LANCOM 7011 VPN –
LANCOM 8011 VPN

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.

Trademarks

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

The LANCOM Systems logo 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.

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, April 2004

110228/0404

Preface

Thank you for placing your trust in this LANCOM product.

The top models of the LANCOM VPN series serve as extremely powerful Dynamic VPN gateways for medium-sized and large locations.

- Due to the Fast Ethernet uplink, LANCOM devices are ideal partners for all connection variants.
- Integrated LANCOM High Security Firewall
- With 200 up to 1000 VPN channels the LANCOM VPN series offers enough capacity for high-bandwidth couplings (LANCOM 8011 VPN with hardware accelerator).
- With the IPSec extension LANCOM dynamic VPN it is possible to connect branch offices with dynamic IP addresses (standard broadband connection) at any time—even if the receiving station is not online.
- DMZ ports and separate internet address ranges (without NAT) support the operation of your own web servers.
- The IP quality of service functions provide dynamic bandwidth management, in particular for Voice over IP telephone systems, for critical applications or for certain user groups.
- Due to its N:N IP address mapping also existing networks can be integrated seamlessly into VPNs.
- The provided management tools LANconfig and LANmonitor support a complete real time monitoring apart from comfortable remote maintenance of the branch offices.
- Further highlights are the extensive Firewall features, for example the Stateful Inspection, Intrusion Detection and protection from Denial-of-Service attacks.
- Regular free software updates of the LANCOM operating system LCOS are available at any time.

Security settings

For a carefree use of your device, we recommend to carry out all security settings (e.g. Firewall, encryption, access protection, charge lock), which are not already activated at the time of purchase of your device. The LANconfig wizard 'Check Security Settings' will support you accomplishing this. Further information regarding this topic can be found in chapter 'Security settings' → page 61.

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

User manual and reference manual

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

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

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

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

Model variants

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

- LANCOM 7011 VPN
- LANCOM 8011 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 VPN.

This documentation was compiled …

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

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

info@lancom.de

Our online services (www.lancom.de) are available to you around the clock should you have any queries regarding the topics discussed in this manual or require any further support. In addition support from LANCOM Systems is also available to you. Telephone numbers and contact information for LANCOM Systems support can be found on a separate insert, or at the LANCOM Systems website.

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

Contents

EN

1 Introduction

The models of the LANCOM VPN series operate as powerful Dynamic VPN gateways with 200, 500 or 1000 VPN channels for remote sites or mobile users.

Due to the Fast Ethernet uplink, the devices are the ideal partner for almost all WAN connection variants. The integrated multi protocol router and the integrated firewall enable a secure internet access for the local network. The ISDN interface is mainly used to establish Dynamic VPN connections to remote sites with dynamic IP addresses.

1.1 Which use does VPN offer?

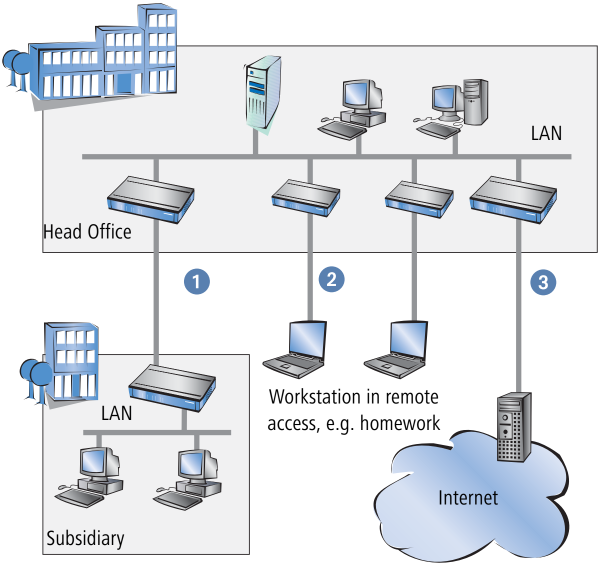
A VPN (**V**irtual **P**rivate **N**etwork) can be used to set up cost-effective, public IP networks, for example via the ultimate network: the Internet.

The models LANCOM 7011 VPN and LANCOM 8011 VPN are equipped with 200 VPN channels by default. With the additional LANCOM VPN Option the LANCOM 8011 VPN can be upgraded to 500 or 1000 channels.

While this may sound unspectacular at first, in practice it has profound effects. To illustrate this, let's first look at a typical corporate network without VPN technology. In the second step, we will see how this network can be optimized by the deployment of VPN.

Conventional network infrastructure

First, let's have a look at a typical network structure that can be found in this form or similar forms in many companies:



The corporate network is based on the internal network (LAN) in the headquarters. This LAN is connected to the outside world in three ways:

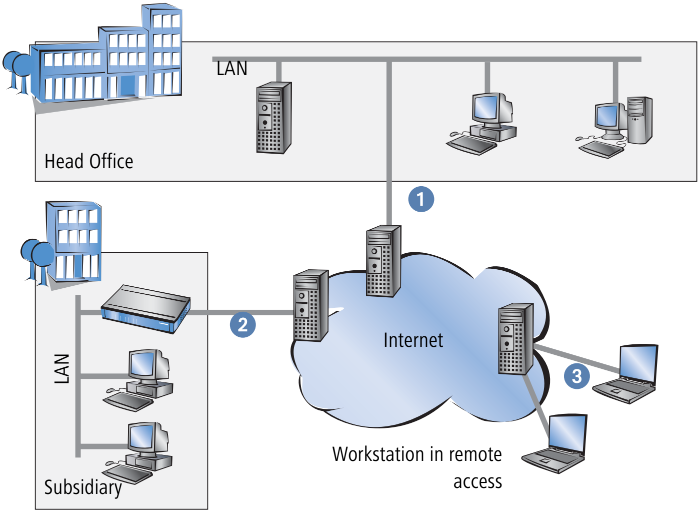
1. A subsidiary is connected to the LAN, typically using a leased line.
2. PCs dial into the central network via modem or ISDN connections (Remote Access Service – RAS).
3. The central LAN has a connection to the Internet so that its users can access the Web, and send and receive e-mail.

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

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

Networking via the Internet

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



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

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.

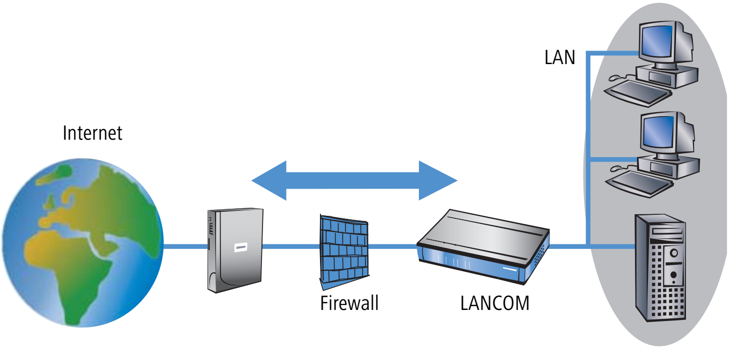
The physical connection no longer exists directly between two participants; instead, the participants rely on their connection to the Internet. The access technology used is not relevant in this case: ideally is the use of broadband technologies such as DSL (Digital Subscriber Line) or G.703 (2-Mbit leased lines). But also a conventional ISDN line can be used.

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

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

1.2 Firewall

The integrated Stateful Inspection Firewall ensures an effective protection against undesired intrusion in your network by permitting only incoming data traffic as reaction to outgoing data traffic. The router's IP masquerading function hides all workstations of the LAN behind a single public IP address. The actual identities (IP addresses) of the individual workstations remain concealed. Firewall filters of the router permit specific IP addresses, protocols and ports to be blocked. With MAC address filters it is also possible to specifically monitor the access of workstations in the LAN to the IP routing function of the device.



Further important features of the Firewall are

- ▶ Intrusion Detection
  Break-in attempts into the local network or on the central Firewall are recognized, repelled and logged by the Intrusion Detection system (IDS) of the LANCOM Wireless DSL. Thereby it can be selected between logging within the device, email notification, SNMP trap or SYSLOG alarms.

