



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

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

- Handbuch
- Manual

**LANCOM**  
Systems

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

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

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

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

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

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

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

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

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

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

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

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

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

Wuerselen, May 2009

# 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.

- 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](http://www.lancom.eu) for the latest information about your product and technical developments, and also to download our latest software versions.

### Components of the documentation

The documentation of your device consists of the following parts:

- Installation Guide
- User manual
- PBX Functions manual
- Reference manual
- Menu Reference Guide

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

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

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

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

**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.

Should you find any errors, or if you would like to suggest improvements, please do not hesitate to send an e-mail directly to:

[info@lancom.eu](mailto:info@lancom.eu)



Our online services [www.lancom.eu](http://www.lancom.eu) are available to you around the clock if you have any questions on the content in this manual, or if you 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 for LANCOM Support, please refer to the enclosed leaflet or the LANCOM Systems Web site.

**Information symbols**

Very important instructions. Failure to observe these may result in damage.



Important instruction that should be observed.



Additional information that may be helpful but is not essential.

# Contents

<b>1 Introduction</b>	<b>11</b>
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
<b>2 Installation</b>	<b>33</b>
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	47
2.6 Software installation	48
2.6.1 Starting Software Setup	48
2.6.2 Which software should I install?	49
<b>3 Basic configuration</b>	<b>50</b>
3.1 What details are necessary?	50
3.1.1 TCP/IP settings	50
3.1.2 Configuration protection	52
3.1.3 Settings for the wireless LAN	53
3.1.4 Charge protection	54
3.2 Instructions for LANconfig	54
3.3 Instructions for WEBconfig	55
3.4 TCP/IP settings for PC workstations	59



<b>4</b>	<b>Setting up Internet access</b>	<b>61</b>
4.1	The Internet Connection Wizard	63
4.1.1	Instructions for LANconfig	63
4.1.2	Instructions for WEBconfig	64
<b>5</b>	<b>Configuring the VoIP functions</b>	<b>65</b>
<b>6</b>	<b>Connecting two networks</b>	<b>66</b>
6.1	Which details are necessary?	67
6.1.1	General information	67
6.1.2	Settings for the TCP/IP router	69
6.1.3	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
<b>7</b>	<b>Providing dial-in access</b>	<b>74</b>
7.1	Which details are necessary?	74
7.1.1	General information	75
7.1.2	Settings for TCP/IP	76
7.1.3	Settings for NetBIOS routing	77
7.2	Settings on the dial-in computer	77
7.2.1	Dialing-in via VPN	77
7.2.2	Dialing-in via ISDN	77
7.3	Instructions for LANconfig	78
7.4	1-Click-VPN for LANCOM Advanced VPN Client	78
7.5	Instructions for WEBconfig	80

<b>8</b>	<b>Advanced wireless LAN configuration</b>	<b>81</b>
8.1	WLAN configuration with the wizards in LANconfig	81
8.2	Point-to-point connections	83
8.2.1	Geometric dimensioning of outdoor wireless network links	83
8.2.2	Antenna alignment for P2P operations	88
8.2.3	Measuring wireless bridges	90
8.2.4	Activating the point-to-point operation mode	90
8.2.5	Configuration of P2P connections	91
8.2.6	Security for point-to-point connections	93
8.3	Client mode	95
8.3.1	Client settings	96
8.3.2	Set the SSID of the available networks	97
8.3.3	Encryption settings	98
<b>9</b>	<b>Sending faxes with LANCAPI</b>	<b>100</b>
9.1	Installation of the LANCOM CAPI Faxmodem	101
9.2	Installation of the MS Windows fax service	102
9.3	Sending a fax	103
9.3.1	Send a fax with any given office application	103
9.3.2	Send a fax with the MS Windows fax service	103
<b>10</b>	<b>Options and accessories</b>	<b>105</b>
10.1	Optional AirLancer Extender antennas	105
10.1.1	Antenna diversity	105
10.1.2	Polarization diversity	106
10.1.3	Installing the AirLancer Extender antennas	106
10.2	LANCOM Public Spot Option	107

<b>11 Security settings</b>	<b>109</b>
11.1 Security in the wireless LAN	109
11.1.1 Suppress SSID broadcast – closed network	109
11.1.2 Access control by MAC address	109
11.1.3 LANCOM Enhanced Passphrase Security	110
11.1.4 Encrypted data transfer	110
11.1.5 802.1x / EAP	112
11.1.6 IPSec over WLAN	113
11.2 Security settings Wizard	113
11.2.1 LANconfig Wizard	114
11.2.2 WEBconfig Wizard	114
11.3 The security checklist	115
<b>12 Configuring the ISDN and analog interfaces in detail</b>	<b>120</b>
12.1 ISDN interface in NT or TE mode	120
12.2 Bus termination, life-line support and power supply	121
12.3 Protocol setting	123
12.4 ISDN connection timing	124
<b>13 Troubleshooting</b>	<b>126</b>
13.1 No DSL connection is established	126
13.2 DSL data transfer is slow	126
13.3 Unwanted connections under Windows XP	127
<b>14 Appendix</b>	<b>128</b>
14.1 Performance data and specifications	128
14.2 Contact assignment	131
14.2.1 ADSL interface	131
14.2.2 ISDN interface ☒	131
14.2.3 ISDN interface 📞	132
14.2.4 ISDN/Analog interface ☒	132
14.2.5 Analog interface 📞	133
14.2.6 Ethernet interface 10/100Base-TX	133
14.2.7 Configuration interface (Outband)	134
14.3 Declaration of conformity	134

# 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 LANCAP, 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.

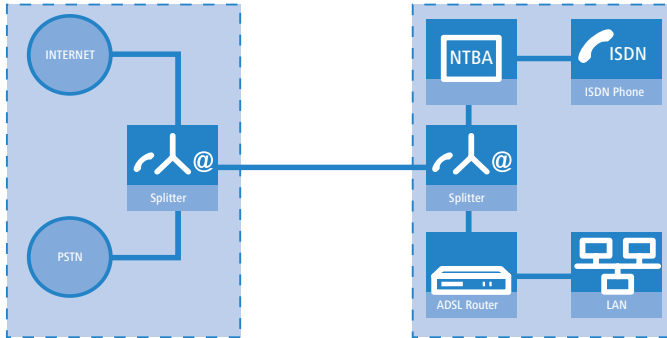
The asymmetric DSL variant ADSL was developed for applications where users receive large amounts of data but transmit only small amounts, such as when surfing in the WWW. ADSL subscribers can receive data at up to 8 Mbps ("downstream") and transmit at up to 800 kbps ("upstream"). ADSL providers are able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

To satisfy the strongly increasing demand for higher bandwidths, the standards ADSL 2 and ADSL 2+ provide 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 interoperable.

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 – Plain Old Telephone Service). 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.

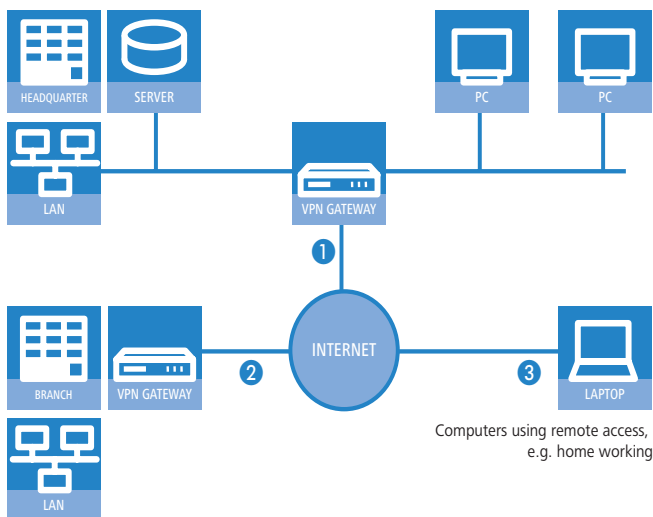
There are even ADSL-over-ISDN connections which are not combined with an ISDN connection, but with a standard analog telephone connection instead.

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**riate **N**etwork) can be used to set up secure data communications over the Internet.

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



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

- ① All that is required is the Internet connection of the LAN in the headquarters. Special switching devices or routers for dedicated lines to individual participants are superfluous.
- ② The subsidiary also has its own connection to the Internet.
- ③ The RAS PCs connect to the headquarters LAN via the Internet.

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

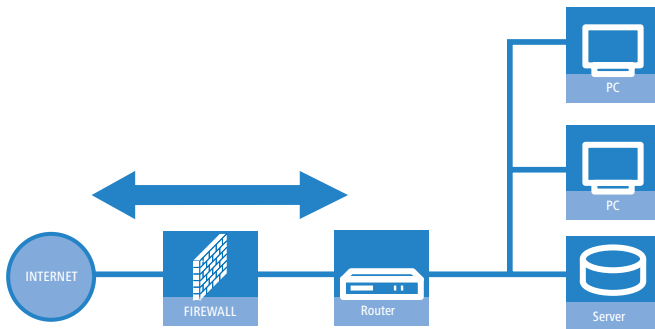
The physical connection no longer exists directly between two participants; instead, the participants rely on their connection to the Internet. The access technology used is not relevant in this case: Broadband technology such as DSL (Digital Subscriber Line) is ideal. A conventional ISDN line can be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

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

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

### 1.3 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

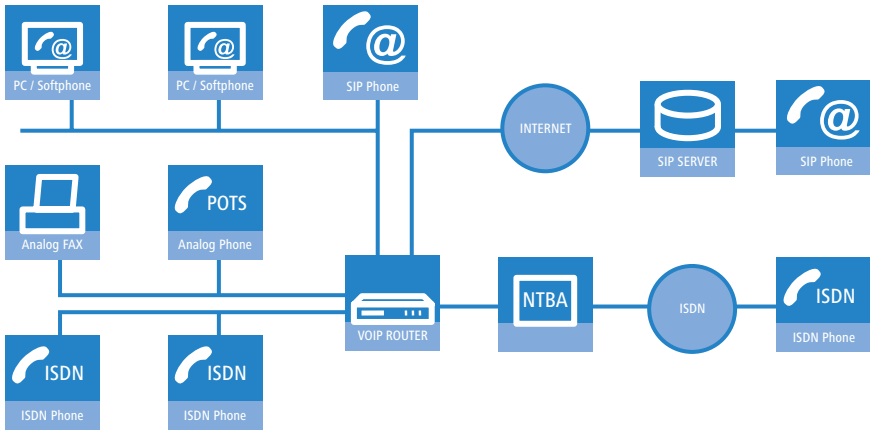
In many cases, LANCOM VoIP Routers can completely replace a local PBX. With up to eight voice channels (e.g. LANCOM 1724 VoIP) to landlines, the



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.

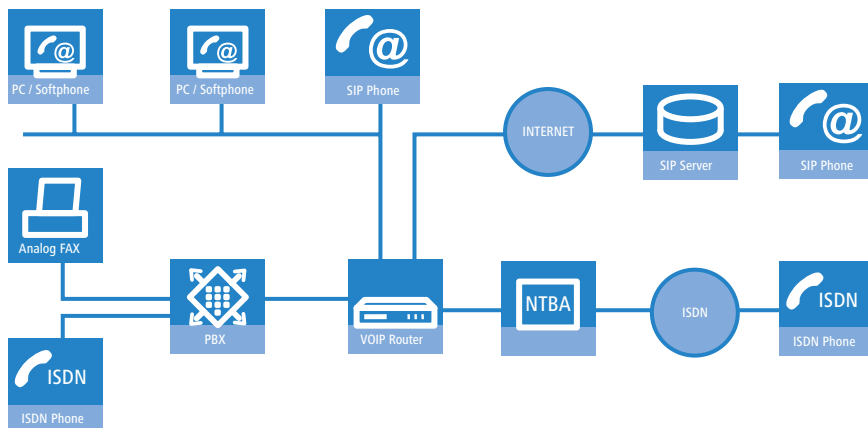
A systematic set of instructions for setting up the LANCOM VoIP Router for this purpose can be found in the PBX Functions manual. Beforehand, we recommend that you read the following chapters on the basic setup of devices and software, and then carry out a basic configuration. You should also have set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

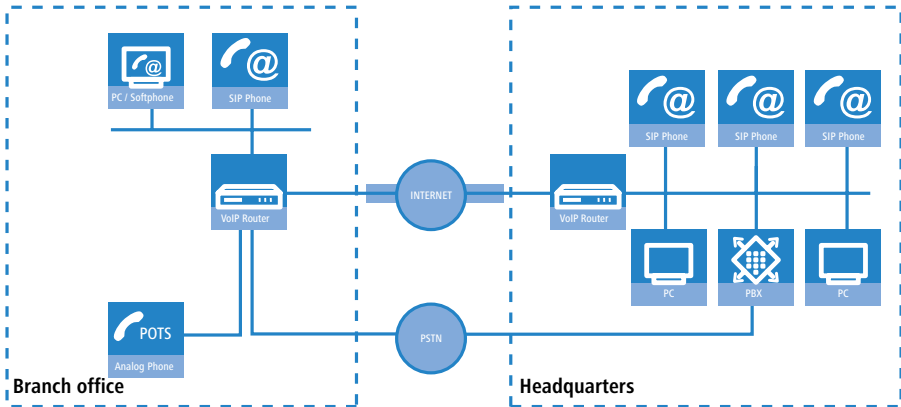
codes to decide upon the switching of a call either via the ISDN interface, or via the Internet as a VoIP call.

