LANCOM 1722 VoIP
LANCOM 1723 VoIP
LANCOM 1724 VoIP
LANCOM 1823 VoIP

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

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

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

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

Trademarks

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

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

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

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

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

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

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom.eu

Wuerselen, September 2007

110570/0907

Preface

Thank you for your confidence in us!

LANCOM VoIP Routers provide the comprehensive functions of an access router, professional firewall and high-quality VPN gateway and WLAN access point in a single, compact device. They thus combine investment protection and cost savings as a reliable voice over IP solution for small and mid-sized enterprises, home and branch offices.

LANCOM 1823 VoIP only

LANCOM Wireless Routers and LANCOM Access Points can be operated either as self-sufficient Access Points with their own configuration (WLAN modules in "Access Point mode“) or as components in a WLAN infrastructure, which is controlled from a central WLAN-Controller ("managed mode"). Please observe the corresponding notices to this in this documentation.

Standard features of the different models are integrated interfaces for ADSL and ISDN, and a LAN switch. LANCOM 1723 VoIP additionally provides interfaces for analog telephone systems. Along with the analog interfaces, LANCOM 1823 VoIP also provides professional WLAN technology.

In addition to data communications functions, VoIP support transforms LANCOM Routers into fully fledged, integrated VoIP communications solutions. Along with Quality of Service functions which are optimized for VoIP, the LANCOM VoIP Routers offer the full range of options required for voice communications over data networks and the step-by-step, cost-effective and simple migration from existing telecommunications systems to corporate Voice over IP. The particular characteristics of LANCOM VoIP Routers include, among others:

- PBX functions for analog, ISDN and SIP subscribers
- Site connectivity of data and voice via VPN
- SIP proxy and registrar for registration with providers and upstream VoIP PBXs
- SIP trunking for multiple parallel lines with extension numbers over a single account with a switchboard number.
- SIP gateway with transparent transition between SIP and ISDN/analog telephony
- SIP remote gateway provides local SIP, ISDN or analog lines to remote IP-PBXs.

EN

- Intelligent call routing and number translation
- Support of point-to-point and point-to-multipoint connections to the ISDN network
- Multiple configurable ISDN interfaces (NT/TE), some with life-line support and power relay to the internal ISDN bus
- WLAN compliant to the standards IEEE 802.11a/h or IEEE 802.11b/g

Information about your model's functionality in detail is available from the table 'Just what can your LANCOM VoIP Router do?'.

LANCOM products undergo continuous development. For precise information about their features and for the latest version of the LCOS operating system, please visit the LANCOM website.

Model variants

This documentation is to be used for different models:

- LANCOM 1722 VoIP
- LANCOM 1723 VoIP
- LANCOM 1724 VoIP
- LANCOM 1823 VoIP

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 VoIP Router.

Security settings

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

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

User manual and reference manual

The documentation of your device consists of the following parts:

- Installation guide
- User manual
- PBX Functions manual
- Reference manual

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

The PBX Functions manual gives you detailed step-by-step instructions on commissioning a LANCOM VoIP Router as a PBX (private branch exchange) for a single location. Also described are the main operating instructions for users, and how to connect terminal equipment.

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

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

This documentation was created by …

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

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

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

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

Contents

1 Introduction **11**

1.1 How do ADSL and ADSL 2+ work? 11

1.2 What does VPN offer? 13

1.3 Firewall 14

1.4 Voice over IP 15

1.4.1 Example Applications 15

1.4.2 The central position of the LANCOM VoIP Router 21

1.4.3 VoIP characteristics of the LANCOM VoIP Routers 24

1.5 Just what can your LANCOM do? 26

2 Installation **33**

2.1 Package content 33

2.2 System requirements 34

2.2.1 Configuring the LANCOM devices 34

2.2.2 Operating access points in managed mode 34

2.3 Introducing the LANCOM Router 34

2.3.1 Status displays 34

2.3.2 Device connectors 41

2.4 Hardware installation 44

2.5 Configuring the ISDN and analog interfaces 46

2.6 Software installation 47

2.6.1 Starting Software Setup 47

2.6.2 Which software should I install? 49

Contents

EN

3 Basic configuration 50

3.1 Which information is necessary? 50
3.1.1 TCP/IP settings 50
3.1.2 Configuration protection 52
3.1.3 Settings for the Wireless LAN 52
3.1.4 Connect charge protection 53
3.2 Instructions for LANconfig 54
3.3 Instructions for WEBconfig 55
3.4 TCP/IP settings to workstation PCs 59

4 Setting up Internet access 61

4.1 Instructions for LANconfig 62
4.2 Instructions for WEBconfig 63

5 Configuring the VoIP functions 64

6 Linking two networks 65

6.1 What information is necessary? 66
6.1.1 General information 66
6.1.2 Settings for the TCP/IP router 68
6.1.3 Settings for the IPX router 69
6.1.4 Settings for NetBIOS routing 70
6.2 Instructions for LANconfig 71
6.3 1-Click-VPN for networks (site-to-site) 72
6.4 Instructions for WEBconfig 73

7 Providing dial-in access **74**

7.1 Which information is required? 74
7.1.1 General information 75
7.1.2 Settings for TCP/IP 76
7.1.3 Settings for IPX 77
7.1.4 Settings for NetBIOS routing 77

7.2 Settings for the dial-in computer 78
7.2.1 Dial-up via VPN 78
7.2.2 Dial-up via ISDN 78

7.3 Instructions for LANconfig 78

7.4 1-Click-VPN for LANCOM Advanced VPN Client 79

7.5 Instructions for WEBconfig 80

8 Point-to-point connections **81**

8.1 Antenna alignment for P2P operations 82

8.2 Configuration 84

8.3 Access points in relay mode 86

8.4 Security for point-to-point connections 86
8.4.1 Encryption with 802.11i/WPA 86
8.4.2 LEPS for P2P connections 88

9 Sending faxes with LANCAPI **89**

9.1 Installation of the LANCOM CAPI Faxmodem 90

9.2 Installation of the MS Windows fax service 91

9.3 Sending a fax 91
9.3.1 Send a fax with any given office application 91
9.3.2 Send a fax with the MS Windows fax service 92

10 Options and accessories **93**

10.1 Optional LANCOM WLAN antennas 93
10.1.1 Antenna Diversity 93
10.1.2 Installation of AirLancer Extender antennas 94

10.2 LANCOM Public Spot Option 94

EN

11 Security settings 96

11.1 The security settings wizard 96
11.1.1 Wizard for LANconfig 96
11.1.2 Wizard for WEBconfig 97
11.2 The firewall wizard 97
11.2.1 Wizard for LANconfig 98
11.2.2 Configuration under WEBconfig 98
11.3 Background WLAN Scanning 98
11.4 The security checklist 101

12 Configuring the ISDN and analog interfaces in detail 104

12.1 ISDN interface in NT or TE mode 104
12.2 Bus termination, life-line support and power supply 105
12.3 Protocol setting 107
12.4 ISDN connection timing 108

13 Troubleshooting 110

13.1 No DSL connection is established 110
13.2 DSL data transfer is slow 110
13.3 Unwanted connections under Windows XP 111

14 Appendix 112

14.1 Performance data and specifications 112
14.2 Contact assignment 115
14.2.1 ADSL interface 115
14.2.2 ISDN interface ☒ 115
14.2.3 ISDN interface ☎ 116
14.2.4 ISDN/Analog interface ☒ 116
14.2.5 Analog interface ☎ 117
14.2.6 Ethernet interface 10/100Base-TX 117
14.2.7 Configuration interface (Outband) 118
14.3 Declaration of conformity 118

EN

1 Introduction

LANCOM VoIP Routers are fully functional routers with an integrated firewall to provide local networks with secure access to the Internet.

With the VPN option included, these devices work as powerful Dynamic VPN gateways for external locations or mobile users.

Along with the ADSL connection, these devices also feature ISDN connections, and some feature analog telephone connections. An ISDN line can be used to backup the WAN connection, for remote management of the router, as a basis for office communications via LANCAPI, and for establishing Dynamic VPN connections to external locations that use dynamic IP addresses.

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

Nur LANCOM 1823 VoIP

LANCOM Wireless Routers and LANCOM Access Points can be operated either as self-sufficient access points with their own configuration (WLAN modules in "Access Point mode") or as components in a WLAN infrastructure, which is controlled from a central WLAN Controller ("managed mode"). Please observe the corresponding notices in this documentation.

1.1 How do ADSL and ADSL 2+ work?

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

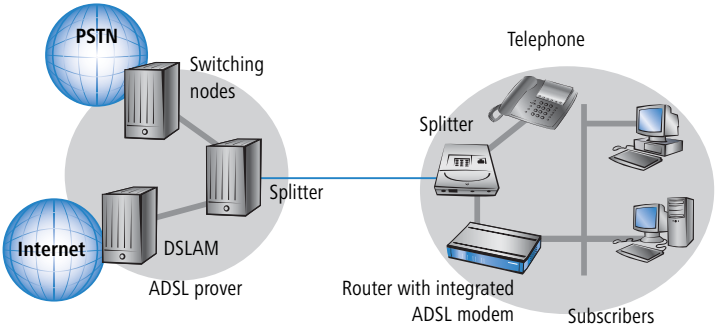
The asymmetric DSL variant ADSL was developed for applications where users receive large amounts of data but transmit only small amounts, such as when surfing in the WWW. ADSL subscribers can receive data at up to 8 Mbps ("downstream") and transmit at up to 800 kbps ("upstream"). ADSL providers are able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

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

shake routines during connection establishment ensure that the standards ADSL, ADSL 2 and ADSL 2+ are intercompatible.

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

The LANCOM VoIP Router features an integrated modem for ADSL/ADSL 2+. It can be directly connected to the splitter with the supplied cable.



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

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

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

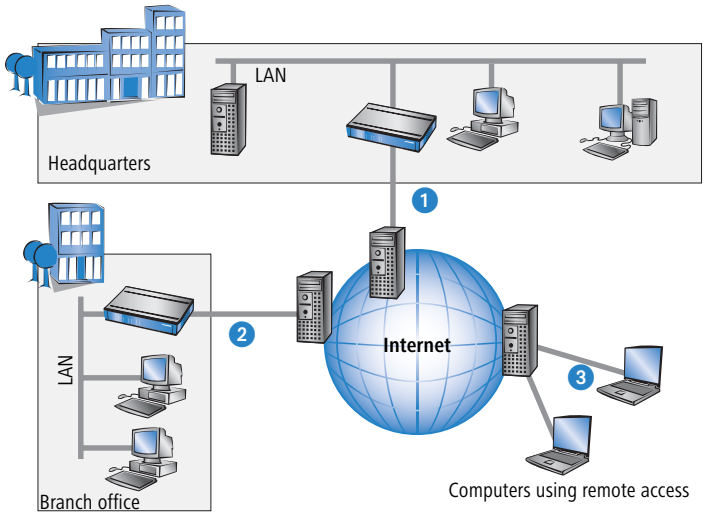
There are even ADSL-over-ISDN connections which are not combined with an ISDN connection, but with a standard analog telephone connection instead.

In Germany, for instance, all T-DSL connections from Deutsche Telekom AG are implemented as ADSL-over-ISDN connections.

1.2 What does VPN offer?

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

The 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.

EN

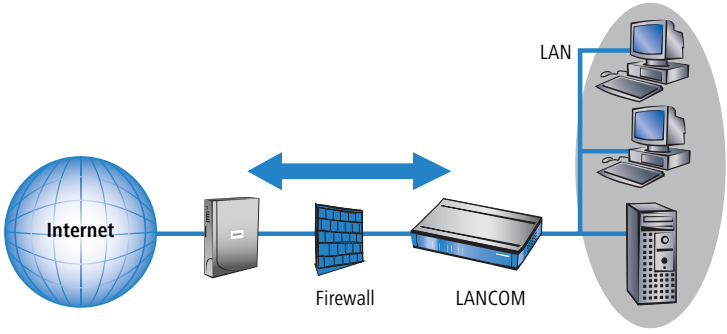
The physical connection no longer exists directly between two participants; instead, the participants rely on their connection to the Internet. The access technology used is not relevant in this case: Broadband technology such as DSL (Digital Subscriber Line) is ideal. A conventional ISDN line can be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

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

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

1.3 Firewall

The integrated stateful-inspection firewall is an effective barrier to unwanted data traffic as it only permits the entry of data as a response to outgoing data traffic. The IP masquerading function in the router conceals LAN workstations accessing the Internet behind a single public IP address. The true identities (IP addresses) of the individual workstations remain masked. Router firewall filters allow the blocking of individual IP addresses, protocols and ports. MAC address filters also offer effective control over the access of LAN workstations to the IP routing functions in the device.



Further important features in the firewall are:

- Intrusion detection

  Attempts to break in to the local network or central firewall are recognized, repelled and recorded by the Intrusion Detection System (IDS) in the LANCOM. There is a choice of alarms including in-device logging, e-mail messaging, SNMP traps or SYSLOG alarms.

- Denial-of-Service protection

  In addition to conventional break-ins, attacks from the Internet may aim to block the availability of individual services. For this reason, the LANCOM router is equipped with appropriate security mechanisms to recognize popular hacker attacks and guarantee router functionality.

- Quality of Service/traffic management

  The term Quality of Service (QoS) embraces a range of functions in your LANCOM. QoS functions consider the powerful classification methods used by firewalls (e.g. restriction to subnets, individual workstations or certain services). These enable Quality of Service to be very precisely controlled.

  By guaranteeing a minimum bandwidth, precedence can be assigned to enterprise-critical applications, VoIP telephony or certain user groups.

Details about the functions of the LANCOM Router stateful-inspection firewall are available in the reference manual.

1.4 Voice over IP

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

1.4.1 Example Applications

Voice over IP solutions offers advantages across a broad spectrum of applications, starting with small companies and extending to large corporations with extensive networks of subsidiaries. In the following section, we will demonstrate a number of examples.

Detailed instructions on configuration are available in the PBX Functions manual or in the LCOS reference manual.

Operation as a PBX

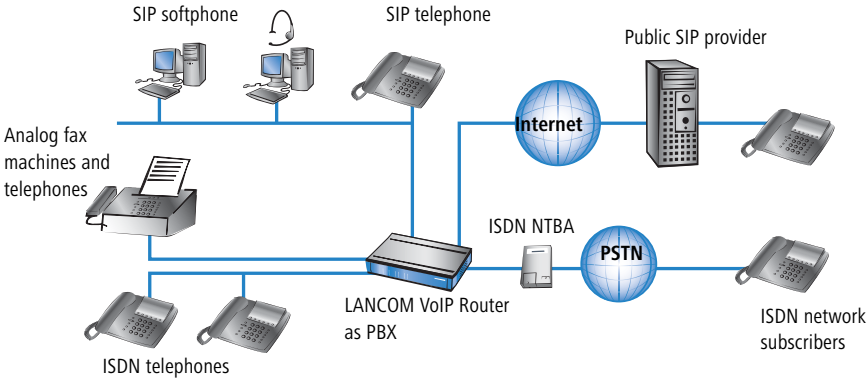
In many cases, LANCOM VoIP Routers can completely replace a local PBX. With up to eight voice channels (e.g. LANCOM 1724 VoIP) to landlines, the

EN

possibility to use SIP accounts and SIP trunking, and the data- and voice networking of various sites, these are powerful and future-ready alternatives to conventional PBX systems.

A systematic set of instructions for setting up the LANCOM VoIP Router for this purpose can be found in the PBX Funtions manual. Beforehand, we recommend that you read the following chapters on the basic setup of devices and software, and then carry out a basic configuration. You should also have set up the Internet access before you continue with setting up the PBX functions.

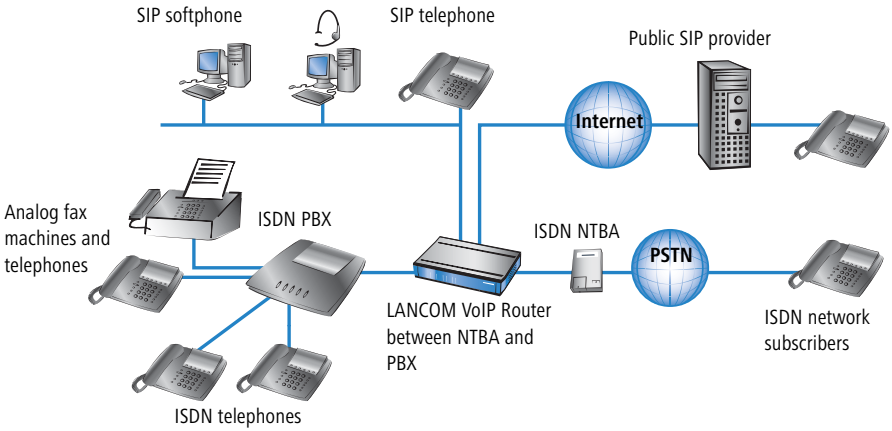
Example: LANCOM VoIP Router As PBX



Supplementing existing PBXs

VoIP functions can be conveniently added in to existing telephone structures by using a LANCOM VoIP Router. The LANCOM VoIP Router is simply connected between the public exchange line (e.g. ISDN NTBA or analog telephone line) and the PBX.