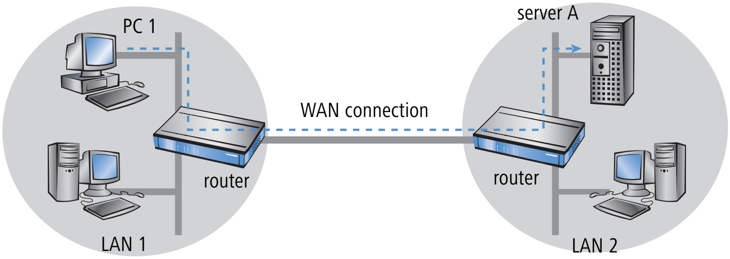
- Denial-of-Service Protection
  Attacks from the Internet can be break-in attempts as well as attacks with the aim of blocking the accessibility and functionality of individual services. Therefore a LANCOM Wireless DSL is equipped with appropriate protective mechanisms, which recognize well-known hacker attacks and which guarantee the functionality.
- Quality-of-Service / Traffic management
  The generic term Quality-of-Service (brief: QoS) summarizes the functions of the LANCOM which guarantee certain service qualities. The advantage is that the QoS functions can take place by means of the existing powerful classification methods of the Firewall (e.g. limitation of subnetworks, single workstations or certain services).
  Guaranteed minimum bandwidths give priority to enterprise critical applications, VoIP PBX installations or certain user groups.

More details about the function of the Stateful Inspection Firewall of your LANCOM VPN can be found in the reference manual on the LANCOM CD.

1.3 What does a router do?

The following sections describe the functionality of routers in general. The functions supported by your device are listed in the table ’What can your LANCOM VPN do?’ → page 15.

Routers connect LANs at different locations and individual PCs to form a Wide Area Network (WAN). With the appropriate rights, any computer in this WAN can access other computers and services of the complete WAN (as with 'PC 1' accessing 'Server A' in the remote LAN in the diagram).



Connecting a LAN to the Internet does not technically differ from coupling two LANs. The only difference is that it is not just a handful of computers behind the Internet provider's router. Instead, it is the net of the networks - the public Internet.

1.3.1 Bridgehead to the WAN

All routers have at least two connections:

- at least one for the LAN
- at least one for WAN connections

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

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

1.3.2 Areas of deployment for routers

Routers are mainly used for the following applications:

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

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

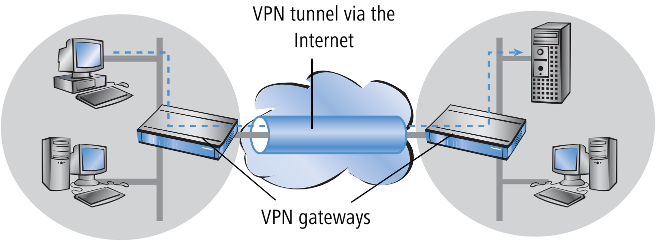
- LAN to LAN coupling (via VPN or ISDN)

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

Not possible with all LANCOM devices.

  - High-speed coupling via VPN
    The fastest and most economical LAN to LAN links are possible with VPN (**V**irtual **P**rivate **N**etwork) technology, as VPN uses the Internet as the basis for its communications. The fast xDSL connection of the router comes into its own here. The precondition: a VPN gateway with

access to the Internet is required on either side of the network interconnection.



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

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

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

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

1.4 What can your LANCOM VPN do?

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

	LANCOM 7011 VPN	LANCOM 8011 VPN
Application		
LAN to LAN coupling via VPN	✓	✓
RAS server (via VPN)	✓	✓
Internet access	✓	✓
IP router	✓	✓
IPX router (via ISDN), e.g. for coupling of Novell networks or dialling into Novell networks	✓	✓

	LANCOM 7011 VPN	LANCOM 8011 VPN
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 existing networks with same IP address ranges	✓	✓
LANCAPI server for the operating with office applications as fax or answering machine via ISDN interface	✓	✓
WAN connection		
Fast Ethernet	✓	✓
ISDN S_0 for establishing Danymic VPN connections to remote sites with dynamic IP addresses	✓	✓
LAN connection		
4 individual Fast Ethernet LAN ports, switchable separately, e.g. as LAN switch or separate DMZ ports, auto crossover.		✓
1 Fast Ethernet LAN port, 1 Fast Ethernet DMZ port	✓	
Security functions		
IP masquerading (NAT, PAT) to hide all workstations of the LAN behind one common public IP address.	✓	✓
Stateful Inspection Firewall	✓	✓
Firewall filters for a selective locking of IP addresses, protocols and ports	✓	✓
MAC address filter control e.g. the access of LAN workstations to IP routing functions	✓	✓
Configuration protection to block “brute force attacks“	✓	✓
Configuration		
Configuration with LANconfig or with web browser, additionally terminal mode for Telnet or other terminal programs, SNMP interface and TFTP server function.	✓	✓
Remote configuration via ISDN (with ISDN-PPP connections e.g. via Windows network and dial-up connections)	✓	✓
Serial configuration interface	✓	✓
Callback function with PPP authentication mechanisms for restriction to fixed ISDN telephone numbers	✓	✓
FirmSafe with firmware versions for absolutely secure software upgrades	✓	✓
Optional software extensions		
ISDN leased line option	✓	✓
LANCOM VPN Option with 500 or 1000 channels		✓

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 7011 VPN	LANCOM 8011 VPN
External power supply	✓	
Cable for integrated power supply		✓
LAN connector cable (green plugs)	✓	✓
WAN connector cable (dark blue plugs)	✓	✓
ISDN connector cable (light blue plugs)	✓	✓
Crossover cable (LAN connector cable) for the DMZ connection	✓	
rubber base, 19” mounting kit		✓
LANCOM CD	✓	✓
Printed user manual	✓	✓
Printed reference manual	✓	✓

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

2.2 System preconditions

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

- Operating system that supports TCP/IP, e.g. Windows XP, Windows Millennium Edition (Me), Windows 2000, Windows 98, Windows 95, Windows NT, Linux, BSD Unix, Apple Mac OS, OS/2, BeOS.
- Access to the LAN via the TCP/IP protocol.

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

2.3 Introducing LANCOM VPN

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

While the information in this section is useful for the installation of the device, it is not absolutely essential. You may therefore skip this section for the time being and go straight forward to 'Hardware installation' → page 25.

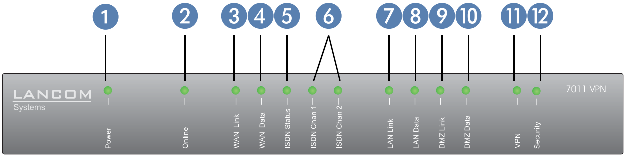
2.3.1 Status displays

The front and the rear panels (LANCOM 7011 VPN) of the unit feature a series of light emitting diodes (LEDs) that provide information on the status of the device. On the LANCOM 8011 VPN a two-lined display additionally shows information on the status.

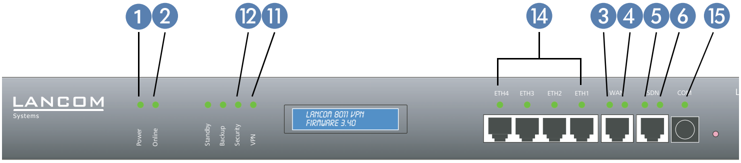
Front side

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

LANCOM 7011 VPN



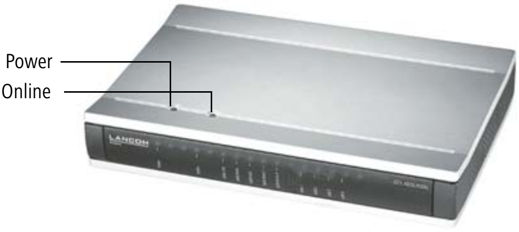
LANCOM 8011 VPN



Top panel

Only LANCOM 7011 VPN

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



Meanings of the LEDs

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

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

Power ❶

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.

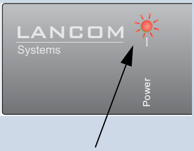
off		Device off
green	blinking	Self-test when powering up
green	constantly on	Device ready for use
red/ green	blinking alternately	Device insecure: configuration password not assigned
red	blinking	Time or connect-charge reached

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' → page 61.

Flashing Power LED but no connection?