### 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.

## 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.

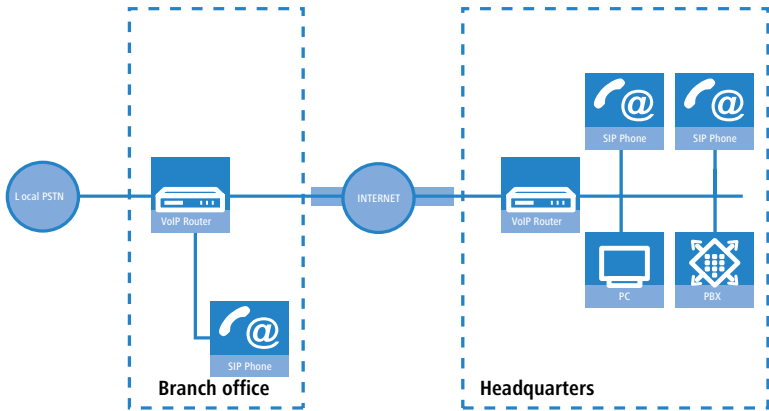
With the SIP trunking function, entire ranges of telephone numbers made up of external numbers and their associated extensions can be mapped by LANCOM VoIP Routers over a single connection to a SIP provider, assuming that the provider also supports Direct Dialing In (DDI) and can provide multiple connections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

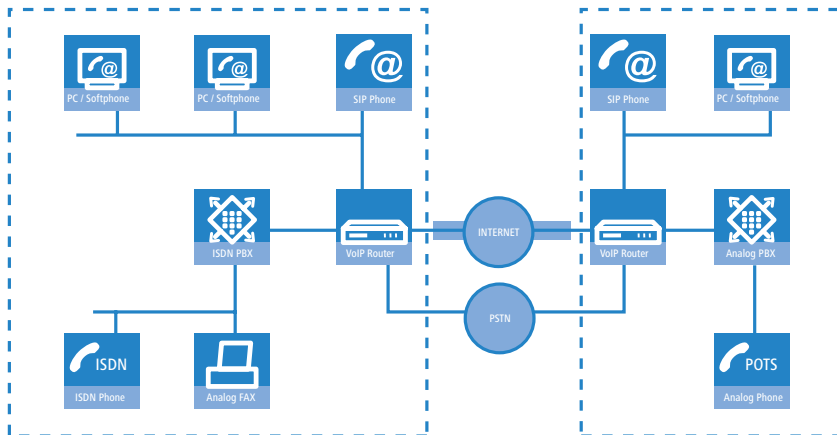
### Connecting sites without a SIP PBX

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.

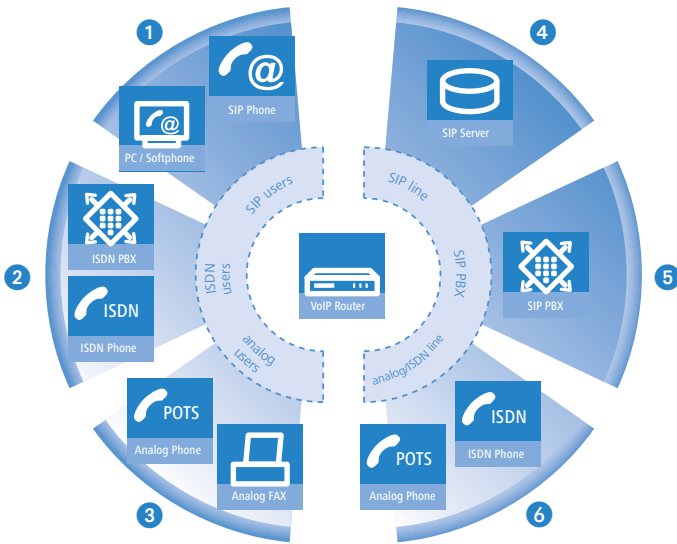
**Example: Sites with ISDN or analog lines**

EN

**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



## 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:

**■ 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.





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 telephone 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.

## 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
<b>Applications</b>				
Internet access	✓	✓	✓	✓
LAN-LAN coupling over VPN	✓	✓	✓	✓
LAN-LAN coupling over ISDN	✓	✓	✓	✓
RAS server (over VPN)	✓	✓	✓	✓
RAS server (over ISDN)	✓	✓	✓	✓
IP router	✓	✓	✓	✓
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				✓
Layer-2 QoS Tagging	✓	✓	✓	✓

		LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
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.		✓	✓	✓	✓
<b>VoIP functions</b> 					
<b>SIP proxy and registrar</b>	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
<b>SIP gateway</b>	Free choice from available ISDN S <sub>0</sub> 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

## ■ Chapter 1: Introduction

		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	✓	✓	✓	✓
<b>Call router</b>	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	✓	✓	✓	✓
<b>Voice processing</b>	Echo canceling and de-jitter buffer for SIP connections	✓	✓	✓	✓
	Transparent pass-through for negotiated codecs	✓	✓	✓	✓
	Interaction on codec negotiation (filter, quality, bandwidth)	✓	✓	✓	✓

	LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
<b>WAN connections</b>				
Connector for DSL or cable modem	✓	✓	✓	✓
Integrated ADSL modem (with ADSL2+)	✓	✓	✓	✓
ISDN S <sub>0</sub> 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 <sub>0</sub> 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 an analog terminal device or an analog PBX (tone dialing).		2		2
Analog FXS connector for connecting the LANCOM VoIP Router to an analog exchange line or to an upstream analog PBX (tone dialing), 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)	✓	✓	✓	✓
<b>WLAN</b>				
Wireless transmission compliant with IEEE 802.11g and IEEE 802.11b				✓
Wireless transmission compliant with IEEE 802.11a and IEEE 802.11b				✓

## ■ Chapter 1: Introduction

	LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Point-to-point mode (six P2P paths can be defined per WLAN interface)				✓
Relay function to link two P2P connections				✓
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)				✓
<b>LAN connection</b>				
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

	LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
<b>USB connector</b>				
USB 2.0 host port (full speed: 12 Mbps) for connecting a USB printer and for future extensions	✓	✓	✓	✓
<b>Security functions</b>				
IPSec encryption via external software (VPN client)	✓	✓	✓	✓
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.	✓	✓	✓	✓
<b>Configuration</b>				
Configuration with LANconfig or via web browser; additional terminal mode for Telnet or equivalent terminal programs; SNMP interface and TFTP server function.	✓	✓	✓	✓
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	✓	✓	✓	✓
<b>Optional software extensions</b>				
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	✓	✓	✓	✓



■ Chapter 1: Introduction

EN

	LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
<b>Optional hardware extensions</b>				
LANCOM Modem Adapter Kit for connecting analog or GSM modems to the serial interface	✓	✓	✓	✓
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

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.

## 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, 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).

Split management can be used to separate the WLAN configuration from the rest of the router configuration. This allows router settings and VPN settings to be adjusted locally, for example in a branch office or home office installation, and the WLAN configuration is regulated by a LANCOM WLAN Controller at the main office.

## 2.3 Introducing the LANCOM Router

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

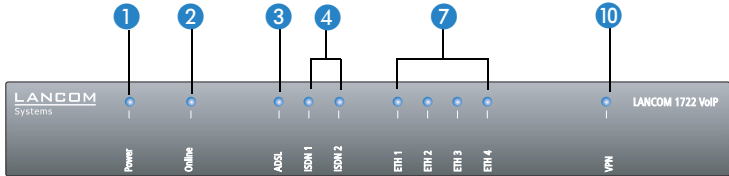
### 2.3.1 Status displays

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

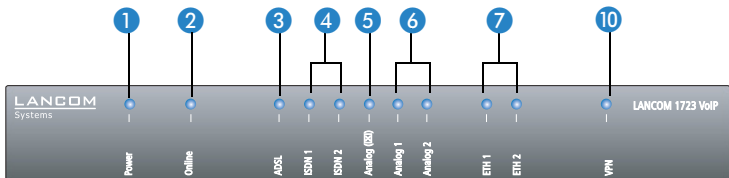
## Front

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

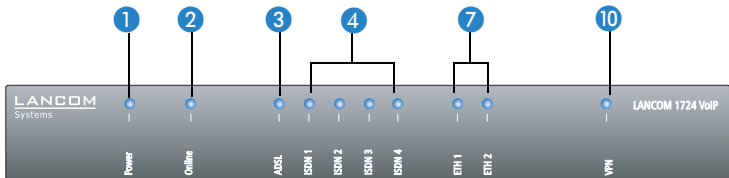
LANCOM 1722 VoIP



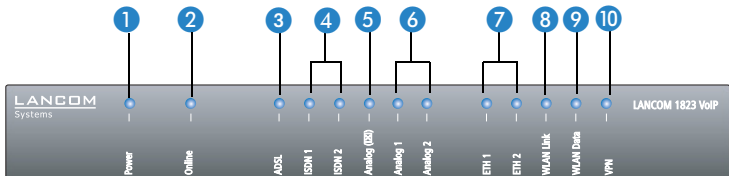
LANCOM 1723 VoIP



LANCOM 1724 VoIP



LANCOM 1823 VoIP



## 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.

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	Time or charge limit on online connections has been reached



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

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

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

There are three ways to remove the lock:

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

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

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



Signal that a charge or time limit has been reached

## Chapter 2: Installation

### 2 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

## 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)



## ■ Chapter 2: Installation

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

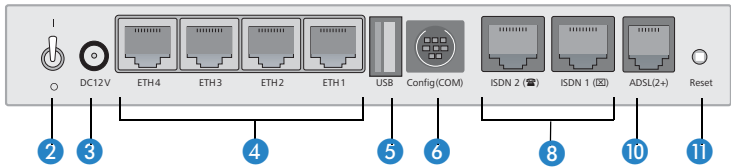
Status of a VPN connection.

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

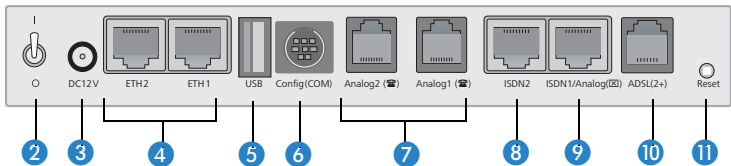
### 2.3.2 Device connectors

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

LANCOM 1722 VoIP

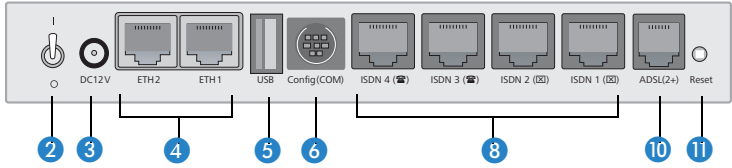


LANCOM 1723 VoIP

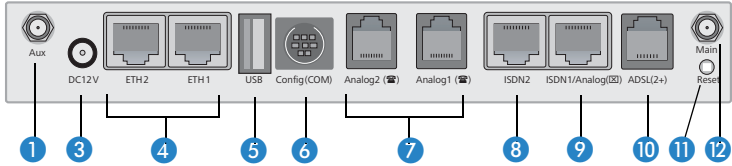


■ Chapter 2: Installation

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

LANCOM 1723 VoIP and LANCOM 1823 VoIP only

- 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<sub>0</sub>, 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

### Reset button functions

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

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

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

### ■ Reset button

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

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



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

- Reset-or-boot (standard setting): Press the button briefly to re-start the device. Pressing the button for 5 seconds or longer restarts the device and resets the configuration to its factory settings.

All LEDs on the device light up continuously.

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



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



- 12 Main connector for the WLAN module.

Only LANCOM  
1823 VoIP

## 2.4 Hardware installation

Installation of the LANCOM Router involves the following steps:

- ① **Antennas** – screw the antennas supplied to the back of the LANCOM VoIP Router.



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!



When assembling separately purchased antennas please note that the maximum allowed transmission power of the wireless LAN according to EIRP in the country in question may not be exceeded. The system operator is responsible for adhering to the threshold values.

- ② **LAN** – 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.

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


**4 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<sub>0</sub> 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 120).



**5 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 120).


- ⑥ **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.
- ⑦ **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 121).

- ⑧ **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.
- ⑨ **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.
- ⑩ **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.

- ⑪ **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 Functions manual.



Detailed information on the significance of DIP switch settings and the setup of individual ISDN and analog interfaces are available in the chapter 'Configuring the ISDN and analog interfaces in detail' → page 120. For other deployment scenarios from those described above, or for other interface configurations, we strongly 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.

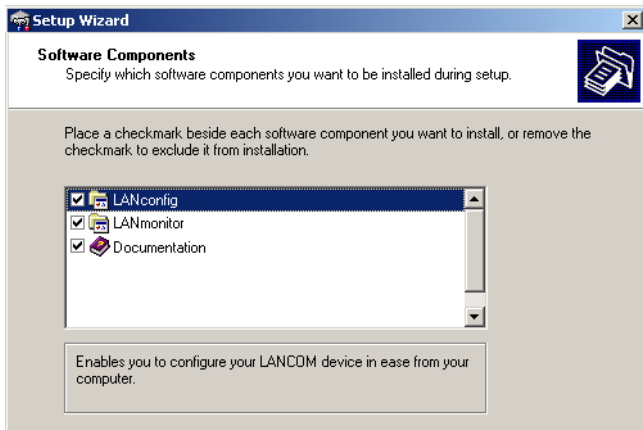
### 2.6.1 Starting Software Setup

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.

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



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

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

## 3 Basic configuration

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

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

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

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

### 3.1 What details are necessary?

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

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

#### 3.1.1 TCP/IP settings

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

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

### New LAN – fully automatic configuration possible

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

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

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

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

### Should you still configure manually?

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

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

### Required information for manual TCP/IP configuration

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

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

- Server: The LANCOM VoIP Router operates as DHCP server in the network; as a minimum its own IP address and the network mask must be assigned.
- Client: The LANCOM VoIP Router obtains its address information from another DHCP server; no address information is required.