Example: ISDN PBX



Telephone calls over the PBX and the telephones connected to it remain possible just as before; the telephones remain available under the familiar telephone numbers. This application additionally offers the following options:

- In addition to the ISDN and analog telephones, SIP telephones or SIP softphones can be included in the telephone infrastructure.
  - SIP subscribers in the internal LAN are also able to call external PSTN subscribers.
  - The ISDN and analog telephones continue to function, and additionally they can call all of the internal SIP telephones and softphones in the LAN.
- Calls to external SIP subscribers who use the same Internet provider are often available at no cost.
- With the appropriate connection to a public SIP provider, other SIP subscribers worldwide can be called. As an alternative to a direct telephone connection, public telephone network subscribers can also be reached over a diversion via the SIP provider. The costs depend on the provider's particular tariff models. Frequently, long-distance and overseas calls via an SIP provider are significantly cheaper than the traditional telephone connection.

In this constellation, the LANCOM VoIP Router takes over the switching of the calls. The device can be individually configured, for example, to use the access

EN

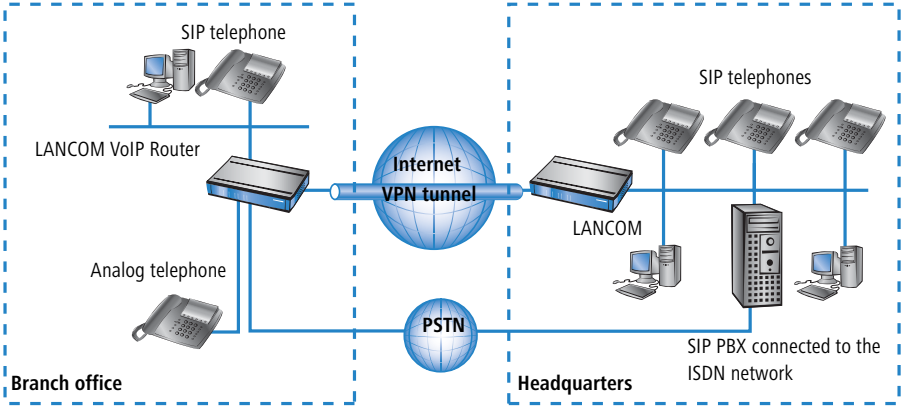
codes to decide upon the switching of a call either via the ISDN interface, or via the Internet as a VoIP call.

Connecting subsidiaries or home offices to the headquarters

Many subsidiaries or home offices already have a connection to the network at headquarters over VPN. These connections are normally limited to conventional data transmission. By using VoIP, internal company calls can be made for free over the existing VPN connection and— thanks to the VPN encryption —these calls are secured against eavesdropping.

With a LANCOM VoIP Router located in the branch or home office, the two worlds of traditional (ISDN and analog) and VoIP telephony can be united in a single telephone: A SIP telephone or an existing analog or ISDN telephone can be used for free telephone calls via VPN to the headquarters, or to make standard calls via the conventional telephone network.

Example: Branch office with analog telephone connection, headquarters with SIP-capable PBX



The advantages of a telephone connection to headquarters:

- The configuration of telephone functions can be carried out centrally in the VoIP PBX at headquarters.
- Subscribers at their branch or home offices connect with the central PBX.
- Calls within the company network are free.
- Outgoing calls are automatically directed to the optimal line for cost optimization.

EN

VoIP for companies through SIP trunking

One of the biggest hurdles for companies that fully migrate to VoIP is to maintain the existing telephone numbers. Normal provider SIP accounts come with a telephone number for the transition to the landline telephone network, but generally these numbers are selected from a pool of numbers available to the provider. However, for companies with a large number of telephone subscribers and numbers, it is of decisive importance that existing telephone and extension numbers are maintained after migrating to VoIP.

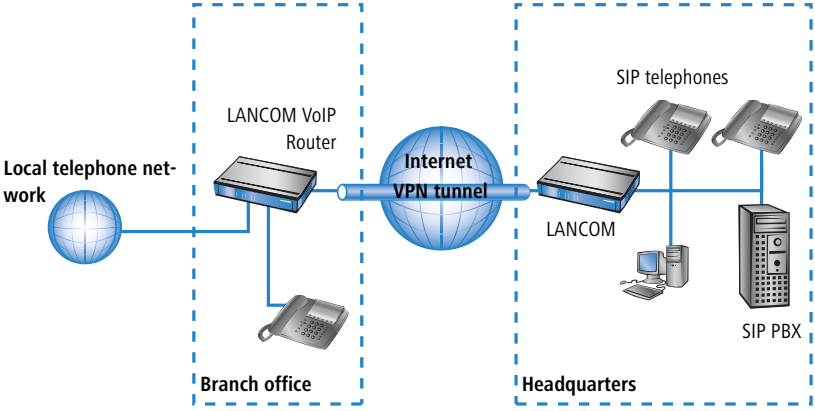
With the SIP trunking function, entire ranges of telephone numbers made up of external numbers and their associated extensions can be mapped by LANCOM VoIP Routers over a single connection to a SIP provider, assuming that the provider also supports Direct Dialing In (DDI) and can provide multiple connections simultaneously. Generally speaking, SIP providers that offer SIP trunking can acquire the existing telephone numbers from the former telecomms provider.

Connecting local exchange lines with a remote SIP gateway

Companies with nation-wide and internationally distributed sites are often interconnected with VPN already. A LANCOM VoIP Router can be used not only to connect the SIP, ISDN or analog telephones at a branch office to the SIP-PBX at headquarters; it can also integrate the branch office's local telephone lines into corporate communications with help of the "SIP Remote Gateway" function.

The SIP remote gateway is active for outgoing and incoming calls.

- A company headquarters in New York can, for example, use a LANCOM VoIP Router with SIP gateway located at the Los Angeles branch office to telephone with customers and suppliers located in Los Angeles at local rates ("local break-out").
- For improved availability to customers located abroad, the New York headquarters can, for example, use a LANCOM VoIP Router with SIP remote gateway located at their sales office in Italy. Customers can then reach support or service numbers via a standard national telephone number. Calls over the local exchange line are received and directed within the company network to the responsible employee. Call routing can be used which identifies the customer's calling number and automatically selects the appropriate connection to be used for forwarding the call.



Advantages of the SIP remote gateway:

- The local telephone connection at any site is available for use by any of the offices throughout the entire company.
- National and international long-distance calls can be mapped to local or regional calls, so saving costs.
- Automatic routing of incoming calls to the responsible employee.

Connecting sites without a SIP PBX

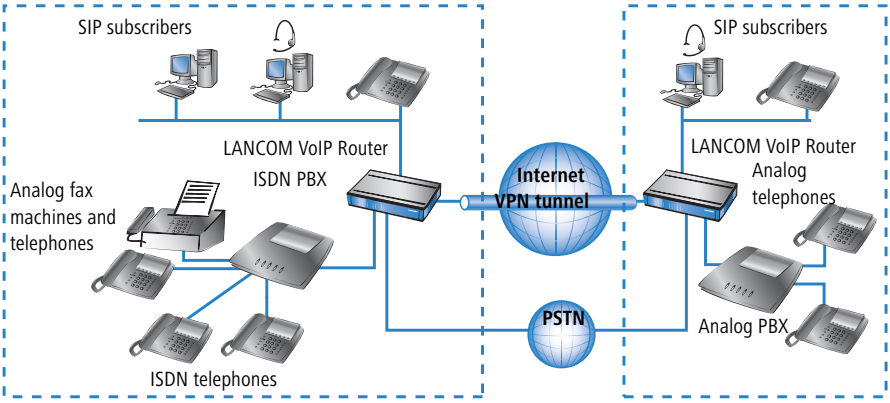
Companies with widely disperse offices and without their own SIP PBX can also take advantage of VoIP site coupling. In this "Peer-to-Peer" scenario, a LANCOM VoIP Router has been implemented at both locations.

Along with data transfer via VPN, it is also possible to use VoIP functions between the two locations.

The advantages of peer-to-peer site coupling

- ISDN and analog PBXs at different locations can form a common internal telephone network.
- An SIP PBX is not necessary.
- Calls within the company network are at no charge.
- Outgoing calls are directed to the optimal line for cost optimization.
- Incoming calls can be switched directly to the appropriate employee at a different location.

Example: Sites with ISDN or analog lines

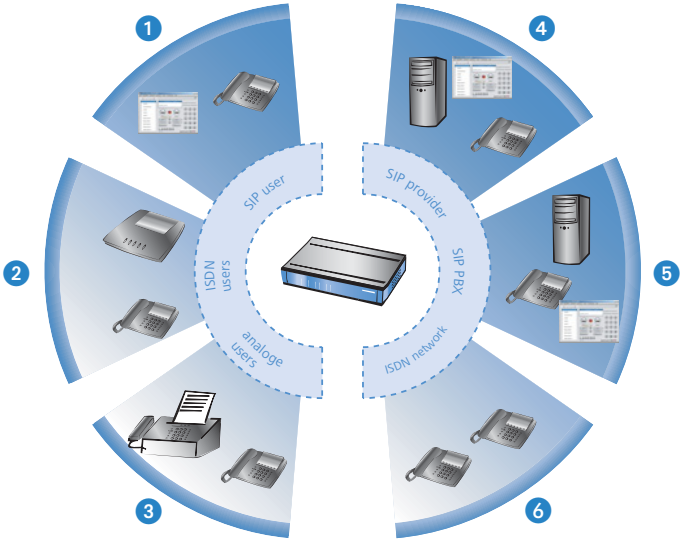


1.4.2 The central position of the LANCOM VoIP Router

LANCOM VoIP Router take up a central position in the switching of telephone calls between internal and external subscribers over the different channels of communication. Depending on the model and equipment, the devices interconnect the following communication participants and channels into a common telephone infrastructure.

1. Internal VoIP terminal devices connected to LAN, WLAN and DMZ, such as SIP telephones and SIP softphones
2. The internal telephone infrastructure with ISDN or analog PBX and ISDN and analog telephones
3. Analog terminal devices, internally connected either into the ISDN network via a PBX with a/b ports, or alternatively into the VoIP network over an ATA (Analog Telephone Adapter)
4. External SIP providers and all of the external subscribers attainable via them
5. Upstream SIP PBXs with all of the internal and external subscribers attainable through it
6. The external telephone world via an exchange line or upstream PBX, and all of the external subscribers available via the land-line network

EN



Users and lines

Telephony subscribers in internal areas can take part in voice communications and, in the LANCOM VoIP environment, are referred to as "users". The LANCOM differentiates between:

- ISDN users

  A maximum of 40 terminal devices connected over the ISDN network, including ISDN and analog devices connected to an upstream ISDN PBX.

  When connecting downstream PBXs to point-to-point lines, the number of possible ISDN subscribers is determined by the length of the extension number (DDI). In this case, all of the telephones and terminal equipment connected to the PBX can be mapped with a single ISDN user entry.

- Analog users

  Two devices connected to the analog interfaces

- SIP users

  A maximum of 32 SIP terminal devices connected over LAN, WLAN and DMZ and analog devices connected with an ATA.

The external paths of communication available to the users are known as "lines". The LANCOM differentiates between the following lines:

EN

- ISDN

  A connection to an ISDN NTBA over the TE interface. The NT interface can additionally be used to connect ISDN terminal devices directly or via a downstream ISDN PBX.

- Analog

  A connection to an analog exchange line or to an extension line of an upstream analog PBX.

- SIP lines

  Maximum 16 SIP lines There are three different types of SIP line:

  - A "Single account" line acts like a normal SIP account with a single telephone number. The internal users can all make use this account for making SIP calls, although only one call can be conducted at a time.

    Depending on the provider services, these lines can be used to reach subscribers in the provider networks, subscribers in other SIP networks (partner networks), or even land-line subscribers. Your own availability at your own telephone number or even solely with an SIP name over the Internet also differs from provider to provider.

  - A "trunk" line acts like an extended SIP account with a main external telephone number and multiple extension numbers. Internal users use this account in parallel and several calls can be made simultaneously (until the maximum available bandwidth is exhausted).
  - As a "SIP gateway" line, the LANCOM VoIP Router provides a remote SIP PBX with a transition to the local ISDN network. The SIP gateway is registered at the SIP PBX with a single number, although several calls can be conducted at once (until the maximum available bandwidth is exhausted). The connection between the SIP PBX and the LANCOM VoIP Router is normally established over a VPN connection.
  - A "link" line acts like a trunk line without limitation to one main external telephone number and multiple extension numbers. Internal users use this account in parallel and several calls can be made simultaneously (until the maximum available bandwidth is exhausted).

- SIP PBXs

  Maximum 4 connections to upstream SIP PBXs. These lines are generally connections to large PBXs in the network at headquarters which can be reached via a VPN connection.

EN

The precise number of users and lines available varies between models and software options.

1.4.3 VoIP characteristics of the LANCOM VoIP Routers

Multiple ISDN/analog interfaces

The ISDN/analog interfaces of the LANCOM VoIP Router can be switched as internal or external connections and, depending on the model, offer up to eight parallel voice channels. This allows, for example, an existing PBX to be additionally equipped with SIP and connected to an upstream VoIP PBX. Subscribers can simultaneously make calls via ISDN and analog telephones, SIP equipment, or softphones to other telephone subscribers, both internally and externally. The transition between SIP and ISDN/analog is automatic and invisible to the user.

Telephone even during a power cut

With life-line support and power relay to the internal ISDN port, it remains possible to telephone over the conventional telephone network even in case of a power outage. ISDN backup, load balancing and VRRP in combination with Ethernet ports as WAN interfaces provide SIP connections with redundancy and high reliability. If a SIP remote station should fail, switching automatically reverts to the conventional telephone network. This ensures that telephony is just as reliable as ever, even with VoIP.

Point-to-multipoint and point-to-point connections with ISDN

For ISDN, LANCOM VoIP Routers support point-to-multipoint and point-to-point connections:

- Point-to-multipoint connection (point-to-multipoint): Up to 8 ISDN terminal devices can be connected to this type of connection. Terminal equipment can include ISDN telephones and ISDN PBXs, which can be used for connecting yet more equipment. As an alternative, a LANCOM VoIP Router can be connected to a point-to-multipoint connection.
- Point-to-point connection (point-to-point): This type of device is suitable for the connection of one ISDN device only, generally an ISDN PBX. As an alternative, a LANCOM VoIP Router can be connected to a point-to-point connection.

To connect a LANCOM VoIP Router, the interface that is used is set up for the type of line in use.

Equipment connected to an ISDN connection can be addressed in two ways:

- The devices are addressed with a multiple subscriber number (MSN) that is linked to the ISDN connection and cannot be influenced.
- Terminal devices are addressed via a Direct Dialing In-Number (DDI). However, only the main external number is associated with the telephone line; the extension numbers that address the individual terminal devices can be chosen at will and are merely suffixes to the main number. The main number, extension and area selection code (not including the leading zero) can be at the most 11 characters long.

The terms "point-to-multipoint connection" and "point-to-point connection" are used in many countries to describe the technical implementation of point-to-multipoint with MSN and point-to-point with DDI. Other countries may use different types of connection and other combinations of protocol and call-number type, or even different names. Please refer to your telephone network operator for the technical specifications of your ISDN connection.

Bandwidth reservation with failover

High-performance VPN functions allow the reliable transmission of voice and data between company sites. This spares the telephone bill from internal communications. A professional firewall, versatile routing functions and excellent Quality of Service mechanisms make the LANCOM VoIP Router a comprehensive solution for secure voice and data communication in a single compact device. All functions are integrated into the central management functions.