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

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



Signal for reached time or connect-charge limit

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

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

Online 2 The Online LED indicates the overall status of all WAN ports:

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

WAN link ❸

Connection status of the WAN connection:

off		Not connected
green	blinking	Establishing first connection
green	flashing	Protocol negotiations
green	constantly on	Connection established

WAN data ❹

Data traffic via the WAN connection:

off		No network device connected
green	constantly on	Connection established
green	flickering	Data traffic (send or receive)
red	flickering	Collision of packets

ISDN status ❺

Connection status of ISDN S_0 connection:

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

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

ISDN Chan 1
ISDN Chan 2 ❻

Data traffic on the ISDN B channels (separate per B channel with LANCOM 7011 VPN, for both ISDN B channels with LANCOM 8011 VPN):

off		No connection established
green	blinking	Dialling
green	flashing	Establishing first connection

green	inverse flashing	Establishing further connection (only if B channel 1 and B channel 2 share display)
green	constantly on	Connection established via B channel
green	flickering	Data traffic (send or receive)

LAN link ⑦ (only LANCOM 7011 VPN)

Connecting status of the LAN interface:

off		No network device connected
green	constantly on	Connection to network device operational, no data traffic

LAN data ⑧ (only LANCOM 7011 VPN)

Data traffic on the LAN interface:

off		No data traffic
green	flickering	Data traffic
red	flickering	Collision of packets

DMZ link ⑨ (only LANCOM 7011 VPN)

Connecting status of the DMZ interface

off		No network device connected
green	constantly on	Connection to network device, no data traffic

DMZ data ⑩ (only LANCOM 7011 VPN)

Data traffic on the DMZ interface.

off		No data traffic
green	flickering	Data traffic
red	flickering	Collision of packets

ETH 1 to ETH 4 ⑭ (only LANCOM 8011 VPN)

Connection status and data traffic of the four LAN ports with integrated switch:.

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

VPN ⑪

VPN connection status

off		No VPN channel established
green	blinking	Connection established
green	flashing	First connection
green	inverse flashing	Further connections
green	constantly on	VPN channel is established

Security ⑫

Status of the Firewall. Shows the state of security settings and blocked attacks on the secured network.

green	constantly on	Security settings are okay. Rules for filtering packets are established
red/ green	blinking	Insecure configuration
red	flickering	Security alarm: filtering packets with Firewall rules

COM ⑮
(only LANCOM
8011 VPN)

Connection status of the serial configuration port:

off		No session logged in
green	constantly on	Serial configuration session logged in
green	flickering	Data transmission on serial configuration session

LCD display

Only LANCOM
8011 VPN

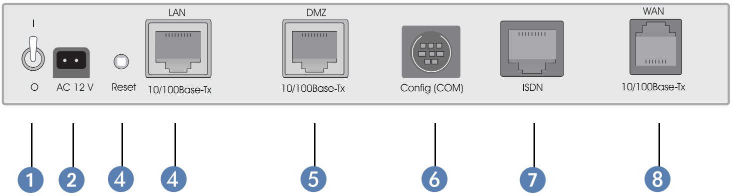
The LCD display of the LANCOM 8011 VPN shows the following information in two lines with 16 characters in revolving alternation:

- Device name
- Firmware version
- Temperature
- Date and time
- CPU usage
- Memory usage
- Number of VPN channels
- Data transfer downstream
- Data transfer upstream

2.3.2 The back of the unit

LANCOM 7011 VPN

The connections and switches of the LANCOM 7011 VPN are located on the back panel:



① Voltage switch

② Connection for the included power adapter

③ Reset switch

④ LAN port as 10/100Base-Tx

⑤ DMZ port

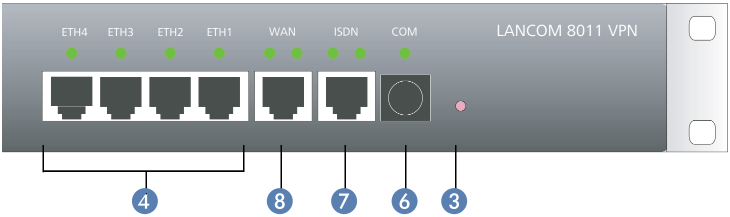
⑥ Serial configuration port

⑦ ISDN/S_0 port

⑧ WAN port

LANCOM 8011 VPN

On the LANCOM 8011 VPN ports and switches of the router are placed on the front and back:



The following ports can be found on the front side:

④ Four 10/100Base Tx ports for local networks

⑧ WAN port

⑦ ISDN/S_0 port

⑥ Serial configuration interface

➌ Reset switch

The following ports can be found on the back:

➊ Voltage Switch

➋ Port for power cable

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.

2.4 Hardware installation

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

Only LANCOM 8011 VPN

① **Mounting** – If desired, mount the device into a free slot of a 19” rack.

② **LAN** – connect the LANCOM VPN 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 ➍ 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 VPN in a network segment at any given time. All unconfigured LANCOM VPN 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 VPN devices one at a time, immediately assigning each device a unique IP address (one that does not end with '254').

Only LANCOM 7011 VPN

③ **DMZ** – connect a PC with the included crossover cable to the DMZ port ❺.

④ **WAN** – connect the WAN port ❽ with the included connector cable (dark blue plug) e. g. with the ethernet port of a DSL modem or of a cable modem.

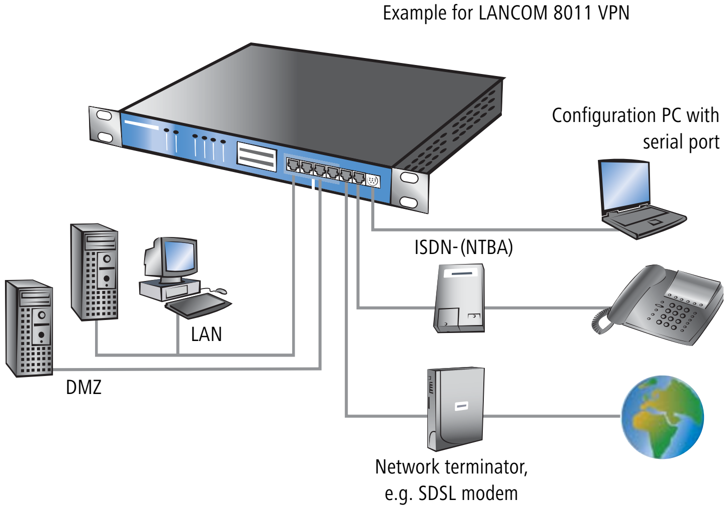
⑤ **ISDN** – to connect the LANCOM VPN to the ISDN, plug one end of the supplied ISDN connector cable (light blue plugs) in the ISDN/S_0 port ❼ of the router and the other end into an ISDN/S_0 multi-device mode or point-to-point mode connection.

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

⑦ **Connect to power** – Connect socket ❷ of the unit to a power supply using the included power adapter and switch it on ❶.

With the LANCOM 7011 VPN only use the included power supply unit! Using an unsuitable power supply unit may cause damage or injury.

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


Example for LANCOM 8011 VPN
Configuration PC with serial port
ISDN- (NTBA)
LAN
DMZ
Network terminator, e.g. SDSL modem

2.5 Software installation

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

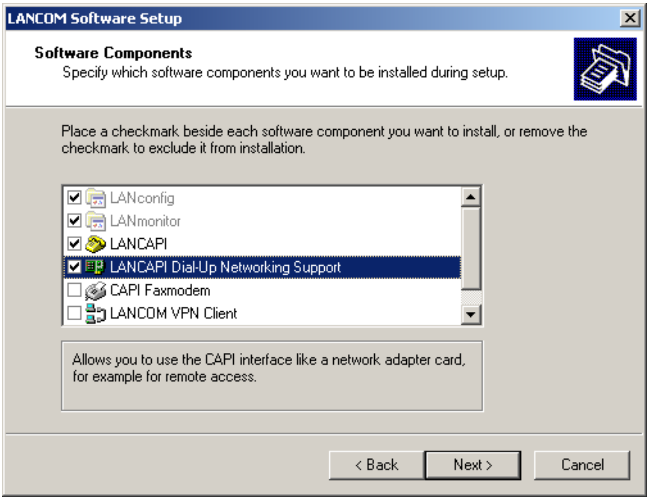
You may skip this section if you use your LANCOM VPN exclusively with computers running operating systems other than Windows.

