LANCOM 1620 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.

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

Trademarks

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

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

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

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

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

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

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

Wuerselen, March 2006

110424/0306

Preface

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

With the LANCOM 1620 VPN you have chosen a powerful router that possesses an integrated ADSL 2+ modem as well as an integrated 4-port switch. With this router you can simply and comfortably connect individual PCs or whole local networks to the high-speed Internet.

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.

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 three parts: the installation guide, the user manual and the reference manual.

You are now reading the user manual. It contains all information you need to start your device. 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)

- Backup Solutions
- LANCAPI
- Further server services (DHCP, DNS, charge management)

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.
ⓘ	Additional instructions which can be helpful, but are not required.

Contents

1 Introduction

The models of the type LANCOM 1620 VPN are fully-featured routers that can be used in combination with the integrated firewall for providing secure Internet access to a complete local network (LAN).

The integrated VPN option enables the LANCOM 1620 VPN to act as powerful Dynamic VPN gateway for external offices or mobile users.

1.1 How does ADSL and ADSL 2+ work?

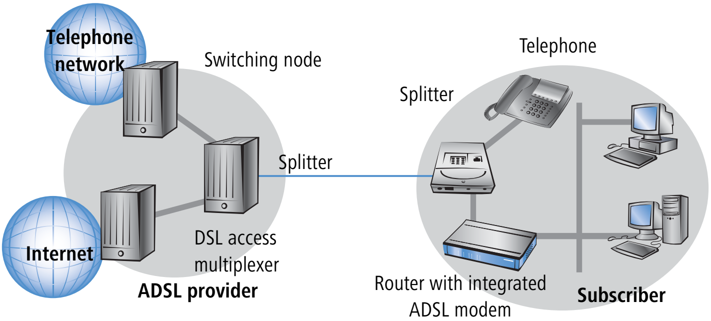
ADSL (Asymmetric Digital Subscriber Line) is currently the most common broadband Internet connection technology. Standard and almost ubiquitous telephone lines (analog or DSL) are the basis for DSL data transfer to the nearest telephone exchange. From here, the data is passed directly on to the Internet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

The asymmetric ADSL version of DSL was designed for applications in which the user receives high volumes of data but only transmits relatively small volumes, e.g. for accessing the world wide web (www). With an ADSL connection, a user can download at up to 8 Mbps (“downstream”) and upload at up to 800 Kbps (“upstream”). These maximum rates can be reduced as required by the ADSL provider.

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

With ADSL, all traditional telephony applications (telephone, fax, answering machine, PBX) can still be used without restrictions. So-called splitters make this possible. Splitters are devices that separate the telephone line's “voice frequencies” from the “data frequencies” and ensure that the signals are forwarded to the appropriate networks.

In the LANCOM 1620 VPN the ADSL/ADSL 2+ modem is integrated directly in the device. It can be directly connected to the splitter with the supplied cable.



ADSL can operate over modern ISDN telephone service as well as conventional analog service (POTS – **P**lain **O**ld **T**elephone **S**ervice). Both telephone systems are using different technical specifications.

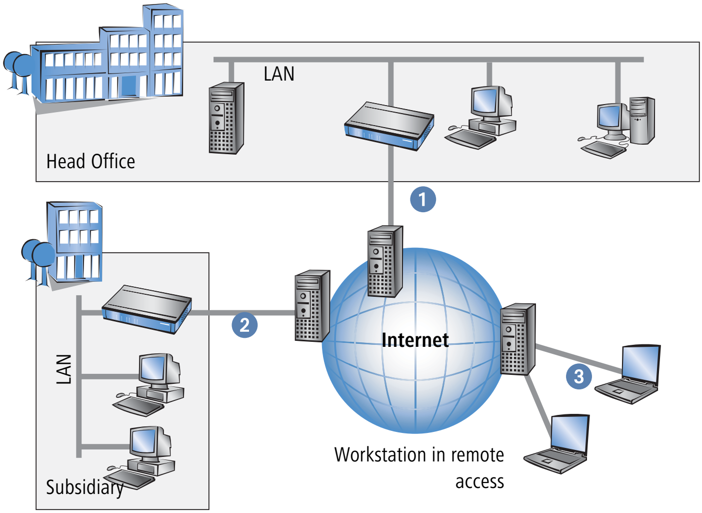
The LANCOM 1620 VPN can only be used with ADSL-over-POTS service.

1.2 Which use does VPN offer?

A VPN (**V**irtual **P**rivate **N**etwork) can be used to set up secure IP networks via Internet.

The model LANCOM 1620 VPN is equipped with 5 channels by default. The additional LANCOM VPN Option can extend VPN support to 25 active tunnels.

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.

