LANCOM Reference Manual LCOS 6.10
Addendum LCOS 6.20

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

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

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

Trademarks

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

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

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

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

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

LANCOM Systems GmbH
Adenauerstrasse 20/B2

Adenauerstr. 20/B2

Germany

www.lancom.de

Wuerselen, September 2006

Contents

1 Preface

New functions in LCOS version 4.00

- 'Encrypted configuration with SSH access' → page 34
- 'VPN connections: High availability with VPN load balancing' → page 314
- 'Managing rights for different administrators' → page 43
- 'Manual definition of the MTU' → page 165
- 'LEPS—LANCOM Enhanced Passphrase Security' → page 356
- 'Standard WEP encryption' → page 357
- 'Port mapping' → page 553
- 'Multiple loopback addresses' → page 49
- 'IEEE 802.11i for point-to-point connections in the WLAN' → page 387
- 'Multi-PPPoE' → page 129
- 'IKE config mode' → page 263
- 'SYSLOG storage in the device' → page 86

New functions in LCOS version 4.10

- 'High availability – backup solutions' → page 491
- 'Operating a modem over the serial interface' → page 156
- 'The ping command' → page 88
- 'Loading firmware, script or device configuration over TFTP' → page 33

New functions in LCOS version 5.00

- 'Scripting' → page 57
- 'Working with digital certificates' → page 275
- 'Address Adaption' → page 374
- 'Client Bridge Support' → page 375
- 'DSL port mapping' → page 132
- 'Dynamic load balancing' → page 135
- 'Policy-based routing' → page 109
- 'Monitoring the switch' → page 89
- 'Anti-Theft Protection with the ISDN Location Check' → page 100
- 'Group configuration with LANconfig' → page 67
- 'Visualization of larger WLANs with WLANmonitor' → page 77
- 'Automatic selection of 5 Ghz WLAN channels over DFS with a "blacklist" and "whitelist".' → page 370

New functions in LCOS version 5.20

- 'Backup Solutions and Load Balancing with VRRP' → page 501
- 'PPPoE Servers' → page 555
- 'Enhanced UMTS Card Support for the LANCOM 3550 Wireless' → page 397
- 'ADSL 2+' → page 166
- 'WAN RIP' → page 166
- 'Routing tags for VPN and PPTP connections' → page 111
- 'NAT Traversal (NAT-T)' → page 306
- 'Configurable VLAN Protocol ID' → page 334
- 'Configurable VLAN IDs' → page 335
- 'Vendor Class and User Class Identifier on the DHCP Client' → page 534
- 'Bandwidth limits in the WLAN' → page 398
- 'Spanning Tree Protocol' → page 167
- 'Demilitarized Zone (DMZ)' → page 127
- 'Device communication over HTTP and HTTPS' → page 56

New functions in LCOS version 6.00

- 'Voice over IP (VoIP)' → page 405

New functions in LCOS version 6.10

- 'Certificate revocation list - CRL' → page 303
- 'Simplified RAS with certificates' → page 305
- 'QoS for WLANs according to IEEE 802.11e (WMM/WME)' → page 245
- 'Extended WLAN protocol filters' → page 381
- 'RADIUS' → page 560
- Voice over IP
  - 'Supporting digital calls' → page 422
  - 'ISDN interface configuration' → page 442
  - 'The LANCOM VoIP Router at a P2P (point-to-point) connection' → page 479
  - 'SIP trunking' → page 482
  - 'Remote gateway' → page 484
- 'VLAN tags on layer 2/3 in the Ethernet' → page 335
- 'Operating printers at the USB connector of the LANCOM' → page 572

User's manual and reference manual

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

- The hardware of the LANCOM devices is documented in the respective user's manuals. Apart from a description of the specific feature set of the different models, you find in the user's manual information about interfaces and display elements of the devices, as well as instructions for basic configuration by means of the wizards.
- You are now reading the reference manual. The reference manual describes all functions and settings of the current version of LCOS, the operating system of all LANCOM routers and LANCOM Wireless Access Points. The reference manual refers to a certain software version, but not to a special hardware.

  It completes the user's manual and describes topics in detail, which are valid for several models simultaneously. These are for example:

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

LCOS, the operating system of LANCOM devices

All LANCOM routers and LANCOM Wireless Access Points use the same operating system: LCOS. The operating system developed by LANCOM Systems itself is not attackable from the outside, and thus offers high security. The consistent use of LCOS ensures a comfortable and constant operation of all LANCOM products. The extensive feature set is available throughout all LANCOM products (provided respective support by hardware), and continuously receives further enhancements by free, regular software updates.

This reference manual applies to the following definitions of software, hardware and manufacturers:

- 'LCOS' describes the device-independent operating system
- 'LANCOM' stands as generic term for all LANCOM routers and LANCOM Wireless Access Points
- 'LANCOM Systems' stands as shortened form for the manufacturer, LANCOM Systems GmbH, Germany

Validity

The present reference manual applies to all LANCOM routers and LANCOM Wireless Access Points with firmware version 6.00 or better.

The functions and settings described in this reference manual are not supported by all models and/or all firmware versions. A table can be found in the appendix denoting the individual functions, from which firmware version they are supported in the respective devices ('Overview of functions for LANCOM models and LCOS* versions' → page 366).

Illustrations of devices, as well as screenshots always represent just examples, which need not necessarily correspond to the actual firmware version.

Security settings

For a carefree use of your device, we recommend to carry out all security settings (e.g. Firewall, encryption, access protection, charge lock), which are not already activated at the time of purchase of your device. The LANconfig wizard 'Check Security Settings' will support you accomplishing this. Further information regarding this topic can be found in chapter 'Security' → page 92.

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

This documentation was compiled …

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

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

info@lancom.de

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

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

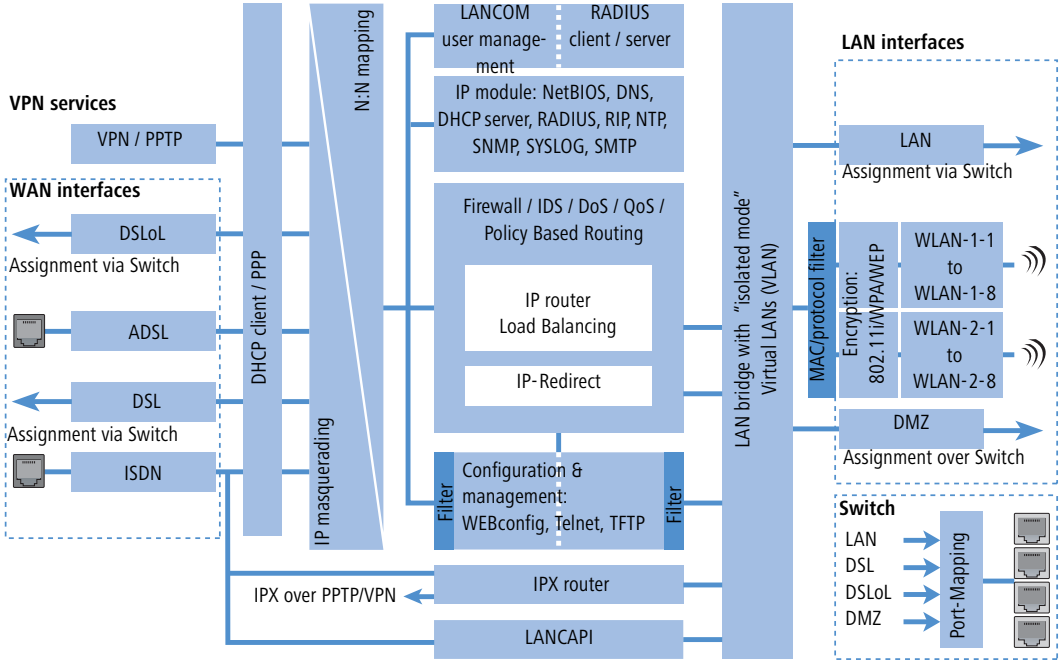
2 System design

2.1 Introduction

The LANCOM operating system LCOS is a collection of different software modules, the LANCOM devices themselves have different interfaces to the WAN and LAN. Depending on the particular application, data packets flow through different modules on their way from one interface to another.

The following block diagram illustrates in abstract the general arrangement of LANCOM interfaces and LCOS modules. In the course of this reference manual the descriptions of the individual functions will refer to this illustration to show important connections of the particular applications and to deduce the resulting consequences.

The diagram can thus explain for which data streams the firewall comes into play, or, in case of address translations (IP masquerading or N:N mapping), at which place which addresses are valid.



Notes regarding the respective modules and interfaces:

- The IP router takes care of routing data on IP connections between the interfaces from LAN and WAN.
- With IP redirect requests in the LAN are redirected to a specific computer
- The firewall (with the services "Intrusion Detection", "Denial of Service" and "Quality of Service") encloses the IP router like a shield. All connections via the IP router automatically flow through the firewall as well.