2.5.1 Starting LANCOM setup

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

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

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



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 VPN Client

Allows you to use the CAPI interface like a network adapter card, for example for remote access.

2.5.2 Which software should you install?

- **LANconfig** is the configuration program for all LANCOM routers and Wireless LAN access points. WEBconfig can be used alternatively or in addition via a web browser.
- **LANmonitor** lets you monitor on a Windows PC all LANCOM routers and Wireless LAN access points.
- **LANCAPI** is a special form of the CAPI-2.0 interface that all workstations of the LAN need to get access to office communication functions as fax or EuroFile transfer. With **LANCAPI Dial-Up Networking Support**, single workstations can realize dial-up connections to an Internet provider via LANCAPI. The **CAPI fax modem** makes you available a first class fax driver.
- The **LANCOM VPN Client** enables a setting of VPN connections from a remote workstation via Internet to a router with LANCOM VPN Option.
- With **LANCOM Online Documentation,** you can copy the documentation files on your PC.

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

3 Basic configuration

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

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

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

At the end of this chapter we will show you the settings that are needed for the LAN's workstations to ensure trouble-free access to the router ('TCP/IP settings to workstation PCs' → page 37).

3.1 Which information is necessary?

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

- TCP/IP settings
- protection of the configuration
- information on DSL connection
- information on ISDN connection
- configuring connect charge protection

3.1.1 TCP/IP settings

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

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

New LAN—fully automatic configuration possible

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

- a single PC is connected to the router
- setup of a new network

Fully automatic TCP/IP configuration will not be available when integrating the LANCOM VPN in an existing TCP/IP LAN. In this case, continue with the section 'Information required for manual TCP/IP configuration' → page 30.

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

Configure manually nevertheless?

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

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

Information required for manual TCP/IP configuration

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

- **IP address and netmask for the LANCOM VPN**
  Assign a free IP address from the address range of your LAN to the LANCOM VPN and specify the netmask.

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

3.1.2 Configuration protection

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

The setup wizard for the basic configuration automatically disables remote configuration access via ISDN, thus protecting your configuration against tampering. ISDN remote configuration access can be enabled at any time using the security wizard (see 'Have you permitted remote configuration?' → page 64).

3.1.3 Settings for the WAN connection

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

3.1.4 Settings for the ISDN connection

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

- One or more ISDN MSNs on which the router will accept calls. MSNs are ISDN subscriber numbers that are assigned to you by your telephone provider. They are normally entered without an area code. These numbers are only relevant for the router functions (LAN to LAN coupling, RAS), not for remote configuration and LANCOM VPN Option.
- A dialing prefix for access to the public telephone network. This is normally required only when using an ISDN PBX. '0' is the usual prefix. It is used for all outgoing calls.
- Finally, you should know whether your telephone provider transmits an ISDN connect-charge pulse. This signal can be used LANCOM VPN for connect-charge budgets and the accounting function.

3.1.5 Connect charge protection

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

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

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

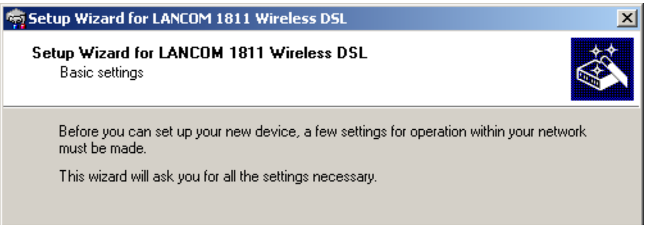
Any budget can be deactivated by entering the value '0'.

It is possible to completely turn off connect charge protection

3.2 Instructions for LANconfig

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

LANconfig automatically detects the new LANCOM VPN in the TCP/IP network. Then the setup wizard starts that will help you make the basic settings of the device or will even do all the work for you (provided a suitable network environment exists).



Setup Wizard for LANCOM 1811 Wireless DSL

Setup Wizard for LANCOM 1811 Wireless DSL
Basic settings

Before you can set up your new device, a few settings for operation within your network must be made.

This wizard will ask you for all the settings necessary.

If the setup wizard does not start automatically, start a manual search for new devices on all ports (if the LANCOM VPN is connected via a serial port) or in the network (**Device ▶ Find**).

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

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

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

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

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

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

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

⑤ 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**.

⑥ Enter the ISDN subscriber numbers (as MSNs, i.e. without area code) on which the router will accept calls. Multiple numbers are separated by semicolons. If you do not specify any MSNs, the router will answer all incoming calls on the ISDN connection.

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

⑦ Connect charge protection can limit the cost of DSL and ISDN 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’ on page 37 will describe the settings required for the individual workstations in the LAN.

3.3 Instructions for WEBconfig

To configure the router with WEBconfig you must know how to address it in the LAN. An unconfigured LANCOM VPN always reacts to a certain IP address, and in some network configurations even to a name.

Does my LANCOM VPN react to a name?

If you do not yet have a DHCP or DNS server on your LAN, the router reacts to any name (like 'LANCOM' or 'Router') that you specify in the URL address field of a web browser.

If you don't know whether IP addresses have been used in your network up until now, display the IP address of your own PC (see the following section). If the 'IP Address' field contains the value '0.0.0.0', this indicates that an IP address has not yet been assigned to the network card.

What is the IP address of the LANCOM VPN?

The IP address of an unconfigured LANCOM VPN results from the IP address of your PC by replacing the last number of its IP address (after the third dot) with 254.

For example, if your PC is assigned the IP address 10.0.0.17, then you will find an unconfigured LANCOM VPN under the address 10.0.0.254. The IP address of your PC can be displayed (depending on the operating system) with the following command line commands (entry under Windows at the command prompt):

Operating system	Command in the command line
Windows Me, Windows 98, Windows 95	winipcfg
Windows XP, Windows 2000, Windows NT 4.0	ipconfig
Linux, UNIX	ipconfig

Starting the wizards in WEBconfig

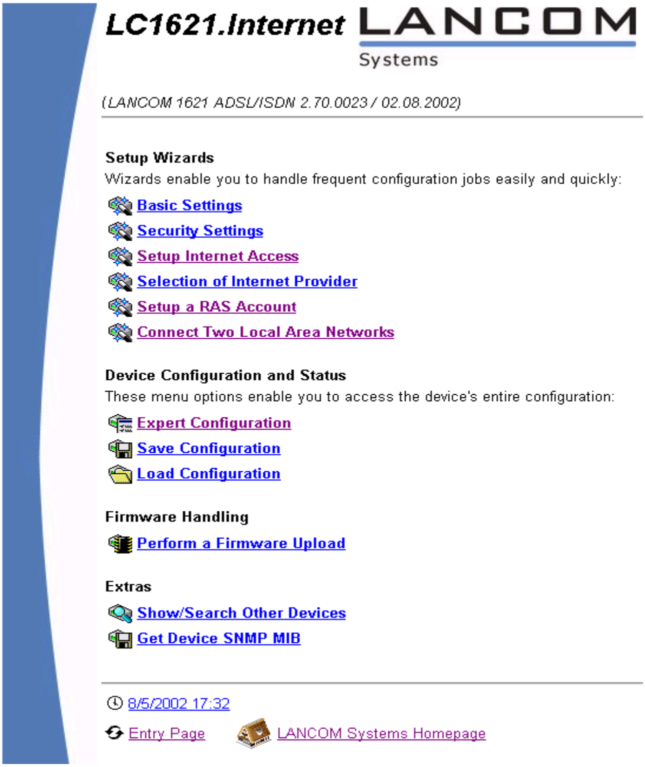
① Start your web browser (e.g. Internet Explorer, Netscape Navigator, Opera) and call the LANCOM VPN there:

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

(or with any desired name)

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

The WEBconfig main menu will be displayed:



LC1621.Internet LANCOM Systems

(LANCOM 1621 ADSL/ISDN 2.70.0023 / 02.08.2002)

Setup Wizards

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

- Basic Settings
- Security Settings
- Setup Internet Access
- Selection of Internet Provider
- Setup a RAS Account
- Connect Two Local Area Networks

Device Configuration and Status

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

- Expert Configuration
- Save Configuration
- Load Configuration

Firmware Handling

- Perform a Firmware Upload

Extras

- Show/Search Other Devices
- Get Device SNMP MIB

8/5/2002 17:32

Entry Page   LANCOM Systems Homepage

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

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

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

③ In the following 'Security settings' window, specify a password for configuration access. Note that the password is case-sensitive and ensure that it is sufficiently long (at least 6 characters).