EN

1.5 Just what can your LANCOM do?

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

	LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Applications				
Internet access	✔	✔	✔	✔
LAN-LAN coupling over VPN	✔	✔	✔	✔
LAN-LAN coupling over ISDN	✔	✔	✔	✔
RAS server (over VPN)	✔	✔	✔	✔
RAS server (over ISDN)	✔	✔	✔	✔
IP router	✔	✔	✔	✔
IPX router (over ISDN), for example for coupling Novell networks or for dialing in to Novel networks	✔	✔	✔	✔
NetBIOS proxy for coupling Microsoft peer-to-peer networks over ISDN	✔	✔	✔	✔
DHCP- and DNS server (for LAN and DMZ)	✔	✔	✔	✔
Advanced Routing and Forwarding (ARF networks)	8	8	8	8
N:N mapping for routing networks with the same IP-address ranges over VPN	✔	✔	✔	✔
Configuring LAN ports as additional WAN ports	✔	✔	✔	✔
Policy-based routing	✔	✔	✔	✔
Load balancing for bundling multiple DSL channels	4 channels	2 channels	2 channels	2 channels
Backup solutions and load balancing with VRRP	✔	✔	✔	✔
PPPoE server	✔	✔	✔	✔
WAN RIP	✔	✔	✔	✔
Rapid Spanning Tree Protocol				✔

EN

		LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Layer-2 QoS Tagging		✔	✔	✔	✔
802.1p		✔	✔	✔	✔
NAT Traversal (NAT-T)		✔	✔	✔	✔
DMZ with configurable IDS checks		✔	✔	✔	✔
ISDN leased lines		✔	✔	✔	✔
LANCAPI server to provide office applications such as fax or answering machine via the ISDN interface.		✔	✔	✔	✔
VoIP functions VoIP					
SIP proxy and registrar	Management of local SIP users (registration/authentication)	✔	✔	✔	✔
	Mapping of public SIP-provider accounts as telephone lines	✔	✔	✔	✔
	SIP trunking for mapping SIP accounts with external root numbers and extensions.	✔	✔	✔	✔
	Registration at and switching to upstream SIP PBXs	✔	✔	✔	✔
	Individual/shared password for authentication	✔	✔	✔	✔
	Automatic registration and forwarding of SIP users	✔	✔	✔	✔
	Automatic bandwidth management and prioritization of SIP connections	✔	✔	✔	✔
	Number of local SIP subscribers (on delivery, upgrade for 32 SIP subscribers with LANCOM VoIP-32 Option)	8	8	8	8
SIP gateway	Free choice from available ISDN S_0 buses	✔	✔	✔	✔
	Operation at exchange lines or extension lines	✔	✔	✔	✔
	Operation at ISDN point-to-multipoint lines or ISDN point-to-point lines	✔	✔	✔	✔
	Automatic registration and authentication of local ISDN subscribers as SIP users, max. number of mapping entries	40	40	40	40

EN

		LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
	Automatic registration and authentication of analog users as SIP users at upstream SIP PBXs, max. number of mapping entries	–	2	–	2
	Switching between local and remote ISDN, analog and SIP users	✔	✔	✔	✔
	Remote gateway function for mapping local exchange lines to a remote SIP PBX	✔	✔	✔	✔
	ISDN supplementary services CLIP, CLIR	✔	✔	✔	✔
	En-block and individual dialing with adjustable wait time until completion	✔	✔	✔	✔
	Inband tone signaling according to European and German standards with country profiles	✔	✔	✔	✔
Call router	Central switching of all connections (SIP and ISDN/analog)	✔	✔	✔	✔
	Number translation by mapping, numeral replacement and number supplementation	✔	✔	✔	✔
	Rules for routing according to dialed, outgoing call number, line and domain	✔	✔	✔	✔
	Multiple cycles, also forced after number replacement	✔	✔	✔	✔
	Up to three destinations per routing rule (double backup)	✔	✔	✔	✔
	Rule-based rejection of calls	✔	✔	✔	✔
	Supplementation of call-number prefixes per line	✔	✔	✔	✔
	Supplement/remove root numbers per line	✔	✔	✔	✔
Voice processing	Echo canceling and de-jitter buffer for SIP connections	✔	✔	✔	✔
	Transparent pass-through for negotiated codecs	✔	✔	✔	✔
	Interaction on codec negotiation (filter, quality, bandwidth)	✔	✔	✔	✔
WAN connections					
Connector for DSL or cable modem		✔	✔	✔	✔

EN

	LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Integrated ADSL modem (with ADSL2+)	✔	✔	✔	✔
ISDN S_0 connection in NT mode for connecting downstream ISDN devices (ISDN telephones, ISDN PBXs) to the LANCOM VoIP Router. Switchable to TE mode. * Not suitable for connection to external exchanges (e.g. telephone network).	1 ✔	1 ✔*	2 ✔	1 ✔*
ISDN S_0 connection in TE mode for connecting the LANCOM VoIP Router to an external ISDN connection, e.g. to an NTBA or to an upstream ISDN PBX. Switchable to NT mode.	1 ✔	1 ✔	2 ✔	1 ✔
Power relay; ISDN voltage available at the external connector is passed through to the internal ISDN port, providing power to any connected equipment.	ISDN1 to ISDN2		ISDN1 to ISDN3	
Internal power supply for the ISDN NT connector, providing power to a maximum of two connected telephones.		✔		✔
Analog FXS connectors to connect analog terminal devices or an analog PBX (tone dialling).		2		2
Analog FXO connector for connecting the LANCOM VoIP Router to an analog exchange line or to an upstream analog PBX (tone dialling), combined with ISDN1.		1		1
Relay of signals and power from the analog exchange line to Analog1 when router switched off (life-line)		✔		✔
Internal power supply for the analog connections, providing power to one connected device each.		✔		✔
Life-line support to ensure functional telephony when device is switched off or with a non-configured VoIP Call Manager	✔	✔		✔
Connection of external analog or GPRS modem to the COM port (requires the LANCOM Modem Adapter Kit)	✔	✔	✔	✔
WLAN				
Wireless transmission compliant with IEEE 802.11g and IEEE 802.11b				✔
Wireless transmission compliant with IEEE 802.11a and IEEE 802.11b				✔
Point-to-point mode (six P2P paths can be defined per WLAN interface)				✔
Relay function to link two P2P connections				✔

EN

	LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Access Point mode				✔
Client mode				✔
Managed mode for central configuration of WLAN modules by a WLAN Controller				✔
Turbo mode: Double the bandwidth at 2.4 GHz and 5 GHz.				✔
Super AG incl. hardware compression and bursting				✔
Multi SSID				✔
Roaming function				✔
802.11i / WPA with hardware AES encryption				✔
WEP encryption (up to 128-bit key lengths, WEP152)				✔
IEEE 802.1x/EAP				✔
MAC address filter (ACL)				✔
Individual passphrases per MAC address (LEPS)				✔
Closed-network function				✔
Integrated RADIUS server				✔
VLAN				✔
Intra-Cell-Blocking				✔
QoS for WLAN (IEEE 802.11e, WMM/WME)				✔
LAN connection				
Separate FastEthernet LAN ports, individually switchable, e.g. as LAN switch or separate DMZ ports; auto crossover. Alternatively switchable as a WAN interface for connecting SDSL modems.	4	2	2	2
USB connector				
USB 2.0 host port (full speed: 12 Mbps) for connecting a USB printer and for future extensions	✔	✔	✔	✔
Security functions				
IPSec encryption via external software (VPN client)	✔	✔	✔	✔

EN

	LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
5 integrated VPN tunnels for secure network connections	✔	✔	✔	✔
IPSec encryption in hardware (optional; activated with the VPN-25 option)	✔	✔	✔	✔
IP masquerading (NAT, PAT) to conceal individual LAN workstations behind a single public IP address.	✔	✔	✔	✔
Stateful-inspection firewall	✔	✔	✔	✔
Firewall filter for blocking individual IP addresses, protocols and ports	✔	✔	✔	✔
MAC address filter regulates, for example, LAN-workstation access to the IP routing function	✔	✔	✔	✔
Protection of the configuration from brute-force attacks.	✔	✔	✔	✔
Configuration				
Configuration with LANconfig or via web browser; additional terminal mode for Telnet or equivalent terminal programs; SNMP interface and TFTP server function.	✔	✔	✔	✔
1-Click-VPN wizard for easiest setup of RAS access and site-to-site LAN coupling via VPN	✔	✔	✔	✔
Remote configuration via ISDN (with ISDN PPP connections, e.g. via Windows Dial-Up Networking).	✔	✔	✔	✔
Serial configuration interface	✔	✔	✔	✔
Call-back function with PPP authentication mechanisms allowing only predefined ISDN call numbers	✔	✔	✔	✔
FirmSafe for no-risk firmware updates	✔	✔	✔	✔
Optional software extensions				
LANCOM VoIP 32 Option for upgrading to 32 local SIP users	✔	✔	✔	✔
LANCOM VPN Option with 25 active tunnels for secure network coupling; includes activation of the hardware accelerator	✔	✔	✔	✔
Optional hardware extensions				
LANCOM Modem Adapter Kit for connecting analog or GSM modems to the serial interface	✔	✔	✔	✔

EN

	LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
19" rackmount adapter	✔	✔	✔	✔
LANCOM ES-1108P PoE switch for Ethernet cabling; simultaneously supplies power over Ethernet, e.g. for the SIP telephone LANCOM VP-100	✔	✔	✔	✔
Lightning-protection adapters SA-5 and SA-LAN				✔

2 Installation

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

2.1 Package content

EN

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

	LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Power adapter	✔	✔	✔	✔
LAN connector cable (green connectors)	1	1	1	1
ADSL connector cable (transparent connectors)	1	1	1	1
ISDN connector cable (light-blue connectors)	1	1	2	1
Adapter to cross-over the contacts for reconfigured ISDN interfaces	1	1	2	1
Analog cable, RJ11 connector to TAE-NF socket (German standard) or UK socket adapter for No. 431A plugs for connecting analog terminal devices or PBXs		2		2
Analog cable, RJ45 connector (yellow marking) to RJ11 connector for connecting to an analog exchange line.		1		1
Adapter, RJ11 socket to TAE-F plug (for Germany) or UK RJ11 socket to UK plug No. 431A		1		1
Connector cable for the configuration interface	✔	✔	✔	✔
LANCOM CD	✔	✔	✔	✔
Printed documentation (Installation Guide, User manual, Manual PBX Functionalities)	✔	✔	✔	✔

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

EN

2.2 System requirements

2.2.1 Configuring the LANCOM devices

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

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

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

2.2.2 Operating access points in managed mode

LANCOM Wireless Routers and LANCOM Access Points can be operated either as self-sufficient Access Points with their own configuration ("Access Point mode") or as components in a WLAN infrastructure, which is controlled from a central WLAN-Controller ("managed mode").

For operation in managed mode the Access Points require firmware of version 7.22 or higher and a current loader (version 1.86 or higher).

2.3 Introducing the LANCOM Router

This section introduces your device. You will find an overview of all status displays, connectors and switches here.

2.3.1 Status displays

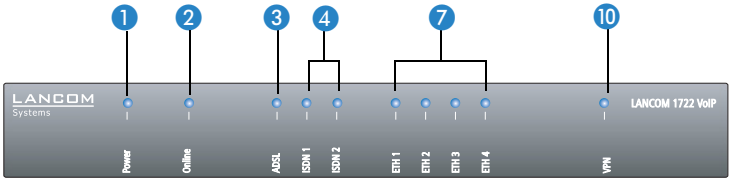
Depending on the range of functions of the model, LANCOM Routers have different numbers of front-mounted status displays.

Front

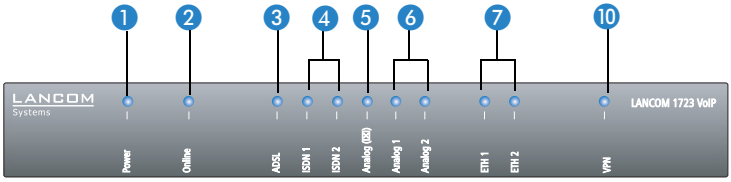
Status displays on the front of the device provide information about operational and connection status:

EN

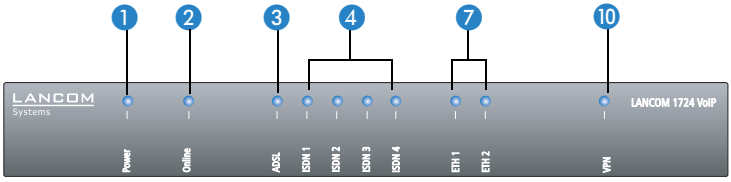
LANCOM 1722 VoIP



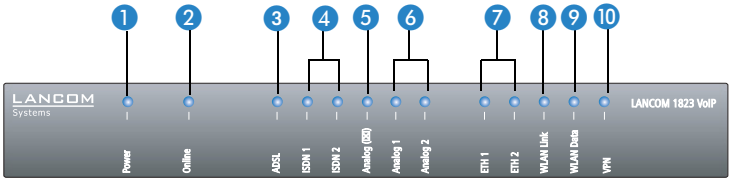
LANCOM 1723 VoIP



LANCOM 1724 VoIP



LANCOM 1823 VoIP



EN

Top

The two top-mounted LEDs enable the main function status to be assessed even if the device is positioned 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 provides information on the device's operating state. After being switched on, it blinks green during the self-test. The LED then shines constantly to indicate operational readiness, unless an error is detected as indicated by a code blinked in red.

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

Orange/green	In the housing cover; blinking alternately with the online LED	At least one WLAN module is in managed mode and has not found a WLAN Controller yet. The corresponding WLAN module(s) is/are switched off until a WLAN Controller is found to supply a configuration, or until being switched manually into another operating mode.
Orange /red	In the housing cover; blinking alternately with the online LED	At least one WLAN module is in managed mode and has found a WLAN Controller. However, the WLAN Controller cannot assign a configuration because the firmware and/or the device's loader version is not compatible with the WLAN Controller.
Red	Blinking	Charge or time limit for online connections reached

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

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

Signal that a charge or time limit has been reached

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

There are three ways to remove the lock:

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

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

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

EN

2 Online

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

Off		No active connection
Green	Flashing	Opening the first connection
Green	Inverse flashing	Opening an additional connection
Green	On (permanently)	At least one connection is established
Red	On (permanently)	Error establishing the last connection
Orange/ green	In the housing cover; blinking alternately with the power LED	At least one WLAN module is in managed mode and has not found a WLAN Controller yet. The corresponding WLAN module(s) is/are switched off until a WLAN Controller is found to supply a configuration, or until being switched manually into another operating mode.
Orange / red	In the housing cover; blinking alternately with the power LED	At least one WLAN module is in managed mode and has found a WLAN Controller. However, the WLAN Controller cannot assign a configuration because the firmware and/or the device's loader version is not compatible with the WLAN Controller.

3 ADSL

Connection status at the ADSL connector:

Off		Interface deactivated
Orange	Blinking	Initialization (establishing contact to provider)
Orange	Flashing	Opening the first connection
Orange	Inverse flashing	Opening an additional connection
Orange	On (permanently)	At least one logical connection is established
Orange	Flickering	Data traffic (send or receive)
Orange	Flashing	Error (CRC error, framing error, etc.)
Red	On (permanently)	No synchronization, searching for remote station
Green	Permanently	Synchronization successful
Green	Blinking/flashing	Handshake/training
Red/ orange	Blinking	Hardware error

EN

4 ISDN

Status display for the ISDN interfaces:

		TE mode (external ISDN connection)	NT mode (internal ISDN connection)
Off		Interface off or Layer 1 deactivated or no Layer 2 TEI	Interface switched off. When switched off, the line may, under certain circumstances, still be connected to another ISDN interface via a life-line relay.
Green	Blinking	Establishing D-channel Layer 1/establishing Layer 2 TEI	
Green	On (permanently)	D-channel activated (Layer 1 active and Layer 2 TEI available)	D channel activated
Orange	Blinking	Establishing the first ISDN connection	
Orange	Flashing	Establishing an additional ISDN connection	
Orange	Inverse flickering	Data traffic being sent	
Red	Blinking	B-channel error	
Red	On (permanently)	Abort due to error in establishing D-channel Layer 1 or Layer 2	Abort due to error in establishing D-channel Layer 1.
Red/ orange	Blinking	ISDN hardware error	

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

5 Analog (1 and 2)

Connection status at the analog terminal equipment connector:

Off		Interface switched off.
Green	On (permanently)	Analog connection is switched on. Handset on-hook or the device is not connected.
Orange	Blinking	Call being established from LANCOM towards the terminal equipment (ringing)

Orange	On (permanently)	Handset off-hook.
Orange / red	Blinking	Hardware error
Red	On (permanently)	Calibration interrupted or temporary error (e.g. in case of shutdown due to temperature)

6 Analog (⊠)

Connection status at the analog exchange line:

Off		Interface switched off.
Green	On (permanently)	Analog exchange line is switched on.
Orange	Blinking	Call being established from exchange towards LANCOM. The line is "ringing" at the LANCOM.
Orange	On (permanently)	The LANCOM has an analog connection—the handset of an analog device is off-hook.
Orange / red	Blinking	Hardware error
Red	On (permanently)	No line voltage available (cable may be interrupted)

7 ETH

LAN connector status in the integrated switch:

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

8 WLAN link

Provides information about the WLAN connections via the internal WLAN modules. The following can be displayed for WLAN link:

Off		No WLAN network defined or WLAN module deactivated. The WLAN module is not transmitting beacons.
Green		At least one WLAN network is defined and WLAN module activated. The WLAN module is transmitting beacons.
Green	Inverse flashing	Number of flashes = number of connected WLAN stations and P2P wireless connections, followed by a pause (default). Alternatively, the frequency of the flashed can indicate the input sensitivity.

Green	Blinking	DFS scanning or other scan procedure.
Red	Flickering	Error in wireless LAN (TX error, e.g. transmission error due to a poor connection)
Red	Blinking	Hardware error in the WLAN module

9 WLAN data

Provides information about the data traffic at the internal WLAN modules. The following can be displayed for WLAN data:

Green	Flickering	TX data traffic.
Red	Flickering	Error in wireless LAN (TX error, e.g. transmission error due to a poor connection)
Red	Blinking	Hardware error in the WLAN module

10 VPN

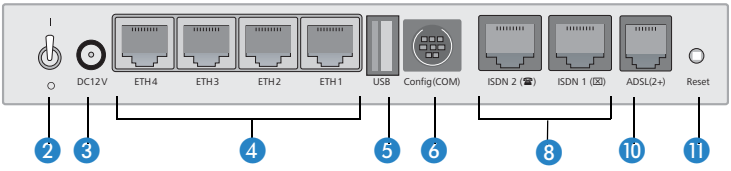
Status of a VPN connection.