- LANCOM devices provide either a separate LAN interface or an integrated switch with multiple LAN interfaces as interfaces to the LAN.
- LANCOM Wireless access points resp. LANCOM routers with wireless modules offer additionally one or, depending on the respective model, also two wireless interfaces for the connection of Wireless LANs. Depending on the model every wireless interface can build up to eight different wireless networks ("multi SSID").
- A DMZ interface enables for some models a 'demilitarized zone' (DMZ), which is also physically separated within the LAN bridge from other LAN interfaces.
- The LAN bridge provides a protocol filter that enables blocking of dedicated protocols on the LAN. Additionally, single LAN interfaces can be separated by the "isolated mode". Due to VLAN functions, virtual LANs may be installed in the LAN bridge, which permit the operating of several logical networks on a physical cabling.
- Applications can communicate with different IP modules (NetBIOS, DNS, DHCP server, RADIUS, RIP, NTP, SNMP, SYSLOG, SMTP) either via the IP router, or directly via the LAN bridge.
- The functions "IP masquerading" and "N:N mapping" provide suitable IP address translations between private and public IP ranges, or also between multiple private networks.
- Provided according authorization, direct access to the configuration and management services of the devices (WEBconfig, Telnet, TFTP) is provided from the LAN and also from the WAN side. These services are protected by filters and login barring, but **do not** require any processing by the firewall. Nevertheless, a direct access from WAN to LAN (or vice versa) using the internal services as a bypass for the firewall is **not** possible.
- The IPX router and the LANCAPI access on the WAN side only the ISDN interface. Both modules are independent from the firewall, which controls only data traffic through the IP router.
- The VPN services (including PPTP) enable data encryption in the Internet and thereby enable virtual private networks over public data connections.
- Depending on the specific model, either xDSL/Cable, ADSL or ISDN are available as different WAN interfaces.
- The DSLoL interface (DSL over LAN) is no physical WAN interface, but more a "virtual WAN interface". With appropriate LCOS settings, it is possible to use on some models a LAN interface as an **additional** xDSL/Cable interface.

3 Configuration and management

This section will show you the methods and ways you can use to access the device and specify further settings. You will find descriptions on the following topics:

- Configuration tools
- Monitoring and diagnosis functions of the device and software
- Backup and restoration of entire configurations
- Installation of new firmware in the device

3.1 Configuration tools and approaches

LANCOM are flexible devices that support a variety of tools (i.e. software) and approaches (in the form of communication options) for their configuration. First, a look at the approaches.

You can connect to an LANCOM with three different access methods (according to the connections available).

- Through the connected network (LAN as well as WAN—inband)
- Through the configuration interface (config interface) on the rear of the router (also known as outband)
- Remote configuration via ISDN access or modem (analog or GSM with LANCOM Modem Adapter Kit)

What is the difference between these three possibilities?

On one hand, the availability: Configuration via outband is always available. Inband configuration is not possible, however, in the event of a network fault. Remote configuration is also dependent on an ISDN connection.

On the other hand, whether or not you will need additional hardware and software: The inband configuration requires one of the computers already available in the LAN or WAN, as well as only one suitable software, such as LANconfig or WEBconfig (see following section). In addition to the configuration software, the outband configuration also requires a the computers with a serial port. The preconditions are most extensive for ISDN remote configuration: In addition to an ISDN capable LANCOM, an ISDN card is needed in the configuration PC or alternatively, access via LANCAPI to an additional LANCOM that is ISDN capable.

3.2 Configuration software

Situations in which the device is configured vary—as do the personal requirements and preferences of the person doing the configuration. LANCOM routers thus feature a broad selection of configuration software:

- **LANconfig** – nearly all parameters of the LANCOM can be set quickly and with ease using this menu-based application. Outband, inband and remote configuration are supported, even for multiple devices simultaneously.
- **WEBconfig** – this software is permanently installed in the router. All that is required on the workstation used for the configuration is a web browser. WEBconfig is thus independent of operating systems. Inband and remote configuration are supported.

- **SNMP** – device-independent programs for the management of IP networks are generally based on the SNMP protocol. It is possible to access the LANCOM inband and via remote configuration using SNMP.
- **Terminal program, Telnet** – an LANCOM can be configured with a terminal program via the config interface (e.g. HyperTerminal) or within an IP network (e.g. Telnet).
- **TFTP** – the file transfer protocol TFTP can also be used within IP networks (inband and remote configuration).

The following table shows, how you can use the configuration:

Configuration software	LAN, WAN, WLAN (Inband)	Config Interface (Outband)	ISDN remote configuration	Analog dail-in (with LANCOM Modem Adapter Kit)
LANconfig	Yes	Yes	Yes	Yes
WEBconfig	Yes	No	Yes	Yes
SNMP	Yes	No	Yes	Yes
Terminal program	No	Yes	No	No
Telnet	Yes	No	No	No
TFTP	Yes	No	Yes	Yes

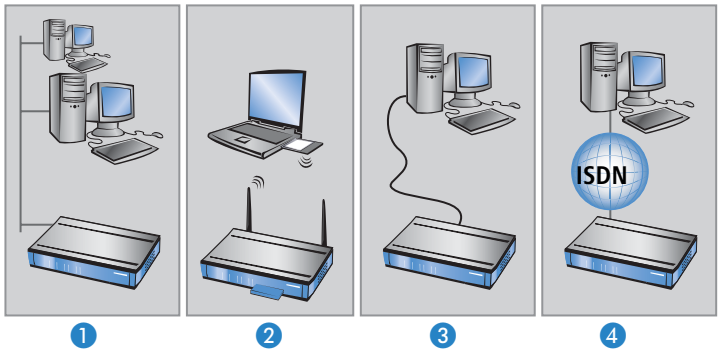
Please note that all procedures access the same configuration data. For example, if you change the settings in LANconfig, this will also have a direct effect on the values under WEBconfig and Telnet.

3.3 Searching and configuring devices

Always switch on your device first before starting the PC for configuration.

A Router or an Access Point can be configured in the following ways (provided that the model is equipped with the according interface):

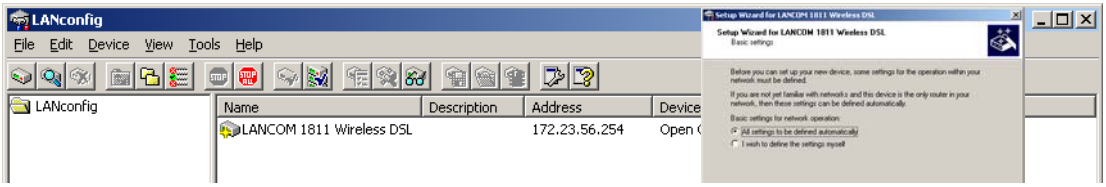
- Via the local network (LAN) 1.
- Via the wireless network (WLAN) 2, if the WLAN encryption (e.g. WEP) of a device with a wireless interface and in the configuration PC has been adjusted correctly and/or has been deactivated.
- Via the serial configuration interface 3.
- Via a ISDN connection 4



3.4 Configuration using different tools

3.4.1 LANconfig

Start LANconfig by, for example, using the Windows Start menu: **Start** ▶ **Programs** ▶ **LANCOM** ▶ **LANconfig**. LANconfig will now automatically search for devices on the local network. It will automatically launch the setup wizard if a device which has not yet been configured is found on the local area network LANconfig.



If the firewall is activated the LANconfig might not be able to find the new device in the LAN. In this occasion deactivate the firewill whilst the configuration.

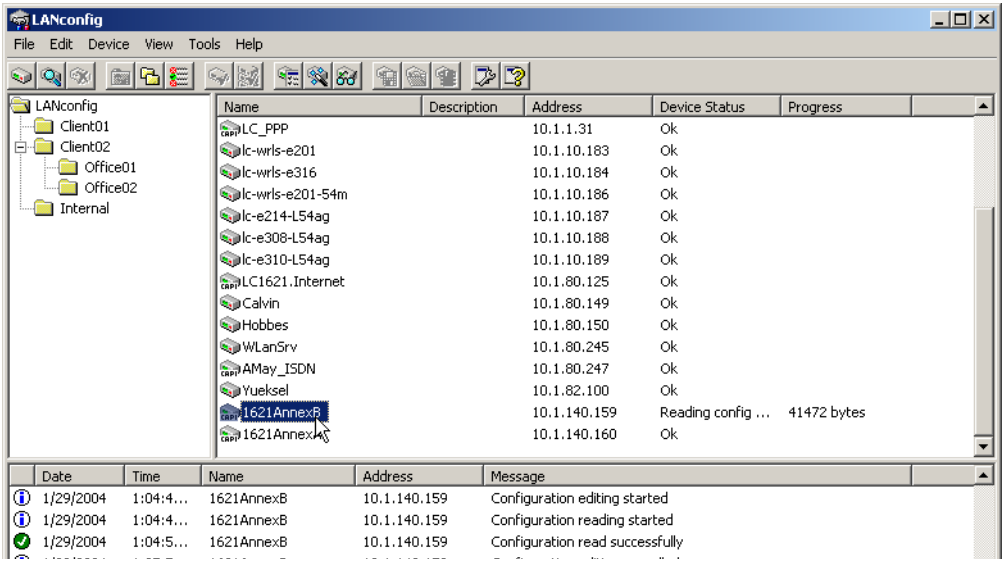
Your LANCOM device is equipped with an extensive firewall and protects your computer even if no further firewall is active.

Find new devices

Click on the **Find** button or call up the command with **Device** ▶ **Find** to initiate a search for a new device manually. LANconfig will then prompt for a location to search. You will only need to specify the local area network if using the inband solution, and then you're off.

Once LANconfig has finished its search, it displays a list of all the devices it has found, together with their names and, perhaps a description, the IP address and its status

.



The expanded range of functions for professionals

Two different display options can be selected for configuring the devices with LANconfig:

- The 'Simple configuration display' mode only shows the settings required under normal circumstances.
- The 'Complete configuration display' mode shows all available configuration options. Some of them should only be modified by experienced users.

Select the display mode in the **View** ▶ **Options** menu.

Double-clicking the entry for the highlighted device and then clicking the **Configure** button or the **Device** ▶**Configure** option reads the device's current settings and displays the 'General' configuration selection.