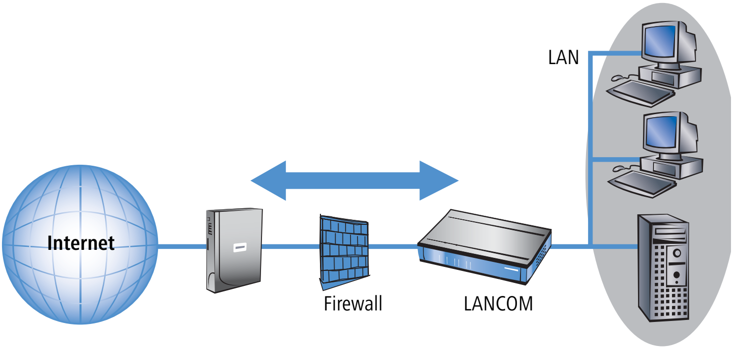
The physical connection no longer exists directly between two participants; instead, the participants rely on their connection to the Internet. The access technology used is not relevant in this case: ideally is the use of broadband technologies such as DSL (Digital Subscriber Line). But also a conventional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

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

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

1.3 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 Router. 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 Router 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 telephony or certain user groups.

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

1.4 What can your LANCOM Router do?

The following table shows the properties and functions of your device

	LANCOM 1620 VPN
Applications	
Internet access	✓
LAN to LAN coupling via VPN	✓
RAS server (via VPN)	✓
IP router	✓
IPX router, e.g. for coupling of Novell networks or dialling into Novell networks	✓
NetBIOS proxy for coupling of Microsoft peer-to-peer networks via ISDN	✓
DHCP and DNS server (for LAN and WAN)	✓
N:N mapping for coupling networks using the same IP address ranges	✓
Port-Mapping to set up LAN ports as additional WAN ports	✓
Policy-based routing for policy-based selection of target routes	✓
Load-balancing for bundling of multiple DSL channels	2 channels
WAN connections	
Integrated ADSL modem (ADSL2+ ready)	✓

	LANCOM 1620 VPN
Port for external modem, analogue or GSM (requires LANCOM modem adapter kit)	✓
LAN connection	
4 individual Fast Ethernet LAN ports, switchable separately, e.g. as LAN switch or separate DMZ ports, auto crossover.	✓
Security functions	
5 integrated VPN tunnels for protection of network connections	✓
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.	✓
Serial configuration interface	✓
FirmSafe with firmware versions for absolutely secure software upgrades	✓
Optional software extensions	
LANCOM VPN Option with 25 active tunnels for protection of network couplings	✓
Optional hardware extensions	
LANCOM Modem Adapter Kit for connection of analog or GSM modems to the serial interface	✓

2 Installation

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

2.1 Package contents

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

	LANCOM 1620 VPN
Power adapter	✓
LAN connector cable (green plugs)	✓
ADSL connector cable (transparent plugs)	✓
Connector cable for the configuration interface	✓
LANCOM CD	✓
Printed documentation	✓

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

2.2 System preconditions

Computers that connect to a LANCOM Router 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.

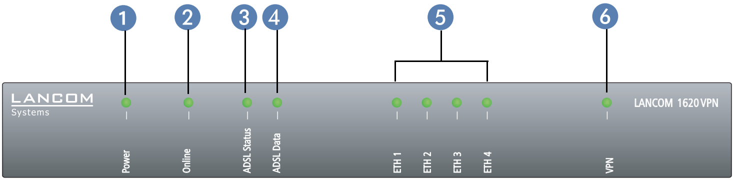
2.3 Introducing the LANCOM Router

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

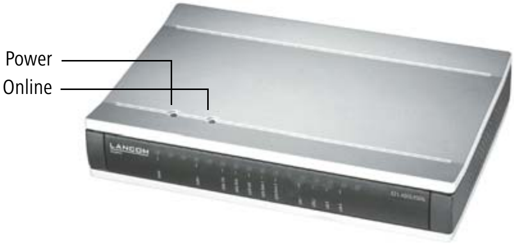
While the information in this section is useful for the installation of the device, it is not absolutely essential. You may therefore skip this section for the time being and go straight forward to 'Hardware installation' → page 19.

2.3.1 Status displays

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



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.

① Power

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

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

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

② Online

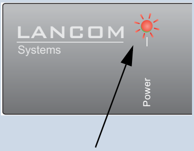
The Online LED indicates the overall status of all WAN ports:

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

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**.

3 ADSL status

Connection status of the ADSL link:

off		not connected
green	blinking	Initialisation
green	constantly on	Synchronisation succsesful
red	flickering	Error (CRC error, framing error etc.)
red	constantly on	Synchronisation failed
red/ orange	blinking	Hardware error

4 ADSL data

Data traffic via the ADSL link:

off		no logic connection
green	flashing	Establishing first connection
green	inverse flashing	Establishing further connection
green	constantly on	Connection(s) established
green	flickering	Data traffic (send or receive)

5 ETH 1 to ETH 4

Status of the four LAN ports in the integrated switch:

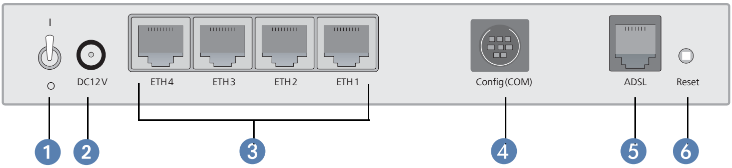
off		No network device connected
green	constantly on	Connection to network device operational, no data traffic
green	flickering	Data traffic
red	flickering	Collision of packets

6 VPN

Status of a VPN connection.