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

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

Remote configuration via a direct ISDN connection is available independently of the WAN remote configuration: in this case, the configuration PC establishes a direct dial-up ISDN connection to the LANCOM VPN, for example using Windows Dial-Up Networking. ISDN remote configuration can be enabled by specifying an MSN/terminal device selection digit for it. In this case, the LANCOM VPN will accept calls on that MSN/terminal device selection digit and can be remotely configured via the ISDN connection.

Confirm your selection with **Apply**.

④ In the next window, select your DSL provider from the list that is displayed. Confirm your choice with **Apply**.

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

⑤ Connect charge protection can limit the cost of DSL and ISDN connections to a predetermined amount if desired. Confirm your choice with **Apply**.

If your devices does not feature an ISDN port, you may now close the setup wizard. Otherwise the wizard will prompt you to configure the ISDN port now. Make your choice and confirm it with **Apply**.

⑥ Enter the ISDN subscriber numbers (as MSNs, i.e. without area code) on which the router will accept calls. Multiple numbers are separated by semicolons. If you do not specify any MSNs, the router will answer all incoming calls on the ISDN connection.

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

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

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:

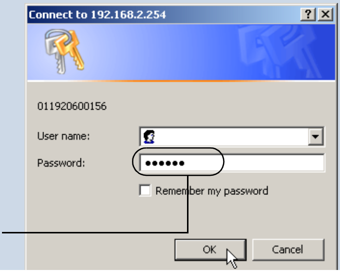
- Default gateway – receives all packets that are not addressed to computers within the local network.
- DNS server – translates network names (www.**lancom.de**) or names of computers (**www**.lancom.de) to actual IP addresses.

The LANCOM VPN 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:

Entering the password in the web browser

When you are prompted for a password by your web browser when accessing the device in the future, enter it in the **Password** field. Please note that the password is case-sensitive. Leave the **User Name** field blank.



Connect to 192.168.2.254

011920600156

User name:

Password: ••••••

□ Remember my password

Entering the configuration password

▶ IP address assignment via the LANCOM VPN (default)

In this operating mode the LANCOM VPN 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 VPN 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 VPN as a DNS server.

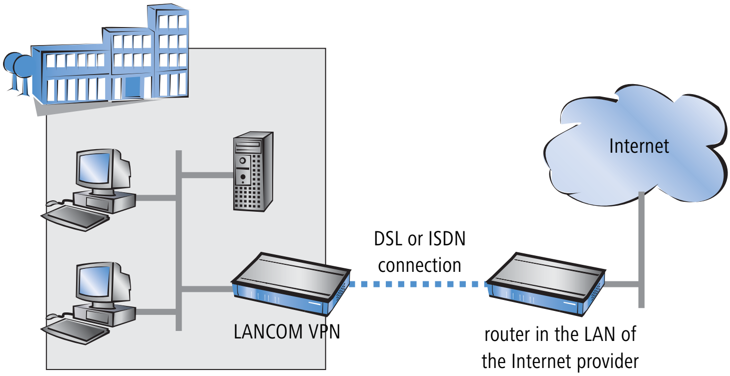
▶ Manual IP address assignment

If the IP addresses in the network are assigned static ally, then for each PC the IP address of the LANCOM VPN 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 VPN, please see the reference manual. For more information on the network configuration of the workstation computers, please refer to the documentation of your operating system.

4 Setting up Internet access

All computers in the LAN can take advantage of the central Internet access of the LANCOM VPN. The connection to the Internet provider can be established via any WAN connection. Internet access via ISDN can be used as a backup connection for DSL, for example.



Does the setup wizard know your Internet provider?

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

Additional information for unknown Internet providers

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

- **DSL**
  - Protocol: PPPoE, PPTP or Plain Ethernet (IPoE)
  - Additionally for Plain Ethernet: own public IP address with netmask (not to be confused with the private LAN IP address), default gateway and DNS server. These values can be received automatically from providers that support DHCP.
  - User name and password

- **ISDN** – dial-in number
  - User name and password

Additional connection options

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

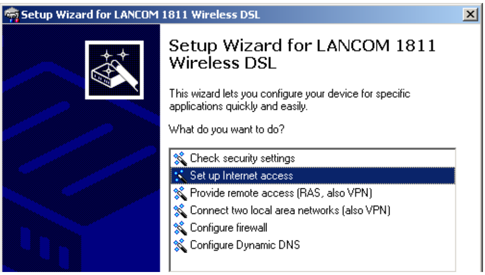
- Time-based billing or flat rate – select the accounting model used by your Internet provider.
  - When using time-based billing, you can set the LANCOM VPN to automatically close existing connections if no data has been transferred within a specified time (the so-called idle time).

    In addition, you can activate a line monitor that identifies inactive remote stations faster and therefore can close the connection before the idle time has elapsed.
  - Active line monitoring can also be used with flat rate billing to continuously check the function of the remote station.

    You also have the option of keeping flat rate connections alive if required. Dropped connections are then automatically re-established.
- Dynamic channel bundling (ISDN only)
  - if required, the second ISDN B-channel will automatically be bundled to the connection. This doubles the available bandwidth; it may also double your connect charges as well, however. What's more, your ISDN connection will be busy in this case, with all other incoming and outgoing calls being rejected.
- Data compression (ISDN only)
  - this permits an additional increase in data throughput.

4.1 Instructions for LANconfig

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



Setup Wizard for LANCOM 1811 Wireless DSL

Setup Wizard for LANCOM 1811 Wireless DSL

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 From the menu, select the **Setup Internet access** wizard and click **Next**.

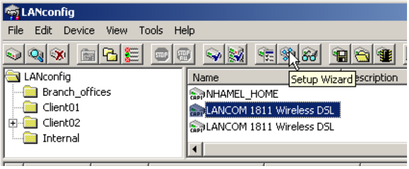
③ In the following window select your country and your Internet provider if possible, and enter your access information.

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

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

LANconfig:
Quick access to the setup wizards

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



4.2 Instructions for WEBconfig

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

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

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

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

5 Linking two networks

With the network interconnection (also known as LAN to LAN coupling) of the LANCOM VPN, 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 VPN routers are being used on both sides. A network interconnection may also be realized with routers from other manufacturers. A mixed setup usually requires more extensive configuration measures for both devices, however. Please refer to the reference manual for more information in this regard.

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

Security aspects

You must, of course, protect your LAN against unauthorized access. A LANCOM VPN 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 VPN and/or ISDN network couplings.

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'
VPN	IP network address of the remote network	'10.0.2.0'		'10.0.1.0'

Coupling	Entry	Gateway 1		Gateway 2
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

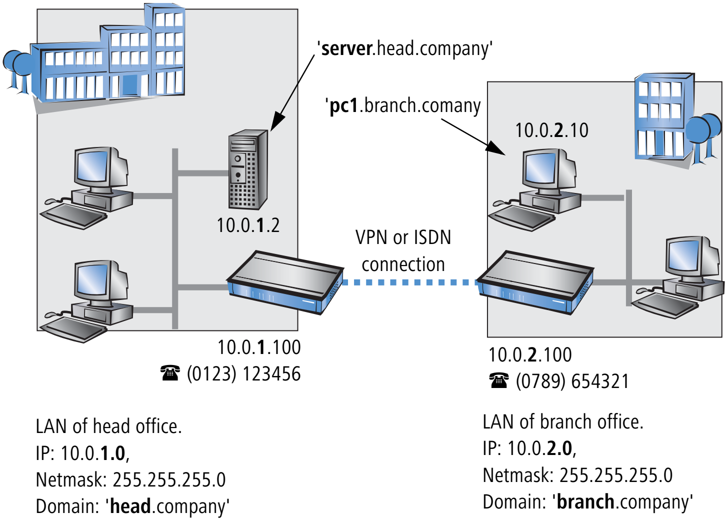
- In case your device has an **ISDN connection**, the wizard asks whether the remote site has ISDN as well.
- The type of IP address must be stated for both sides for VPN connections via the Internet. There are two types of IP addresses: static and dynamic. An explanation of the two **IP address types** 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 VPN, the wizard will ask you for a new, **unique device name.** With this entry, you will rename your LANCOM VPN. 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 VPN 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 VPN 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.