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

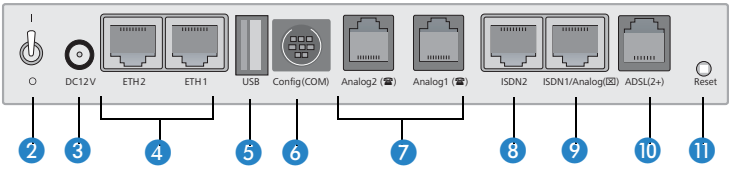
2.3.2 Device connectors

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

LANCOM 1722 VoIP

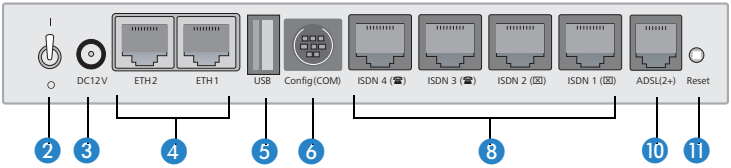


LANCOM 1723 VoIP

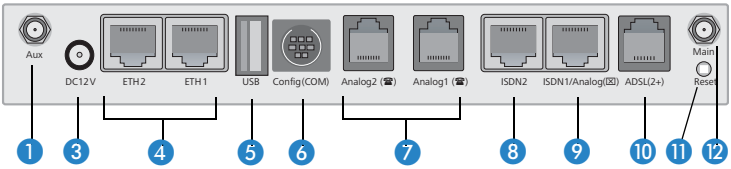


EN

LANCOM 1724 VoIP



LANCOM 1823 VoIP



Only LANCOM 1823 VoIP

1. Aux connector for the WLAN module. The Aux connectors are used for connecting the diversity antennas.

Not including LANCOM 1823 VoIP

2. Power switch
3. Connection for the supplied power adapter
4. Switch with 10/100Base-Tx connectors
5. USB connector (USB host)
6. Serial configuration port (RS 232/V.24)

LANCOM 1723 VoIP and LANCOM 1823 VoIP only

7. Connectors for analog terminal equipment (FXS)
8. ISDN connections

   - Default LANCOM 1722 VoIP

     ISDN 1: TE mode, corresponds to the external ISDN line, alternatively switchable to NT mode

     ISDN 2: NT mode, corresponds to the internal ISDN S_0, alternatively switchable to TE mode

   - Default LANCOM 1724 VoIP

     ISDN 1 and ISDN 2: TE mode, alternatively switchable to NT mode

     ISDN 3 and ISDN 4: NT mode, alternatively switchable to TE mode

   - Default LANCOM 1723 VoIP and LANCOM 1823 VoIP

     ISDN 2: NT mode, alternatively switchable to TE mode

For safety reasons, interface ISDN 2 on the models LANCOM 1723 VoIP and LANCOM 1823 VoIP must not be directly or indirectly connected to an external exchange (e.g. the telephone network)!

9 Combined ISDN-analog interface (FXO)

- Default LANCOM 1723 VoIP and LANCOM 1823 VoIP

  ISDN 1: TE mode, alternatively switchable to NT mode or as an interface to the analog exchange line

10 ADSL connector (ADSL, ADSL 2, ADSL 2+)

11 Reset switch

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

Some devices simply cannot be installed under lock and key. There is consequently a risk that the configuration will be deleted by someone pressing the reset button too long. With the suitable setting, the behavior of the reset button can be controlled accordingly.

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

Reset button

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

- Ignore: The button is ignored.

Please observe the following notice: The settings 'Ignore' or 'Boot only' makes it impossible to reset the configuration to the factory settings. If the password is lost for a device with this setting, then there is no way to access the configuration! The device may become unserviceable, or it can only be operated in its current configuration.

- Boot only: A press of the button prompts a restart, regardless of how long the it is held down.
- Reset-or-boot (standard setting): Press the button briefly to restart the device. Pressing the button for 5 seconds or longer restarts the device and resets the configuration to its factory settings. All LEDs on

the device light up continuously. Once the switch is released the device will restart with the restored factory settings.

This hard reset causes the device to start with the default factory settings; all previous settings are lost!

Note that resetting the device leads to a loss on the WLAN encryption settings within the device and that the default WEP key is active again.

Only LANCOM 1823 VoIP

⑫ Main connector for the WLAN module.

2.4 Hardware installation

Installation of the LANCOM Router involves the following steps:

① **LAN** – first of all connect your LANCOM Router to the LAN or to an individual PC. Plug in one end of the supplied network cable (green connectors) to a LAN connector on the device ④, and the other end into an available network connector socket in your local network, a free socket on a switch or hub, or the networking connector of an individual PC.

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

Avoid having multiple unconfigured LANCOMs at once within a single network segment. Any unconfigured LANCOM takes on the same IP address (ending in '254'), and so address conflicts could arise. To avoid problems, multiple LANCOMs should be configured one after the other with the respective device being assigned with a new and unique IP address (not ending in '254') each time.

② **ADSL** – connect the ADSL interface ⑩ with the splitter by using the supplied ADSL connector cable (transparent connectors).

③ **Connection to the ISDN** – to connect the LANCOM VoIP Router to the ISDN, plug in one end of a supplied ISDN cable (light-blue connectors) to an ISDN interface in TE mode. When shipped, the ISDN interfaces marked with ☒ are set up in TE (external) mode. Plug in the other end of the ISDN cable into an ISDN/S_0 point-to-point line connector or point-to-multipoint line connector.

For the models LANCOM 1723 VoIP and LANCOM 1823 VoIP, the interface ISDN2 is not to be connected to the ISDN network, even after being reset to TE mode!

Please also observe the notices about configuring the ISDN interfaces (→ page 104).

④ **Connecting ISDN terminal devices**—to connect ISDN terminal devices (ISDN telephones or ISDN PBXs) to the LANCOM VoIP Router, connect these to an ISDN interface in NT mode. When shipped, the ISDN interfaces marked with ☎ are set to NT (internal ISDN connection) mode.

For the models LANCOM 1723 VoIP and LANCOM 1823 VoIP, the ISDN2 interface 8 can supply a maximum of two telephones with power from the ISDN feed. Please also observe the notices about configuring the ISDN interfaces (→ page 104).

⑤ **Connecting to the analog telephone network**—to connect the LANCOM VoIP Router to the analog telephone network, plug the end of the supplied analog connector cable marked in yellow (RJ45) into the combined ISDN/analog interface 9. The other end of the analog connector cable (RJ11) is to be plugged into an analog exchange line (e.g. a splitter). If the exchange line has a TAE-N/F socket, you can use the supplied adapter (RJ11 socket to TAE plug) or in case of UK No. 431A socket type the UK FXS adapter (RJ11 socket to BAT plug) if supplied.

⑥ **Connecting analog terminal equipment**—use an analog interface (FXS) on the LANCOM VoIP Router (RJ11 socket marked with ☎) for connecting analog terminal equipment (telephones or PBXs). If your terminal equipment features a TAE-F or TAE-N connector, please use the supplied adapter cable (RJ11 plug to TAE-N/F socket) or in case your terminal equipment features BT No. 431A type plugs you may use the analog adapter cables (RJ11 plug to BAT socket) if supplied..

The LANCOM VoIP Router supplies power to the analog terminal equipment connected to it. With life-line support, the voltage supplied from the analog exchange line is relayed to the terminal equipment via the Analog1 interface (☎). Please also observe the notices about life-line support (→ page 105).

⑦ **Configuration interface** – optionally, the router can be connected directly to the serial interface (RS-232, V.24) of a PC. Use the connection

cable supplied for this. Connect the LANCOM configuration interface 6 to an available serial interface on the PC.

⑧ **Connecting an external modem**—optionally, an external analog or GPRS modem can be connected to the device's serial interface with the LANCOM Modem Adapter Kit, so enabling tasks such as remote maintenance, backup connections or Dynamic VPN to be implemented over an additional WAN connection via an analog line.

⑨ **Power supply** – the socket 2 is for connecting the supplied power supply unit.

Use only the supplied power supply unit! The use of the wrong power supply unit can be of danger to the device or persons.

⑩ **Ready for operation?** – After a brief self-test, the power LED lights up continuously. Green LAN LEDs show which LAN connectors are being used for a connection.

Devices with integrated ADSL modems can become very warm during operation. For these models, environmental temperatures are not to exceed 35°C. Sufficient ventilation is of vital importance. Do not stack the devices and do not expose them to direct sunlight.

2.5 Configuring the ISDN and analog interfaces

LANCOM VoIP Router routers feature several interfaces for connection to ISDN or analog exchange lines, or for connecting ISDN or analog terminal equipment.

A fundamental decision is whether an internal PBX is to be connected and made VoIP-capable by the LANCOM VoIP Router (e.g. for a single site or for the networking of branches) or whether the LANCOM VoIP Router is to replace a local PBX.

- If a PBX is to be made VoIP-capable, simply leave the ISDN interfaces with their standard factory settings. On the underside of the device, check that all of the DIP switches are in the standard position as shown on the sticker. Connections of this type do not require an ISDN cross-over adapter.
- If the LANCOM VoIP Router is to replace a PBX, you can use all of the suitable ISDN interfaces to connect to the PSTN (public services telephone network). Set the DIP switches on the underside of the device accordingly

and use one or two ISDN cross-over adapters (LANCOM 1724 VoIP only). Details of this configuration are available in the PBX Funtions manual.

Detailed information on the significance of DIP swtich settings and the setup of individual ISDN and analog interfaces are available in the chapter 'Configuring the ISDN and analog interfaces in detail' → page 104. For other deployment scenarios from those described above, or for other interface configurations, we stronly recommend that you refer to the corresponding chapter with sample configurations in the reference manual (on the supplied CD or in the Internet).

2.6 Software installation

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

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

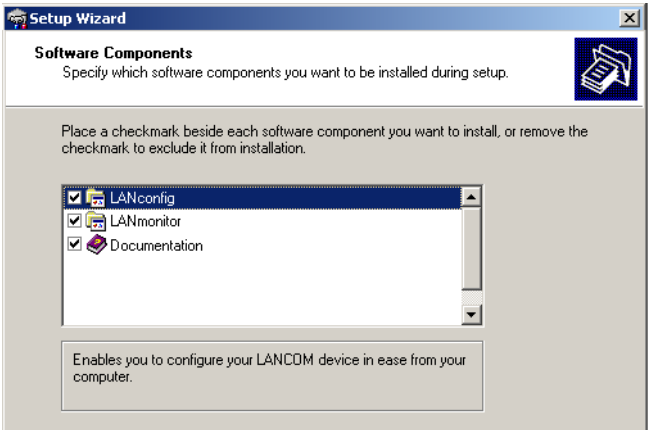
2.6.1 Starting Software Setup

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

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

EN

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



EN

2.6.2 Which software should I install?

- **LANconfig** is the Windows configuration program for all LANCOM routers and LANCOM access points. WEBconfig can be used alternatively or in addition via a web browser.
- With **LANmonitor** you can use a Windows computer to monitor all of your LANCOM routers and LANCOM access points.
- **WLANmonitor** enables the observation and surveillance of wireless LAN networks. Clients connected to the access points are shown, and even non-authenticated access points and clients can be displayed as well (rogue AP detection and rogue client detection).
- **LANCAPI** is a special form of the CAPI-2.0 interface which provides LAN workstations with access to office communications functions such as fax and EuroFile transfer. With the **LANCAPI Dial-up Networking support**, individual computers can use LANCAPI dial-up connections to access an Internet provider. The **CAPI Fax Modem** provides you with a driver for Class 1 fax.
- The **LANCOM Advanced VPN Client** enables VPN connections to be established over the Internet from a remote computer to a VPN router.
- The **LANCOM Advanced VoIP Client** provides the functions of a professional PC softphone which can optionally be integrated into Outlook or Lotus Notes via a plug-in. Combined with the LANCOM VoIP USB Handset or a headset, the client transform PCs or laptops into powerful and convenient system telephones with CTI and TAPI.
- With **Documentation** you copy the documentation files onto your PC.

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

EN

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 device.

3.1 Which information is necessary?

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

- TCP/IP settings
- protection of the configuration
- information related to the Wireless LAN
- 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.

EN

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 LANCOM VoIP Router
- setup of a new network

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

The result of the fully automatic TCP/IP configuration: the router will be assigned the IP address '172.23.56.1' (netmask '255.255.255.0'). In addition, the integrated DHCP server will be enabled so that the LANCOM VoIP 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 VoIP Router**
  Assign a free IP address from the address range of your LAN to the LANCOM VoIP Router and specify the netmask.

EN

3.1.2 Configuration protection

The password for configuration access to the LANCOM protects the configuration against unauthorized access. The configuration of the device 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.

In the managed mode (see following) the LANCOM Wireless Routers and LANCOM Access Points automatically receive the same root password as the WLAN-Controller, assuming that no root password has been set in the device itself.

3.1.3 Settings for the Wireless LAN

The network name (SSID)

The basic configuration wizard asks for the network name of the base station (often designated as SSID – **S**ervice **S**et **Id**entifier). The network name will be registered in the base stations of the Wireless LAN. You can choose any name. Several base stations with the same network name form a common Wireless LAN.

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

Open or closed Wireless LAN?

Mobile radio stations dial-in the wanted Wireless LAN by declaration of the network name. The specification of the network name is facilitated by two technologies:

- Mobile radio stations can search for Wireless LANs in the environs („scan“) and offer for selection the found Wireless LANs in a list.
- By using the network name 'ANY', the mobile radio station will enrol in the next available Wireless LAN.

The Wireless LAN can be „closed" to prevent this procedure. In this case, no enrolment with the network name 'ANY' will be accepted.

For standard, LANCOM base stations are responsive under the network name 'LANCOM'. The wireless basic configuration of a base station takes therefore place via this network name. If another network name is set during the basic configuration, also the Wireless LAN access of the configuring mobile base station must be changed to this new network name after closing the basic configuration.

Selection of a radio channel

The base station operates in a certain radio channel. The radio channel will be selected from a list of up to 11 channels in the 2.4 GHz frequency range or up to 19 channels in the 5 GHz frequency range. (in various countries some radio channels are restricted, see appendix).

The used channel and frequency range define the operating of the common radio standard, in doing so the 5 GHz frequency range correspond to the IEEE 802.11a/h standard and the 2.4 GHz frequency range to the IEEE 802.11g and IEEE 802.11b standard.

If no further base stations operate in reach of the base station, any radio channel can be adjusted. Otherwise, the channels in the 2.4 GHz band must be chosen in the way that they preferably do not overlap one another or have a distance as great as possible respectively. The automatic setting is normally enough in the 5 GHz band, in which the LANCOM Router base station itself adjust the best channel via TPC and DSF.

3.1.4 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 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.'

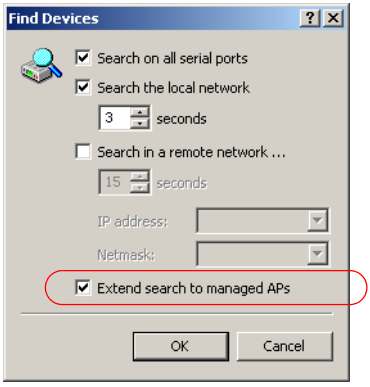
In basic settings the charge protection is defined to maximum 600 minutes within seven days. Adapt this setting to your personal needs or deactivate the charge protection if you have arranged a flatrate with your provider.

EN

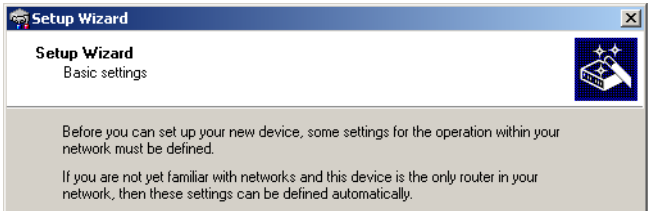
3.2 Instructions for LANconfig

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

② As standard, LANCOM Wireless Routers and LANCOM Access Points in managed mode are **not** displayed by LANconfig carrying out its device search. To display these devices, activate the option 'Extend search for managed APs'.



③ If an unconfigured device is being found during searching, the setup wizard starts that will help you make the basic settings of the device or will even do all the work for you (provided a suitable network environment exists).



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

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

④ If you would like to configure the TCP/IP settings manually, assign an available address from a suitable address range to the LANCOM. Confirm your choice with **Next**.

⑤ Specify whether or not the router should act as a DHCP server. Make your selection and confirm with **Next**.

⑥ 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.

⑦ 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**.

⑧ 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**.

⑨ Connect charge protection can limit the cost of DSL connections to a predetermined amount if desired. Confirm your choice with **Next**.

⑩ 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

EN

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.

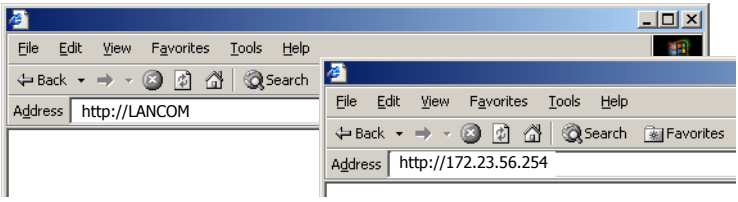
After powered on, unconfigured LANCOM devices check first, whether a DHCP server is already active in the LAN. Dependent on the situation, the device is able to switch on its own DHCP server or, alternatively, to activate its DHCP client mode. In this second operating mode, the device itself can obtain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

If a LANCOM Wireless Router or LANCOM Access Point is centrally managed from a LANCOM WLAN Controller, the DHCP mode is switched from auto-mode to client mode.