#### ■ IP address and network mask for the LANCOM VoIP Router

Assign the LANCOM VoIP Router a free IP address from your LAN's address range and enter the network mask.

#### ■ Gateway address

Enter the gateway's IP address if you have selected 'Off' as the DHCP mode of operation or if another network device is assuming the role of gateway in the 'Server' mode of operation.

#### ■ DNS server

Enter the IP address of a DNS server to resolve domain names if you have selected 'Off' as the DHCP mode of operation or if another network device is assuming the role of DNS server in the 'Server' mode of operation.

### 3.1.2 Configuration protection

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



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



In the managed mode 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

#### Network name (SSID)

The Basic Settings Wizard prompts for the access point's network name (frequently referred to as SSID – **S**ervice **S**et **I**dentifier). The name is of your own choice. Several access points with the same name form a common wireless LAN.

#### Open or closed wireless LAN?

Mobile wireless devices select the desired wireless LAN by specifying the network name. Two methods serve to facilitate the specification of network name:

- Mobile wireless devices can search ("scan") the vicinity for wireless LANs and offer the wireless LANs they find in a list for selection.
- By using the network name 'ANY' the mobile wireless device registers with the nearest available wireless LAN.

The wireless LAN can be "closed" in order to prevent this procedure. In this case it will not accept any devices attempting to register with the network name 'ANY'.

#### Selecting a radio channel

The access point operates in a specific radio channel. The radio channel is selected from a list of up to 13 channels in the 2.4 frequency band or up to 19 channels in the 5 GHz frequency band (individual radio channels are blocked in some countries. Please refer to the appendix for more details).

The channel and frequency range used determine the operation if the common wireless standard, with the 5 GHz frequency range corresponding to the IEEE 802.11a/h standard and the 2.4 GHz frequency range determining operation in the IEEE 802.11g and IEEE 802.11b standards.

If no other access points are operating within the access point's range, any radio channel can be set. Otherwise the channels in the 2.4 GHz band must be selected in such a way that they do not overlap and are as far apart as possible. In the 5 GHz band the automatic setting, where the LANCOM Access Point uses TPC and DFS to select the best channel is normally sufficient.



Please refer to the LCOS reference manual for more information on TPC and DFS.

### 3.1.4 Charge protection

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

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

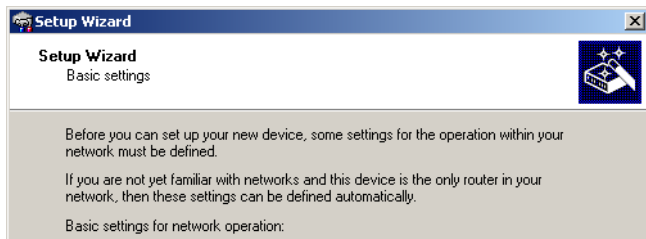
The budget can be completely deactivated by entering a value of '0'.



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

## 3.2 Instructions for LANconfig

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



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

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




③ Give the LANCOM an address from the applicable IP address range. Confirm with **Next**.

④ In the window that follows, you first set the password to the configuration. Entries are case sensitive and should be at least 6 characters long.

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


---

 Be aware that releasing this option also allows remote configuration over the Internet. Whichever option you select, make sure that configuration access is password protected.

⑤ Charge protection is a function which can place a limit on the costs from WAN connections. Accept your entries with **Next**.

⑥ Close the configuration with **Finish**.

---

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

### 3.3 Instructions for WEBconfig


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

#### Secure with HTTPS

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

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

---

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



## Accessing the device with WEBconfig

To carry out a configuration with WEBconfig, you need to know how to contact the device. Device behavior and accessibility for configuration via a Web browser depend on whether the DHCP server and DNS server are active in the LAN already, and whether these two server processes share the assignment in the LAN of IP addresses to symbolic names. WEBconfig accesses the LANCOM either via its IP address, the device name (if configured), or by means of any name if the device has not yet been configured.

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



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 upon provision of the WLAN configuration.

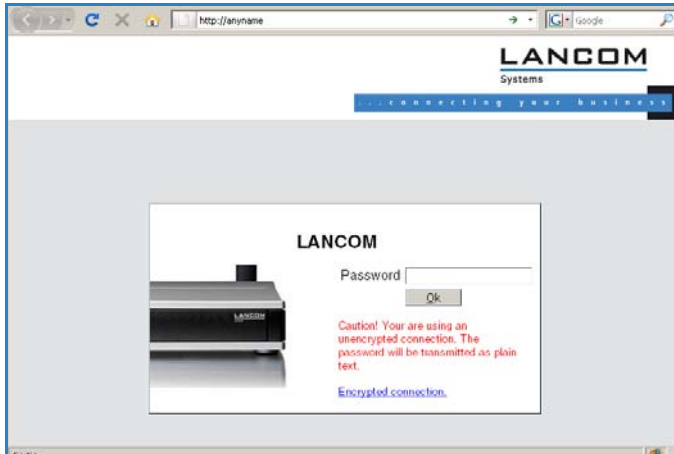
## Network without a DHCP server

Not for centrally managed LANCOM Wireless Routers or LANCOM Access Points

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



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

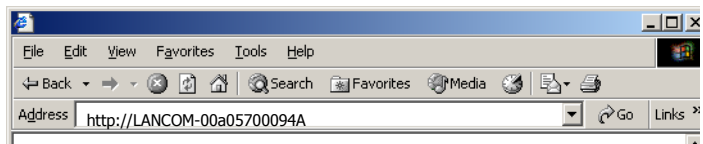


If the configuration computer does not retrieve its IP address from the LANCOM DHCP server, it determines the current IP address of the computer (with **Start ▶ Run ▶ cmd** and command **ipconfig** at the prompt under Windows 2000 or Windows XP or Windows Vista, with **Start ▶ Run ▶ cmd** and command **winipcfg** at the prompt under Windows Me or Windows 9x, or with command **ifconfig** in the console under Linux). In this case, the LANCOM can be accessed with address **x.x.x.254** (the "x"s stand for the first three blocks in the IP address of the configuration computer).

### Network with DHCP server

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

- If the LAN also has a DNS server for name resolution and this communicates the IP address/name assignment to the DHCP server, the device can be reached under name "LANCOM-<MAC address>", e.g. "LANCOM-00a057xxxxx".





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

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

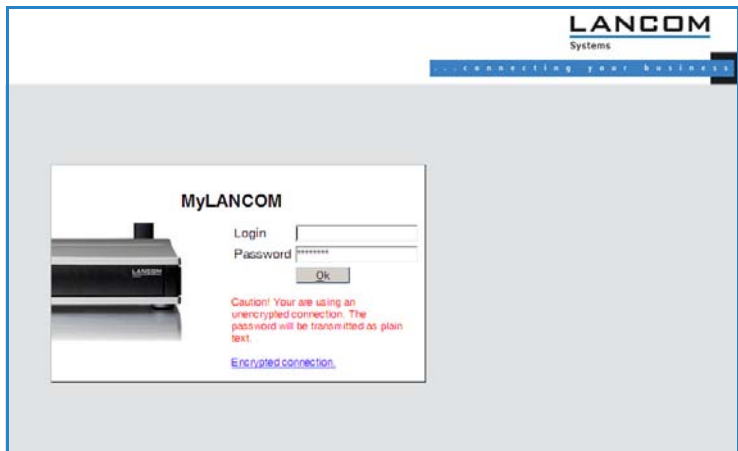
### Login

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

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

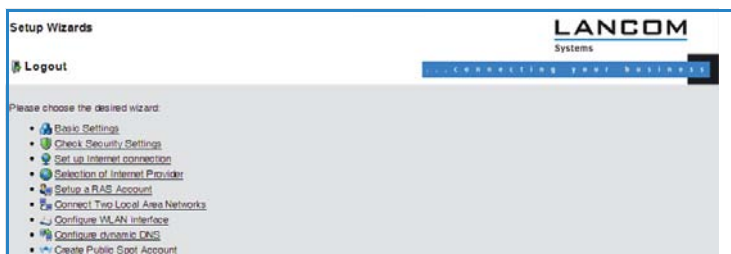


As an alternative, the login dialog provides a link for an encrypted connection over HTTPS. Always use the HTTPS connection for increased security whenever possible.



## Setup Wizards

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



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

## 3.4 TCP/IP settings for PC workstations

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

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

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

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

### ■ IP address allocation by a LANCOM

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

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

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

**■ Manual IP address assignment**

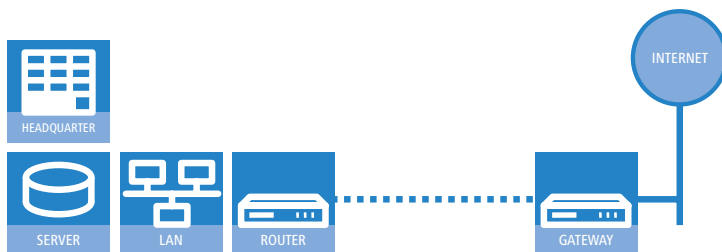
If IP addresses in a network are statically assigned, then the IP address of the LANCOM is to be set as the standard gateway and DNS server in the TCP/IP configuration of each PC in the LAN.



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

## 4 Setting up Internet access

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



### Which WAN interface?

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

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

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

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

### Internet provider unknown

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

### Other connection options

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

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

### Creating a backup connection to the Internet

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

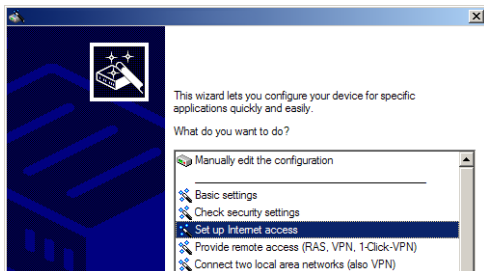


When configuring the backup connection you can set up an alternative provider, if available. This allows you not only to overcome problems with the physical line, but also problems in your provider's own network as well.

## 4.1 The Internet Connection Wizard


### 4.1.1 Instructions for LANconfig

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



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

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

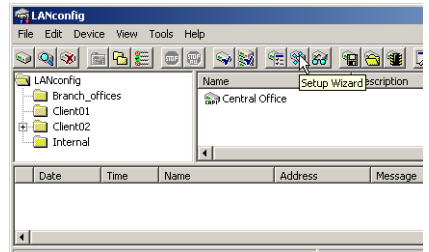
-  Please be aware that in the case of backup via UMTS, some of the services provided over the main Internet connection may not be available. Some UMTS service providers either prevent the use of VPN tunnels or VoIP applications or only allow them after payment of additional fees. Other providers assign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



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

### LANconfig: Fast starting of the Setup Wizards

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



#### 4.1.2 Instructions for WEBconfig

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

## 5 Configuring the VoIP functions

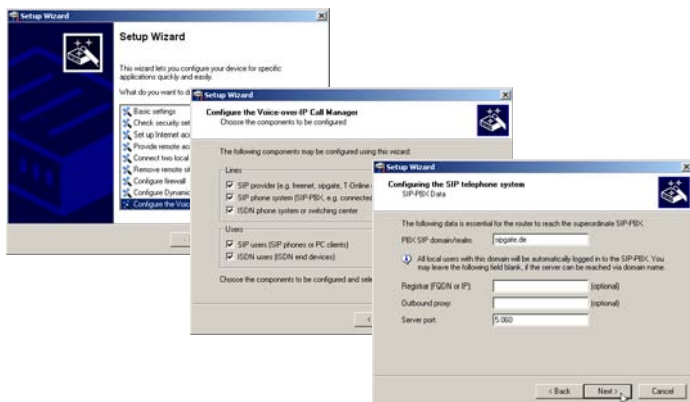
If you wish to employ the LANCOM VoIP Router as a PBX, you should initially carry out the basic settings and then read the manual on the VoIP PBX functions. This describes the quickest way to set up the PBX with connections to landlines (ISDN or analog).

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 Connecting two networks

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

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

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

### Always configure both ends

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



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

### Security aspects

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

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



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

## 6.1 Which details are necessary?

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

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






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

### 6.1.1 General information

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



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

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

## ■ Chapter 6: Connecting two networks

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

Notes on the different settings:

- If your own device features an **ISDN connection**, the Wizard will ask you whether the remote site also has one.
- For VPN connections over the Internet, the type of IP address at each end must be specified. There are two **types of IP address**. Static and dynamic. The differences between these two IP address types are explained in the Reference Manual.

The Dynamic VPN function makes it possible to establish VPN connections between gateways with dynamic IP addresses, and not only between gateways with static (fixed) IP addresses. An ISDN connection is required to actively establish VPN connections to remote sites that use dynamic IP addresses.