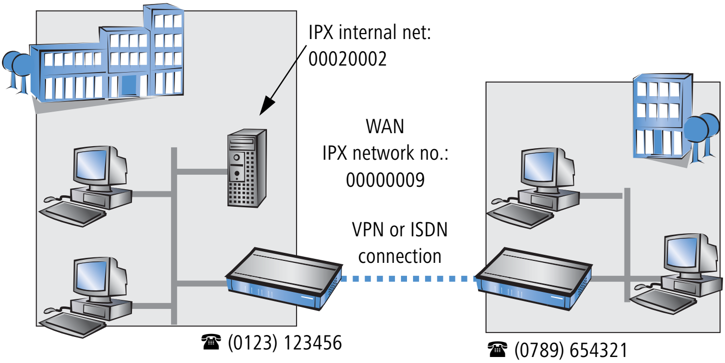
5.1.3 Settings for the IPX router

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.



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

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

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

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

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

5.1.4 Settings for NetBIOS routing

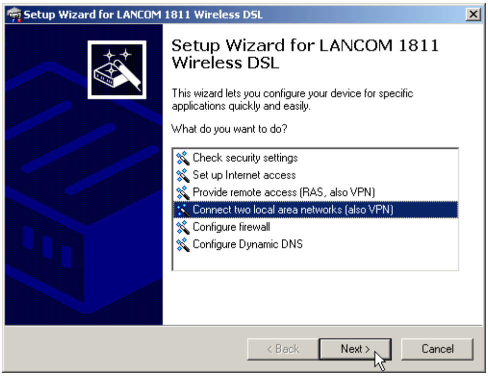
NetBIOS routing can be set up quickly: All that is required in addition to the information for the TCP/IP protocol used is the name of a Windows workgroup from in the router's own LAN.

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

5.2 Instructions for LANconfig

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

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



Setup Wizard for LANCOM 1811 Wireless DSL

Setup Wizard for LANCOM 1811 Wireless DSL

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

5.3 Instructions for WEBconfig

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

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

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

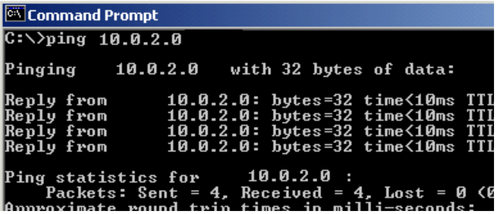
② The wizard will return a message to indicate that it has all the information it needs. Close the wizard with **Terminate**.

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

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

6 Providing dial-up access

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

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

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

Security aspects

You must, of course, protect your LAN against unauthorized access. An LANCOM VPN 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 and/or an ISDN connection. .

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 VPN uses the optional ISDN caller ID as an additional user authentication. This security function should not be used when users dial in from differing locations.

Please refer to chapter ’Linking two networks’ → page 42 for advice about the other values required for the installation of a RAS access.

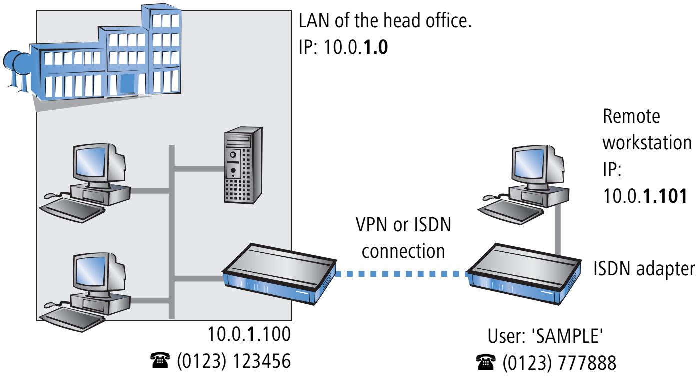
The ISDN calling line identity (CLI)

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 VPN 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 VPN should use for RAS users.

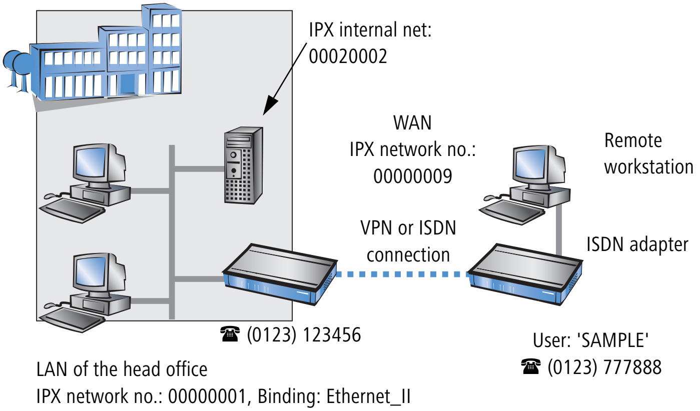
During both manual and automatic IP address assignment, please ensure that only free addresses from the address range of your local network are used. In our example, the IP address '10.0.1.101' will be assigned to the PC when connecting.

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 VPN via Dial-Up Networking first. When connected, they can search for and access computers in the remote network (via **Find** ▶ **Computer**s, not through the Network Neighbourhood).

6.2 Settings for the dial-in computer

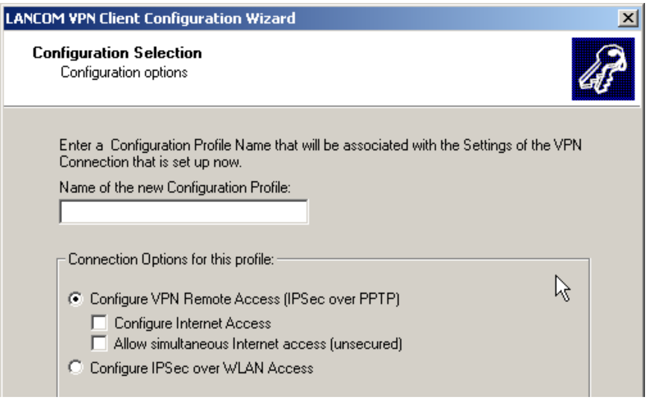
6.2.1 Dial-up via VPN

For dialing into a network via VPN a workstation requires:

- an Internet access
- a VPN client

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

For configuring a new profile, select the option 'Configure VPN Remote Access (IPSec over PPTP)' in the LANCOM VPN Client configuration wizard.



LANCOM VPN Client Configuration Wizard

Configuration Selection

Configuration options

Enter a Configuration Profile Name that will be associated with the Settings of the VPN Connection that is set up now.

Name of the new Configuration Profile:

Connection Options for this profile:

● Configure VPN Remote Access (IPSec over PPTP)

□ Configure Internet Access

□ Allow simultaneous Internet access (unsecured)

○ Configure IPSec over WLAN Access

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

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

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

6.2.2 Dial-up via ISDN

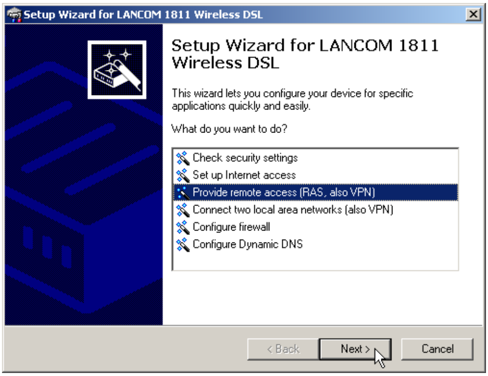
A number of settings must be configured on the dial-in computer. These are briefly listed here, based on a Windows computer:

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

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

6.3 Instructions for LANconfig

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



Setup Wizard for LANCOM 1811 Wireless DSL

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' → page 49).

6.4 Instructions for WEBconfig

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

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

⑤ Configure Dial-Up Networking access on the dial-in PC as described. Next, test the connection (see box 'Ping – quick testing for TCP/IP connections' → page 49).