Network without DHCP server

Not for centrally managed LANCOM Wireless Router or LANCOM Access Points

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



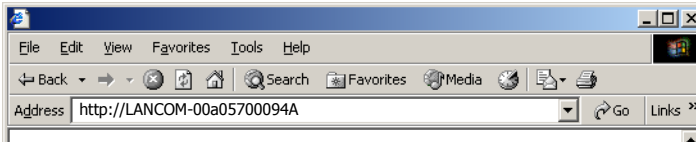
If the configuration PC does not obtain its IP address from the LANCOM DHCP server, figure out the current IP address of this PC (with **Start ▶ Execute ▶ cmd** and command **ipconfig** at the prompt under Windows 2000 or Windows XP, with **Start ▶ Execute ▶ cmd** and the command **winipcfg** at the 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").



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

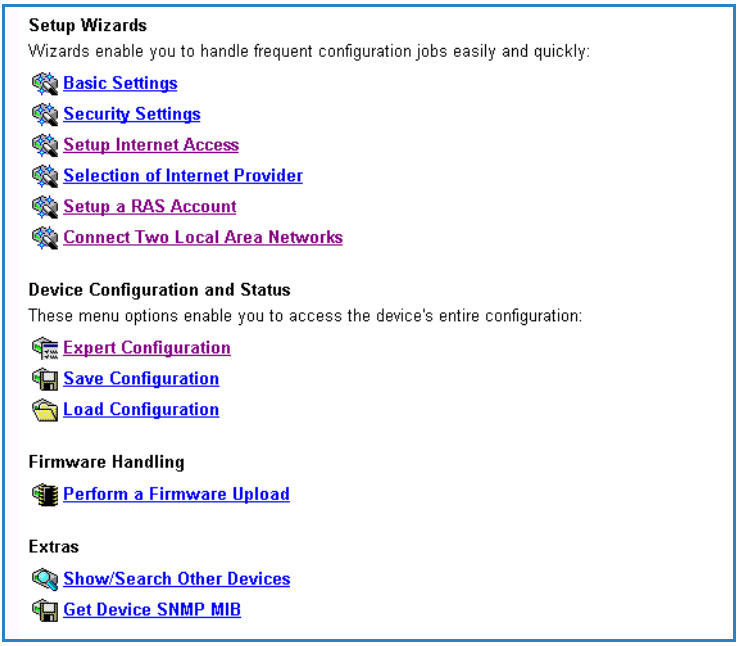
1. Start your web browser (e.g. Internet Explorer, Firefox, Opera) and call the LANCOM Router there:

   `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:



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.

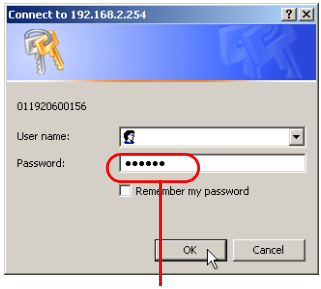
Please note that enabling this will also permit remote configuration via the Internet. You should always make sure that the configuration access is suitably protected, e.g. with a password.

EN

Entering the password in the web browser

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

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



Entering the configuration password

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

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

⑥ Connect charge protection can limit the cost of DSL connections to a 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**.

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.

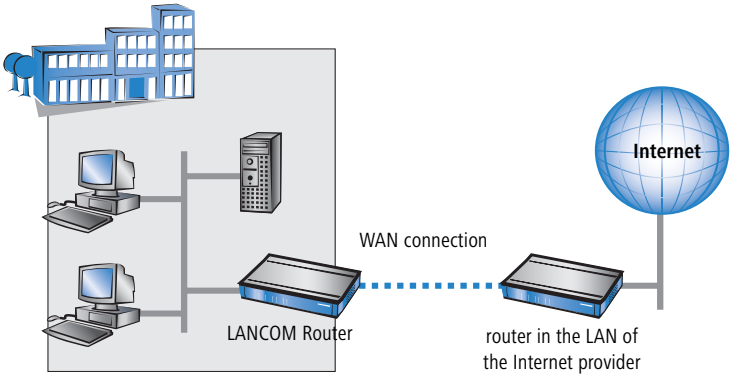
- **Manual IP address assignment**

  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.



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.

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.

EN

- 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).

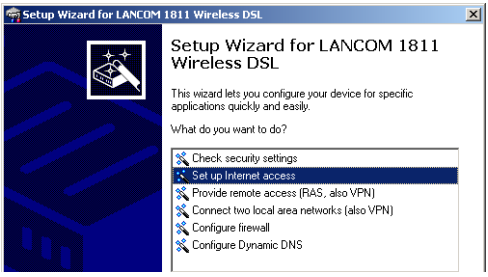
  In addition, you can activate a line monitor that identifies inactive remote stations faster and therefore can close the connection before the idle time has elapsed.

- 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.

4.1 Instructions for LANconfig

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



② From the menu, select the **Setup Internet access** wizard and click **Next**.

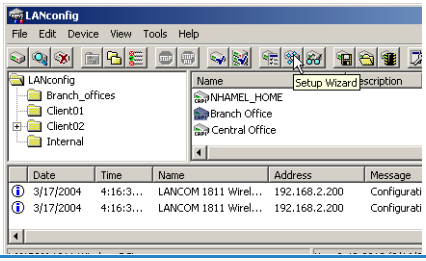
③ In the following window select your country and your Internet provider if possible, and enter your access information.

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

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**.

EN

5 Configuring the VoIP functions

If you wish to employ the LANCOM VoIP Router as a PBX, you should initially carry out the basic settings and then read the manual on the VoIP PBX functions. This describes the quickest way to to set up the PBX with connections to landlines (ISDN or analog).

If you wish to operate an ISDN PBX behind the LANCOM VoIP Router, and thus you would like to leave the telephony interfaces in the default configuration, then please continue with the configuration described here, which uses the VoIP Call Manager wizard.

For more specialized applications, please refer to the corresponding chapters in the LCOS reference manual.

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

② In the selection menu, select the Setup Wizard, **Configure Voice over IP Call Manager** and confirm the selection with **Continue**.

③ In the following windows, you will choose the lines and subscribers that you want to create. Enter the required information for this.

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

6 Linking two networks

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

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

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

Always configure both sides

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

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

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

Security aspects

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

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

EN

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 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.

6.1.1 General information

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

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

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

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

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

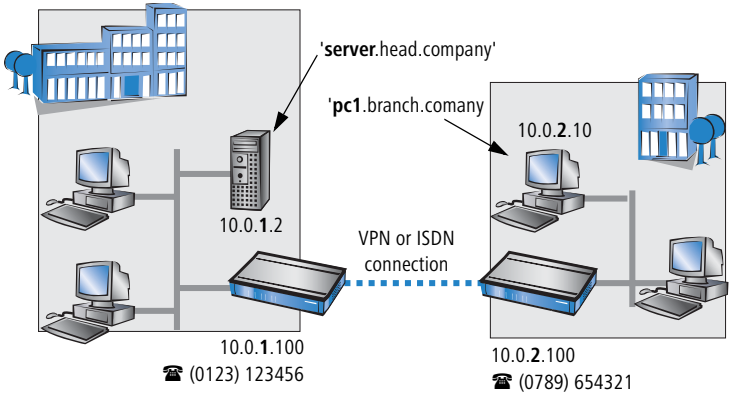
  Thanks to Dynamic VPN, connections can be enabled not only between gateways with fixed, static IP addresses, but even between gateways with dynamic IP addresses. The active initiation of VPN connections towards remote sites with dynamic IP addresses requires ISDN.
- If you haven't already named your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

EN

- 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.

6.1.2 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.



LAN of head office.
IP: 10.0.**1.0**,
Netmask: 255.255.255.0
Domain: '**head**.company'

LAN of branch office.
IP: 10.0.**2.0**,
Netmask: 255.255.255.0
Domain: '**branch**.company'

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

DNS access to the remote LAN

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

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

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

Extranet VPN

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

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

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

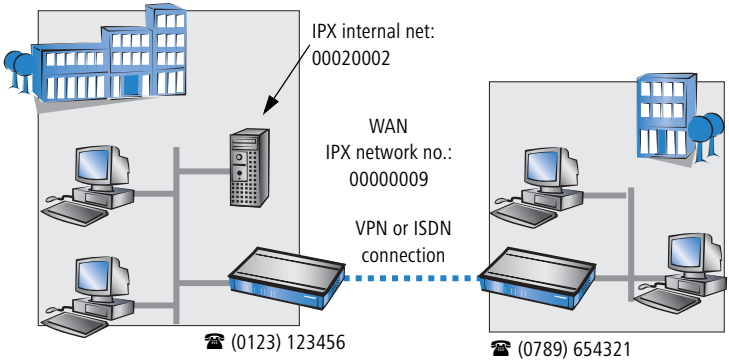
6.1.3 Settings for the IPX router

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

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

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

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



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

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

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

6.1.4 Settings for NetBIOS routing

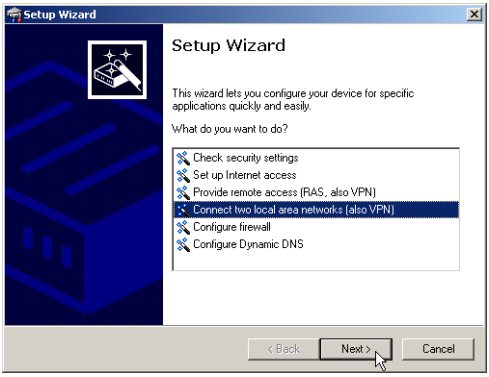
NetBIOS routing can be set up quickly: All that is required in addition to the information for the TCP/IP protocol used is the name of a Windows workgroup from in the router's own LAN.

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

6.2 Instructions for LANconfig

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

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



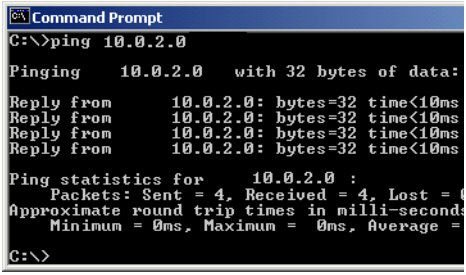
② The wizard will return a message to indicate that it has all the information it needs. Close the wizard with **Finish**.

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

Ping – quick testing for TCP/IP connections

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

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



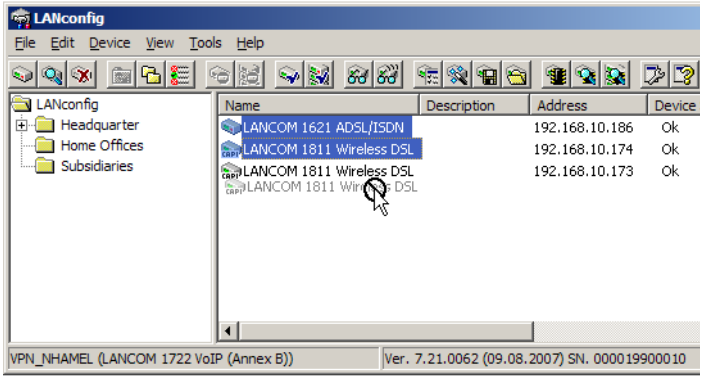
EN

6.3 1-Click-VPN for networks (site-to-site)

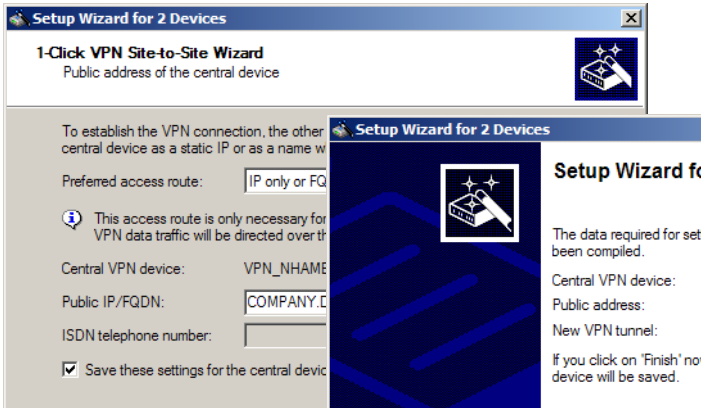
The site-to-site coupling of networks is now very simple with the help of the 1-Click-VPN wizard. It is even possible to simultaneously couple multiple routers to a central network.

① In LANconfig, mark the routers at branch offices which are to be coupled to a central router via VPN.

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



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



④ Select whether connection establishment is to take place via the name or IP address of the central router, or via an ISDN connection. Enter the address or name of the central router, or its ISDN number.

⑤ The final step is to define how the networks are to intercommunicate:

- The INTRANET at headquarters only is to be provided to the branch offices.
- All private networks at the branch offices can also be connected to one another via headquarters.

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

6.4 Instructions for WEBconfig

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

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

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

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

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

EN

7 Providing dial-in access

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

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

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

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

Security aspects

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

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

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

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

7.1 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.

7.1.1 General information

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

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

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

Notes to the individual values:

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

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

The ISDN calling line identity (CLI)

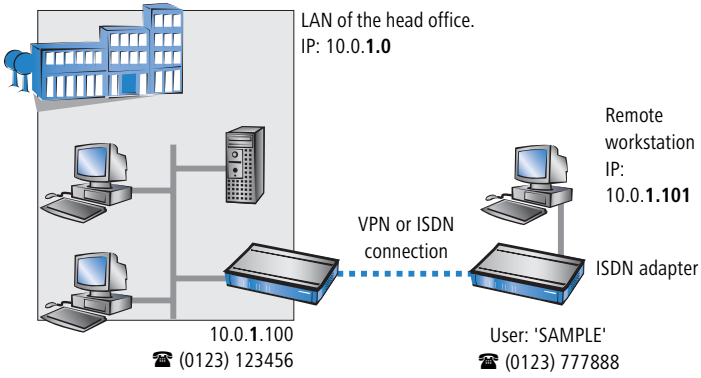
The ISDN caller ID—also known as CLI (**C**alling **L**ine **I**dentity)—this is the telephone number of the caller which is transmitted to the participant receiving the call. As a rule, it consists of the country and area codes and an MSN.

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).

EN

7.1.2 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.

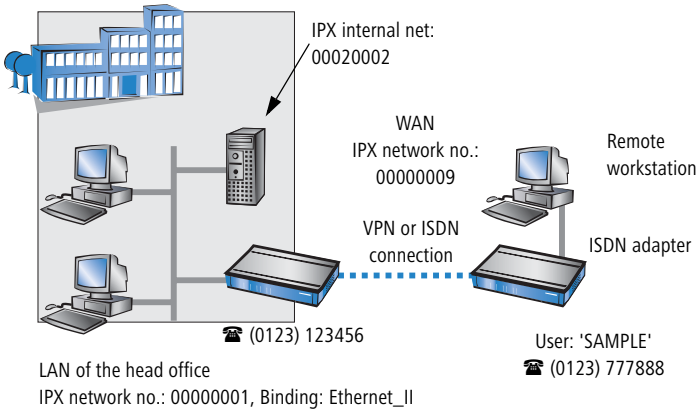
This IP address makes the computer a fully-fledged member of the LAN: with the appropriate rights, it can access all of the other devices in the LAN. The

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

7.1.3 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.

7.1.4 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).

7.2 Settings for the dial-in computer

7.2.1 Dial-up via VPN

For dialing into a network via VPN a workstation requires:

- an Internet access
- a VPN client

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

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

7.2.2 Dial-up via ISDN

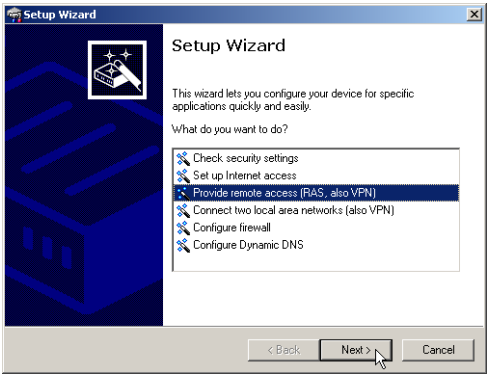
A number of settings must be configured on the dial-in computer. These are briefly listed here, based on a Windows computer:

- 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.

7.3 Instructions for LANconfig

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



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

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

7.4 1-Click-VPN for LANCOM Advanced VPN Client

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

① Use LANconfig to start the 'Set up a RAS Account' wizard and select the 'VPN connection'.

② Activate the options 'LANCOM Advanced VPN Client' and 'Speed up configuration with 1-Click-VPN'.

③ Enter a name for this access and select the address under which the router is accessible from the Internet.

④ In the final step you can select how the access data is to be entered:

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

- ☐ Print out profile

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

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

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

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

7.5 Instructions for WEBconfig

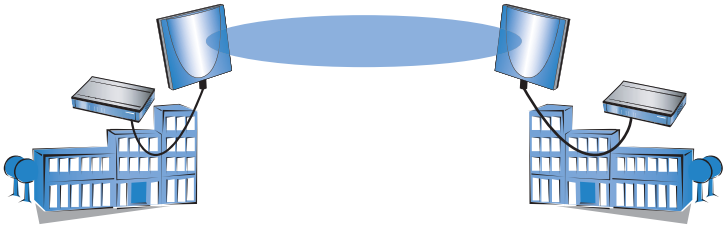
RAS access via VPN cannot be configured using the wizard under WEBconfig yet. It can only be set up in the expert configuration. For details, please refer to the reference manual.