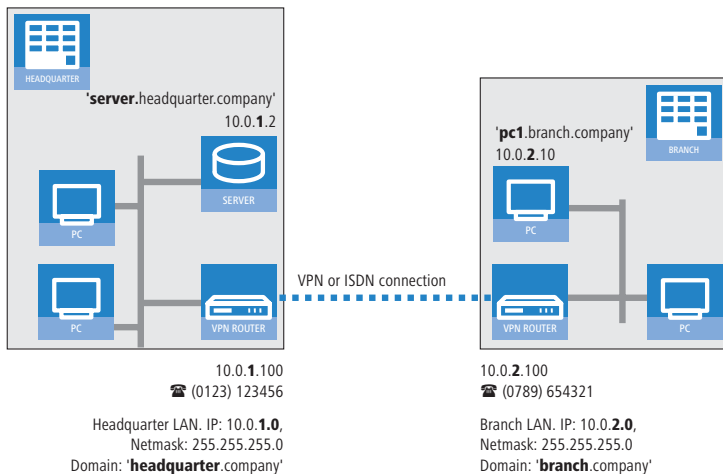
- If you have not yet given a name to your LANCOM, the Wizard will ask you to enter a new **name for your device**. Entering a name will cause your LANCOM to be renamed. Ensure that you give different names to the two remote devices.
- The **name of the remote site** is required for identifying the devices.
- In the field **ISDN number** the telephone number of the remote ISDN site is specified. Enter the full telephone number for the remote site, including all necessary prefixes (e.g. area codes).
- The **ISDN calling line ID** specified is used to identify and authenticate the caller. If a LANCOM Router is called, it compares the ISDN calling line ID entered for the remote site to the ID that is actually received over the D

channel from the caller. An ISDN ID generally consists of the country code and an MSN.

- The **password for the ISDN connection** is an alternative to the ISDN calling line ID. This is used to authenticate the caller if no ISDN calling line ID is received. The password must be entered identically at both ends. It is used for calls in both directions.
- The **shared secret** is the central password for the VPN connection's security. It must be entered identically at both ends.
- Data compression improves transmission speeds without incurring extra costs. This is completely different to the bundling of two ISDN channels by MLPPP (**M**ulti**L**ink-**P**PP): This doubles the bandwidth, although this generally doubles the connection costs as well.

### 6.1.2 Settings for the TCP/IP router

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



Unlike with Internet access, network connectivity makes all of IP addresses visible in all participating networks, including those in the remote LAN, and not just that of the router. The computer with the IP address 10.0.2.10 in the branch-office LAN sees the server 10.0.1.2 at the main office and, with the appropriate rights, has access to it. The same applies in the other direction.

## DNS access to the remote LAN

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

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



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

## VPN extranet

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

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

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

### 6.1.3 Settings for NetBIOS routing

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

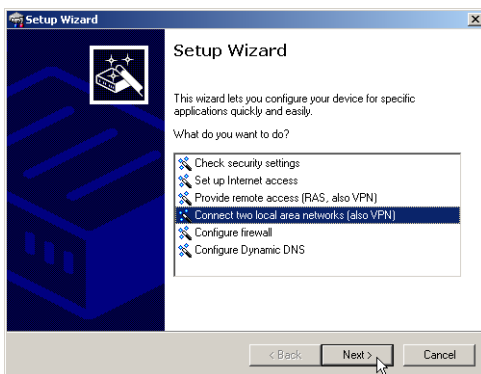


Remote Windows workgroups do not appear in the Windows network environment, but they can be contacted directly (e.g. by searching for a computer of known name).

## 6.2 Instructions for LANconfig

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

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



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

### Ping – the quick test of a TCP/IP connection

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

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

```

C:\>ping 10.0.2.0

Pinging 10.0.2.0 with 32 bytes of data:

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

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

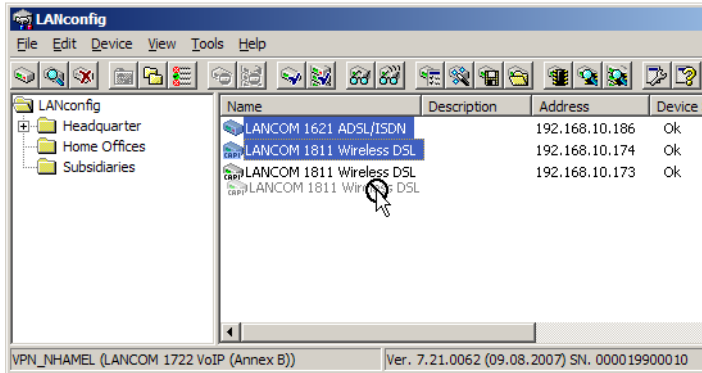
```



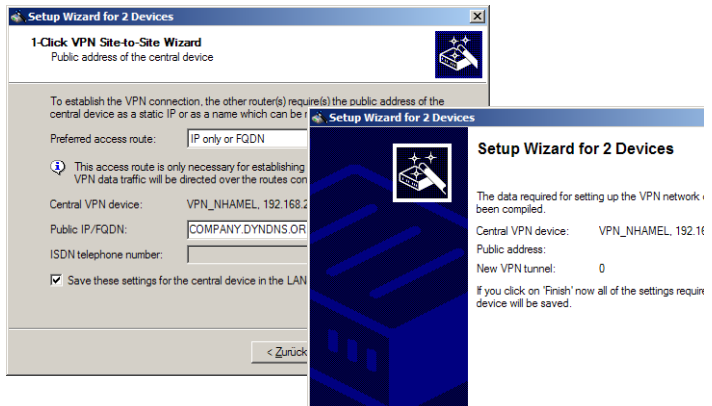
## 6.3 1-Click-VPN for networks (site-to-site)

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

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




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




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

---

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

## 6.4 Instructions for WEBconfig

---

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

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

- ① In the main menu, launch the Wizard 'Connect two local area networks'. Follow the Wizard's instructions and enter the necessary data.
- ② The Wizard will inform you when the required information is complete. You can then close the Wizard with **Next**.
- ③ Once you have completed the set-up of both routers, you can start testing the network connection. Try to communicate with a computer in the remote LAN (e.g. with `ping`). The LANCOM Router should automatically connect to the remote site and make contact to the requested computer.

## 7 Providing dial-in access

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

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

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

### Security aspects

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

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

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



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

### 7.1 Which details are necessary?

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

### 7.1.1 General information

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



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

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

Notes on the different settings:

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



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

### The ISDN calling line ID (CLI)

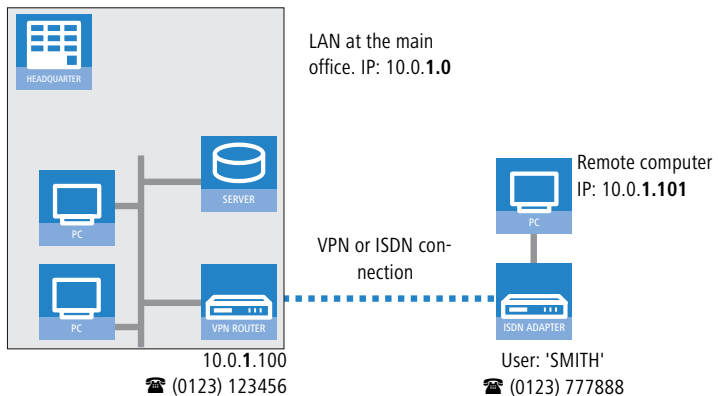
The ISDN Calling Line Identity (CLI) is the phone number of the calling party as transmitted to the called party. This is a number generally made up of the national dial code and an MSN.

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

EN

## 7.1.2 Settings for TCP/IP

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



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

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

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

### 7.1.3 Settings for NetBIOS routing

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



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

## 7.2 Settings on the dial-in computer

### 7.2.1 Dialing-in via VPN

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

- Internet access
- A VPN client

LANCOM Systems offers you a 30-day test version of the LANCOM Advanced VPN Client on the CD supplied. A precise description of the VPN client and notes on its setup are also to be found on the CD.

The Wizard then requests the parameters that were specified when setting up the RAS access in the LANCOM Router.

### 7.2.2 Dialing-in via ISDN

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

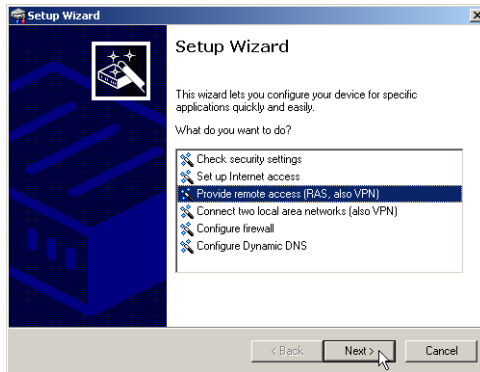
- Dial-Up Networking (or any other PPP client) installed correctly.
- Network protocol (TCP/IP) installed and associated with the dial-up adapter
- New connection in Dial-Up Networking with the phone number of the router
- Terminal adapter or ISDN card set up for PPPHDLC
- PPP selected and the dial-up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

- 'IP header compression' deactivated

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

## 7.3 Instructions for LANconfig

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



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

## 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 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

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

## 8 Advanced wireless LAN configuration

The configuration of the LANCOM Access Points for your wireless LAN is conducted with the aid of highly convenient installation wizards.

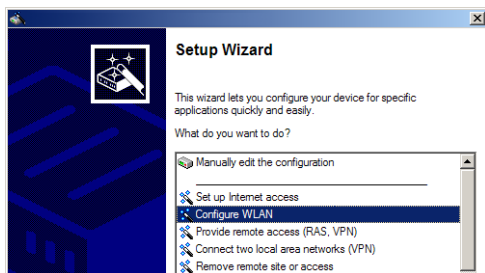
The settings include the general, far-reaching parameters and also the individual settings for one or more logical wireless LAN networks (WLAN radio cells or SSIDs).

### 8.1 WLAN configuration with the wizards in LANconfig

Highly convenient installation wizards are available to help you with the configuration of LANCOM Access Points for your wireless LAN.

The settings include the general shared parameters and also the individual settings for one or more logical wireless LAN networks (WLAN radio cells or SSIDs).

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



- 2 In the selection menu, select the Setup Wizard, **Configure WLAN interface** and confirm the selection with **Continue**.
- 3 Make the settings as requested by the wizard and as described as follows.

#### Country settings

Regulations for the operation of WLAN cards differ from country to country. The use of some radio channels is prohibited in certain countries. To operate the LANCOM Access Points while observing the regulations in various countries, all physical WLAN interfaces can be set up for the country where they are operated.

## WLAN module operation

The WLAN modules can be operated in various operating modes:

- As a base station (Access Point mode), the device makes the link between WLAN clients and the cabled LAN. Parallel to this, point-to-point connections are possible as well.
- In Managed Mode the Access Points also accept WLAN clients into the network, although the clients then join a WLAN infrastructure that is configured by a central WLAN-Controller. In this operating mode, no further WLAN configuration is necessary as all WLAN parameters are provided by the WLAN-Controller.
- In client mode, the device itself locates the connection to another Access Point and attempts to register with a wireless network. In this case the device serves, for example, to link a cabled network device to an Access Point over a wireless connection. In this operating mode, parallel point-to-point connections are **not** possible.

For further information please refer to section → Client Mode.

## Physical WLAN settings

Along with the radio channels, the physical WLAN settings can also be used to activate options such as the bundeling of WLAN packets (TX Burst), hardware compression, or the use of QoS compliant with 802.11e. You also control the settings for the diversity behavior here.

## Logical WLAN networks

Each WLAN module can support up to eight logical WLAN networks for mobile WLAN clients to register with. The following parameters have to be set when configuring a logical WLAN network:

- The network name (SSID)
- Open or closed radio LAN
- Encryption settings
- MAC filter
- Client-bridge operation
- Filter settings

### Point-to-point settings

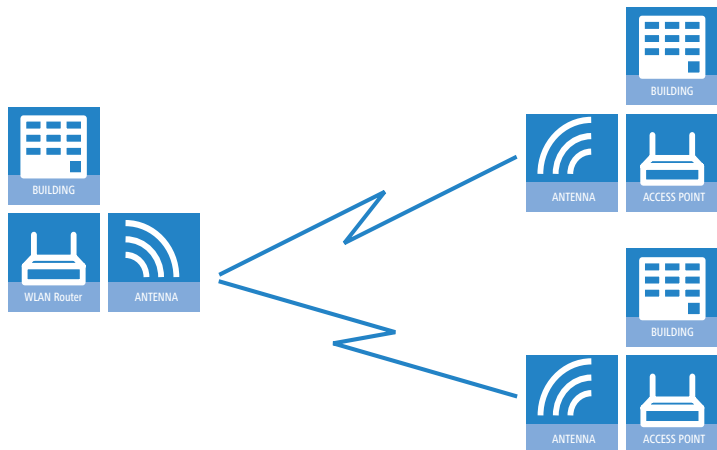
The configuration of P2P connections involves setting not only the operating mode but also the station name that the Access Point can connect to. Also, the role as "Master" or "Slave" is set here.

Along with the settings for the Access Point itself, also to be defined is the remote site that the Access Point can contact via the P2P connection.

For further information please refer to section → Point-to-point connections.

## 8.2 Point-to-point connections

LANCOM Access Points can serve not only as central stations in 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.



This chapter introduces the basic principles involved in designing point-to-point links and provides tips on aligning the antennas.

### 8.2.1 Geometric dimensioning of outdoor wireless network links

The following basic questions must be answered when designing wireless links:

- Which antennas are necessary for the desired application?

---

**■ Chapter 8: Advanced wireless LAN configuration**

- How do the antennas have to be positioned to ensure problem-free connections?
- What performance characteristics do the antennas need to ensure sufficient data throughput within the legal limits?

**Selection of antennas using the LANCOM Antenna Calculator**

You can use the LANCOM Antenna Calculator to calculate the output power of the access points as well as the achievable distances and data rates. The program can be downloaded from our Web site at [www.lancom.eu](http://www.lancom.eu).

After selecting your components (access points, antennas, lightning protection and cable) the calculator works out the data rates, ranges, and the antenna gain settings that have to be entered into the access point.



Please note that when using 5 GHz antennas additional technologies such as dynamic frequency selection (DFS) may be stipulated depending on the country of use. The operator of the wireless LAN system is responsible for ensuring that local regulations are met.