7 Sending faxes with LANCAPI

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

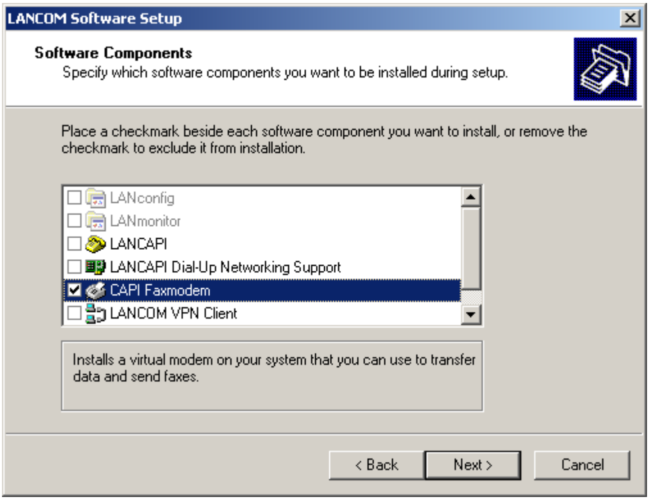
- the **LANCAPI client**. It provides the connection between your workstation PC and the LANCAPI server.
- the **CAPI fax modem**. This tool simulates a fax device on your workstation PC.
- the **MS Windows fax service**. This is the interface between the fax applications and the virtual fax.

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

7.1 Installation of the LANCOM CAPI fax modem

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

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



LANCOM Software Setup

Software Components

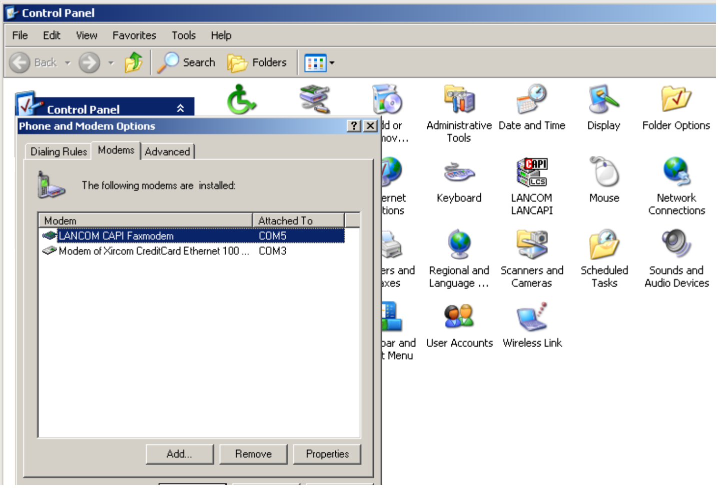
Specify which software components you want to be installed during setup.

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 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 fax modem is entered into the **Phone and Modem Options** of the control panel.



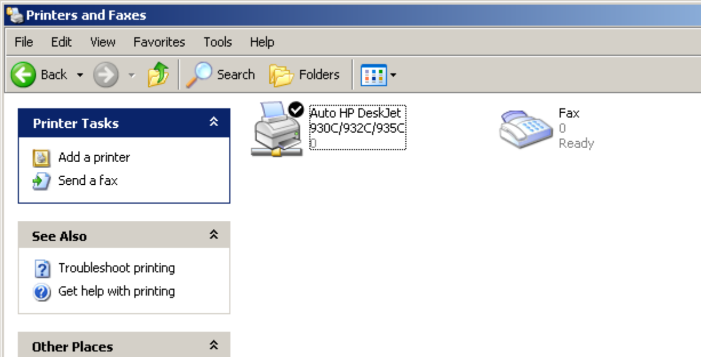
The following modems are installed:

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

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.



Auto HP DeskJet 930C/932C/935C
0

Fax
0
Ready

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

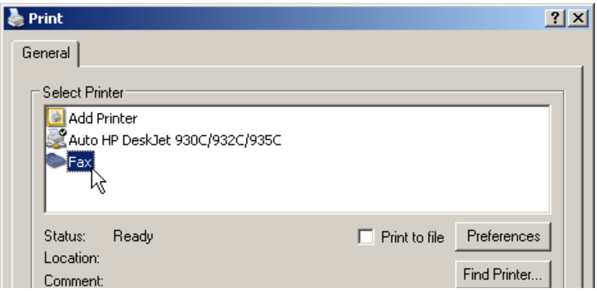
7.3 Sending a fax

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

7.3.1 Send a fax with any given office application

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

② Adjust the fax device as printer.



Status: Ready

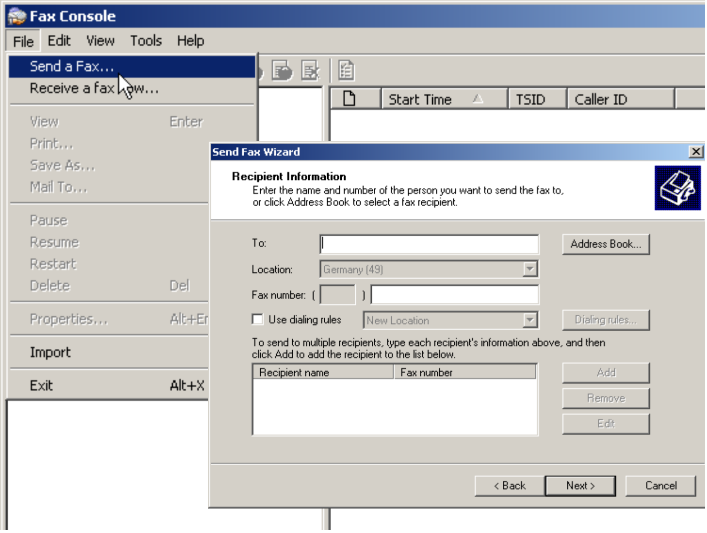
③ Click on OK. A wizard appears, that will guide you through the remaining sending process.

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 VPN has numerous security functions. You find in this chapter all information you need for an optimal protection.

8.1 The security settings wizard

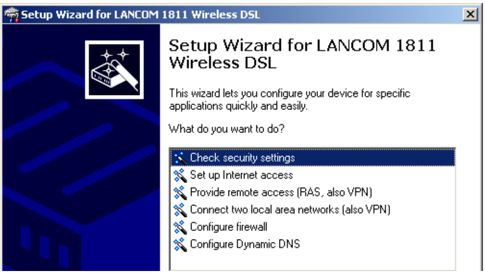
Access to the configuration of a device permits not only to read out critical information such as WEP key or Internet password. Rather, also the entire settings of the security functions (e.g. firewall) can be altered then. So an unauthorized configuration access endangers not only a single device, but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

Your LANCOM VPN 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.

8.1.1 Wizard for LANconfig

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



Setup Wizard for LANCOM 1811 Wireless DSL

Setup Wizard for LANCOM 1811 Wireless DSL

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

What do you want to do?

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

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

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

⑤ Now 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
- the MSN for remote configuration via ISDN
- parameters of configuration lock (number of failed log-in attempts and duration of the lock)

8.2 The firewall wizard

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

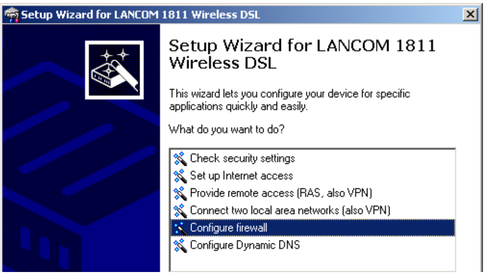
The firewall wizard assists you to create new firewall rules quickly and comfortably.

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

8.2.1 Wizard for LANconfig

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

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



Setup Wizard for LANCOM 1811 Wireless DSL

Setup Wizard for LANCOM 1811 Wireless DSL

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 **Configuring Firewall** and confirm your choice with **Next**.

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

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

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

8.2.2 Configuration under WEBconfig

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

8.3 The security checklist

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

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

- Have you assigned a password for the configuration?

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

- Have you permitted remote configuration?

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

- Have you provided the SNMP configuration with a password?

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

- Have you activated IP masquerading?

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

- Have you closed critical ports with filters?

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

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

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

- Is your saved LANCOM VPN configuration stored in a safe place?

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

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 access provider. During this process, the Online LED 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 the WAN. This cable must be connected to the Ethernet port of your broadband access device. The WAN link LED must light green indicating the physical connection.

Has the correct transfer protocol been selected?

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

You can monitor and correct the protocol settings under:

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

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.