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

⑥ Configure Dial-Up Networking access on the dial-in PC as described. Next, test the connection (see box 'Ping – quick testing for TCP/IP connections' → page 46).

8 Point-to-point connections

LANCOM Wireless access points serve not only as central stations within a wireless network, they can also operate in point-to-point mode to bridge longer distances. For example, they can provide a secure connection between two networks that are several kilometers apart—without direct cabling or expensive leased lines.

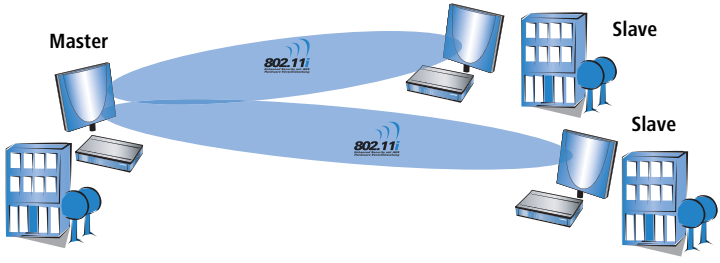


The behavior of an access point when exchanging data with other access points is defined in the "Point-to-point operation mode".

- **Off:** The access point only communicates with mobile clients
- **On:** The access point can communicate with other access points and with mobile clients
- **Exclusive:** The access point only communicates with other base stations

In the 5 GHz band, the automatic search for vacant WLAN channels can lead to several simultaneous test transmissions from multiple access points, with the result that they do not find each other. This stalemate situation can be avoided with the appropriate "Channel selection scheme":

- **Master:** This access point takes over the leadership when selecting a free WLAN channel.
- **Slave:** All other access points will search for a channel until they have found a transmitting Master.



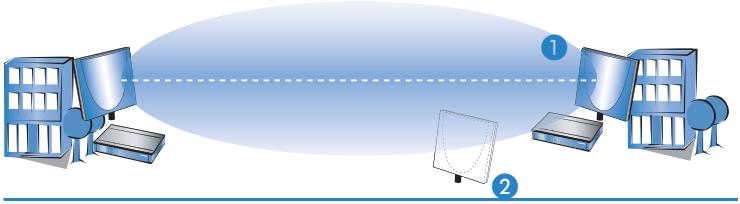
EN

Thus it is recommended for the 5 GHz band that one central access point should be configured as 'Master' and all other point-to-point partners should be configured as 'Slave'. In the 2.4 GHz band, too, this setting simplifies the establishment of point-to-point connections if the automatic channel search is activated.

It is imperative that the channel selection scheme is configured correctly if the point-to-point connections are to be encrypted with 802.11i/WPA.

8.1 Antenna alignment for P2P operations

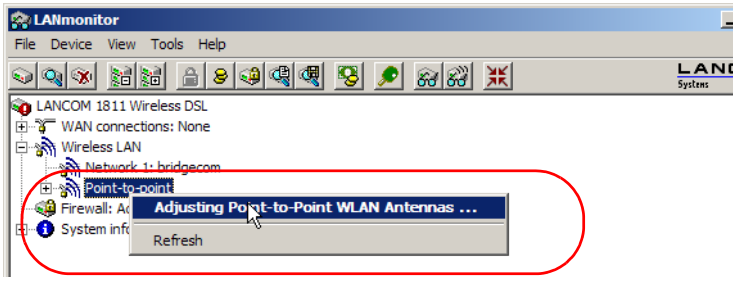
The precise alignment of the antennas is of considerable importance in establishing a P2P path. The more central the receiving antenna is located in the "ideal line" of the transmitting antenna, the better is the actual performance and the effective bandwidth 1. If the receiving antenna is outside of this ideal area, however, significant losses in performance will be the result 2.



Further information about the geometrical alignment of wireless paths and the alignment of antennas with the help of LANCOM software can be found in the LCOS reference manual.

To help find the best possible alignment for the antennas, LANmonitor can display the current signal quality over a P2P connection. The connection-quality display is opened with the context menu in LANmonitor. A click with

the right-hand mouse key on the 'Point-to-point' entry prompts the command 'Adjusting Point-to-Point WLAN Antennas'



Configuration tool	Call
LANmonitor	Point-to-point ▶ context menu ▶ Adjusting Point-to-Point WLAN Antennas...

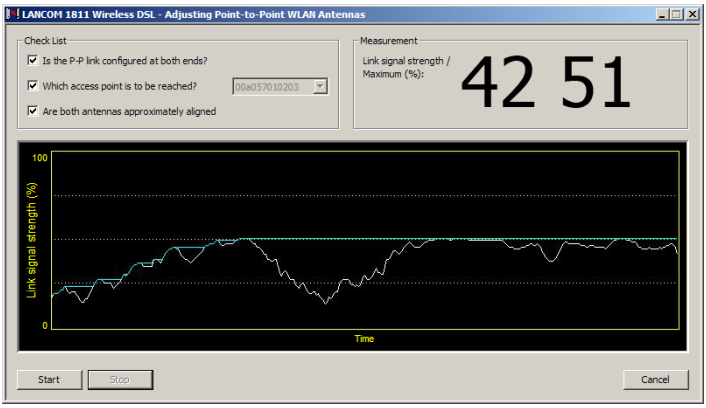
The entry 'Point-to-point' is only visible in LANmonitor if the monitored device has at least one base station defined as a remote station for a P2P connection (LANconfig: **Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Point-to-Point**).

In the dialog for setting up point-to-point connections, LANmonitor requests the required information for establishing the P2P connection:

- Assuming that the P2P path is configured at both ends, i.e. the two remote base stations are entered with their respective MAC addresses; has the point-to-point operating mode been activated?
- Which access point is to be monitored? All of the base stations defined as P2P remote stations in the respective device can be selected here.
- Are both antennas approximately aligned? The connection over the P2P path has to be functioning basically before you start fine-tuning with the aid of LANmonitor.

Once signal monitoring has commenced, the P2P dialog displays the absolute values for the current signal strength and the maximum value since starting

the measurement. The development of the signal strength over time and the maximum value are displayed in a diagram.



Initially you should only adjust one of the two antennas until a maximum value is achieved. This first antenna is then fixed and the second antenna is then adjusted to attain the best signal quality.

8.2 Configuration

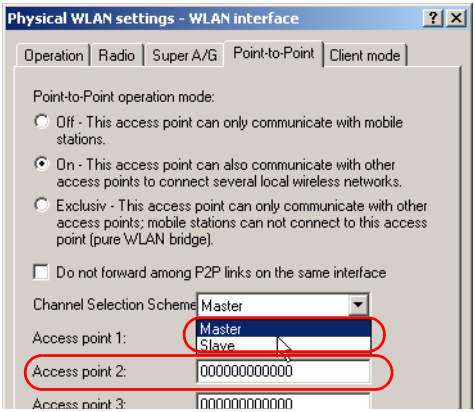
In the configuration of point-to-point connections, entries have to be made for the point-to-point operation mode, the channel selection scheme and the MAC addresses of the remote sites.

Configuration with LANconfig

For configuration with LANconfig you will find the settings for P2P connections under the configuration area 'Interfaces' on the 'Wireless LAN' tab.

① Click on the button **Physical WLAN settings** to open the corresponding WLAN interface and select the tab for 'Point-to-Point'.

② Activate the suitable point-to-point operation mode here and set the channel selection scheme to either 'Master' or 'Slave'. Enter the appropriate MAC address for the WLAN card at the remote station (maximum 6).



Please observe that only the MAC addresses of the WLAN cards at the other end of the connections are to be entered here! Not the access point's own MAC address, and not the MAC addresses from any other interfaces that may be present in the access points.

You will find the WLAN MAC address on a sticker below the corresponding antenna connector. Only use the string that is marked as the "WLAN MAC" or "MAC-ID". The other addresses that may be found are not the WLAN MAC address but the LAN MAC address.

Alternatively you will find the MAC addresses for the WLAN cards in the devices under WEBconfig, Telnet or a terminal program under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Status ▶ WLAN-statistics ▶ Interface-statistics
Terminal/Telnet	`Status/WLAN-statistics/Interface-statistics`

EN

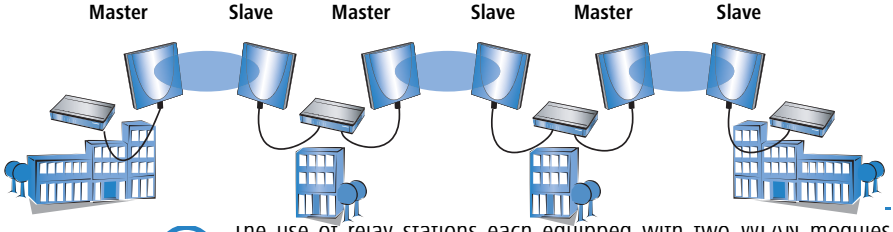
Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you can set the settings for the point-to-point connections under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ Interfaces ▶ WLAN-Interfaces▶ Interpoint-Settings
Terminal/Telnet	`cd /Setup/Interfaces/WLAN-Interfaces/Interpoint-Settings`

8.3 Access points in relay mode

Access points equipped with two wireless modules can be used to establish wireless bridges across multiple stations. Each wireless module is configured as a 'Master' and then 'Slave' in turn.



The use of relay stations each equipped with two WLAN modules simultaneously solves the problem of the "hidden station", by which the MAC addresses of the WLAN clients are not transferred over multiple stations.

8.4 Security for point-to-point connections

IEEE 802.11i can be used to attain a significant increase in the security of WLAN point-to-point connections. All of the advantages of 802.11i such as the simple configuration and the powerful encryption with AES are thus available for P2P mode, as are the improved security of the passphrase from the LANCOM Enhance Passphrase Security (LEPS).

8.4.1 Encryption with 802.11i/WPA

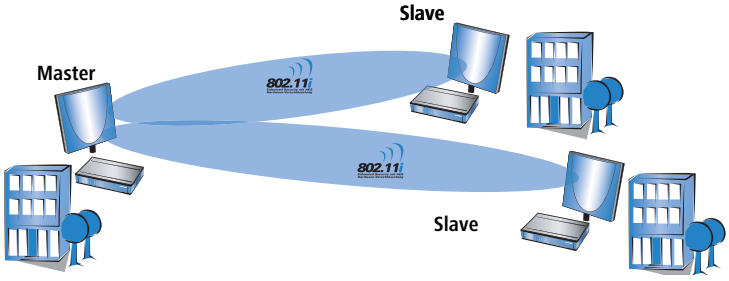
To activate the 802.11i encryption for a correctly configured P2P connection, adjust the settings for the first logical WLAN network in the appropriate WLAN interface (i.e. WLAN-1 if you are using the first WLAN card for the P2P

connection, WLAN-2 if you are using the second card, e.g. as with an access point with two WLAN modules).

- Activate the 802.11i encryption.
- Select the method '802.11i (WPA)-PSK'.
- Enter the passphrase to be used.

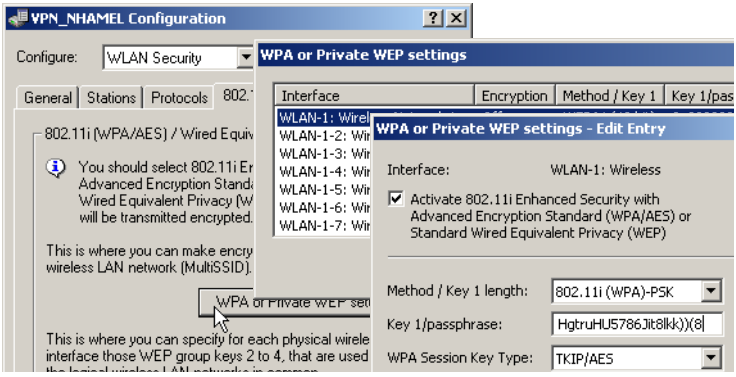
The passphrases should consist of a random string at least 22 characters long, corresponding to a cryptographic strength of 128 bits.

When set as P2P Master, the passphrase entered here will be used to check the Slave's authorization to access. When set as P2P Slave, the access point transfers this information to register with the remote site.



Configuration with LANconfig

For configuration with LANconfig you will find the encryption settings under the configuration area 'WLAN Security' on the '802.11i/WEP' tab.



EN

Configuration with WEBconfig or Telnet

The encryption settings for the individual logical WLAN networks can be found under WEBconfig or Telnet under the following paths:

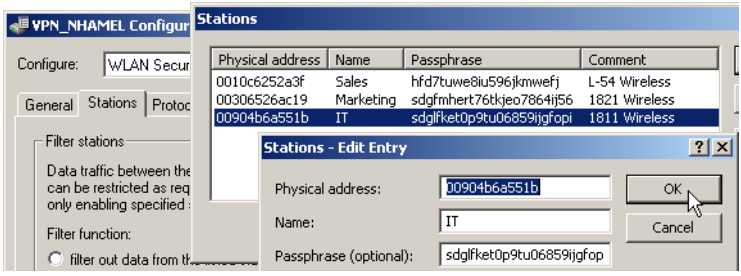
Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ Interfaces ▶ WLAN-Interfaces ▶ Encryption-Settings
Terminal/Telnet	`/Setup/Interfaces/WLAN-Interfaces/Encryption-Settings`

8.4.2 LEPS for P2P connections

A further gain in security can be attained by additionally using LANCOM Enhanced Passphrase Security (LEPS) which involves the matching of MAC address and passphrase.

LEPS can be used to secure single point-to-point (P2P) connections with an individual passphrase. Even if an access point in a P2P installation is stolen and the passphrase and MAC address become known, all other WLAN connections secured by LEPS remain secure, particularly when the ACL is stored on a RADIUS server.

When using LANconfig for the configuration, you enter the passphrases of the stations approved for the WLAN in the configuration area 'WLAN Security' on the 'Stations' tab under the button **Stations**.



Configuration with WEBconfig or Telnet

The access list for the matching of MAC addresses to the passphrases (LEPS) can be found under WEBconfig or Telnet under the following paths:

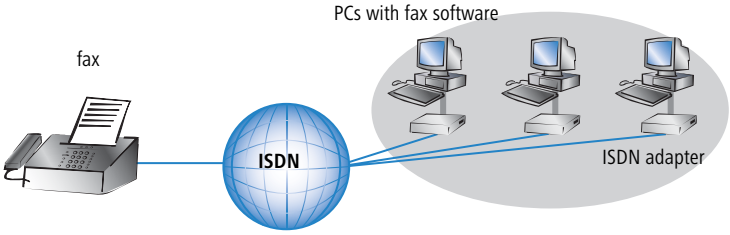
Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ WLAN-module ▶ Access-list
Terminal/Telnet	`Setup/WLAN-module/Access-list`

EN

9 Sending faxes with LANCAPI

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

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



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

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

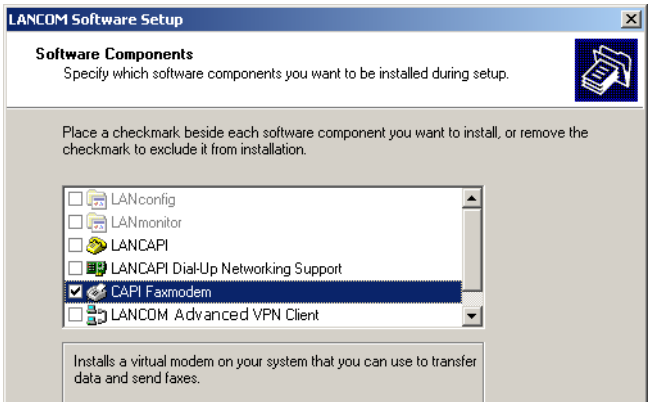
The installation of the LANCAPI client is described in the reference manual. This chapter shows the installation of LANCOM CAPI Faxmodem and MS Windows fax service.