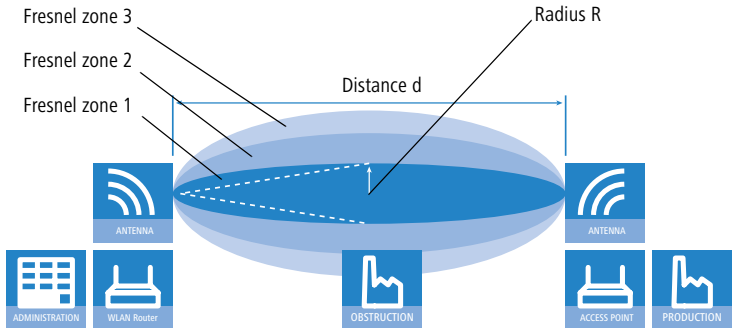


The areas where the waves amplify or cancel themselves out are known as Fresnel zones.



Protecting the components employed from the consequences of lightning strikes and other electrostatic influences is one of the most important aspects to be considered when designing and installing wireless LAN systems for outdoor use. Please refer to the appropriate notes on →'Lightning and surge protection' as otherwise LANCOM Systems cannot provide any guarantee for damage to LANCOM and AirLancer components.

Information on the installation of WLAN systems for outdoor deployment is available in the 'LANCOM Outdoor Wireless Guide'.



The Fresnel zone 1 must remain free from obstruction in order to ensure that the maximum level of output from the transmitting antenna reaches the receiving antenna. Any obstructing element protruding into this zone will significantly impair the effective signal power. The object not only screens off a portion of the Fresnel zone, but the resulting reflections also lead to a significant reduction in signal reception.

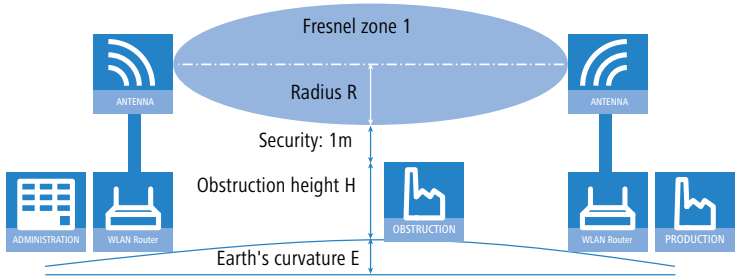
The radius (R) of Fresnel zone 1 is calculated with the following formula assuming that the signal wavelength ( $\lambda$ ) and the distance between transmitter and receiver (d) are known.

$$R = 0.5 * \sqrt{\lambda * d}$$

The wavelength in the 2.4 GHz band is approx. 0.125 m, in the 5 GHz band approx. 0.05 m.

**Example:** With a separating distance of 4 km between the two antennae, the radius of Fresnel zone 1 in the 2.4-GHz band is **11 m**, in the 5-GHz band **7 m**.

To ensure that the Fresnel zone 1 remains unobstructed, the height of the antennas must exceed that of the highest obstruction by this radius. The full height of the antenna mast (M) should be as depicted:



$$M = R + 1\text{m} + H + E \text{ (earth's curvature)}$$

The allowance for the curvature of the earth (E) can be calculated at a distance (d) as  $E = d^2 * 0.0147$  – i.e. at a distance of 8 km this is almost 1m

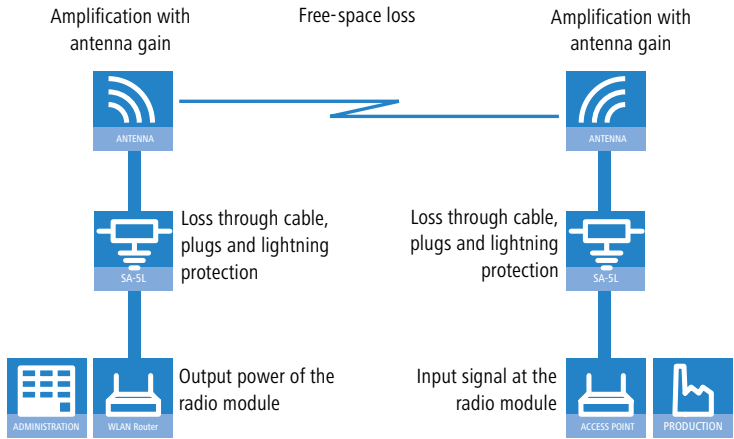
**Example:** With a distance of 8 km between the antennae, the result in the 2.4-GHz band is a mast height above the level of the highest obstruction of approx. **13 m**, in the 5-GHz band **9 m**.

### Antenna power

The power of the antennas must be high enough to ensure acceptable data transfer rates. On the other hand, the country-specific legal regulations regarding maximum transmission power should not be exceeded.

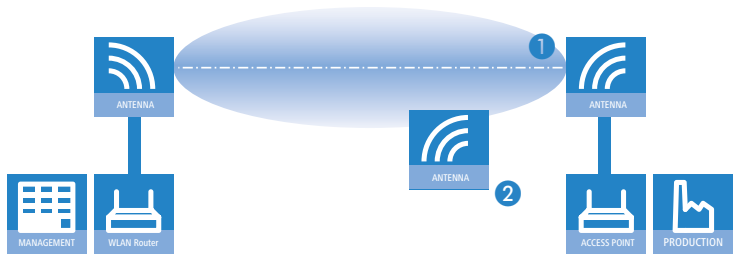
The calculation of effective power considers everything from the radio module in the transmitting access point to the radio module in the receiving access point. In between there are attenuating elements such as the cable, plug connections or simply the air transmitting the signals and amplifying elements such as the external antennas.





## 8.2.2 Antenna alignment for P2P operations

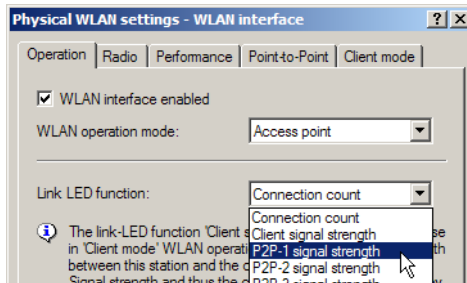
The precise alignment of the antennas is of considerable importance in establishing P2P connections. The more central the receiving antenna is located in the "ideal line" of the transmitting antenna, the better are the actual performance and the effective bandwidth **1**. If the receiving antenna is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



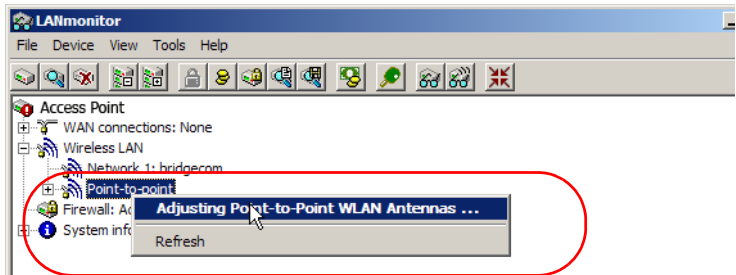
You can find further information on the geometrical design of wireless paths and the alignment of antennas with the help of LANCOM software in the LCOSreference manual.

The current signal quality over a P2P connection can be displayed on the device's LEDs or in the LANmonitor in order to help find the best possible alignment for the antennas.

The display of signal quality on the LEDs must be activated for the wireless LAN interface (LANconfig: **Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Operation**). The faster the LED blinks the better the connection (a blinking frequency of 1 Hz represents a signal quality of 10 dB, double the frequency indicates that the signal strength is twice as high).



In LANmonitor the connection quality display is opened with the context menu. Right-clicking with the mouse on 'Point-to-point' activates the option 'Adjusting Point-to-Point WLAN Antennas...'



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

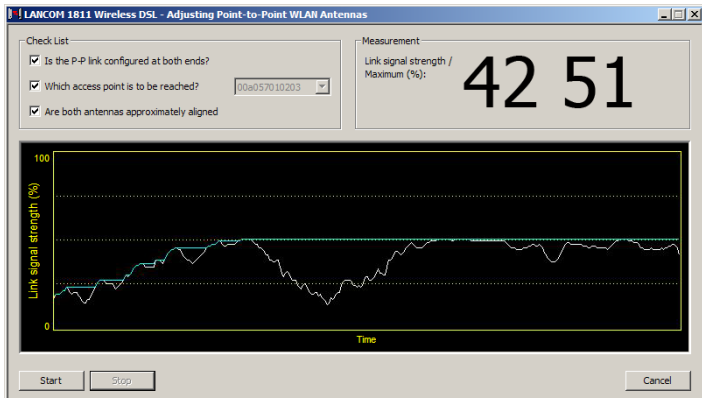
In the dialog for setting up point-to-point connections, LANmonitor prompts for the information required to establish the P2P connection:

- Is the P2P connection configured at both ends (remote base station defined with MAC address or station name)?
- Is the point-to-point mode of operation activated?
- Which access point is to be monitored? All of the base stations defined as P2P remote sites in the device concerned can be selected here.

## ■ Chapter 8: Advanced wireless LAN configuration

- Are both antennas approximately aligned? The basic P2P connection has to be working before fine-tuning can be performed 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, too.



Initially only one of the two antennas should be adjusted 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.

### 8.2.3 Measuring wireless bridges

After planning and installation, the wireless bridge can be analyzed to determine the actual data throughput. Further information about the available tools and taking measurements can be found in the LANCOM Techpaper "The performance of outdoor P2P connections", available as a download from [www.lancom.eu](http://www.lancom.eu).

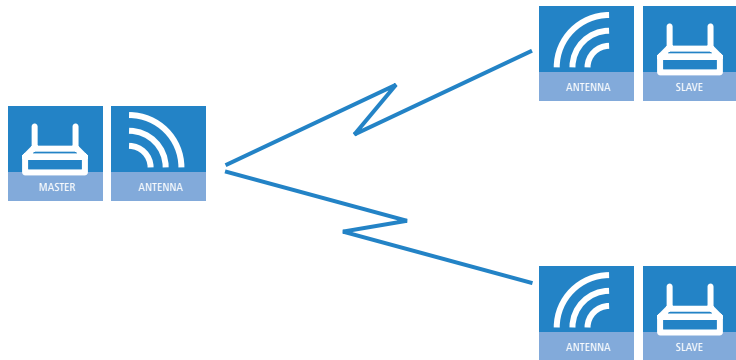
### 8.2.4 Activating the point-to-point operation mode

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
- **To:** 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.



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 (a master as authentication server and a slave as client).

## 8.2.5 Configuration of P2P connections

In the configuration of point-to-point connections, entries have to be made for the point-to-point operation mode and the channel selection scheme, along with the MAC addresses or station names 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.

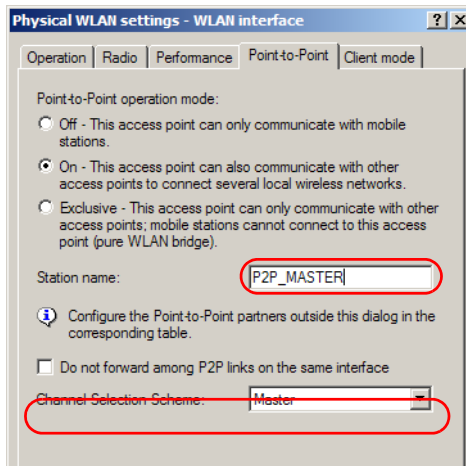


The configuration of the P2P connections can also be carried out with the WLAN Wizards in LANconfig.

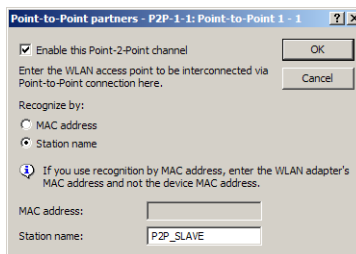
- ① Click on the button **Physical WLAN settings** to open the corresponding WLAN interface and select the tab for 'Point-to-Point'.
- ② Activate the suitable point-to-point operation mode here and set the channel selection scheme to either 'Master' or 'Slave'. If the peers of the P2P connections are to be identified via their station names, then enter a unique name for this WLAN station.



For models with multiple WLAN modules, the station name can be entered separately for each physical WLAN interface.



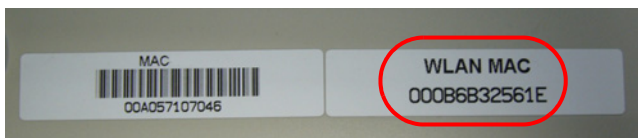
- ③ Close the physical WLAN settings and open the list of **Point-to-point partners**. For each of the maximum of six P2P connections, enter either the MAC address of the WLAN card at the remote station or enter the WLAN station's name (depending on the chosen method of identification).





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 located under each of the antenna connectors. 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

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


## 8.2.6 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).

### 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 module for the P2P connection, WLAN-2 if you are using the second module, e.g. as with an access point with two WLAN modules).

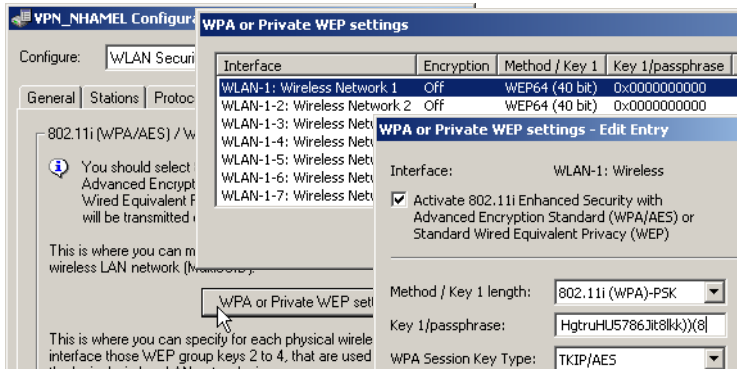
- Activate the 802.11i encryption.
- Select the method '802.11i (WPA)-PSK'.
- Enter the passphrase to be used.