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

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



1 Voltage switch

2 Connection for the included power adapter

3 Switch with four 10/100Base-Tx connections

4 Serial configuration port

5 ADSL port

6 Reset switch

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

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

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

2.4 Hardware installation

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

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

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

You should never have more than one unconfigured LANCOM Router in a network segment at any given time. All unconfigured LANCOM Router devices use the same IP address (with the final digits '254'), which would result in an address conflict. To avoid problems, always configure multiple LANCOM Router devices one at a time, immediately assigning each device a unique IP address (one that does not end with '254').821/1621 only

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

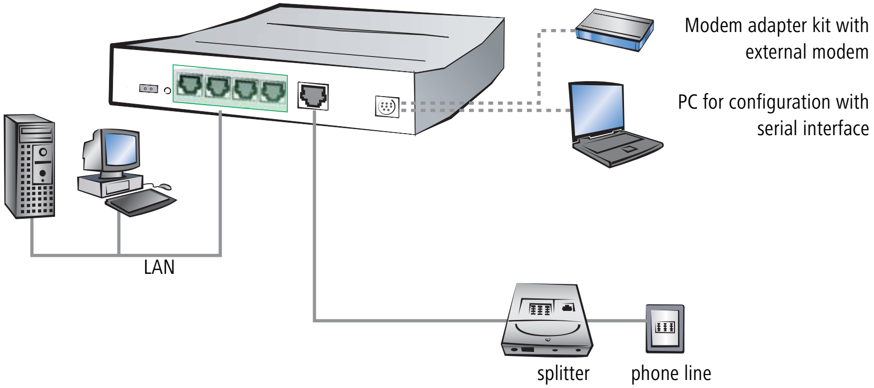
③ **Configuration port** – you may optionally connect the router directly to the serial port (RS-232, V.24) of a PC. Use the cable supplied for this purpose. Connect the configuration port ❹ with a free serial port of the PC.

④ Alternatively you may connect an external modem (analogue or GSM) to the serial port using the LANCOM modem adapter kit, if you would like to make use of an additional WAN line for remote maintenance, backup connections or dynamic VPN.

⑤ **Connect to power** – Connect socket ❷ of the unit to a power supply using the included power adapter.

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

⑥ **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.


Modem adapter kit with external modem
PC for configuration with serial interface
LAN
splitter
phone line

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

2.5 Software installation

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

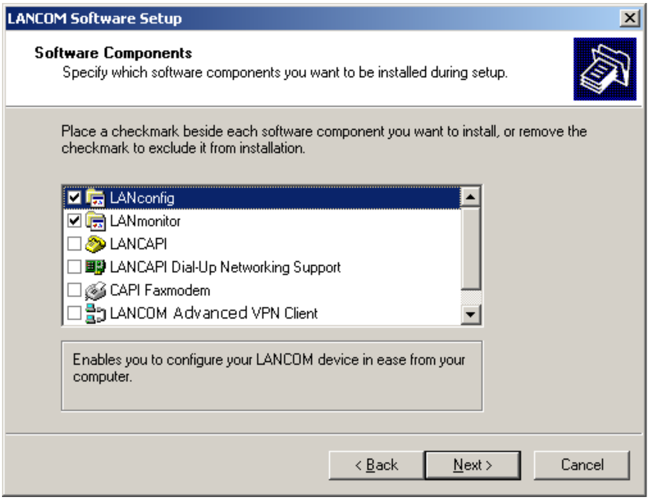
You may skip this section if you use your LANCOM Router exclusively with computers running operating systems other than Windows.

2.5.1 Starting LANCOM setup

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

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

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



LANCOM Software Setup

Software Components

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

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

☑ LANconfig

☑ LANmonitor

□ LANCAPI

□ LANCAPI Dial-Up Networking Support

□ CAPI Faxmodem

□ LANCOM Advanced VPN Client

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

2.5.2 Which software should you install?

- **LANconfig** is the configuration program for all LANCOM routers and LANCOM Router base stations. WEBconfig can be used alternatively or in addition via a web browser.
- **LANmonitor** lets you monitor on a Windows PC all LANCOM routers and LANCOM Router base stations
- With **LANCOM Online Documentation,** you can copy the documentation files on your PC.

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

3 Basic configuration

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

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

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

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

3.1 Which information is necessary?

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

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

3.1.1 TCP/IP settings

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

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

New LAN—fully automatic configuration possible

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

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

Fully automatic TCP/IP configuration will not be available when integrating the LANCOM Router in an existing TCP/IP LAN. In this case, continue with the section ʼInformation required for manual TCP/IP configurationʼ.

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

Configure manually nevertheless?