The integrated Help function

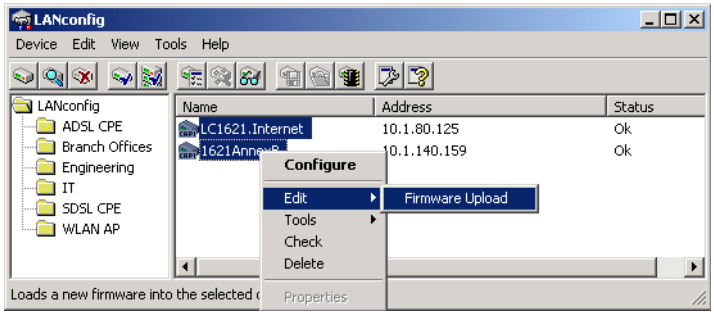
The remainder of the program's operation is self-explanatory or you can use the online help. You can click on the 'Help' button top right in any window or right-click on an unclear term at any time to call up context-sensitive help.

Management of multiple devices

LANconfig supports multi device remote management. Simply select the desired devices, and LANconfig performs all actions for all selected devices then, one after the other. The only requirement: The devices must be of the same type.

In order to support an easy management, the devices can be grouped together. Therefore, ensure to enable 'Folder Tree' in the View menu, and group the devices by 'drag an drop' into the desired folders.

LANconfig shows only those parameters that are suitable for multi device configuration when more than one device is selected, e.g. MAC Access Control Lists for all LANCOM Wireless Access Points.



3.4.2 WEBconfig

You can use any web browser, even text-based, for basic setup of the device. The WEBconfig configuration application is integrated in the LANCOM. All you need is a web browser in order to access WEBconfig.

Functions with any web browser

WEBconfig offers setup wizards similar to LANconfig and has all you need for easy configuration of the LANCOM—contrary to LANconfig but under all operating systems for which a web browser exists.

A LAN or WAN connection via TCP/IP must be established to use WEBconfig. WEBconfig is accessed by any web browser via the IP address of the LANCOM, via the name of the device (if previously assigned), or via any name if the device has not been configured yet.

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

Secure with HTTPS

WEBconfig offers an encrypted transmission of the configuration data for secure (remote) management via HTTPS.

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

For maximum security, please ensure to have installed the latest version of your Internet browser. For Windows 2000, LANCOM Systems recommends to use the "High Encryption Pack" or at least Internet Explorer 5.5 with Service Pack 2 or above.

Access to the device over WEBconfig

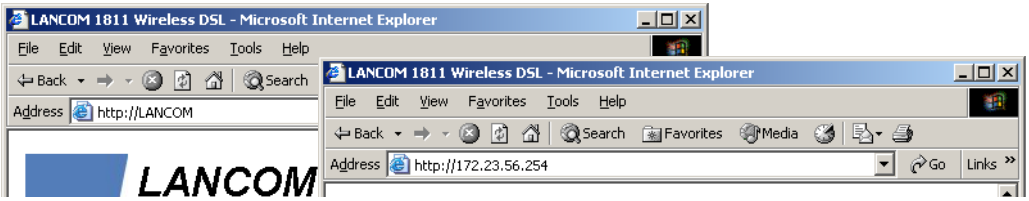
For the usage of WEBconfig the PC must be connected to the LAN or WAN over TCP/IP. WEBconfig runs with the help of a web browser and accesses the device either with the IP address of the LANCOM, with the name of the device (if already assigned) or with a any desired name, in case the device has not been configured yet.

The reaction of Routers and Access Points, as well as their accessibility for configuration via web browser is dependent on whether a DHCP server and a DNS server are already active in the LAN, and whether these two server processes exchange the assignment of IP addresses to symbolic names within the LAN between each other.

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

Network without DHCP server

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

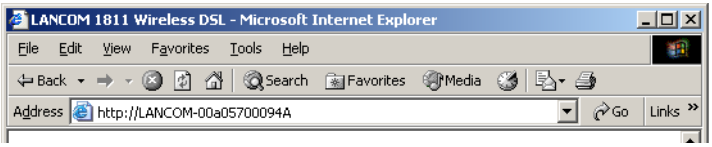


If the configuration PC does not obtain its IP address from the LANCOM DHCP server, figure out the current IP address of this PC (with **Start** ▶ **Execute** ▶ **cmd** and command **ipconfig** at the prompt under Windows 2000 or Windows XP, with **Start** ▶ **Execute** ▶ **cmd** and the command **winipcfg**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

Network with DHCP server

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

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



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

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

3.4.3 Telnet

Launching Telnet

Start configuration using Telnet, e.g. from the Windows command line with the command:

```
C:\>telnet 10.0.0.1
```

Telnet will then establish a connection with the device using the IP address.

After entering the password (if you have set one to protect the configuration), all configuration commands are available.

Linux and Unix also provide Telnet over SSL encoded connections. Depending on your distribution you might have to replace your version with one that provides SSL. The encoded Telnet connection is started with the command

```
C:\>telnet -z ssl 10.0.0.1 telnets
```

Change the language of the display.

The terminal can be set to English and German modes. The display language of your LANCOM is set to English at the factory. In the remaining documentation, all configuration commands will be provided in English. To change the display language to German, use the following commands:

Configuration tool	Run (when English is the selected language)
WEBconfig	Expert configuration ▶ Setup ▶ Config ▶ Language
Telnet	`set /Setup/Config/Language German`

Terminating Telnet

To terminate the configuration using Telnet, e.g. from the Windows command line with the command:

```
C:\>exit
```

The structure of the command line interface

The LANCOM command line interface is always structured as follows:

- **Status**
  Contains all read-only statistics of the individual SW modules
- **Setup**
  Contains all configurable parameters of all SW modules of the device
- **Firmware**
  Contains all firmware-management relevant actions and tables
- **Other**
  Contains dialling, boot, reset and upload actions

Command line reference

Navigating the command line can be accomplished by DOS and UNIX style commands as follows:

For executing some commands Supervisor rights are required.

Command	Description
beginscript	Begins script mode. In this state following entered commands are not directly transmitted into the configuration RAM of the LANCOM, but into the script memory of the device (LANCOM 'Scripting' → page 57).
cd [path]	Change the current directory. Certain abbreviations exists, e.g. "cd ../.." can be abbreviated to "cd ..." etc.
del [name]	Delete the table entry with the index <name>
default [-r] [path]	Resets single parameters, tables or hole indexes. Shows `PATH` on the directory of the index, the option `-r` (recursive) must be entered.
dir [path] list[path] ls [path] ll [path]	Display the contents of a directory. The detached parameter „-a" additionally to the contents of the request shows the SNMP-ID. Thereby the output begins with the SNMP ID of the device, followed by the SNMP ID of the present menu. In front of the single entries you can then find the SNMP IDs of the subitems.
do [path] [parameters]	Execute the action [path] in the current directory. Additional parameters can be entered.
echo <ARG>...	Display argument on the console
exit/quit/x	Close the console session
feature <code>	Unlock the feature with the specified feature code
flash Yes/No	The changes of the configuration with the commands in the command line are written directly into the boot resistent Flash memory of the devices (flash yes). If the update of the configuration is inhibited by the Flash (flash no), the changes are only saved in the RAM and are deleted when booting ('flash Yes/No' → page 66).
history	Shows a list of the previously executed commands. With the command „!#" the command of the list with the number (#) is directly executed: For instance „!3" specifies the third command of the list.

Command	Description
killscript	Deletes the not yet processed contents of a script session. The script session is specified by it's name 'Scripting' → page 57
loadconfig	Load the configuration via TFTP client into the device
loadfirmware	Load firmware via TFTP client into the device
loadscript	Load script via TFTP client into the device
passwd	Change the passwords
passwd -n new [old]	Change Password (without prompt)
ping [IP address]	Issues an ICMP echo request to the specified IP address
readconfig	Display the complete configuration of the device in "readconfig" syntax
readmib	Display SNMP Management Information Base
readscript [-n] [-d] [-c] [-m] [path]	Display all commands and parameters, which are important for the configuration of the LANCOM in present state ('Scripting' → page 57).
repeat [VALUE] <command>	repeats command every VALUE seconds until terminated by new input
sleep [-u] Value[suffix]	Delays processing the configuration commands for a certain time or terminates them at a certain time. As a suffix `s`, `m`, or `h` for seconds, minutes or hours, without suffix the command works in milliseconds. With the option switch `-u` the sleep command time of the form `MM/DD/YYYY hh:mm:ss` (english) or the form `DD.MM.YYYY hh:mm:ss` (german) is used. The date as parameters is only accepted if the system time is set.
stop	stop ping
set [path] <value(s)>	Set a configuration item to the specified value. If the item is a table entry, multiple values must be given (one for each table column). A "*" as a value indicates that the column in question should be left at its previous value.
set [path]	Show which values are allowed for a configuration item. If [path] is empty, this is displayed for each item in the current directory.
setenv <NAME> <VALUE>	Set environment variable
unsetenv <NAME>	Remove environment variable
getenv <NAME>	Read out environment variable (no newline)
printenv	Dump environment variable
show <options>	Shows internal data. Run show ? for a list of available items, e.g. boot history, firewall filter rules, vpn rules and memory usage
sysinfo	Shows basic system information
testmail	Sends an e-Mail. Parameter see 'testmail ?'
time	Set time (DD.MM.YYYY hh:mm:ss)
trace […]	Configures the trace output system for several modules, see 'How to start a trace' → page 81
who	List active sessions

Command	Description
writeconfig	Accept a new configuration in "readconfig" syntax. All subsequent lines are interpreted as configuration values until two blank lines in a row are encountered
writeflash	Load new firmware via TFTP
!!	Repeat previous command
!<num>	Repeat command <num>
!<prefix>	Repeat last command beginning with <prefix>
#<blank>	Comment

- PATH:
  - Qualifier for a menu or parameter separated by / or \
  - .. stands for upper level
  - . stands for current level
- VALUE:
  - Possible input
  - "" stands for an empty input
- NAME:
  - Sequence of _ 0..9 A..Z
  - first character must not be numeric
  - case does not matter
- All commands and directory/item names may be abbreviated as long as no ambiguity exists. For example, it is valid to shorten the "`sysinfo`" command to "`sys`" or a "`cd Management`" to "`c ma`". Not allowed would be "`cd /s`", since that could mean either "`cd /Setup`" or "`cd /Status`".
- Names with blanks in them must be enclosed in double quotes.
- Additionally, there is a command-specific help function available by calling functions with a question mark as the argument, i.e. entering "`ping ?`" displays the options for the built-in PING command.
- A complete listing of available commands for a particular device is available by entering '`?`' from the command line.