 The passphrases should consist of a random string of 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.

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

Configuration with LANconfig



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:

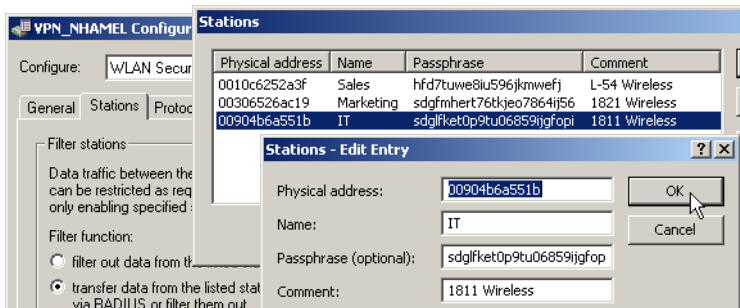
Configuration tool	Menu/Table
WEBconfig	Expert configuration ► Setup ► Interfaces ► WLAN-Interfaces ► Encryption-Settings
Terminal/Telnet	/Setup/Interfaces/WLAN-Interfaces/Encryption-Settings

## 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.

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



Configuration with  
WEBconfig or Telnet

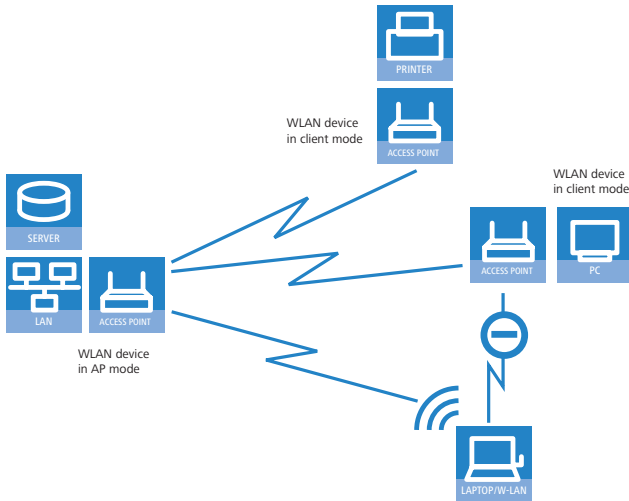
The access list for the matching of MAC addresses to the passphrases (LEPS) can be found under WEBconfig or Telnet under the following paths:

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

## 8.3 Client mode

To connect individual devices with an Ethernet interface into a wireless LAN, LANCOM devices with a WLAN module can be switched to "client mode", whereupon they act as conventional wireless LAN adapters and not as access points (AP). The use of client mode therefore allows devices fitted with only an Ethernet interface, such as PCs and printers, to be integrated into a wireless LAN.



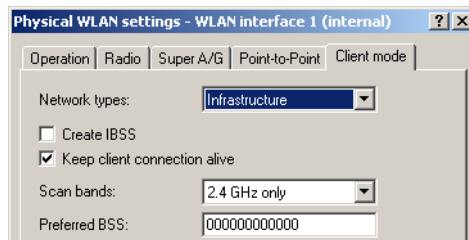


**i** Multiple WLAN clients can register with a WLAN device in AP mode, which is not the case for a WLAN device in client mode.

### 8.3.1 Client settings

For LANCOM Access Points and LANCOM Wireless Routers in client mode, further settings/client behavior can be configured from the 'Client mode' tab under the settings for the physical interfaces.

**i** The configuration of the client settings can also be carried out with the WLAN Wizards in LANconfig.



**1** To edit the settings for client mode in LANconfig, go to the 'Client mode' tab under the physical WLAN settings for the desired WLAN interface.

- ② In 'Scan bands', define whether the client station scans just the 2.4 GHz, just the 5 GHz, or all of the available bands to locate an access point.

Under WEBconfig or Telnet the settings for client mode can be found under the following paths:

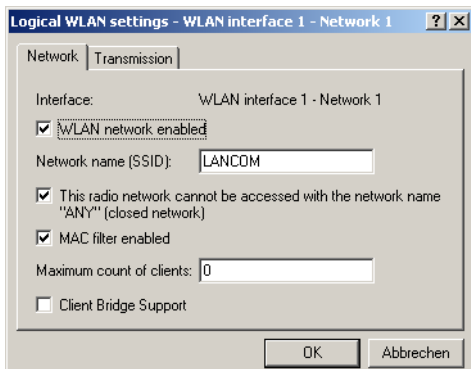
Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ Interfaces ▶ WLAN ▶ Client modes
Terminal/Telnet	Setup/Interfaces/WLAN/Client modes

EN

### 8.3.2 Set the SSID of the available networks

In the WLAN clients, the SSIDs of the networks to which the client stations are to connect must be entered.

- ① To enter the SSIDs, change to the 'General' tab under LANconfig in the 'Wireless LAN' configuration area. In the 'Interfaces' section, select the **first** WLAN interface from the list of logical WLAN settings.



- ② Enable the WLAN network and enter the SSID of the network the client station should log onto.

Under WEBconfig or Telnet the network settings for the logical WLAN interfaces can be found under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ► Setup ► Interfaces ► WLAN ► Network
Terminal/Telnet	Setup/Interfaces/WLAN/ Network settings

### 8.3.3 Encryption settings

For access to a WLAN, the appropriate encryption methods and key must be set in the client station.

- ① To enter the key, change to the '802.11i/WEP' tab under LANconfig in the 'Wireless LAN' configuration area. From 'WPA / private WEP settings', select the **first** WLAN interface from the list of logical WLAN settings.

- ② Enable encryption and match the encryption method to the settings for the access point.
- ③ In WLAN client operating mode, the LANCOM Access Points and LANCOM Wireless Routers can authenticate themselves to another access point using EAP/802.1X. For this, select the desired client EAP method here. Note that the selected client EAP method must match the settings of the access point that the device is attempting to log onto.



Depending on the EAP method, the appropriate certificates must be stored in the device.

■ *Chapter 8: Advanced wireless LAN configuration*

- For TTLS and PEAP - the EAP/TLS root certificate only; the key is entered as a combination username:password.
- For TLS in addition; the EAP/TLS device certificate including the private key.

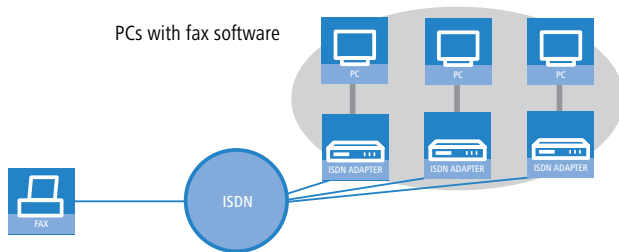
Under WEBconfig or Telnet the network settings for the logical WLAN interfaces can be found under the following paths:

Configuration tool	Call
WEBconfig, Telnet	Expert configuration > Setup > Interfaces > WLAN > Encryption > WLAN 1

## 9 Sending faxes with LANCAPI

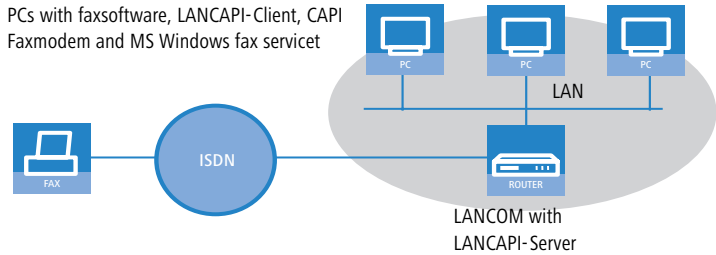
LANCAPI from LANCOM Systems is a special version of the popular CAPI interface. CAPI (Common ISDN Application Programming Interface) establishes the connection between ISDN adapters and communications programs. For their part, these programs provide the computers with office communications functions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

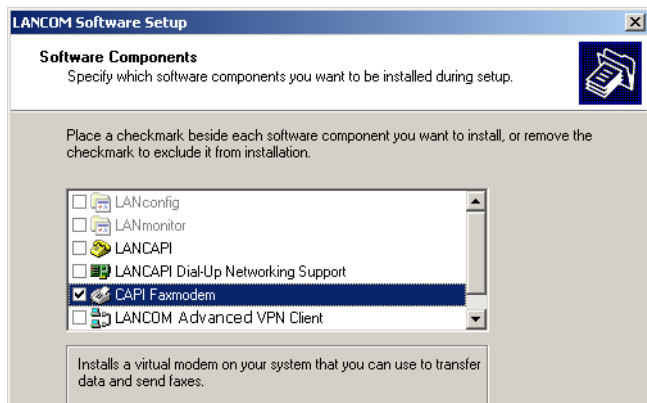
- the **LANCAPI client**. It provides the connection between your workstation PC and the LANCAPI server.
- the **CAPI Faxmodem**. This tool simulates a fax device on your workstation PC.
- the **MS Windows fax service**. This is the interface between the fax applications and the virtual fax.



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.

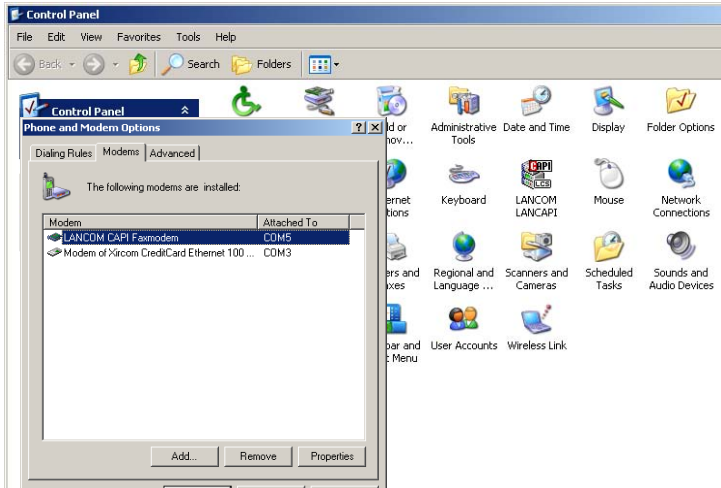
## 9.1 Installation of the LANCOM CAPI Faxmodem

- 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.



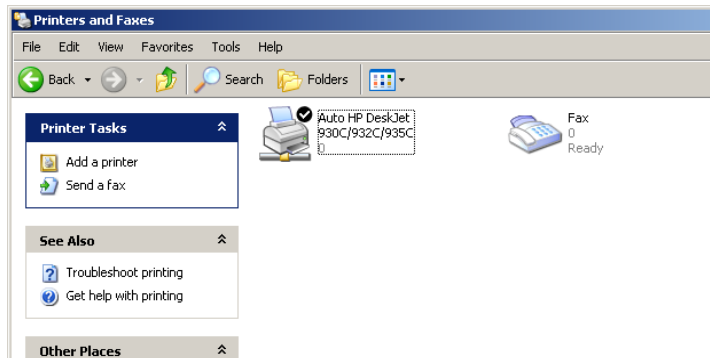
## ■ Chapter 9: Sending faxes with LANCAPI

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



## 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.



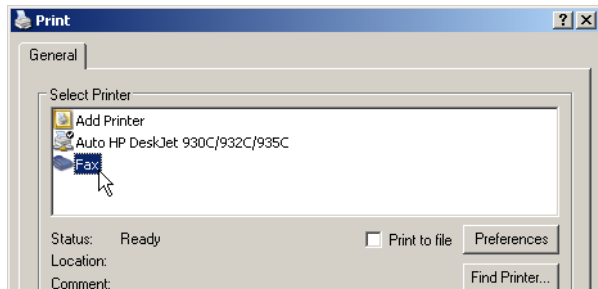
For checking the installation, click with the right mouse button on the fax-icon and select **Properties**. The LANCOM CAPI Faxmodem should now be entered into register 'devices'.

## 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**.
- ② Adjust the fax device as printer.



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

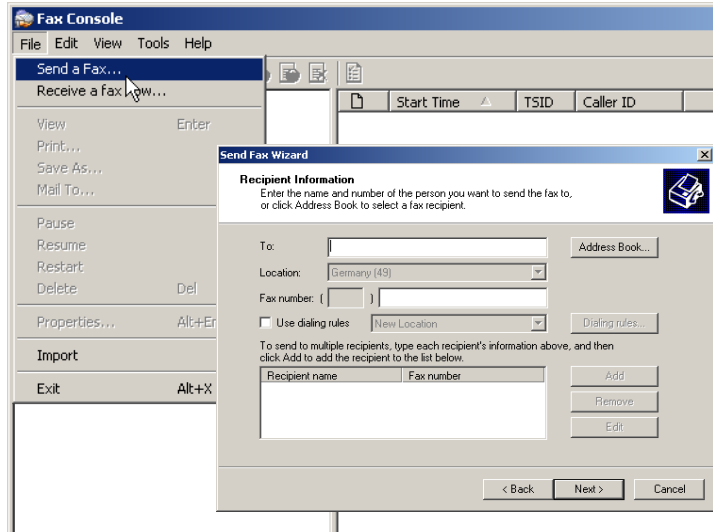
### 9.3.2 Send a fax with the MS Windows fax service

- 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.



## ■ Chapter 9: Sending faxes with LANCAPI

- 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 AirLancer series and can be adapted to special conditions of environs.
- With the LANCOM Public Spot Option option it is possible to extend the LANCOM for additional billing and accounting functions in order to upgrade it to a Wireless Public Spot.