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

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

Information required for manual TCP/IP configuration

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

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

- **Enable DHCP server?**
  Disable the DHCP server function in the LANCOM Router 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 Router protects the configuration against unauthorized access. The configuration of the router contains a considerable amount of sensitive information such as your Internet access information. We therefore strongly recommend protecting it with a password.

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

3.1.3 Connect charge protection

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

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

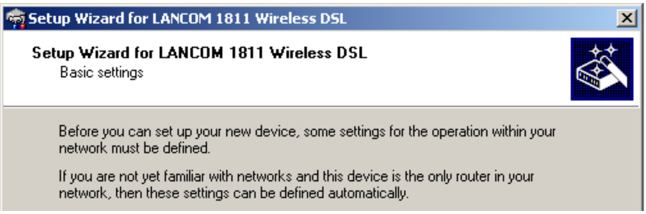
Any budget can be deactivated by entering the value '0.'

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

3.2 Instructions for LANconfig

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

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



Setup Wizard for LANCOM 1811 Wireless DSL
Basic settings

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

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

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

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

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

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

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

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

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

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

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

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

⑧ Complete the configuration with **Finish**.

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

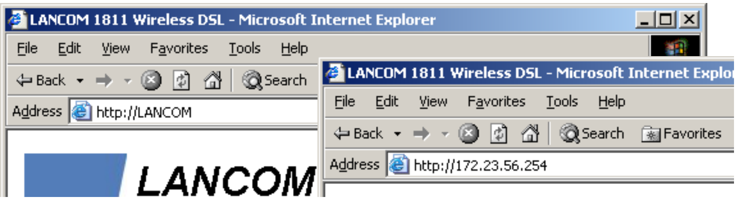
3.3 Instructions for WEBconfig

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

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

Network without DHCP server

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

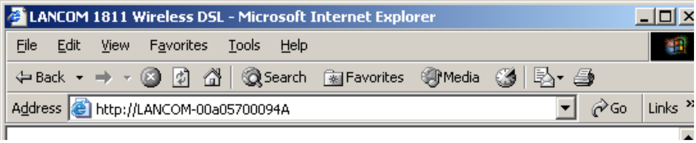

LANCOM 1811 Wireless DSL - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search
Address http://LANCOM
LANCOM
LANCOM 1811 Wireless DSL - Microsoft Internet Explo
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.23.56.254

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

Network with DHCP server

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

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


LANCOM 1811 Wireless DSL - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://LANCOM-00a05700094A
Go Links

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

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

Starting the wizards in WEBconfig

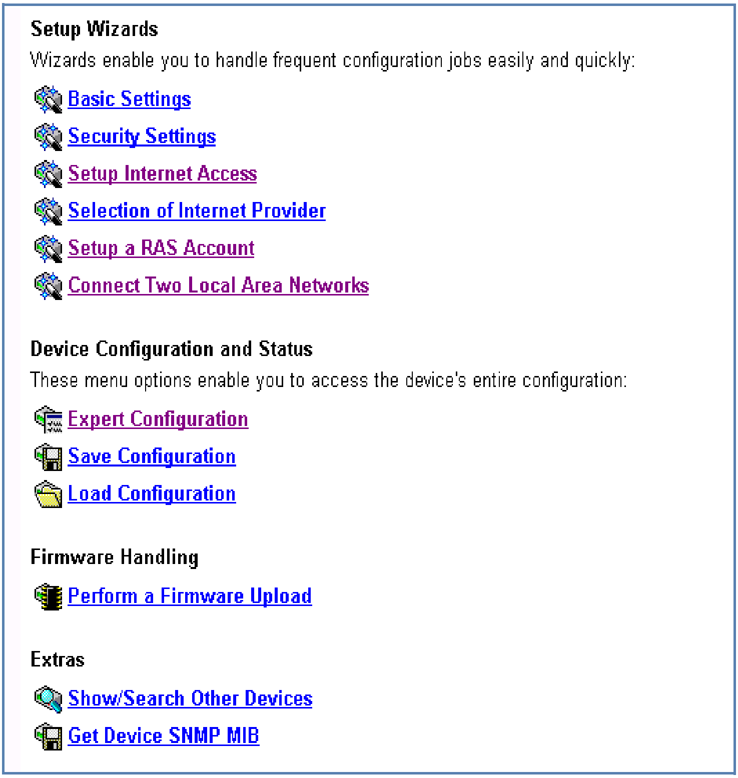
① Start your web browser (e.g. Internet Explorer, Netscape Navigator, Opera) and call the LANCOM Router there:

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

(or with a name as discribed above)

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

The WEBconfig main menu will be displayed:



Setup Wizards

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

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

Device Configuration and Status

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

- Expert Configuration
- Save Configuration
- Load Configuration

Firmware Handling

- Perform a Firmware Upload

Extras

- Show/Search Other Devices
- Get Device SNMP MIB

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

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

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

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

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

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

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

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

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

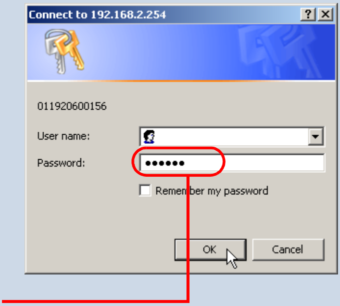
⑥ Connect charge protection can limit the cost of DSL connections to a predetermined amount if desired. Confirm your choice with **Apply**.