3.4.4 TFTP

Certain functions cannot be run at all, or not satisfactorily, with Telnet. These include all functions in which entire files are transferred, for example the uploading of firmware or the saving and restoration of configuration data. In this case TFTP is used.

TFTP is available by default under the Windows 2000 and Windows NT operating systems. It permits the simple transfer of files with other devices across the network.

The syntax of the TFTP call is dependent on the operating system. With Windows 2000 and Windows NT the syntax is:

```
tftp -i <IP address Host> [get|put] source [target]
```

With numerous TFTP clients the ASCII format is preset. Therefore, for the transfer of binary data (e.g. firmware) the binary transfer must usually be explicitly selected.This example for Windows 2000 and Windows NT shows you how to achieve this by using the '-i' parameter.

If the device is password protected, username and password needs to be inserted into the TFTP command. The file name is either made up of the master password and the command to be executed, or of the combined user name and password separated by a colon, plus with the command as a suffix. Thus a command sent by TFTP resembles the following:

- <Master password><Command> or
- <User name>:<Password>@<Command>

Futher information concerning TFTP commands and user rights can be foung in 'Rights for the administrators' → page 43 and 'Access with TFTP' → page 45.

Loading firmware, script or device configuration over TFTP

Instead of loading firmware or configuration files with LANconfig or WEBconfig onto a device, Telnet or SSH can directly load these files over a TFTP server. Using a TFTP server simplifies the administration of regular firmware and/or configuration updates in large installations.

For this purpose firmware files and configuration files are provided on a TFTP server, which works similar to a FTP server but applies a different protocol. The files on a TFTP server can be loaded with the following commands:

- `LoadConfig`
- `LoadFirmware`
- `LoadScript`

These commands can be used with following parameters:

- `-s <server IP address or server name>`
- `-f <directory and file name>`

  In directory and file name the following variables are permitted:

  - %m - LAN MAC address (hexadecimal, no characters, no seperators)
  - %s - serial number
  - %n - device name
  - %l - location
  - %d - device type

Examples:

The following example shows how a firmware file named 'LC-1811-5.00.0019.upx' in the directory 'LCOS/500' from a server with the IP address '192-168.2.200' is loaded onto the device:

- `LoadFirmware -s 192-168.2.200 -f LCOS/500/LC-1811-5.00.0019.upx`

The following example shows how a script matching to the MAC address from a server with the IP address '192-168.2.200' is loaded onto the device:

- `LoadScript -s 192-168.2.200 -f L%m.lcs`

If the case that the parameters `-s` and/or `-f` are not entered, the device uses standard values which are set under the directory `/setup/config/TFTP-Client`:

- `Config-address`
- `Config-filename`
- `Firmware-address`
- `Firmware-filename`

It is recommendable to use the standard values as long as the configuration and firmware update is continually saved under the same name and directory. Using this procedure the current files can be loaded with the commands `LoadConfig` and `LoadFirmware`.

3.4.5 SNMP

The Simple Network Management Protocol (SNMP V.1 as specified in RFC 1157) allows monitoring and configuration of the devices on a network from a single central instance.

There are a number of configuration and management programs that run via SNMP. Commercial examples are Tivoli, OpenView from Hewlett-Packard, SunNet Manager and CiscoWorks. In addition, numerous programs also exist as freeware and shareware.

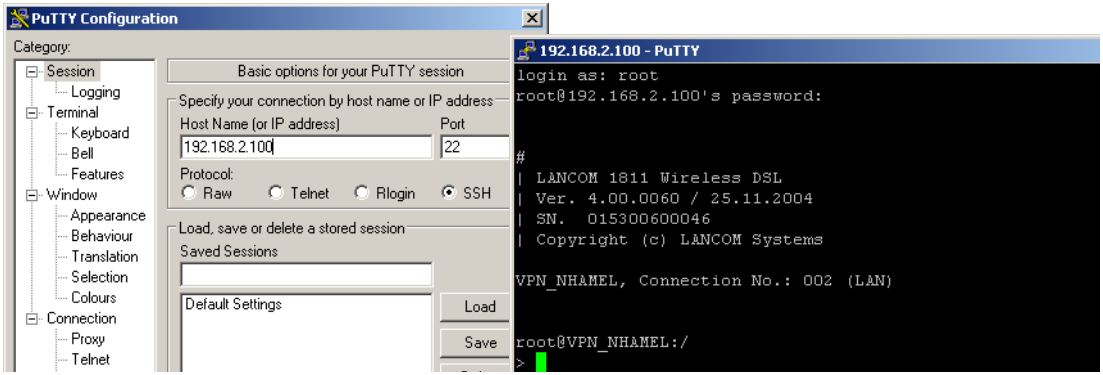
Your LANCOM can export a so-called device MIB file (**M**anagement **I**nformation **B**ase) for use in SNMP programs.

Configuration tool	Run
WEBconfig	Get Device SNMP MIB (in main menu)
TFTP	`tftp 10.0.0.1 get readmib file1`

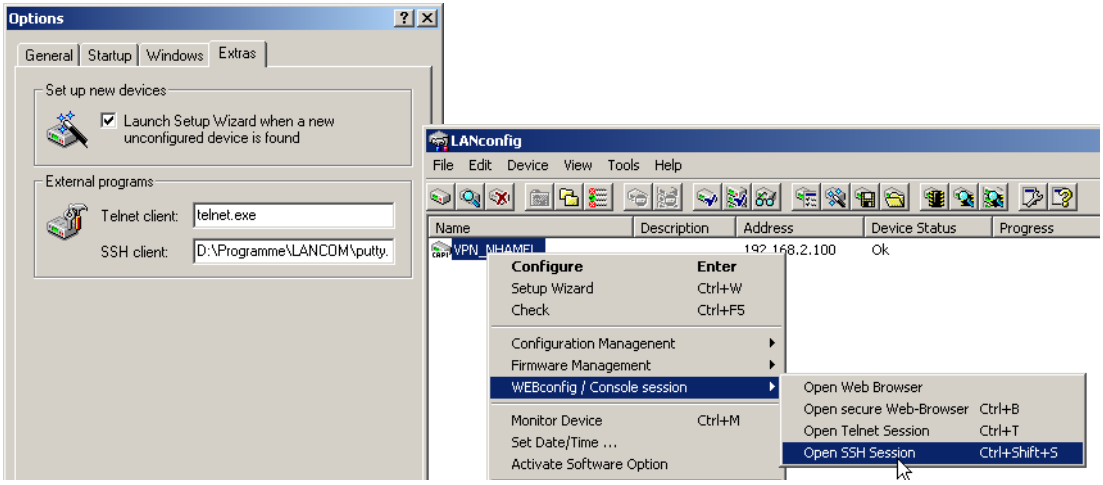
3.4.6 Encrypted configuration with SSH access

In addition to the option to configure a LANCOM with Telnet or a terminal program, LCOS version 4.00 and later provides an additional option of access via SSH. With a suitable SSH client such as PuTTy, you can set up an encrypted connection to the device and thus prevent the data being transferred during configuration from being intercepted within the network.

Start PuTTy (for example) and enter the LANCOM device's IP address as the host name. Use the command prompt that follows to log in by entering your user data.



Alternatively, you can use LANconfig under **Tools** ▶ **Options** ▶ **Extras** to enter your SSH client as an "external program"; then start the SSH access with a right-mouseclick on the device and open **WEBconfig/Console session** ▶ **Open SSH session**.



The configuration is carried out with the same commands as used under Telnet or other terminal program ('Command line reference' → page 30).

3.4.7 ISDN Remote configuration via Dial-Up Network

The complete section on remote configuration applies only to LANCOM with ISDN interface or a serial interface (with LANCOM Modem Adapter Kit).

Configuring routers at remote sites is particularly easy using the remote configuration method via a Dial-Up Network from Windows. The device is accessible by the administrator immediately without any settings being made after it is

switched on and connected to the ISDN interface. This means that you save a lot of time and costs when configuring at separate locations because you do not have to travel to the other network or instruct the staff on-site on configuring the router.

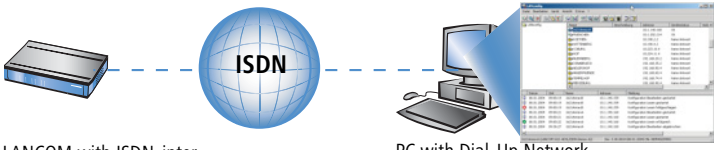
You can also reserve a special calling number for remote configuration. Then the support technician can always access the router even if it is really no longer accessible due to incorrect settings.