### 10.1 Optional AirLancer Extender antennas

AirLancer Extender antennas are capable of extending the operating range of the devices, or of adapting access point coverage to local conditions. An overview of the supported antennas is available from the LANCOM Web site under [www.lancom.eu](http://www.lancom.eu).



You will also find further information on calculating the best configuration for AirLancer Extender antennas and third-party antennas that you wish to connect to the LANCOM under [www.lancom.eu](http://www.lancom.eu).



When assembling separately purchased mobile radio antennas please note that the maximum allowed transmission power of the wireless LAN according to EIRP in the country in question may not be exceeded. The system operator is responsible for adhering to the threshold values.



For internal lightning protection, the surge adapter AirLancer Extender SA-5L is **always necessary**—the AirLancer Extender SA-5L is mounted between the Access Point and the antenna, as close to the antenna as is possible.



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. 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).

Each wireless LAN module is equipped with two send/receive units, each of which can be connected to an antenna. In the case of antenna diversity, the WLAN module checks which send/receive unit (antenna) is receiving the strongest signal from a client. Only the stronger signal is used. The Access Point stores the information on which send/receive unit was used to receive data and proceeds to use the same unit for the transmission to the client. Antenna diversity ensures that the various clients associated with the Access Point always use the send/receive unit with the best signal.

### 10.1.2 Polarization diversity

Other diversity techniques process the two signals and combine them into a single signal. The most common methods are space diversity and polarization diversity. LANCOM Systems supplies various polarization diversity antennas for connection to LANCOM devices. With these models, two orthogonally polarized signals are received at a transmitter/receiver unit and combined to form a single signal which is stronger than the two individual signals. This improvement is the polarization gain. Further information about this technique is available in our "Polarization Diversity" techpaper.

### 10.1.3 Installing the AirLancer Extender antennas

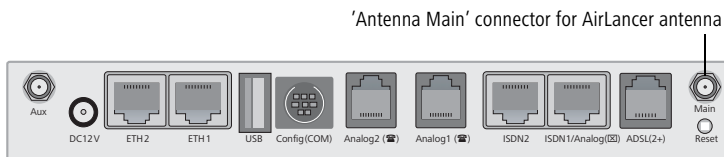
The following diversity antennas are available as accessories for the LANCOM VoIP Routers:

- AirLancer Extender O-D80g (2.4 GHz band ), item no. 61221
- AirLancer Extender O-D60a (5 GHz), item no. 61222
- AirLancer Extender O-D9a (5 GHz), item no. 61224



Before mounting external antennas, please observe the information on lightning protection in the LANCOM Outdoor Wireless Guide (supplied or available as a download from [www.lancom.eu](http://www.lancom.eu)). Mounting antennas without adequate lightning protection could lead to serious damage to the access point and the network infrastructure connected to it.

To install an optional AirLancer antenna, switch the device off by unplugging the power cable. Now carefully unplug the two diversity antennas from the back by unscrewing them. Connect the AirLancer antenna to the connector marked 'Antenna Main'.



## 10.2 LANCOM Public Spot Option

Wireless Public Spots are publicly accessible areas where users can use their own mobile computers to access a wireless network (such as a company network or the Internet).



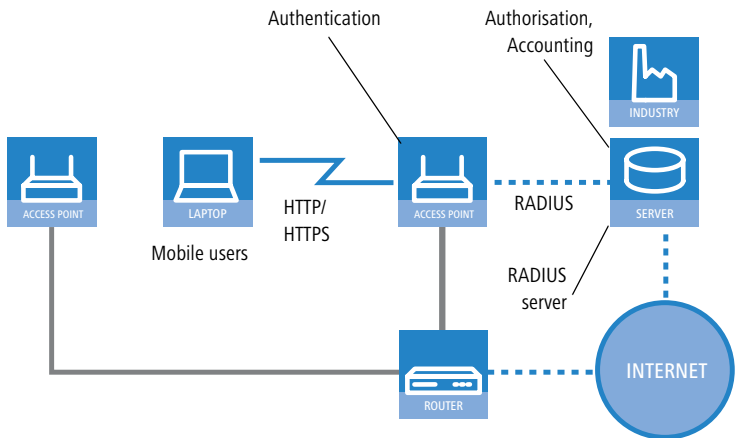
Please note that operating a LANCOM VoIP Router with the LANCOM Public Spot Option (also referred to as a HotSpot) can be subject to legal regulation in your country. Before installing a LANCOM VoIP Router, please inform yourself about any applicable regulations. More information on this subject is available in our white paper "Public Spot - Rechte und Pflichten eines Betreibers" available for download from [www.lancom.eu](http://www.lancom.eu).

Wireless LAN technology is ideal for offering wireless Internet services to the public in locations such as airports, railway stations, restaurants or cafes via so-called HotSpots. The LANCOM Public Spot Option is intended for operators of public wireless networks. It enables the easy installation and maintenance of public HotSpots by providing LANCOM Access Points and LANCOM Routers with additional functions for authentication and billing for public Internet services.

Authentication and billing for individual users is implemented with user-friendly Web pages, enabling client PCs with a WiFi-certified wireless card (e.g. AirLancer) and standard Internet browser to go directly online.

The LANCOM Public Spot Option is the ideal solution for public wireless LAN. Wireless LAN are very well suited for company networks and for wireless networking in the home. However, for public access services the standard setup

lacks important mechanisms for authentication and billing of individual users (AAA — authentication, authorization, accounting). This is remedied by the LANCOM Systems Open User Authentication (OUA), the core component of the LANCOM Public Spot Option. OUA implements the authentication of all wireless clients by user name and password. It checks the authorization of each user with a RADIUS server. Accounting data (online time, volumes) on a per user and per session basis can be passed on to the central RADIUS server. All the client PC needs is a wireless card (e.g. AirLancer), TCP/IP, and an Internet browser. No further software is required. The Public Spot Option is optimally suited for setting up wireless Internet access services in hotels, restaurants, cafes, airports, railway stations, exhibition grounds or universities.



The LANCOM Public Spot Option equips an access point with these functions and upgrades it to a wireless Public Spot.

## 11 Security settings

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



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

### 11.1 Security in the wireless LAN

Wireless LANs are potentially a significant security risk. It is a common assumption that it is simple to misuse data transferred by wireless.

Wireless LAN devices from LANCOM Systems enable the latest security technologies to be used.

- Suppress SSID broadcast – closed network
- Access control by MAC address
- LANCOM Enhanced Passphrase Security (LEPS)
- Encrypted data transfer (802.11i/WPA or WEP)
- 802.1x / EAP
- Optional IPSec-over-WLAN VPN

#### 11.1.1 Suppress SSID broadcast – closed network

Every wireless LAN compliant with IEEE 802.11 has its own network name (SSID). This network name facilitates the identification and servicing of wireless LANs.

A wireless LAN can be set up so that any user has access. These networks are known as open networks. An open network is accessible to users even if they do not know the network name. Access is possible simply by entering the network name 'ANY'.

A closed network denies access to clients trying to access 'ANY'. The user must enter the correct network name for this to work. Hidden networks remain invisible.

#### 11.1.2 Access control by MAC address

Every network device has a unique identification number. This identification number is known as the MAC address (**M**edia **A**ccess **C**ontrol) and it is unique worldwide.

The MAC address is programmed into the hardware. Wireless LAN devices from LANCOM Systems display their MAC number on the housing.

Access to an infrastructure network can be limited to certain wireless LAN devices by defining MAC addresses. The access points have filter lists in (ACL – access control list) for storing authorized MAC addresses.

### 11.1.3 LANCOM Enhanced Passphrase Security

With LEPS (LANCOM **E**nanced **P**assphrase **S**ecurity), LANCOM Systems has developed an efficient method that makes use of the simple configuration of IEEE 802.11i with passphrase, but that avoids the potential error sources in passphrase distribution. LEPS uses an additional column in the ACL to assign an individual passphrase consisting of any 4 to 64 ASCII characters to each MAC address. The connection to the access point and the subsequent encryption with IEEE 802.11i or WPA is only possible with the right combination of passphrase and MAC address.

LEPS can be used locally in the device and can also be centrally managed with the help of a RADIUS server, and it works with all WLAN client adapters currently available on the market without modification. Full compatibility to third-party products is assured as LEPS only involves configuration in the access point.

An additional security aspect: LEPS can also 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 protected, particularly when the ACL is stored on a RADIUS server.



**Guest access with LEPS:** LEPS can also be set up to allow access to guests. To this end, all users of the internal WLAN network are given individual passphrases. Guests can make use of their own dedicated SSID and a global passphrase. To avoid abuse, the this global passphrase can be changed on a regular basis—every few days, for example.

### 11.1.4 Encrypted data transfer

Encryption takes on a special role in the transfer of data in wireless LANs. Wireless communication with IEEE 802.11 is supplemented with the encryption standards 802.11i/WPA and WEP. The aim of the encryption

methods is to provide wireless LAN with levels of security equivalent to those in cabled LANs.



LANCOM Systems's recommendation for the most secure passphrase variant is to employ 802.11i (WPA2) in combination with AES. The key should be randomly selected from the largest possible range of numbers and should be as long as possible (32 to 63 characters). The prevents dictionary attacks.

- Use encryption on the data transferred in the WLAN. Activate the strongest possible encryption method available to you ((802.11i with AES, TKIP or WEP) and enter the appropriate keys or passphrases into the access point and the WLAN clients.
- The passphrases for 802.11i or WPA do not have to be changed quite so regularly as new keys are generated for each connection anyway. This is not the only reason that the encryption with 802.11i/AES or WPA/TKIP is so much more secure than the now obsolete WEP method. If you use WEP to be compatible to legacy WLAN clients regularly change the WEP key in your access point.
- If the data is of a high security nature, further improvements include additionally authenticating the client with the 802.1x method ('802.1x / EAP' → page 112) or activate an additional encryption of the WLAN connection as used for VPN tunnels ('IPSec over WLAN' → page 113). In special cases, a combination of these two mechanisms is possible.



Detailed information about WLAN security and the various encryption methods are to be found in the LCOS reference manual.



Please also observe the information in the box "Standard encryption with WPA".

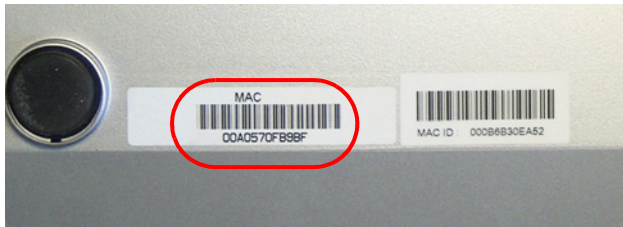


### Standard encryption with WPA

The factory settings (or those after resetting the device) are different in LANCOM Access Points than in LANCOM Wireless Routers.

- Unconfigured Access Points with standard factory settings cannot be commissioned by means of the WLAN interface. The WLAN modules are switched off and the devices search the LAN for a LANCOM WLAN Controller which will supply a configuration profile.
- Unconfigured Wireless Routers with standard factory settings cannot be commissioned by means of the WLAN interface. Furthermore, the WPA encryption standard described here is used as standard.

The preshared key (PSK) for the standard WPA encryption consists of the first letter “L” followed by the LAN MAC address of the access point in ASCII characters. The LAN MAC addresses of the LANCOM devices always begin with the character string “00A057”. You will find the LAN MAC address on a sticker on the base of the device. **Only** use the number labeled as “MAC address” that starts with “00A057”. The other numbers that may be found are **not** the LAN MAC address.



A device with the LAN MAC address “00A0570FB9BF” thus has a standard preshared key of “L00A0570FB9BF”. This key is entered into the ‘Private WPA settings’ of the device for each logical WLAN network as ‘Key 1’.

To use a WLAN adapter to establish a connection to a LANCOM Wireless Router that has factory settings, the WPA encryption must be activated for the WLAN adapter and the standard 13-character preshared key entered.



After registering for the first time, change the WPA preshared key to ensure that you have a secure connection.

#### 11.1.5 802.1x / EAP

The international industry standard IEEE 802.1x and the **Extensible Authentication Protocol (EAP)** enable access points to carry out reliable and secure access checks. The access data can be managed centrally on a RADIUS server

(integrated RADIUS/EAP server in the LANCOM VoIP Router or external RADIUS/EAP server) and accessed by the access point when required. The dynamically generated and cryptographically secure key material for 802.11i (WPA1/2) replaces the manual key management.

The IEEE-802.1x technology has already been fully integrated since Windows XP. Client software exists for other operating systems. The drivers for the LANCOM AirLancer wireless cards feature an integrated 802.1x client.

### 11.1.6 IPSec over WLAN

With the help of the IPSec-over-WLAN technology in addition to the security measures described already, a wireless network for the exchange of especially sensitive data can be optimally secured. Required for this is a base station with VPN support and the LANCOM Advanced VPN Client that operates under Windows 2000, XP and Windows Vista™. Client software from third parties is available for other operating systems.

## 11.2 Security settings Wizard

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

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

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

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

## 11.2.1 LANconfig Wizard

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



- 2 In the selection menu, select the Setup Wizard, **Check security settings** and confirm the selection with **Next**.
- 3 In the dialogs that follow you can set the password and select the protocols to be available for accessing the configuration from local and remote networks.
- 4 In a subsequent step, you can set parameters for locking the configuration such as the number of incorrect password entries and the duration of the lock.
- 5 For devices with a WLAN interface, you have the option of specifying the security parameters of the wireless network. This includes the name of the wireless network, the closed-network function, and encryption by 802.11i/WPA or WEP. For devices with an optional second WLAN interface, you can set the parameters for both wireless networks separately.
- 6 For the WLAN interface, you can subsequently define the access control lists (ACL) and the protocols. This allows you to place limitations on the data exchange between the wireless network and the LAN.
- 7 For the firewall, you can activate stateful inspection, ping blocking, and the stealth mode.
- 8 The Wizard will inform you as soon as the entries are complete. Close the configuration with **Finish**.