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

Entering the password in the web browser

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

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



Connect to 192.168.2.254

011920600156

User name:

Password: ••••••

□ Remember my password

Entering the configuration password

3.4 TCP/IP settings to workstation PCs

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

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

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

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

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

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

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

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

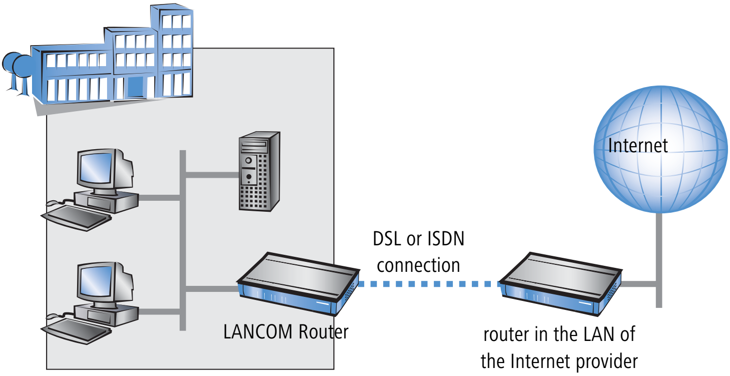
- **Manual IP address assignment**

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

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

4 Setting up Internet access

All computers in the LAN can take advantage of the central Internet access of the LANCOM Router. The connection to the Internet provider can be established via any WAN connection. 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.

- **ADSL**
  - □ Protocol: PPP (PPPoA), PPPoE, Plain IP (IPoA) or Plain Ethernet
  - □ ATM parameter: VPI (Virtual Path Identifier) and VCI (Virtual Circuit Identifier), VC or LLC-based Multiplexing
  - □ Additionally for plain IP (IPoA) and Plain Ethernet: a dedicated 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.

Additional connection options

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

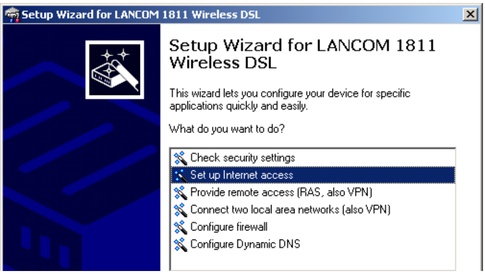
- Time-based billing or flat rate – select the accounting model used by your Internet provider.
  - □ When using time-based billing, you can set the LANCOM Router to automatically close existing connections if no data has been transferred within a specified time (the so-called idle time).

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

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

4.1 Instructions for LANconfig

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



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?

Setup Wizard for LANCOM 1811 Wireless DSL
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**.

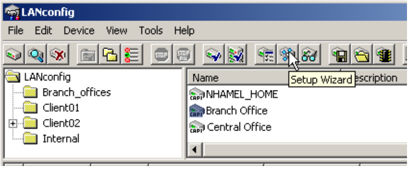
③ In the following window select your country and your Internet provider if possible, and enter your access information.

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 Router, two local networks are linked. While 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.

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

! Using different methods LANCOM routers permit the establishment of VPN connections between devices with dynamic IP addresses. Please refer to the LCOS reference manual for more information and configuration examples.

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.

i The following instructions will assume that LANCOM Router 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.

Security aspects

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

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

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.

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

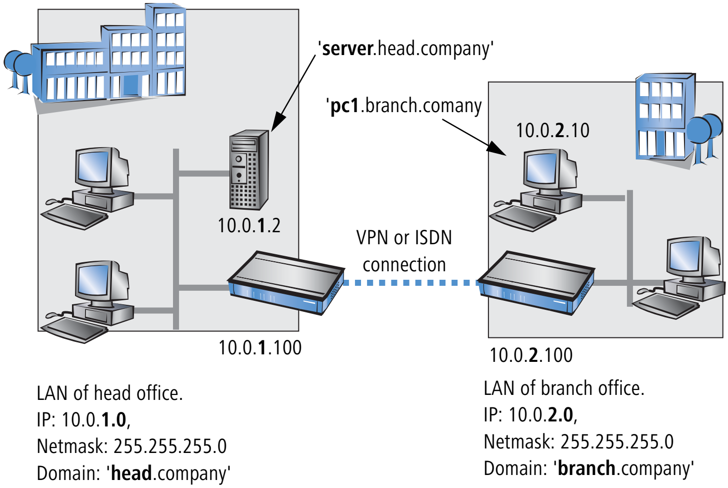
Entry	Gateway 1		Gateway 2
Type of the local IP address	static/dynamic	⤨	static/dynamic
Type of the remote IP address	static/dynamic		static/dynamic
Name of the local device	'HEAD'	⤨	'BRANCH'
Name of the remote station	'BRANCH'		'HEAD'
Password for secure transmission of the IP address	'Password'	↔	'Password'
Shared secret for encryption	'Secret'	↔	'Secret'
IP address of remote station	'10.0.2.100'		'10.0.1.100'
IP network address of the remote network	'10.0.2.0'		'10.0.1.0'
Netmask of the remote network	255.255.255.0		255.255.255.0
Domain name of the remote network	'head'		'branch'
Hide local stations for access to remote network (Extranet VPN)?	yes/no		yes/no
NetBIOS routing for access to remote network?	yes/no		yes/no
Name of remote workgroup (NetBIOS only)	'workgroup1'		'workgroup2'