This is what you need for ISDN remote configuration

- An LANCOM with an ISDN connection
- A computer with a PPP client, e.g. Windows Dial-Up Network
- A program for inband configuration, e.g. LANconfig or Telnet
- A configuration PC with an ISDN card or access via *LANCAPI* to an LANCOM with ISDN access.

The first remote connection using Dial-Up Networking

For the remote connection of a LANCOM with LANconfig using Dial-Up Networking proceed as follows:



LANCOM with ISDN-interface for the configuration

PC with Dial-Up Networking, ISDN adapter (alternatively access to LANCAPI) and LANconfig

① In the LANconfig program select **Device** ▶ **New**, enable 'Dial-Up connection' as the connection type and enter the calling number of the ISDN interface to which the LANCOM is connected. If you wish, you can also enter the time period after which an idle connection is to be disconnected automatically.

② LANconfig now automatically generates a new entry in the Dial-Up Network. Select a device that supports PPP (e.g. the NDIS-WAN driver included with the LANCAPI) for the connection and press **OK** to confirm.

③ Then the LANconfig program will display a new device with the name 'Unknown' and the dial-up call number as the address in the device list.

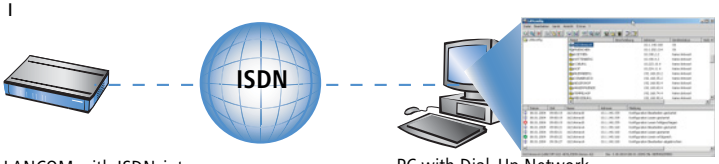
When an entry in the device list is deleted, the related connection in the Windows Dial-Up Network is also deleted.

④ You can configure the device remotely just like all other devices. LANconfig establishes a dial-up connection enabling you to select a configuration.

Always provide additional protection for the settings of the device by setting a password by switching to the 'Security' tab in the 'Management' configuration section.

The first remote connection using a PPP client and Telnet

Instead of a remote configuration with LANconfig it is also possible to access over ISDN with Telnet. For a remote configuration of a LANCOM with Telnet over any PPP client proceed as follows:



LANCOM with ISDN-interface for the configuration

PC with Dial-Up Networking, ISDN adapter (alternatively access to LANCAPI) and LANconfig

① Establish a connection to the LANCOM with your PPP client using the following details:

- User name 'ADMIN'
- The password selected in LANCOM
- An IP address for the connection, only if required

② Open a Telnet session to the LANCOM. Use the following IP address for this purpose:

- '172.17.17.18', if you have not defined an IP address for the PPP client. The LANCOM automatically uses this address if no other address has been defined. The PC making the call will respond to the IP '172.17.17.17'.
- Raise the IP address of the PC by one, if you have defined an address. Example: You have set the IP '10.0.200.123' for the PPP client, the LANCOM then responds to '10.0.200.124'. Exception: If the digits '254' are at the end of the IP address, the router responds to 'x.x.x.1'.

③ You can configure the LANCOM remotely just like all other devices.

Always provide additional protection for the settings of the device by setting a password. Alternatively, enter the following command during a Telnet or terminal connection:

```
passwd
```

You will then be prompted to enter and confirm a new password.

The default layer for remote field installations

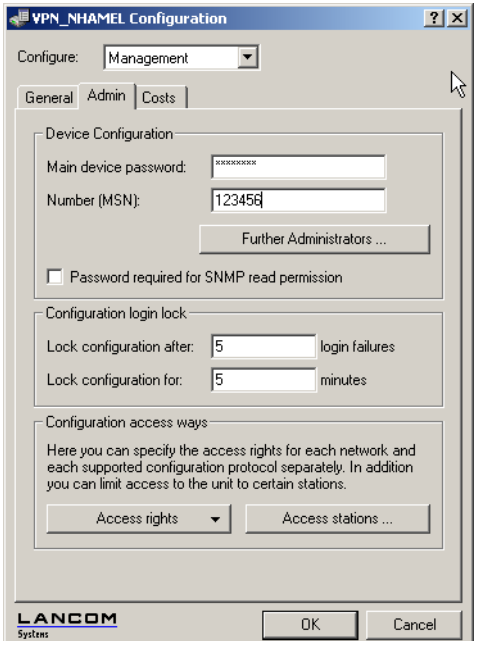
The PPP connection of any other remote site to the router, of course, will only succeed if the device answers every call with the corresponding PPP settings. This is the case using the factory default settings because the default protocol (default layer) is set to PPP.

You may, however, want to change the default layer for LAN-to-LAN connections, for example, to a different protocol after the first configuration run. Then the device will no longer take calls on the dial-up connection using the PPP settings. The solution to this is to agree upon a special calling number for configuration access:

The administrator access for ISDN remote management

If the device receives a call on this number, it will always use PPP, regardless of any other settings made on the router. Only a specific user name which is automatically entered by the LANconfig program during call establishment will be accepted during the PPP negotiations:

① Switch to the 'Admin' tab in the 'Management' configuration section.



② Enter a number (MSN) at your location which is not being used for other purposes in the 'Device Configuration' area.

Alternatively, enter the following command:

```
set /setup/config/Farconfig 123456
```

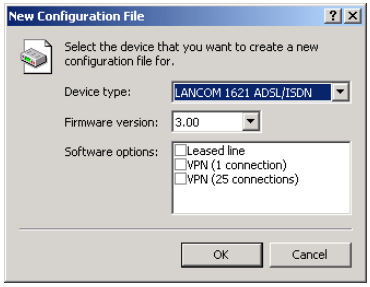
As long as no MSN is entered for the configuration access, a non-configured LANCOM accepts the calls on all MSNs. As soon as the first change is saved in the configuration, the device only takes calls on the configured MSN!

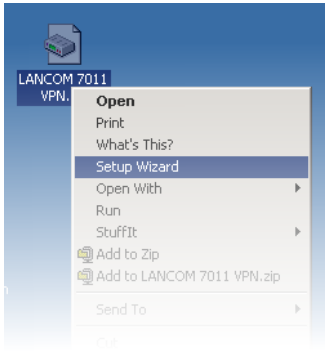
If no MSN configuration is entered the remote access is switched off and the device is protected against access over ISDN.

3.5 Working with configuration files

The current configuration of an LANCOM can be saved as a file and reloaded in the device (or in another device of the same type) if necessary.

Additionally, configuration files can be generated and edited offline for any LANCOM device, firmware option and software version:





Backup copies of configuration

With this function you can create backup copies of the configuration of your LANCOM.

Convenient series configuration

However, even when you are faced with the task of configuring several LANCOM of the same type, you will come to appreciate the function for saving and restoring configurations. In this case you can save a great deal of work by first importing identical parameters as a basic configuration and then only making individual settings to the separate devices.

Running function

Configuration tool	Run
LANconfig	Device ▶ Configuration Management ▶ Save to File Device ▶ Configuration Management ▶ Restore from File Edit ▶ New Configuration File Edit ▶ Edit Configuration File Device ▶ Configuration Management ▶ Print ...
WEBconfig	Save Configuration ▶ Load Configuration (in main menu)
TFTP	`tftp 10.0.0.1 get readconfig file1 tftp 10.0.0.1 put file1 writeconfig`

3.6 New firmware with LANCOM Systems FirmSafe

The software for devices from LANCOM Systems is constantly being further developed. We have fitted the devices with a flash ROM which makes child's play of updating the operating software so that you can enjoy the benefits of new features and functions. No need to change the EPROM, no need to open up the case: simply load the new release and you're away.

3.6.1 This is how LANCOM Systems FirmSafe works

LANCOM Systems FirmSafe makes the installation of the new software safe: The used firmware is not simply overwritten but saved additionally in the device as a second firmware. Therewith your device is protected against the results of a power blackout or a disconnection while installing the firmware.

Of the two firmware versions saved in the device only one can ever be active. When loading a new firmware version the active firmware version is not overwritten. You can decide which firmware will be activated after the upload:

- 'Immediate': The first option is to load the new firmware and activate it immediately. The following situations can result:
  - The new firmware is loaded successfully and works as desired. Then all is well.
  - The device no longer responds after loading the new firmware. If an error occurs during the upload, the device automatically reactivates the previous firmware version and reboots the device.
- 'Login': To avoid problems with faulty uploads there is the second option with which the firmware is uploaded and also immediately booted.
  - In contrast to the first option, the device will wait for the adjusted firmsafe timeout (using WEBconfig in the menu **Expert Configuration ▶ Firmware ▶ Timeout-firmsafe**, using Telnet adjust with 'Firmware/Timeout-firmsafe') until it is logged on over Telnet, a terminal program or WEBconfig. Only if this login attempt is successful does the new firmware remain active permanently.
  - If the device no longer responds or it is impossible to log in, it automatically loads the previous firmware version and reboots the device with it.

- 'Manual': With the third option you can define a time period during which you want to test the new firmware yourself. The device will start with the new firmware and wait for the preset period until the loaded firmware is manually activated and therefore becomes permanently effective. Activate the new firmware using LANconfig with **Device ▶ Firmware Management ▶ Activate Firmware running in Test Mode**, using Telnet under 'firmware/firmsafe table' with the command 'set # active' (# is the position of the firmware in the firmsafe table). Using WEBconfig you can find the firmsafe table under **Expert Configuration▶ Firmware**.

The modus for the firmware upload can be adjusted using WEBconfig in the menu **Expert Configuration ▶ Firmware ▶ Mode-firmsafe**, using Telnet under 'firmware/timeout firmsafe'. Using LANconfig select the modus when selecting the new firmware file.