EN

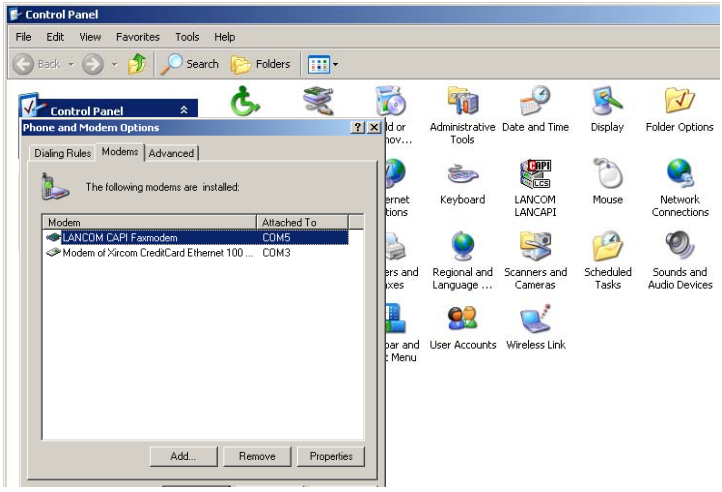
9.1 Installation of the LANCOM CAPI Faxmodem

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

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



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

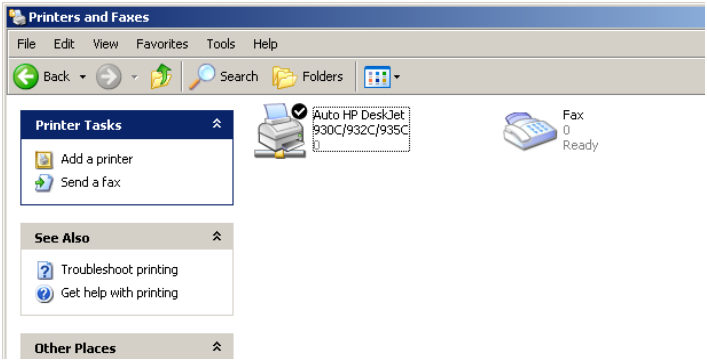


EN

9.2 Installation of the MS Windows fax service

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

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



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

9.3 Sending a fax

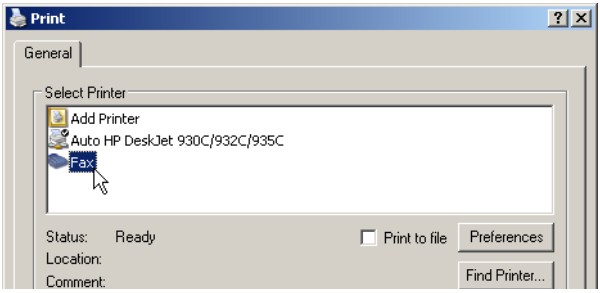
After installing all required components, you have several possibilities to send a fax from your workstation PC. If you have already an existing data file, you can send it directly from your respective application. If you only want to send a short message, select the MS Windows fax service. You can use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

9.3.1 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**.

EN

② Adjust the fax device as printer.



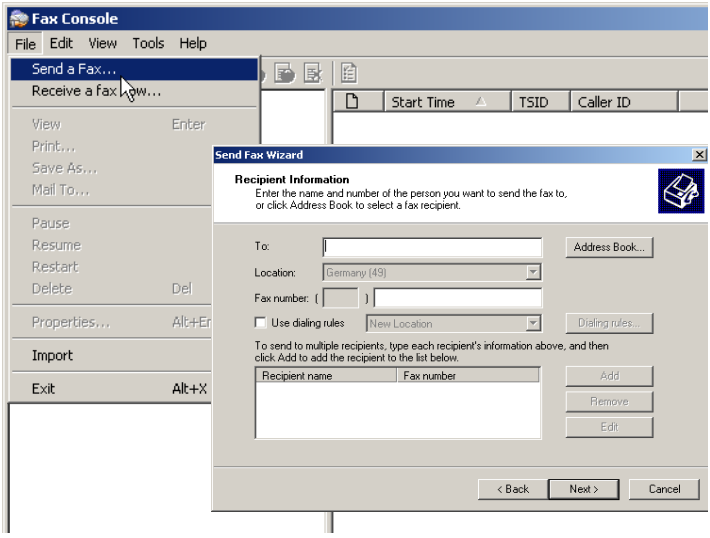
③ Click on OK. A wizard appears, that will guide you through the remaining sending process.

9.3.2 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.



10 Options and accessories

Your LANCOM device has numerous extensibilities and the possibility to use a broad choice of LANCOM accessories. You find in this chapter information about the available accessories and how to use them with your base station.

- The range of the base station can be increased by optional antennas of the LANCOM Wireless Router series and can be adapted to special conditions of environs.
- With the LANCOM Public Spot Option option it is possible to extend the LANCOM Router for additional billing and accounting functions in order to upgrade it to a Wireless Public Spot.

10.1 Optional LANCOM WLAN antennas

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

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

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

Antennas are only to be attached or changed when the device is switched off. Mounting or demounting antennas while the device switched on may cause the destruction of the WLAN module!

10.1.1 Antenna Diversity

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

EN

Transmission quality can be improved with so-called "diversity" methods. The principle of diversity methods relies on the fact that a transmitted signal is often received multiple times (generally twice). With appropriate processing, these signals can be re-combined into a single signal. The most common methods are space diversity and polarization diversity.

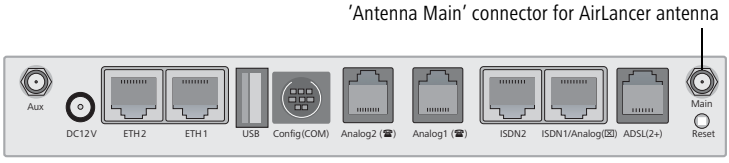
LANCOM Systems supplies a variety of polarization-diversity antennas as accessories for LANCOM Wireless Router. These models enable two orthogonally polarized signals to be received with a single antenna. Further information about this technique is available in our "Polarization Diversity" techpaper.

Polarization diversity antennas from LANCOM Systems:

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

10.1.2 Installation of AirLancer Extender antennas

For installation of an optional AirLancer antenna turn off the LANCOM Wireless Router by pulling out the power supply cable of the device. Remove now carefully the two diversity antennas on the back by screwing them out. Connect the AirLancer antennas to the antenna connector with the inscription 'Antenna Main'.



10.2 LANCOM Public Spot Option

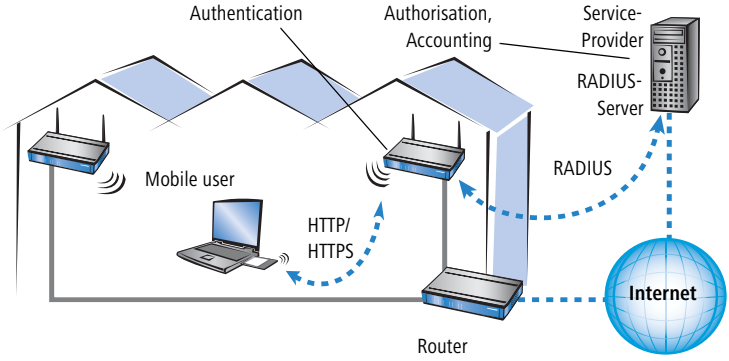
Wireless public spots are publicly accessible points, at which users with their own mobile computers can dial wirelessly into a network, usually into the Internet.

The Wireless LAN technology is ideally suitable to offer wireless Internet services to the public at places such as airports, hotels, stations, restaurants or cafés, so-called Public Hot Spots. The LANCOM Public Spot Option is intended for operators of public wireless networks, and unveils additional functions for authentication and billing of public Internet services for the LANCOM Router base station, thus enabling a simple set-up and maintenance of public hot spots.

EN

The authentication and billing of the individual users is realized via user-friendly web sites, so that client PCs with a Wi-Fi certificated radio card (e.g. AirLancer) and a standard Internet browser can directly go online.

The LANCOM Public Spot Option is the optimal solution for public Wireless LANs. Wireless LANs are very suitable for company networks and for wireless networking at home. But for public access services, there is a lack of mechanisms for authentication and billing of single users (AAA - Authentication / Authorisation / Accounting). This lack remedies the LANCOM Systems Open User Authentication (OUA), the main part of the LANCOM Public Spot Option. The OUA procedure realizes the authentication of all wireless clients via user name and password, and checks the authorization of single users via RADIUS. Accounting data (online time and data volume) can be transferred per user and per session to a central RADIUS server. Client PCs need only radio card (e.g. AirLancer), TCP/IP and an Internet browser. Additional software is not needed. Therefore, the public spot option is ideally suitable to install wireless Internet access services in hotels, restaurants, cafés, airports, stations, exhibition centres or universities.



With the LANCOM Public Spot Option you extend a base station additionally with these functions and upgrade it to a Wireless Public Spot.

EN

11 Security settings

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

11.1 The security settings wizard

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

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

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

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

11.1.1 Wizard for LANconfig

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

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

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

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

⑤ Now 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**.

11.1.2 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)

11.2 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.

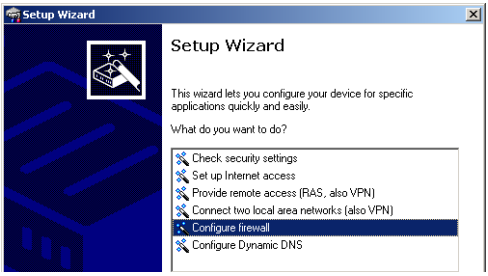
The firewall wizard assists you to create new firewall rules quickly and comfortably.

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

EN

11.2.1 Wizard for LANconfig

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



② Select in the selection menu the setup wizard **Configuring Firewall** and confirm your choice with **Next**.

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

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

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

11.2.2 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.**

11.3 Background WLAN Scanning

LANCOM 1823 VoIP only

In order to identify other access points within the device's local radio range, the LANCOM Wireless Router can record the beacons received (management frames) and store them in the scan table. Since this recording occurs in the background in addition to the access points' "normal" radio activity, it is called a "background scan".

Background scanning is used for rogue AP and rogue client detection, among others. WLAN devices that make unauthorized attempts at accessing a WLAN

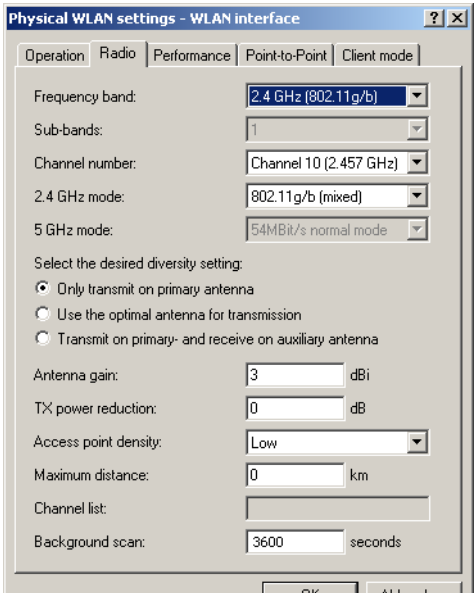
by posing as an access point or client are called rogues. An example of rogue APs are access points that a company's employees connect to the network without the knowledge or permission of the system administrators, thereby consciously or unconsciously making the network vulnerable to potential attackers via unsecured WLAN access. Not quite as dangerous, but disruptive all the same are access points that belong to third-party networks yet are within the range of the local WLAN. If such devices also use the same SSID and channel as the local AP (default settings), then local clients could attempt to log on to external networks.

Unidentified access points within the range of the local network frequently pose a possible threat and security gap. At the very least, they are a disturbance. Therefore, background scanning identifies rogue APs and rogue clients and helps to decide whether further measures in securing the local network need to be introduced.

EN

Configuring the background scan

When configuring the background scan, a time period is defined in which all available WLAN channels are to be scanned once for the receiving beacons.



Configuration tool	Call
LANconfig	WLAN interfaces ▶ Physical WLAN settings ▶ Radio
WEBconfig, Telnet	Expert configuration > Setup > Interfaces > WLAN > Radio settings

For rogue AP detection, the scan interval should be adjusted to correspond to the time span in which unauthorized access points should be recognized, e.g. 1 hour.

To avoid adverse effects on data transfer rates, the interval between channel scans should be at least 20 seconds. Lesser values will be corrected to this minimum value automatically. For example, with 13 channels to scan in the 2.4GHz band, one scan of the full spectrum takes at least 13 x 20s = 260 seconds.

11.4 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.

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

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

  For self-sufficient operations, the configuration for a WLAN interface being managed by a LANCOM WLAN Controller is stored in flash memory for a certain time only, or even in the RAM only. This device configuration is deleted if contact to the WLAN-Controller is lost or if the power supply is interrupted for longer than the set time period.

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

  ome devices simply cannot be installed under lock and key. There is consequently a risk that the configuration will be deleted by mistake of a co-worker presses the reset button too long.

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

EN

12 Configuring the ISDN and analog interfaces in detail

12.1 ISDN interface in NT or TE mode

Depending on the model, the ISDN interfaces can be used for connecting to an ISDN exchange line or for connecting up ISDN terminal equipment. The interfaces are switched into the NT or TE mode for this:

- ISDN TE interface ("external ISDN connection"): An ISDN interface in TE mode for connection to the ISDN bus of an upstream ISDN PBX or to an ISDN NTBA. This ISDN interface can be used for backup connections over ISDN or as a dial-in interface for remote stations.

With the models LANCOM 1723 VoIP and LANCOM 1823 VoIP, the ISDN2 interface can be switched into TE mode, but it must not be connected to the telephone network (NTBA), either directly or indirectly via a PBX (by means of relay/emergency switching)!

- ISDN NT interface ("internal ISDN connection"): With its ISDN interface in NT mode, the LANCOM VoIP Router itself provides an internal ISDN bus. This ISDN interface can be used to connect ISDN PBXs or ISDN telephones.

The factory settings have the ISDN interfaces marked with ☒ set to TE mode and the ISDN interfaces marked with ☎ set to NT mode. These ISDN settings can be altered according to your requirements:

- Multiple TE interfaces provide, for example, all available B channels as a backup or for dial-in.
- With multiple NT interfaces, for example, a downstream ISDN PBX can be provided with all available B channels.

Depending on the combination of ISDN interfaces in TE and NT mode, the hardware must be set up with the functions for bus termination, life-line support and power relay, and the software must be set up with the appropriate protocol. The setting for the protocol allows for the type of ISDN connection to be used (point-to-multipoint or point-to-point).

The supplied adapter must be used if a connection is to be made to an ISDN interface which is set differently to its default settings. This adapter serves to cross-over the contacts in the ISDN interface. Not using the adapter can cause damage to both the LANCOM VoIP Router and to the devices connected with it!

12.2 Bus termination, life-line support and power supply

The hardware function modes of the ISDN interfaces are set by DIP switches on the underside of the device.

- **Bus termination** is obligatory with an ISDN interface in NT mode.

  Bus termination is generally deactivated for ISDN interfaces in TE mode. If the LANCOM VoIP Router is the last device at a longer ISDN bus and this itself is not terminated, it may be advantageous to activate the bus termination for an ISDN interface in TE mode.

Not including LANCOM 1724 VoIP

- If **life-line support** is activated, the interfaces ISDN 1 and ISDN 2 are bridged if the device is unavailable due to a power outage or if the ISDN 2 interface is switched off (default: on). The life-line support is used when the LANCOM 1722 VoIP is connected to an external ISDN line over a TE interface with the simultaneous operation of ISDN terminal devices at the internal ISDN connection of an NT interface. If bridged, the ISDN devices can then use the external ISDN bus directly.

  To activate life-line support, all four DIP switches (3 to 6) must be up; to deactivate, all four DIP switches must be down.

Life-line support is to be deactivated when both ISDN interfaces are to be operated in the same mode, i.e. as two TE or two NT interfaces. The interfaces are not to be bridged in case of power failure when being operated in this manner!

LANCOM 1722 VoIP and LANCOM 1724 VoIP only

- The **ISDN power relay** means that the bus voltage of an external ISDN bus at ISDN 1 is switched through to the terminal equipment connected to ISDN 2 (LANCOM 1722 VoIP) and/or ISDN 3 (LANCOM 1724 VoIP). As a consequence, ISDN equipment operated at the internal ISDN bus of the LANCOM VoIP Router can be operated without its own power supply.

Be sure to deactivate the ISDN power relay if both ISDN interfaces are to be operated in TE mode, such as when both ISDN interfaces are connected to an ISDN NTBA, for example. A power relay in this situation would result in a short-circuit which would damage the device and the ISDN NTBAs!

To activate the power relay, the corresponding DIP switches (7 and 8 on the LANCOM 1722 VoIP, 5 and 6 on the LANCOM 1724 VoIP) must be up; to deactivate, the DIP switches must be down.

EN

LANCOM 1723 VoIP and LANCOM 1823 VoIP only

- With the **internal power supply**, the models LANCOM 1723 VoIP and LANCOM 1823 VoIP support a maximum of two telephones without their own supply; power is fed from the ISDN2 interface 8.

  To activate the internal power supply, the corresponding DIP switches (1 and 2) must be up; to deactivate, the DIP switches must be down.

The power supply switches off automatically in case of overload, and switches on again once the load drops.

① Before altering the DIP switch settings, remove all cables from their sockets.

② Remove the see-through cover of the DIP switch.

③ We suggest that you use a screwdriver to set the DIP switch to the desired position.

	LANCOM 1722 VoIP		LANCOM 1723 VoIP	
DIP	**Meaning**	**Default**	**Meaning**	**Default**
1 + 2	ISDN 2 Rx/Tx (100 Ω bus termination)	up (on)	Power supply ISDN2	up (on)
3 + 4	Life-line support	up (on)		
5 + 6		up (on)	Life-line support	up (on)
7 + 8	ISDN power relay ISDN 1 > ISDN 2	up (on)		up (on)
9 + 10	ISDN 1 Rx/Tx (100 Ω bus termination)	down (off)	ISDN 1 Rx/Tx (100 Ω bus termination)	down (off)

	LANCOM 1724 VoIP		LANCOM 1823 VoIP	
DIP	**Meaning**	**Default**	**Meaning**	**Default**
1 + 2	ISDN 4 Rx/Tx (100 Ω bus termination)	up (on)	Power supply ISDN2	up (on)
3 + 4	ISDN 3 Rx/Tx (100 Ω bus termination)	up (on)		
5 + 6	ISDN power relay ISDN 1 > ISDN 3	down (off)	Life-line support	up (on)
7 + 8	ISDN 2 Rx/Tx (100 Ω bus termination)	down (off)		up (on)
9 + 10	ISDN 1 Rx/Tx (100 Ω bus termination)	down (off)	ISDN 1 Rx/Tx (100 Ω bus termination)	down (off)

④ Plug the cable in again and start the device.