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

- The **name of the remote station** is needed for its identification.
- The **Shared Secret** is the central password for security within the VPN. The exact same password has to be entered on both sides

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 Router reference manual.

Extranet VPN

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

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

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

5.1.3 Settings for the IPX router

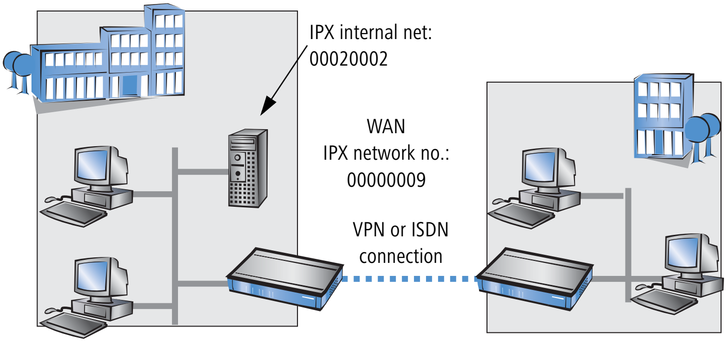
The coupling of IPX networks via VPN cannot be configured using the wizard. It can only be set up in the expert configuration. For details, please see the reference manual.

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

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

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

The three required network numbers are designated as “External Network Numbers” by the IPX conventions. Like IP network addresses, the apply to an entire LAN segment. On the other hand, internal IPX numbers are used to address specific Novell servers in the LAN. All three specified network num-



bers 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

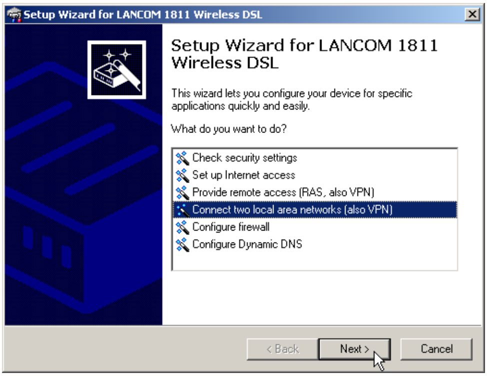
NetBIOS routing can be set up quickly: All that is required in addition to the information for the TCP/IP protocol used is the name of a Windows workgroup from in the router's own LAN.

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?

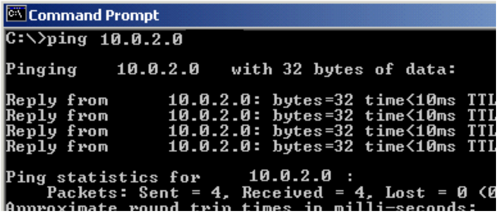
② The wizard will return a message to indicate that it has all the information it needs. Close the wizard with **Finish**.