LIt is only possible to upload a second firmware, if the device has enough memory for two firmware versions. Current firmware versions (in occasion with additional software options) may use up more than half of the available memory. In this case the configuration software notifies a conflict and recommends the use of the "converter".

This converter can be downloaded free of charge from the LANCOM Systems website. With the converter the memory in the LANCOM is divided into a larger area for the new firmware version and a smaller area for the existing version.

While uploading the new firmware a minimal version of the previous firmware is loaded into the smaller memory area. This version is used as a safety copy with the following restrictions:

- The minimal version of the firmware only partly provides the LCOS functions to restore the previous state or to load another firmware. Internet access is possible with this version.
- A LANCOM with an active minimal firmware can only be addressed over the LAN, the WLAN or the outband interface. The remote configuration is not possible, not even over ISDN.
- The minimal firmware can not be configurated. Changes in the configuration over LANconfig, WEBconfig or Telnet are not saved in the device.

3.6.2 How to load new software

There are various ways of carrying out a firmware upload, all of which produce the same result:

- LANconfig
- WEBconfig
- Terminal program
- TFTP

All settings will remain unchanged by a firmware upload. All the same you should save the configuration first for safety's sake (with **Device ▶ Configuration Management ▶ Save to File** if using LANconfig, for example). Before uploading you should also save a version of the current firmware. If you do not have the firmware as a file, you can download it from www.lancom.de.

If the newly installed release contains parameters which are not present in the device's current firmware, the device will add the missing values using the default settings.

LANconfig

When using LANconfig, highlight the desired device in the selection list and click on **Device ▶ Firmware Upload**, or click directly on the **Firmware Upload** button. Then select the directory in which the new version is located and mark the corresponding file.

LANconfig then tells you the version number and the date of the firmware in the description and offers to upload the file. The firmware you already have installed will be replaced by the selected release by clicking **Open**.

You also have to decide whether the firmware should be permanently activated immediately after loading or set a testing period during which you will activate the firmware yourself. To activate the firmware during the set test period, click on **Edit ▶ Firmware Management .** After upload, start the new firmware in test mode.

WEBconfig

Start WEBconfig in your web browser. On the starting page, follow the **Perform a Firmware Upload** link. In the next window you can browse the folder system to find the firmware file and click **Start Upload** to start the installation.

Terminal program (e.g. Telix or Hyperterminal in Windows)

If using a terminal program, you should first select the 'set mode-firmsafe' command on the 'Firmware' menu and select the mode in which you want the new firmware to be loaded (immediately, login or manually). If desired, you can also set the time period of the firmware test under 'set Timeout-firmsafe'.

Select the 'do Firmware-upload' command to prepare the router to receive the upload. Now begin the upload procedure from your terminal program:

- If you are using Telix, click on the **Upload** button, specify 'XModem' for the transfer and select the desired file for the upload.
- If you are using Hyperterminal, click on **Transfer ▶ Send File**, select the file, specify 'XModem' as the protocol and start the transfer with **OK**.

The firmware upload over a terminal program is only possible over a serial configuration interface.

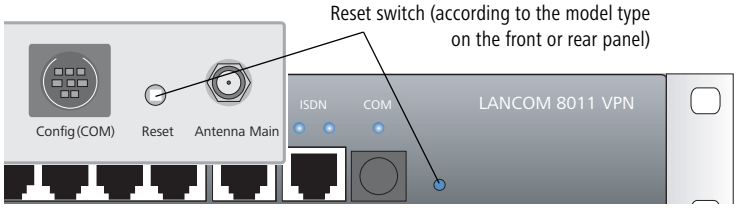
TFTP

TFTP can be used to install new firmware on LANCOM. This can be done with the command (or target) **writeflash**. For example, to install new firmware in a LANCOM with the IP address 10.0.0.1, enter the following command under Windows 2000 or Windows NT:

```
tftp -i 10.0.0.1 put Lc_16xxu.282 writeflash
```

3.7 How to reset the device?

If you have to configure the device regardless of possible existing settings, or if a connection to the device configuration failed, you can put back the device into the factory default state with a **Reset**. To do so, **push** the **Reset button** until the device LEDs will light up (approx. 5 seconds).



After applying the reset, the device will start fresh with factory defaults. **All** settings will be lost. Therefore, you should save the current configuration if possible **before** the reset!

Please notice that also the WLAN encryption settings of the device will get lost in case of a reset and the standard WEP key comes into effect again. The wireless configuration of a device with WLAN interface will only succeed after a reset, if the standard WEP key is programmed into the WLAN adapter!

3.8 Managing rights for different administrators

Multiple administrators can be set up in the configuration of the LANCOM, each with differing access rights. For a LANCOM, up to 16 different administrators can be set up.

Besides these administrators set up in the configuration, there is also the "root" administrator with the main password for the device. This administrator always has full rights and cannot be deleted or renamed. To log in as root administrator, enter the user name "root" in the login window or leave this field empty.

As soon as a password is set for the "root" administrator in the device's configuration, then WEBconfig will display the button **Login** that starts the login window. After entering the correct user name and password, the WEBconfig main menu will appear. This menu only displays the options that are available to the administrator who is currently logged in.

If more than one administrator is set up in the admin table, the main menu features an additional button **Change Administrator** which allows other users to log in (with different rights, if applicable).

3.8.1 Rights for the administrators

Two different groups are differentiated regarding administrators' rights.

- Each administrator belongs to a certain group that has globally defined rights assigned to it.

- Each administrator also has "function rights" that determine the personal access to certain functions such as the Setup Wizards.

Administrator groups

Description under Telnet/Terminal	Description under LANconfig	Rights
Supervisor	All	Supervisor — member of all groups
Admin-RW	Limited	Local administrator with read and write access
Admin-RO	Read only	Local administrator with read access but no write access
None	None	No access to the configuration

- Supervisor: Has full access to the configuration
- Local administrator with read and write access: Also has full access to the configuration, although the following options are prohibited:
  - Upload firmware onto the device
  - Upload configuration onto the device
  - Configuration with LANconfig

Local administrators with write access can also edit the admin table. However, a local administrator can only change or create entries for users with the same or less rights than himself. It follows that a local administrator cannot create a supervisor access and assign himself those rights.

- Local administrator with read access: Can read the configuration with Telnet or a terminal program, but cannot change any values. The administrators can be assigned certain configuration options via their function rights.
- None: Cannot read the configuration. The administrators can be assigned certain configuration options via their function rights.

Function rights

Function rights can be used to grant the following options to users:

- Basic Settings Wizard
- Security Settings Wizard
- Internet Connection Wizard
- Selection of Internet Provider Wizard
- RAS Account Wizard
- LAN-LAN Connection Wizard
- Change time and date

- Search for further devices
- WLAN link test
- a/b Wizard

3.8.2 Administrators' access via TFTP and SNMP

The additional access possibilities for administrators are generally used for configuring the device with Telnet, terminal programs or SSH access. However, the other administrators can also access the device via TFTP or SNMP.

Access with LANconfig

A user with supervisor rights can login to LANconfig by entering his user data into the Password field of the login window in the combination <Username>:<Password>.

Access with TFTP

In TFTP, the user name and password are coded in the source (TFTP read request) or target file names (TFTP write request). The file name is either made up of the master password and the command to be executed, or of the combined user name and password separated by a colon, plus with the command as a suffix. Thus a command sent by TFTP resembles the following:

- <Master password><Command> or
- <Username>:<Password>@<Command>

Examples (the LANCOM has the address mylancom.intern, the master password is 'RootPwd' and a user has been set up named 'LocalAdmin' with the password 'Admin'):

- Read the configuration from the device (supervisor only)

  ```
  tftp mylancom.intern GET RootPwdreadconfig mylancom.lcf
  ```

- Write the configuration to the device (supervisor only)

  ```
  tftp mylancom.intern PUT mylancom.lcf RootPwdwriteconfig
  ```

- Read out the device MIB (for the local administrator)

  ```
  tftp mylancom.intern GET localadmin:Adminreadmib
  mylancom.lcf mylancom.mib
  ```

For the menus and available commands, the same limitations on rights apply as with Telnet.

Access with SNMP management systems

For the administration of networks with the help of SNMP tools such as HP OpenView, the various levels of administrator access can be used for the precise control of rights.

Under SNMP, user name and password are coded in the "community". Here, the 'public' community can be selected or one of either the master password or a combination of user name and password divided by a colon can be selected.