A change to the software configuration is also necessary if the ISDN interfaces are to be set to a different mode. If devices are to be connected to an ISDN interface which is set differently to its default settings, the supplied adapter must be used. This adapter serves to cross-over the contacts in the ISDN interface.

12.3 Protocol setting

Parameters for the ISDN interfaces are entered into LANconfig in the configuration area 'Interfaces' on the 'WAN' tab. Under WEBconfig, Telnet or SSH client you will find the settings for the ISDN interface parameters under `Setup/Interfaces/WAN`.

Select the protocol for each ISDN interface according to its application and the ISDN connection type: Point-to-multipoint and point-to-point connections can be used in various combinations at a LANCOM VoIP Router. The following options are available:

- **Automatic** for automatic selection of the operating mode (only in TE mode)
- **DSS1 TE (Euro ISDN)** for connection to a point-to-multipoint ISDN bus.
- **DSS1 TE point-to-point** for connection to a point-to-point ISDN bus.
- **1TR6 TE (German ISDN)** for connection an ISDN bus which uses this protocol (in Germany only).
- **DSS1 NT (Euro ISDN)** to provide point-to-multipoint ISDN interfaces
- **DSS1 NT reverse** to provide point-to-multipoint interfaces while maintaining the ISDN timing of the connected ISDN line, please refer to 'ISDN connection timing'
- **DSS1 NT (point-to-point)** to provide point-to-point ISDN interfaces
- **DSS1 NT point-to-point reverse** to provide point-to-point interfaces while maintaining the ISDN timing of the connected ISDN line, please refer to 'ISDN connection timing'

LANCOM 1724 VoIP only

- **DSS1 timing** to adopt the ISDN timing of the connected ISDN line (please refer to 'ISDN connection timing'), without signaling and other functions
- **Leased-line GRP0** for Group 0 leased lines over ISDN
- **Off**

NT mode operation always has to be set manually. With the LANCOM 1722 VoIP, if the ISDN 2 connector is set to 'Off' there may be a connection to ISDN 1 in the case that the device has been set up for lifeline support by means of the DIP switches.

If an ISDN device is attached to an ISDN interface that is set to auto and is not recognized properly, set the required protocol manually.

EN

12.4 ISDN connection timing

To ensure trouble-free transmission, all of the components in the ISDN system (LANCOM VoIP Router, upstream and downstream ISDN PBXs, ISDN terminal devices and external ISDN telephone networks) have to use the same ISDN timing. In the LANCOM VoIP Router, an ISDN interface in TE mode can take on the timing of the ISDN line. The TE interface enables the device itself to behave like a terminal device. In NT mode, the LANCOM VoIP Router can pass on the on this timing over the ISDN interfaces to any connected terminal equipment or downstream ISDN PBXs. The NT interface enables the device itself to behave like an exchange.

Various settings are available to define the ISDN interfaces with which a LANCOM VoIP Router receives the ISDN timing (to be passed on to the devices at the NT interfaces).

- **PCM synchronization bus**: Automatically selects one of all TE or (reverse configured) NT interfaces currently supplying a timing. If the selected interface stops supplying a timing (e.g. because the bus is inactive), the LANCOM VoIP Router switches to the next available interface that is supplying a timing.
- **ISDN/S0 Bus**: This setting takes on the ISDN timing from the connection for use by the LANCOM VoIP Router and further devices connected over the NT interface. In this way, the timing can be switched through in parallel to an existing ISDN PBX at a point-to-point connection.

The selected ISDN interface has to be configured for TE mode.

The ISDN-interface settings contain two more modes which play a particular role in this context:

- **DSS1 NT reverse** or **DSS1 NT point-to-point reverse**: When all ISDN interfaces are operated in NT mode, the timing system runs "freely" because there is no TE interface to take on the ISDN timing. If in this case

the ISDN connections are connected, for example, to an ISDN PBX which is being supplied with ISDN timing from another source, then interference to the transmission may arise because the timing of the LANCOM VoIP Router is not synchronous to that of the PBX. In such cases, the reverse setting allows the ISDN timing to be taken from an NT-mode interface, so ensuring that the LANCOM VoIP Router runs synchronously with the overall system.

The PBX or remote station with an interface in TE mode must be able and configured to transmit the timing.

EN

EN

13 Troubleshooting

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

13.1 No DSL connection is established

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

Problems with the cabling?

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

Has the correct transfer protocol been selected?

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

You can monitor and correct the protocol settings under:

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

13.2 DSL data transfer is slow

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

Increasing the TCP/IP window size under Windows

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

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

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

13.3 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**.

EN

14 Appendix

14.1 Performance data and specifications

		LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Connections	Ethernet LAN	4 x RJ-45 Ethernet IEEE 802.3 (Switch), 10/100Base-T-Autosensing, Node/Hub-Autodetection	2 x RJ-45 Ethernet IEEE 802.3 (Switch), 10/100Base-T-Autosensing, Node/Hub-Autodetection		
	WAN/ADSL	'Annex A' devices : ADSL over POTS as per ITU G.992.1 Annex A, ANSI T1.413, ITU G.992.2 (G.Lite), G.994.1 (G.hs);), ADSL over POTS as per ITU G.992.5 Annex A, ADSL 2+; 'Annex B' devices : ADSL over ISDN as per ITU G.992.1 Annex B, as well as proprietary ADSL over ISDN (Texas Instruments, ADI, Alcatel), ETSI TS 101 388, ADSL over ISDN as per ITU G.992.5 Annex B, ADSL 2+			
	ISDN	2 ISDN interfaces. Default: 1x NT (S_0), 1x TE.	2 ISDN interfaces. Default: 1x NT (S_0), 1x TE.	4 ISDN interfaces. Default: 2x NT (S_0), 2x TE.	2 ISDN interfaces. Default: 1x NT (S_0), 1x TE.
		ISDN interfaces are switchable with cross-over adapter to NT oder TE. Bus termination for each interface switchable by DIP switch.			
	Analog		2 analog interfaces to connect analog terminal devices or analog PBXes. 1 analog interface for connecting to analog exchange line.		2 analog interfaces to connect analog terminal devices or analog PBXes. 1 analog interface for connecting to analog exchange line.
	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			
WLAN	Frequency range				2400 - 2483,5 MHz (ISM) or 5150 - 5750 MHz
	Antennas				2 dualband dipol antennas
VoIP	Features	SIP proxy and registrar, SIP gateway/remote gateway, PBX functions for analog (1723/1823 VoIP only), ISDN and SIP subscribers			

		LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
	Voice processing	■ echo cancelling (G.168) ■ automatic adaptive de-jitter buffer ■ transparent pass-through for negotiated codecs ■ interaction on codec negotiation (filter, quality, bandwdith) ■ voice coding with G.711 µ-Law/A-Law (64 kBps), (G.726 16, 24, 32, 40 kBps), G.722 High Quality Codec (for UDI calls), G.729 Annex A Low Bandwidth Codec ■ Fax-over-IP (FoIP) with SIP and T.38 protocol			
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)			EU (CE certification: EN 55022, EN 55024, EN 60950), ETS 300 328, EN 55022, EN 301 489-1, EN 301 489-17, EN 60950
Environment / temperature range		Temperature range 5 °C to + 35 °C at 80 % max. humidity (non condensing)			

EN

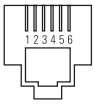
		LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Options		■ LANCOM VoIP-32 Option for upgrading to a total of 32 local SIP users (item no. 61617) ■ LANCOM VPN Option 25 channels (hardware accelerated, max. 25 simultaneous connections, 50 connections configurable) for VPN in WAN (item no.60083) ■ LANCOM Public Spot Option (item no. 60642)			
Accessories		■ LANCOM Modem Adapter Kit for connecting modems (analog or GSM) to the serial configuration interface (item no. 61500) ■ LANCOM Rack Mount Option (item no. 61501)			
Optional antennas and accessories		For all LANCOM Router models ■ LANCOM Advanced VPN Client for Windows 98SE-XP, 1 License, item no. 61600 ■ LANCOM Advanced VPN Client for Windows 98SE-XP, 10 Licenses, item no. 61601 ■ LANCOM Advanced VPN Client for Windows 98SE-XP, 25 Licenses, item no. 61602 ■ LANCOM Advanced VoIP Client for Windows 2000, XP and Windows Vista™ 1 Licenses, item no. 61610 ■ LANCOM Advanced VoIP Client for Windows 2000, XP and Windows Vista™, 10 Licenses, item no. 61611 ■ LANCOM VP-100 VoIP telephone compliant with the SIP standard, item no. 61613 ■ LANCOM VP-100 5-piece bulk set; 5 VoIP telephones compliant with the SIP standard, item no. 61614 ■ LANCOM ES-1108P compact, robust 8-port Ethernet switch with 4 PoE interfaces, item no. 61450 Only LANCOM 1823 VoIP: ■ AirLancer Extender I-180 2,4 GHz indoor antenna item no. 60914 ■ AirLancer Extender I-60ag dualband indoor antenna item no. 61214 ■ AirLancer Extender O-30 2,4 GHz outdoor antenna item no. 60478 ■ AirLancer Extender O-70 2,4 GHz outdoor antenna item no. 60469 ■ AirLancer Extender O-D80g 2,4GHz polarization diversity outdoor antenna item no. 61221 ■ AirLancer Extender O-360ag omni-directional dual-band antenna item no. 61223 ■ AirLancer Cable NJ-NP 3m extension cable item no. 61230 ■ AirLancer Cable NJ-NP 6m extension cable item no. 61231 ■ AirLancer Cable NJ-NP 9m extension cable item no. 61232 ■ AirLancer Extender SA-5 lightning protection for antenna cable item no.. 61212 ■ AirLancer Extender SA-LAN lightning protection for LAN cable item no.. 61213 ■ AirLancer Extender O-18a 5 GHz outdoor antenna item no. 61210 ■ AirLancer Extender O-D60a 5GHz polarization diversity outdoor antenna item no. 61222 ■ AirLancer Extender O-9a 5GHz directional outdoor antenna item no. 6122			

EN

14.2 Contact assignment

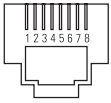
14.2.1 ADSL interface

6-pin RJ11 socket

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

14.2.2 ISDN interface ☒

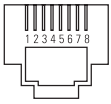
8-pin RJ45 socket, corresponding to ISO 8877, EN 60603-7, assembled as ISDN-TE for direct connection to an ISDN exchange line (NTBA)

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

EN

14.2.3 ISDN interface ☎

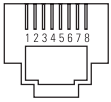
8-pin RJ45 socket, corresponding to ISO 8877, EN 60603-7, assembled as ISDN-NT for connection of ISDN terminal endpoint devices

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

14.2.4 ISDN/Analog interface ☒

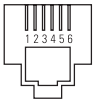
8-pin RJ45 socket, assembled as:

- ISDN-TE for direct connection to an ISDN exchange line (NTBA)
- for connection to an analog exchange line

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

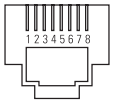
14.2.5 Analog interface ☎

6-pin RJ11 socket

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

14.2.6 Ethernet interface 10/100Base-TX

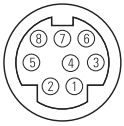
8-pin RJ45 socket, corresponding to ISO 8877, EN 60603-7

Connector	Pin	IAE
	1	T+
	2	T-
	3	R+
	4	PoE/G
	5	PoE/G
	6	R-
	7	PoE/-48 V
	8	PoE/-48 V

EN

14.2.7 Configuration interface (Outband)

8-pin mini-DIN socket

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

14.3 Declaration of conformity

CE

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

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

Index

Numerics

10/100Base-TX 42
3-DES 65, 74
802.11i 30
802.1x 30

A

Access point mode 3, 34
ADSL
  Connections 43
  Transfer rates 11
ADSL over ISDN 112
ADSL over POTS 112
AES 65, 74
Annex A 12
Annex B 12
Anschlussbelegung
  Konfigurationsschnittstelle 118
Answering machine 12
Antenna
  Outdoor 93
Autosensing 44

B

Background scanning 98
Blowfish 65, 74

C

Call-back function 31
Callback function 65, 74
Calling Line Identity (CLI) 76
CAPI interface 89
CAST 65, 74
Charge limiter 37
Common ISDN Application Programming Interface (CAPI) 89
Configuration access 55, 59
Configuration interface 31
  Connector cable 33
Configuration port 42
Configuration protection 31, 52
Connect charge protection 55, 59
Contact assignment 115
  ADSL interface 115
  DSL interface 117
  LAN interface 117
  Outband 118

D

Data frequencies 12
DDI 25
Default gateway 59
Denial-of-Service protection 15
DHCP 60
  DHCP server 26, 51, 55, 58, 60
Dial-up access 74
Dial-up adapter 78
Direct Dialing In 25
DNS
  access to the remote LAN 69
  DNS server 26, 60
Documentation 33
Domain 69
Download 6
Downstream 11
DSL
  provider 55, 59
  transfer protocol 59
DSL connection
  problems establishing the connection 110
DSL transfer protocol 55

E

EAP 30
Encryption 65, 74

EN

F

Fax 12
Firewall 14, 31, 102
Firewall filter 97
FirmSafe 31
Firmware 6
Flat rate 61

H

Hardware installation 44

I

ICMP 102
Information symbols 6
Installation 33
  ADSL 44
  Configuration interface 45
  ISDN 45
  LAN 44
  LANtools 47
  Power supply unit 46
Interconnection 65
  Security aspects 65
Internet access 26, 61
  Authentication data 61
  Flat rate 61
Internet provider 61
Intrusion detection 14
IP
  Filter 102
  Lock ports 102
IP address 44, 51, 70
IP masquerading 14, 31
IP router 26
IPSec 65, 74
IPX 78
  Binding 70, 77
  External Network Number 70, 77
  Frame type 70
  Internal-Net-Number 77
IPX conventions 70
IPX router 26
  Settings 69
ISDN
  caller ID 67, 75, 76
  Connector cable 33
  D channel 76
  password for connection 68
ISDN leased-line option 27
ISDN life line 105
ISDN modem 74
ISDN power relay 105
ISDN S_0 connection 29

L

LAN
  Connector cable 33
LAN to LAN coupling 65
  Required information 66
LANCAPI 27
LANCOM setup 47
LANconfig 49, 54
  run setup wizards 63
LAN-LAN coupling 26
LANmonitor 49
LANtools
  System requirements 34
LEPS 30
Life line 24, 105
Life-line support 29, 105
Load balancing 24
Loader 34
local break out 19

M

MAC address filter 14, 30, 31
Managed mode 3, 34
Minimum bandwidth 15
MSN 25, 76
Multi SSID 30
Multiple subscriber number 25

N
NAT – see IP masquerading
NetBIOS 70
NetBIOS proxy 26
Netmask 51
Network segment 44, 70

O
Optional antennas 93
Options and accessories 93

P
Package content 33
Password 52, 55, 65, 74
PAT – see IP masquerading
PBX 12
Ping 71
Point-to-multipoint 24, 104
Point-to-multipoint connection 25, 27
Point-to-point 24, 104
Point-to-point connection 25, 27
POTS 12
Power relay 24, 29, 105
Power supply unit 33, 42
Power switch 42
PPP 74
PPP client 78
Preshared Key
  Shared Secret 68
Public Spot Option 94

Q
Quality of Service 15

R
RAS 13
Remote Access Service (RAS)
  Configuring the dial-in computer 78
  Enable software compression 78
  IPX 77
  NetBIOS 77
  Searching for Windows workgroups 77
  Security aspects 74
  Server 26
  setup 74
  TCP/IP 76
  User name 75
Remote configuration 55, 59
Remote configuration via ISDN 31
Reset switch 43, 44
Reset the toll protection 37
Router function 11

S
SDSL modem 30
Searching for Windows workgroups 70
Security
  Firewall wizard 97
Security checklist 101
self-sufficient 3, 34
Setting up Internet access 61
SIP gateway 19
SIP PBX 20
SIP provider 17
Software installation 47
SSID 52, 55, 58
Stateful Inspection Firewall 97
Stateful-inspection firewall 14
Status display 34
  Power 36, 37
  Wireless link 41
Super AG 30
Support 6
Switch 42
System requirements 34

T
TCP 102
TCP/IP 34, 78
  check connection 71
  Settings 50, 55, 58
  Settings to PCs in the LAN 59
  Windows size 111

EN

EN

TCP/IP configuration
  Automatic 58
  fully automatic 50, 51
  manual 50, 51
TCP/IP filter 14, 31, 102
TCP/IP router
  Settings 68
TCP/IP-Filter 14
T-DSL 13
Telephone 12
Transfer protocol 110
Turbo Mode 30

U

UDP 102
Upstream 11

V

Virtual Private Network 13
Virtual Private Networks (VPN) 26
Voice communication 15
Voice frequencies 12
Voice over IP 15
VoIP 15
  Connecting subsidiaries or home offices 18
  Peer-to-peer 20
VoIP lines 22
VoIP PBX 18
VoIP users 22
VPN 13
VPN client 78
VRRP 24

W

WEBconfig 55
  password 59
  System requirements 34
WEP 30
WLAN
  Background scanning 98
WPA 30