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

Ping – quick testing for TCP/IP connections

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

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



Command Prompt

```
C:\>ping 10.0.2.0

Pinging    10.0.2.0    with 32 bytes of data:

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

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

5.3 Instructions for WEBconfig

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

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

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

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

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

6 Providing dial-up access

Your LANCOM Router supports dial-up connections to permit individual computers full access to your network. This service is also known as RAS (Remote Access Service). The RAS access is established over a specially secured connection through the public Internet.

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

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

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.

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

Configuration parameter
User name
Password
Shared secret for encryption
Hide local stations for access to remote network (Extranet VPN)?
TCP/IP routing for access to remote network
IPX routing for access to remote network

EN

Configuration parameter
IP addresses for the dial-up PCs: static or dynamic by address range (IP address pool)
NetBIOS routing for access to remote network?
Name of remote workgroup (NetBIOS only)

Notes to the individual values:

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

Please refer to chapter "Linking two networks" on page 95 for advice about the other values required for the installation of a RAS access.

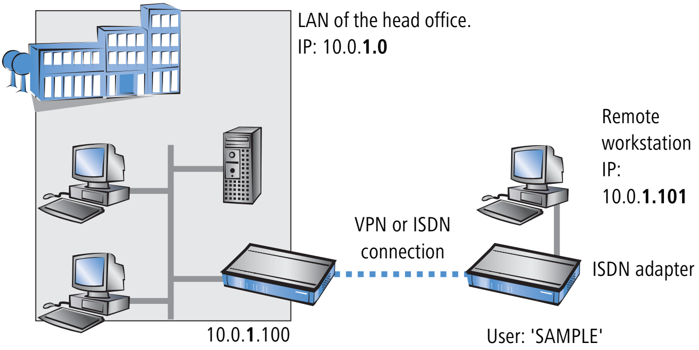
The ISDN calling line identity (CLI)

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

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

6.1.2 Settings for TCP/IP

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



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

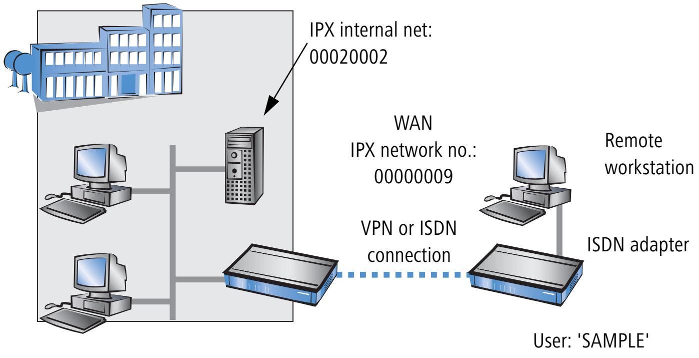
During both manual and automatic IP address assignment, please ensure that only free addresses from the address range of your local network are used. In our example, the IP address '10.0.1.101' will be assigned to the PC when connecting.

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

6.1.3 Settings for IPX

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

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



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

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

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

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

6.1.4 Settings for NetBIOS routing

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

The connection is not established automatically. The RAS user must manually establish a connection to the LANCOM Router via Dial-Up Networking first. When connected, they can search for and access computers in the remote network (via **Find** ▶ **Computer**s, not through the Network Neighbourhood).

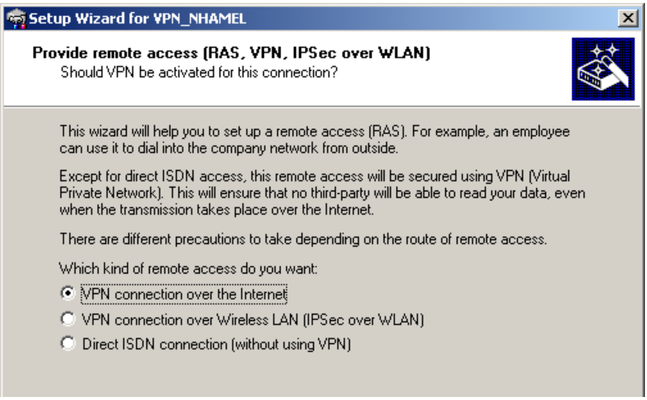
6.2 Settings for the dial-in computer

For dialing into a network via VPN a workstation requires:

- an Internet access
- a VPN client

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

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



Setup Wizard for VPN_NHAMEL

Provide remote access (RAS, VPN, IPSec over WLAN)

Should VPN be activated for this connection?

This wizard will help you to set up a remote access (RAS). For example, an employee can use it to dial into the company network from outside.

Except for direct ISDN access, this remote access will be secured using VPN (Virtual Private Network). This will ensure that no third-party will be able to read your data, even when the transmission takes place over the Internet.

There are different precautions to take depending on the route of remote access.

Which kind of remote access do you want:

● VPN connection over the Internet

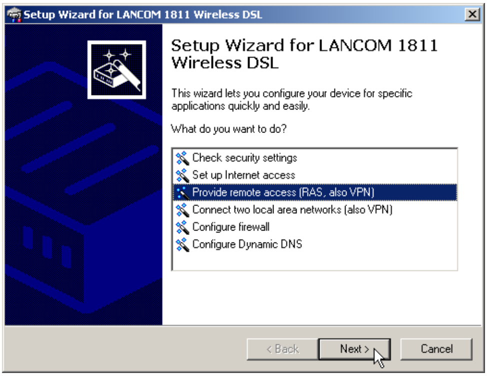
○ VPN connection over Wireless LAN (IPSec over WLAN)

○ Direct ISDN connection (without using VPN)

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

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

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” on page 102).

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” on page 102).

7 Security settings

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

7.1 The security settings wizard

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

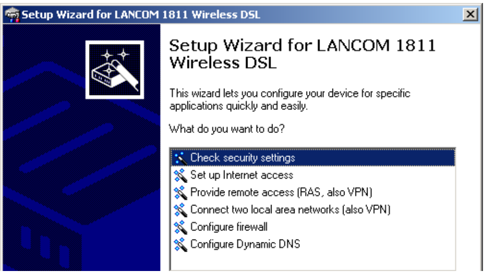
Your LANCOM Router has a password protection for the configuration access. This protection is already activated during the basic configuration by entering a password.

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

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

7.1.1 Wizard for LANconfig

① Mark your LANCOM Router 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 **Control Security Settings** and confirm your choice with **Next**.

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

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