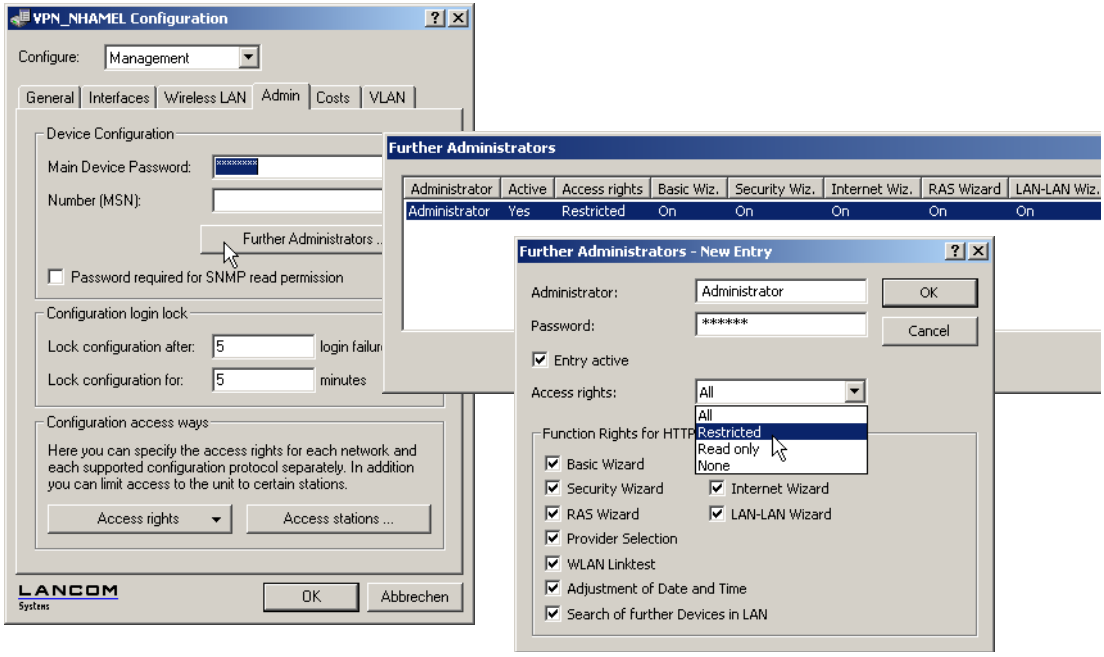
The community 'public' corresponds with the rights of a local administrator with read-only access, as long as the SNMP read access without password is enabled ('Password protection for SNMP read-only access.' → page 55). If this access is not allowed, then the 'public' community will have access to no menus at all.

Otherwise, the same limitations on rights apply for the menus as with Telnet.

3.8.3 Configuration of user rights

LANconfig

When using LANconfig for the configuration, you will find the list of administrators in the configuration area 'Management' on the 'Admin' tab under the button **Further administrators**.



Enter the following values:

- Name for the new administrator with password.
- Access rights
- Function rights

You can temporarily deactivate the entries without having to delete them completely with the button 'Entry active'.

WEBconfig, Telnet or terminal program

Under WEBconfig, Telnet or a terminal program, you will find the settings for the serial interface under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ Config ▶ Admin.-table
Terminal/Telnet	`Setup/Config/Admin.-table`

The different user groups are represented by the following values:

Description	Rights
Supervisor	Supervisor — member of all groups
Admin-RW	Local administrator with read and write access
Admin-RO	Local administrator with read access but no write access
None	No access to the configuration

The different function rights are represented by the following hexadecimal values:

Value	Rights
0x00000001	The user can run the Basic Configuration Wizard
0x00000002	The user can run the Security Wizard
0x00000004	The user can run the Internet Wizard
0x00000008	The user can run the Wizard for selecting Internet providers
0x00000010	The user can run the RAS Wizard
0x00000020	The user can run the LAN-LAN Coupling Wizard
0x00000040	The user can set the date and time (also applies for Telnet and TFTP)
0x00000080	The user can search for additional devices
0x00000100	The user can run the WLAN Link test (also applies for Telnet)
0x00000200	The user can run the a/b Wizard

The entry results from the sum of the first, second and third columns from the right. If, for example, the user is to receive rights to use the "Security Wizard", "Selection of Internet provider", "RAS Wizard", "Change time" and "WLAN Link Test", then the resulting values are as follows:

- First column from the right: 2 (Security Wizard) + 8 (Selection of Internet Provider) = "a" (hexadecimal)
- Second column from the right: 1 (RAS Wizard) + 4 (Change Time) = "5" (hexadecimal)
- Third column from the right: 1 (WLAN-Linktest) = "1" (hexadecimal)

For this example, the function rights are entered with the value "0000015a".

Said differently it is a disjunction of the hexadecimal values:

Description	Value
Security Wizard	0x00000002
Selection of Internet provider	0x00000008
RAS Wizard	0x00000010
Change time	0x00000040
WLAN Link Test	0x00000100
Disjunction	0x0000015a

Examples:

The following command sets up a new user in the table who, as local administrator "Smith" with the password "BW46zG29", can select the Internet provider. The user will be activated immediately:

```
set Smith BW46zG29 yes Admin-RW 00000008
```

The following command extends the function rights such that user "Smith" can also run the WLAN link test (the asterisks stand for the values which are not to be changed):

```
set Smith * * * 00000108
```

3.8.4 Limitation of the configuration commands

The availability of commands when configuring the devices with Telnet or a terminal program depends on the user's rights:

Command	Supervisor	Local administrator	Remark
activateimage	✔		
cfgreset	✔		
linktest	✔		The 'linktest' command can also be executed if the user possesses the function right to carry out a WLAN link test
readconfig	✔		
writeconfig	✔		
writeflash	✔		
setenv	✔	✔	

Command	Supervisor	Local administrator	Remark
testmail	✔	✔	
time	✔	✔	The 'time' command can also be executed if the user possesses the function right to set the system time
unsetenv	✔	✔	
delete/rm	✔	✔	
readmib	✔	✔	
WLA	✔	✔	
set	✔	✔	

All other commands (such as 'cd', 'ls', 'trace', etc...) can be used by all users. The user must possess at least write access to be able to operate commands that cause changes to the system (e.g. 'do' or 'time').

The commands listed above are not available in all LCOS versions or LANCOM models.

3.9 Multiple loopback addresses

In a local network, a LANCOM can be contacted with its intranet IP address or with its DMZ IP address. In large network structures that are managed centrally, it can occur that multiple devices have the same intranet IP number. Devices in this scenario can still be unambiguously addressed by using additional, freely definable IP addresses.

Up to 16 of these additional "loopback" addresses can be set up in a LANCOM router. Loopback addresses serve as additional IP addresses for the device and can be selected freely from the pool of private IP addresses. These loopback addresses do not have to belong to the same range of IP addresses as those used in the intranet or DMZ. Thus, for the management of multiple or rigorously structured networks, all of the LANCOM routers can be identified with loopback addresses of consecutive IP addresses selected from a certain range of IP numbers. Each device is then uniquely identifiable by its loopback address and SNMP traps can be assigned to the corresponding source based on the loopback address.

WEBconfig, Telnet or terminal program

Under WEBconfig, Telnet or a terminal program, you will find the loopback list under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ TCP-IP ▶ Loopback-list
Terminal/Telnet	`Setup/TCP-IP/Loopback-list`

4 Network management with the LANtools

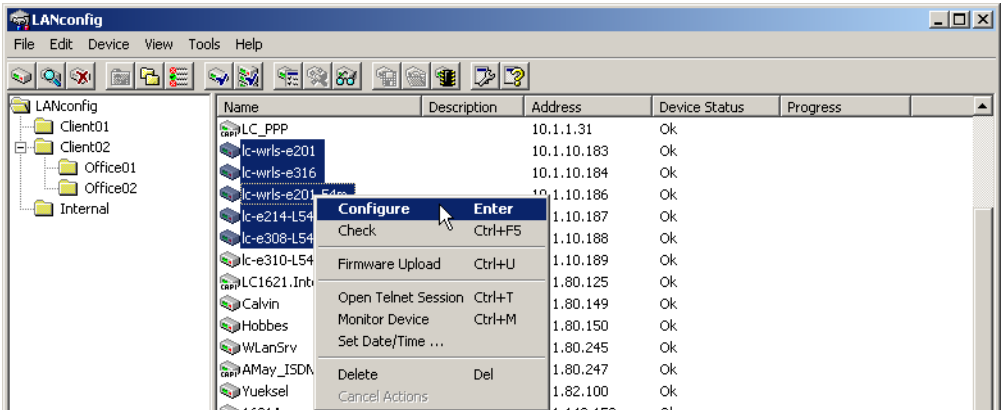
The LANtools (consisting of LANconfig and LANmonitor) are ideally suited to configuring and monitoring LANCOM devices in complex application scenarios. Multiple routers and/or wireless access points in a network can be administered from a central location, as can devices in remote networks—for example, when a service company maintains a device located with the customer.

Network management with the LANtools primarily involves the following functions:

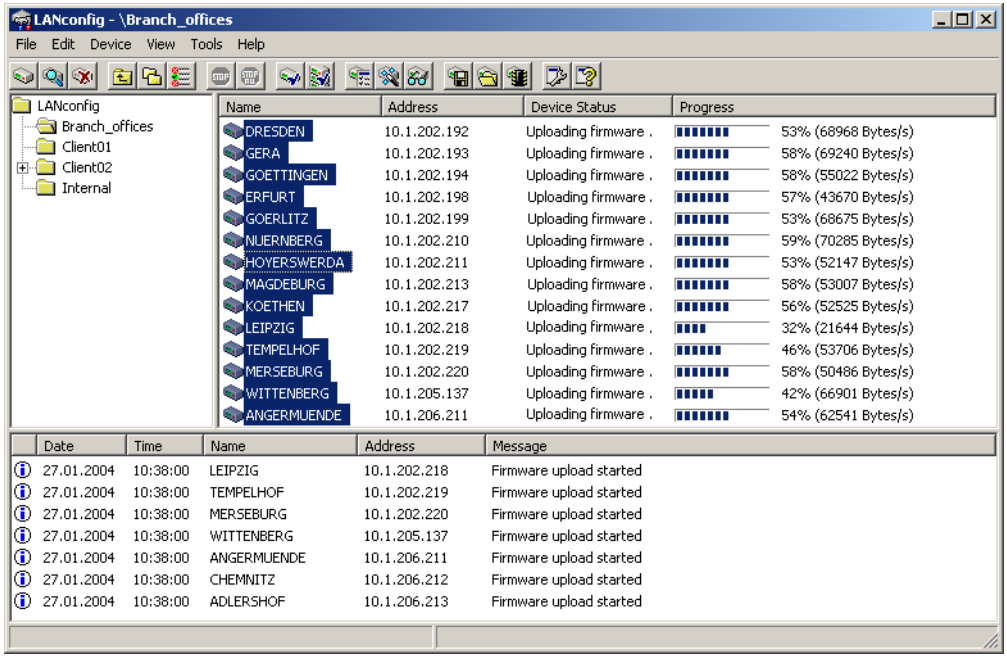
- Device configuration
- Management of configurations, i.e. save and restore the settings
- Carries out updates to the latest firmware versions
- Activates additional software options
- Monitors device status
- Connection monitoring (including VPN)
- Monitoring of firewall actions