## 11.2.2 WEBconfig Wizard

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

- Device password
- The protocols to be available for accessing the configuration from local and remote networks
- The parameters for locking the configuration (the number of incorrect password entries and the duration of the lock)
- Security parameters such as WLAN name, closed-network function, WPA passphrase, WEP key, ACL lists, and protocol filters

## 11.3 The security checklist

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



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

### ■ Have you secured your wireless network with encryption and access control lists?

With the help of 802.11i, WPA or WEP, you can encrypt the data in your wireless network with different encryption methods such as AES, TKIP or WEP. LANCOM Systems recommends the strongest possible encryption with 802.11i and AES. If the WLAN client adapters do not support these, then you should use TKIP or at least WEP. Make sure that the encryption function in your device is activated, and that at least one passphrase or WEP key has been entered and selected for application.



For security reasons, LANCOM Systems strongly advises you not to use WEP! You should only ever use WEP under exceptional circumstances. When using WEP encryption, use additional security mechanisms additionally.



Ex-factory, WPA encryption is activated for every unconfigured device as standard. This WPA encryption in WLAN devices being managed by a LANCOM WLAN Controller is overwritten by the central encryption settings in the profiles of the WLAN-Controller.

To check the settings, open LANconfig, go to the configuration area and select 'Wireless LAN' on the '802.11i/WEP' tab to view the encryption settings for the logical WLAN interfaces.



Change the default WPA preshared key immediately after configuring the device for the first time.

With the access control list (ACL) you can permit or prevent individual clients accessing your wireless LAN. The decision is based on the MAC address that is permanently programmed into wireless network adapters. To check the access-control list, go to the configuration area in LANconfig and select 'WLAN security' on the 'Stations' tab.

The LANCOM Enhanced Passphrase Security (LEPS) uses an additional column in the ACL to assign an individual passphrase consisting of any 4 to 64 ASCII characters to each MAC address. The connection to the access point and the subsequent encryption with IEEE 802.11i or WPA is only possible with the right combination of passphrase and MAC address.

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

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

#### ■ **Have you permitted remote configuration?**

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

#### ■ **Have you password-protected the SNMP configuration?**

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

### ■ Have you activated the firewall?

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



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

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

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

### ■ Have you activated IP masquerading?

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

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

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

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

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

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

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

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

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

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

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

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

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?**

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



## 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.

- 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!

- 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.

Not including  
LANCOM 1724  
VoIP


LANCOM 1722  
VoIP and LANCOM  
1724 VoIP only

■ *Chapter 12: Configuring the ISDN and analog interfaces in detail*

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		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'
- **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**

LANCOM 1724  
VoIP only



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 life-line 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.

## 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.

## 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](http://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**.



# 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 <sub>0</sub> ), 1x TE.	2 ISDN interfaces. Default: 1x NT (S <sub>0</sub> ), 1x TE.	4 ISDN interfaces. Default: 2x NT (S <sub>0</sub> ), 2x TE.	2 ISDN interfaces. Default: 1x NT (S <sub>0</sub> ), 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	<ul style="list-style-type: none"> <li>■ echo cancelling (G.168)</li> <li>■ automatic adaptive de-jitter buffer</li> <li>■ transparent pass-through for negotiated codecs</li> <li>■ interaction on codec negotiation (filter, quality, bandwidth)</li> <li>■ voice coding with G.711 <math>\mu</math>-Law/A-Law (64 kbps), G.722 High Quality Codec (for UDI calls), G.729 Annex A Low Bandwidth Codec</li> <li>■ Fax-over-IP (FoIP) with SIP and T.38 protocol</li> </ul>			
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)			

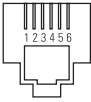
■ Chapter 14: Appendix

		LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Options		<ul style="list-style-type: none"> <li>■ LANCOM VoIP-32 Option for upgrading to a total of 32 local SIP users (item no. 61617)</li> <li>■ LANCOM VPN Option 25 channels (hardware accelerated, max. 25 simultaneous connections, 50 connections configurable) for VPN in WAN (item no.60083)</li> <li>■ LANCOM Public Spot Option (item no. 60642)</li> </ul>			
Accessories		<ul style="list-style-type: none"> <li>■ LANCOM Modem Adapter Kit for connecting modems (analogue or GSM) to the serial configuration interface (item no. 61500)</li> <li>■ LANCOM Rack Mount Option (item no. 61501)</li> </ul>			
Optional antennes and accessories		<p>For all LANCOM Router models</p> <ul style="list-style-type: none"> <li>■ LANCOM Advanced VPN Client for Windows 98SE-XP, 1 License, item no. 61600</li> <li>■ LANCOM Advanced VPN Client for Windows 98SE-XP, 10 Licenses, item no. 61601</li> <li>■ LANCOM Advanced VPN Client for Windows 98SE-XP, 25 Licenses, item no. 61602</li> <li>■ LANCOM VP-100 VoIP telephone compliant with the SIP standard, item no. 61613</li> <li>■ LANCOM VP-100 5-piece bulk set; 5 VoIP telephones compliant with the SIP standard, item no. 61614</li> <li>■ LANCOM ES-1108P compact, robust 8-port Ethernet switch with 4 PoE interfaces, item no. 61450</li> </ul> <p>Only LANCOM 1823 VoIP:</p> <ul style="list-style-type: none"> <li>■ AirLancer Extender I-180 2,4 GHz indoor antenna item no. 60914</li> <li>■ AirLancer Extender I-60ag dualband indoor antenna item no. 61214</li> <li>■ AirLancer Extender O-30 2,4 GHz outdoor antenna item no. 60478</li> <li>■ AirLancer Extender O-70 2,4 GHz outdoor antenna item no. 60469</li> <li>■ AirLancer Extender O-D80g 2,4GHz polarization diversity outdoor antenna item no. 61221</li> <li>■ AirLancer Extender O-360ag omni-directional dual-band antenna item no. 61223</li> <li>■ AirLancer Cable NJ-NP 3m extension cable item no. 61230</li> <li>■ AirLancer Cable NJ-NP 6m extension cable item no. 61231</li> <li>■ AirLancer Cable NJ-NP 9m extension cable item no. 61232</li> <li>■ AirLancer Extender SA-5 lightning protection for antenna cable item no.. 61212</li> <li>■ AirLancer Extender SA-LAN lightning protection for LAN cable item no.. 61213</li> <li>■ AirLancer Extender O-18a 5 GHz outdoor antenna item no. 61210</li> <li>■ AirLancer Extender O-D60a 5GHz polarization diversity outdoor antenna item no. 61222</li> <li>■ AirLancer Extender O-9a 5GHz directional outdoor antenna item no. 6122</li> </ul>			

## 14.2 Contact assignment

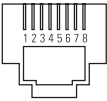
### 14.2.1 ADSL interface

6-pin RJ11 socket

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

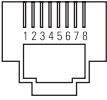
### 14.2.2 ISDN interface ☒

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	–	–

### 14.2.3 ISDN interface

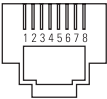
8-pin RJ45 socket, corresponding to ISO 8877, EN 60603-7, assembled as ISDN-NT for connection of ISDN terminal endpoint devices

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

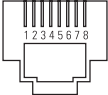
## 14.2.5 Analog interface

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

## 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



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

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

# Index

## Numerics

10/100Base-TX	42
3 DES	66, 74
802.11i	30, 109, 110, 114, 115
802.11i/	111
802.1x	30, 109, 111, 112

## A

Access point mode	3, 34
Access-control list	110
ACL	110
ADSL	
Connections	43
Transfer rates	11
ADSL over ISDN	128
ADSL over POTS	128
AES	66, 74, 111
Annex A	12
Annex B	12
Anschlussbelegung	
Konfigurationsschnittstelle	134
Answering machine	12
Antenna Calculator	84
Antenna power	87
Autosensing	45

## B

Blowfish	66, 74
----------	--------

## C

Call-back function	31, 66, 74
Calling Line Identity (CLI)	76
CAPI interface	100
Charge limiter	37
Charge protection	54, 55
Client mode	95, 96
Closed Network	109
Common ISDN Application Programming Interface (CAPI)	100

Configuration access	55
Configuration file	118
Configuration interface	31
Connector cable	33
Configuration password	116
Configuration port	42
Configuration protection	31, 52
Contact assignment	131
ADSL interface	131
DSL interface	133
LAN interface	133
Outband	134

## D

Data frequencies	12
DDI	25
Default gateway	117
Denial-of-Service protection	15
DFS	84
DHCP	59
DHCP server	26, 51, 60
Dial-in access	74
Dial-up adapter	77
Direct Dialing In	25
DNS	
DNS access to the remote LAN	70
DNS server	26, 59
Documentation	33
Domain	70
Download	6
Downstream	11
DSL connection	
problems establishing the connection	126
Dynamic Frequency Selection	84
Dynamic frequency selection	84

## E

EAP	30, 109, 112
-----	--------------



## ■ Index

Encryption	66, 74	ISDN	
Encryption methods	98	Connector cable	33
<b>F</b>		D channel	76
Fax	12	ISDN calling line ID	68, 75, 76
Firewall	14, 31, 117	ISDN leased-line option	27
Block stations	118	ISDN life line	121
FirmSafe	31	ISDN modem	74
Firmware	6	ISDN number	68
Flatrate	62	ISDN power relay	121
Fresnel zone	86	ISDN S <sub>0</sub> connection	29
<b>H</b>		<b>L</b>	
Hardware installation	44	LAN	
HTTPS	55	Connector cable	33
<b>I</b>		LANCAPI	27
ICMP	117	LANCOM Enhanced Passphrase Security	
Information symbols	6	109	
Installation	33	LANCOM Public Spot Option	107
ADSL	45	LANCOM setup	48
Antennas	44	LANconfig	49, 54
Configuration interface	46	Starting the Wizards	64
ISDN	45	LAN-LAN connectivity	66
LAN	44	Required information	67
LANtools	48	LAN-LAN coupling	26
Power supply unit	46	LANmonitor	49
Internet access	26, 61	LANtools	
Authentication data	61	System requirements	34
Flatrate	62	LEPS	30, 110
Internet access setup	61	Life line	24, 121
Internet provider	61	Life-line support	29, 121
Intrusion detection	14	Load balancing	24
IP		Loader	34
Block ports	117	local break out	19
Filter	117	<b>M</b>	
IP address	45, 51, 52, 118	MAC address	112
IP masquerading	14, 31, 117	MAC address filter	14, 30, 31
IP router	26	Managed mode	3, 34
IPsec	66, 74	Minimum bandwidth	15
IPSec over WLAN	109	MSN	25, 76
		Multi SSID	30

Multiple subscriber number	25	Activate compression in software	77
<b>N</b>		Configuring the dial-in computer	77
NAT – see IP masquerading		NetBIOS	77
NetBIOS	70	Server	26
NetBIOS proxy	26	Setup	74
Netmask	51	TCP/IP	76
Network connectivity	66	User name	75
Security aspects	66, 74	Windows workgroup search	77
Network mask	52, 118	Remote configuration	55
Network segment	45	Remote configuration via ISDN	31
<b>O</b>		Reset switch	43
Optional antennas	105	Reset the toll protection	37
Options and accessories	105	Router function	11
<b>P</b>		Routing table	117
P2P	110	<b>S</b>	
Package content	33	SDSL modem	30
Password	52, 55, 66, 74	Security	
Password for the ISDN connection	69	Internet access	109
PAT – see IP masquerading		Protecting the configuration	109
PBX	12	Security checklist	115
Ping	71	self-sufficient	3, 34
Point-to-multipoint	24, 120	SIP gateway	19
Point-to-multipoint connection	25, 27	SIP PBX	20
Point-to-point	24, 83, 110, 120	SIP provider	17
Point-to-point connection	25, 27	SNMP	
POTS	12	Configuration protection	116
Power relay	24, 29, 121	Software installation	48
Power supply unit	33, 42	SSID	53, 97
Power switch	42	Standard gateway	59
PPP	74	Stateful-inspection firewall	14
PPP client	77	Status display	34
<b>Q</b>		Power	36, 37
Quality of Service	15	Wireless link	41
<b>R</b>		Super AG	30
RADIUS	112	Support	6
RAS	13	Switch	42
Remote Access Service (RAS)		System requirements	34
		<b>T</b>	
		TCP	117

■ *Index*

TCP/IP	34, 77	Voice communication	15
Connect test	71	Voice frequencies	12
Settings	50	Voice over IP	15
Windows size	127	VoIP	15
TCP/IP configuration		Connecting subsidiaries or home offices	18
Fully automatic	50, 51	Peer-to-peer	20
Manual	50, 51	VoIP lines	22
TCP/IP filter	14, 31, 117	VoIP PBX	18
TCP/IP router		VoIP users	22
Settings	69	VPN	13
TCP/IP-Filter	14	VPN client	77
T-DSL	13	VRRP	24
Telephone	12	<b>W</b>	
Telnet	118	WEBconfig	55
TFTP	118	HTTPS	55
Transfer protocol	126	System requirements	34
Turbo Mode	30	WEP	30, 109, 110, 114, 115
<b>U</b>		Windows workgroup search	70
UDP	117	WLAN	
Upstream	11	Bands scanned	97
<b>V</b>		Client mode	96
Virtual Private Network	13	WPA	30, 109, 110, 114, 115
Virtual Private Networks (VPN)	26		