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

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

7.1.2 Wizard for WEBconfig

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

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

7.2 The firewall wizard

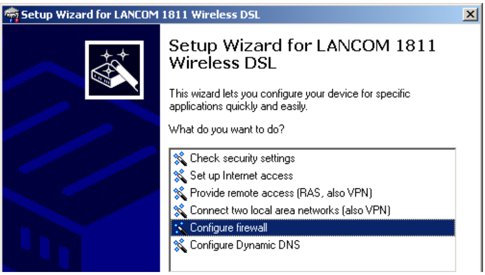
The LANCOM Router incorporates an effective protection of your LAN when accessing the Internet by its Stateful Inspection firewall and its firewall filters. Basic idea of the Stateful Inspection firewall is that only self-initiated data transfer is considered allowable. All unasked accesses, which were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

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

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

7.2.1 Wizard for LANconfig

① Mark your LANCOM Router 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 **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**.

7.2.2 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.**

7.3 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 box for entering the password is located in LANconfig in the 'Management' configuration area on the 'Security' tab. It is particularly advisable to assign a password to the configuration if you want to allow remote configuration.

- **Have you permitted remote configuration?**

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

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

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

- **Have you activated the Firewall?**

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

- **Do you make use of a ’Deny All’ Firewall strategy?**

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

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

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

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

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

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

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

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

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

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

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

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

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

8 Troubleshooting

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

8.1 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

8.2 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).

8.3 Unwanted connections under Windows XP

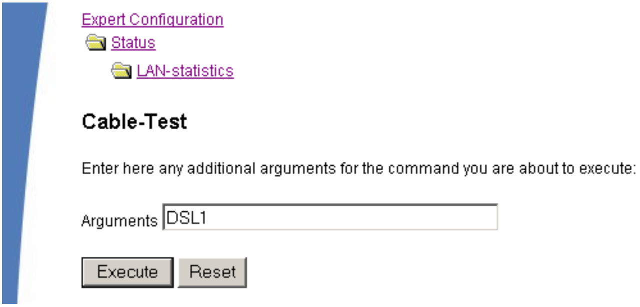
Windows XP computers attempt to compare their clocks with a timeserver on the Internet at start-up. This is why when a Windows XP in the WLAN is started, a connection to the Internet is established by the LANCOM.

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**.

8.4 Cable testing

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

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



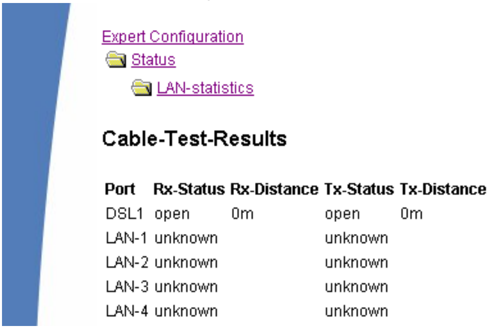
Expert Configuration
Status
LAN-statistics

Cable-Test

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

Arguments 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.



Expert Configuration
Status
LAN-statistics

Cable-Test-Results

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

The following results can occur:

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

9 Appendix

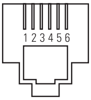
9.1 Performance data and specifications

		LANCOM 1620 VPN
Connections	Ethernet LAN	4 x RJ-45 Ethernet IEEE 802.3 (Switch), 10/100Base-T-Autosensing, Node/Hub-Autodetection
	ADSL	ADSL over POTS as per ITU G.992.1 Annex A, ANSI T1.413, ITU G992.3 and ITU 992.5 Annex A
	Outband	serial V.24/V.28 port (8 pol. mini DIN), in combination with LANCOM modem adapter kit suited for connection of external analogue or GSM modems
	Power supply	12V over external power adapter
Housing		210 x 143 x 45 mm (W x H x D), rugged plastic case, connectors on the rear side, stackable, provision for wall mounting
Standards		EU (CE certification: EN 55022, EN 55024, EN 60950)
Environment / temperature range		Temperature range 5 °C to + 40 °C at 80 % max. humidity (non condensing)
Options		■ LANCOM VPN Option 25 channels (max. 25 simultaneous connections, 50 connections configurable) for VPN in WAN (Art. no.60083)
Accessories		■ LANCOM Modem Adapter Kit for connecting modems (analogue or GSM) to the serial configuration interface (Art. no. 110288) ■ LANCOM Advanced VPN Client (Art. no. 61600) ■ LANCOM Advanced VPN Client (10 Bulk) (Art. no. 61601) ■ LANCOM Advanced VPN Client (25 Bulk) (Art. no. 61602) ■ LANCOM Rack Mount Kit (Art. no. 61501)

9.2 Contact assignment

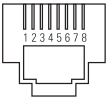
9.2.1 ADSL interface

6-pin RJ45 socket

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

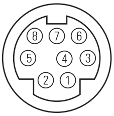
9.2.2 Ethernet interfaces 10/100Base-T

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	–

9.2.3 Configuration interface (Outband)

8-pin mini-DIN socket

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

9.3 Declaration of conformity

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

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

Index

EN