
		LANCOM 821+	LANCOM 1721 VPN	LANCOM 1711+ VPN
Connections	Ethernet LAN	4x 10/100Base-TX, auto sensing, switch with node/hub auto sensing		
	WAN/ADSL	ADSL over ISDN as per ITU G.992.1 Annex B (compatible to U-R2 connections of the Deutsche Telekom) or ADSL over POTS as per ITU G.992.1 Annex A ADSL over ISDN as per ITU 992.3, ITU G.992.5 Annex B (ADSL2+) or ADSL over POTS as per ITU G992.3 and ITU G.992.5 Annex A		10/100Base-TX, auto sensing
	ISDN	ISDN S0 bus		
	Outband	serial V.24/V.28 port (8 pol. mini DIN), in combination with LANCOM modem adapter kit suited for connection of external analogue or GSM modems		
	Power supply	12V DC via external power supply. Permitted power supplies: ■ NEST 12V/1A DC/S Hohlstkr 2.1/5.5mm (RoHS) LANCOM item no. 110524 Type identification on the power supply „Type: 15.2230S“		
Housing		210 x 143 x 45 mm (W x H x D), rugged plastic case, connectors on the rear side, stackable, provision for wall mounting		
Standards		EU (CE certification: EN 55022, EN 55024, EN 60950)		
Environment / temperature range		Temperature range 0 °C to + 40 °C at 80 % max. humidity (non condensing)		Temperature range 0 °C to +55 °C at 80 % max. humidity (non condensing)
Options			LANCOM VPN Option 25 channels (hardware accelerated, max.25 simultaneous connections, 50 connections configurable) for VPN in WAN (Art. no.60083)	
Accessories		LANCOM Modem Adapter Kit for connecting modems (analogue or GSM) to the serial configuration interface (Art. no. 110288) LANCOM Rack Mount Option (Art. no. 61501)		
			LANCOM Advanced VPN Client (Art. no. 61600) LANCOM Advanced VPN Client (10 bulk) (Art. no. 61601) LANCOM Advanced VPN Client (25 bulk) (Art. no. 61602)	

10.2 Contact assignment

10.2.1 WAN interface

Only LANCOM 1711+ VPN

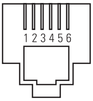
8-pin RJ45 socket

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

10.2.2 ADSL interface

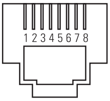
Only LANCOM 821+ and LANCOM 1721 VPN

6-pin RJ11 socket

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

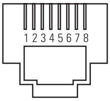
10.2.3 ISDN S_0 interface

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

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

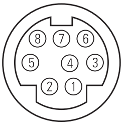
10.2.4 Ethernet interface 10/100Base-TX

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

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

10.2.5 Configuration interface (Outband)

8-pin mini-DIN socket

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

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).

Index