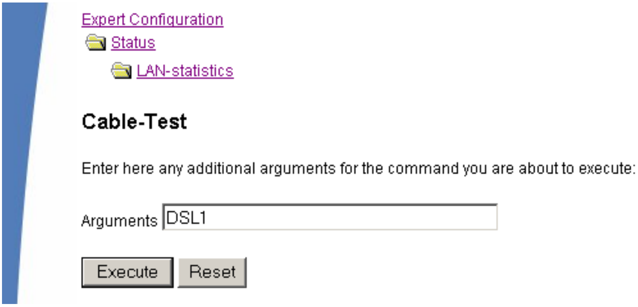
To resolve this issue, you can turn off the automatic time synchronization on the Windows XP computers under **Right mouse click on the time of day ▶ Properties ▶ Internet time**.

9.4 Cable testing

LANCOM 8011 VPN only

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**.

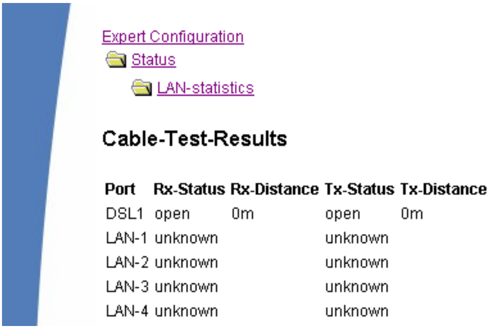


Cable-Test

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

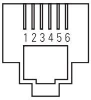
	LANCOM 7011 VPN	LANCOM 8011 VPN
Firewall	Stateful inspection, IP packet filter with port ranges; masquerading (NAT/PAT) of TCP, UDP, ICMP, FTP, PPTP, H.323, NetMeeting IRC and IPSec; DNS forwarding; inverse masquerading for IP services from the Intranet such as web server; support of 2 local networks; e.g. DMZ with own IP address range without NAT.	
Quality of Service	Dynamic bandwidth management with IP traffic-shaping/limiting with dynamic, absolute or per connection transfer limits or guaranteed minimum bandwidths, separated from send or receive site, TOS or DiffServ priority queuing, automatic packet size adoption incl. PMTU adjustment or fragmentation.	
Security	Intrusion detection (IP spoofing, login attempt, port scans), denial-of-service protection (fragmentation error, SYNflooding, automatic closing of ports/connections). DNS hitlist as well as wild card filter (URL blocking). High availability with ISDN dial backup for Internet access or VPN connections. Email alerting, SNMP traps and SYSLOG. PAP, CHAP and MS-CHAP as PPP authentification, password-protected configuration remote access per interface, access control list (IP, MAC and protocol filter) for configuration access and LANCAPI, ISDN remote access list. FirmSafe with two firmware versions for absolute secure software upgrades.	
VPN/IPSec	200 IPSec sessions parallel. Encryption methods: AES and 3-DES (for LANCOM 8011 VPN with hardware acceleration), Blowfish, CAST, MD-5 or SHA-1 Hashes IKE with Preshared Keys	
IPSec clients	LANCOM VPN client free of charge, for Windows 2000 and Windows XP (IPSec over PPTP; allocation of a local intranet address to the VPN client), 3rd-Party VPN clients with IKE Aggressive Mode.	
LANCOM Dynamic VPN	Connection to dynamic IP addresses: transferring of the dynamic IP address via ISDN B or D channel, IKE main mode. Connection from dynamic to static IP addresses: encrypted transferring of the dynamic IP address via ICMP or UDP packet, IKE Main Mode.	
Router modes, services and interfaces	IP, IPX and NetBIOS/IP multi protocol Router, HTTP and HTTPS Server (WEBconfig), DNS Client, DNS Server, DNS Relay, DNS Proxy, DHCP Client, DHCP Relay and DHCP Server incl. auto detection, Dynamic DNS Client, NTP Client, SNTP Server, NetBIOS/IP Proxy, N : N IP address mapping	
LAN protocols	IP: ARP, Proxy ARP, IP, ICMP, UDP, TCP, TFTP, RIP-1, RIP-2, DHCP, DNS, SNMP, HTTP, HTTPS, BOOTP, NTP/SNTP, NetBIOS, RADIUS, LANCAPI IPX: RIP, SAP, IPX and SPX watchdogs, NetBIOS watchdogs	
WAN protocols WAN protocols (ISDN)	(Ethernet) PPPoE, PPTP (PAC or PNS) and Plain Ethernet (with and without DHCP) D channel: 1TR6, DSS1 (Euro ISDN); B channel: PPP (asynchronous/synchronous), X.75, HDLC, ML PPP for channel bundling, V.110/GSM/HSCSD, CAPI 2.0 via LANCAPI, Stac data compression, optional leased line support for D64, D64S2, D64SY	

	LANCOM 7011 VPN	LANCOM 8011 VPN
Interfaces	WAN/LAN/DMZ: 10/100 Mbps Fast Ethernet ISDN (RJ-45): ISDN S0 Bus Serial config (8 pol. Mini DIN); COM port: 9600-11500 baud	WAN: 10/100 Mbps Fast Ethernet LAN/DMZ/Switch: 4 ports, 10/100 Mbps Fast Ethernet ISDN (RJ-45): ISDN S0 Bus Serial config (8 pol. Mini DIN) COM port: 9600-11500 baud
Data rate	IPSec encryption >7 MBit/s (Blowfish)	IPSec encryption >22 MBit/s (AES, 3-DES)
Management	Outband: command line interface, serial V.24/V.28 port (8 pol. mini-DIN) Inband: LANconfig (Windows configuration program), incl. setup wizard; LANmonitor (Windows status monitor); WEBconfig (integrated Web Server); telnet; SNMP management via SNMP V2; remote maintenance via ISDN or Dynamic DNS; RADIUS user management for dial in (PPP/PPTP and ISDN CLIP); browser (HTTP/HTTPS); VPN tunnel; WAN or LAN access separately activatable; simultaneous remote configuration and management of several devices with LANconfig/LAN monitor, supervisor alarm via SNMP traps, SYSLOG and email; scheduled events of all parameters and actions (e.g. firewall filter or connections) via CRON service. Tools: LANconfig (Windows program), LANmonitor (Windows status display), WEBconfig (integrated Web-server)	
Statistics	Very extensive Ethernet, IP and DNS statistics; SYSLOG error counter, connecting and online time as well as transfer quantity per station; accounting information exportable via LANmonitor and SYSLOG	
Diagnosis	Very extensive LOG and TRACE mechanism, integrated PING and TRACEROUTE.	
Hardware	Design without ventilator and with high MTBF, external power adapter (230 V) temperature 5–40 °C; humidity 0–80 %; non-condensing. robust plastic case 210 x 140 x 45 mm (B x H x T), ports on the back, prepared for wall mounting, Kensington-style lock	Design without rotating ports and with high MTBF, internal power supply (110-230 V) temperature 5–40 °C; humidity 0–80 %; non-condensing. Robust metal case, 19" 1HE (435 x 45 x 207 mm), connectors on the front, 19" rack mount bit
Approvals	EU (CE certification: EN 55022, EN 55024, EN 60950)	
Package contents	CD, printed manual English, German Power adapter, cable for outband interface, ISDN connection cable, LAN twisted pair cable (DMZ)	CD incl. firmware and tools (LANconfig, LANmonitor, LANCAPI), printed manual (English, German), power adapter, cable for outband interface, ISDN connection cable, 2 Ethernet cable (WAN, LAN)
Service	Warranty: 3 years Support: Via hotline and Internet	
Options	61501 19'' rack mount adapter 00789 ISDN leased line option (D64S, D64S2, D64SY) 61401 Service option (product replacement, 4 years warranty)*	61401 Service option (advanced replacement, 4 years warranty)* 61402 LANCOM VPN option 500 channels 61403 LANCOM VPN option 1000 channels 00789 ISDN leased line option (D64S, D64S2, D64SY)

10.2 Contact assignment

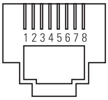
10.2.1 DSL interface

6-pin RJ45 socket

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

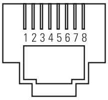
10.2.2 ISDN-S_0 interface

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	–	–

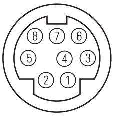
10.2.3 Ethernet interfaces 10/100Base-T

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

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

10.2.4 Configuration interface (Outband)

8-pin mini-DIN socket

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

10.3 CE declaration of conformity

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

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

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

11 Index