4.1 Project management with LANconfig

LANconfig facilitates the configuration of various devices within a project with a range of functions that can be run on several devices at once. If the list in LANconfig contains multiple devices, just click on the device of your choice with the right mouse key to open a context menu offering the following actions:



- Configure: Opens up the LANconfig configuration dialog for the selected device
- Check: Checks if the selected device can be contacted
- Firmware upload: Uploads firmware simultaneously to all selected devices
- Apply Script: Applies a configuration script to all selected devices



- Open Telnet session: Opens up multiple DOS windows and sets up a Telnet connection to each device
- Monitor device: Starts LANmonitor for the surveillance of the selected devices
- Set date/time: Sets the same time on all selected devices.

When setting the time, please observe the functions of the LANCOM as NTP client and NTP server ('Time server for the local net' → page 548).

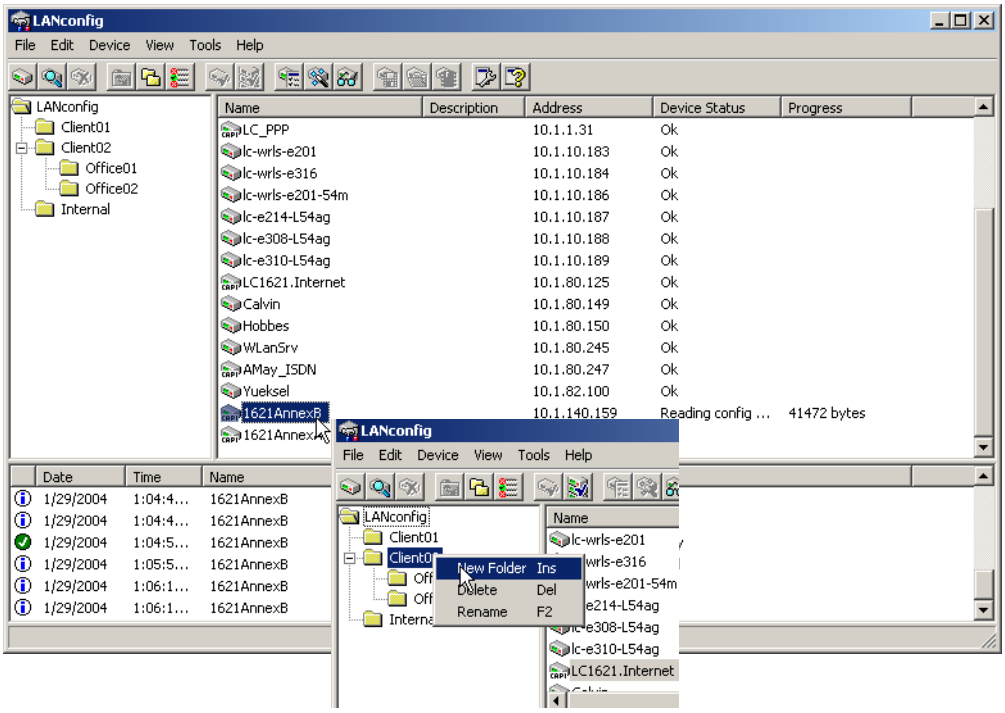
- Delete: Deletes the selected devices from the LANconfig list.

4.1.1 Directory structure

LANconfig uses a directory structure for a clear overview when managing multiple devices. Folders dedicated to projects or customers can be set up to organize the relevant devices:

- Create a new folder by clicking on the parent directory with the right mouse key and selecting "New Folder" from the context menu.
- Just use the mouse to drag and drop the devices into the appropriate folder. Devices can also be moved from one folder to another in this way.

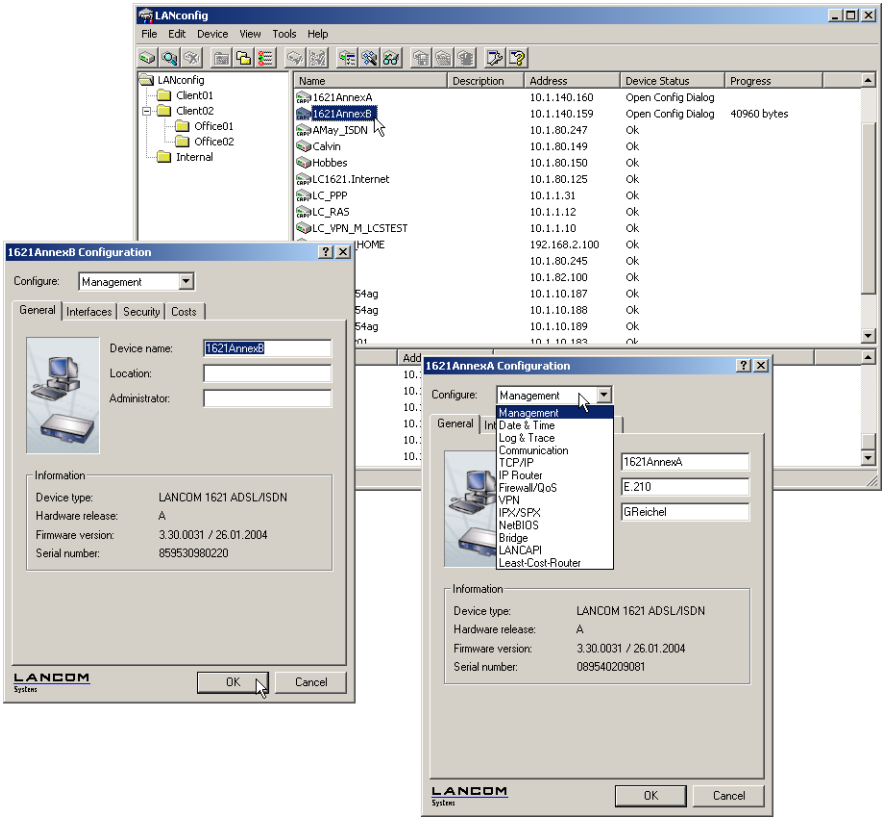
The arrangement of devices in folders effects only the display of the devices within LANconfig. The organization of the folders has no influence on the configuration of the devices.



The directory structure in the left margin of the LANconfig window can be switched on and off with the **F6** function key or by using the menu **View ▶ Folder Tree**.

4.1.2 Multithreading

The management of larger projects can be aided by simultaneously opening up configuration windows for multiple devices to compare similarities and differences. LANconfig allows multiple configuration dialogs to be opened at the same time ("multithreading"). After opening the configuration for a device, simply open up further configurations from the device list in LANconfig. All of the configurations can be processed in parallel.



"Cut and paste" can be used to transfer content between the configuration windows via the Windows clipboard.

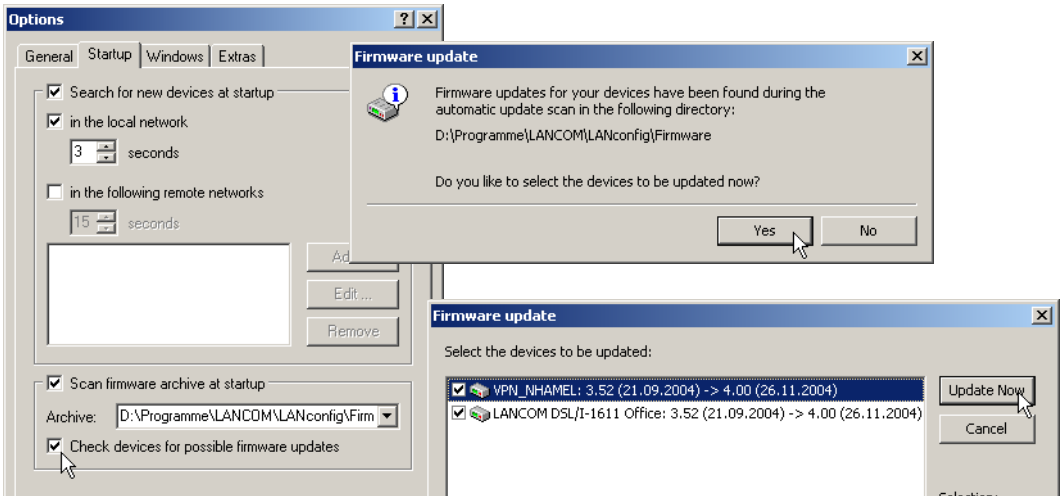
Multithreading allows changes to both the internal configurations of the available devices and to the configuration files. Each configuration is written separately to the file and to the device when the dialog is closed.

4.1.3 Manual and automatic searches for firmware updates

To make the update of LANCOM devices with new firmware as convenient as possible, the firmware files for the various LANCOM models and LCOS versions are, ideally, saved to a central archive directory. The search for new versions of the firmware in this directory can either be initiated manually or automatically after starting LANconfig.

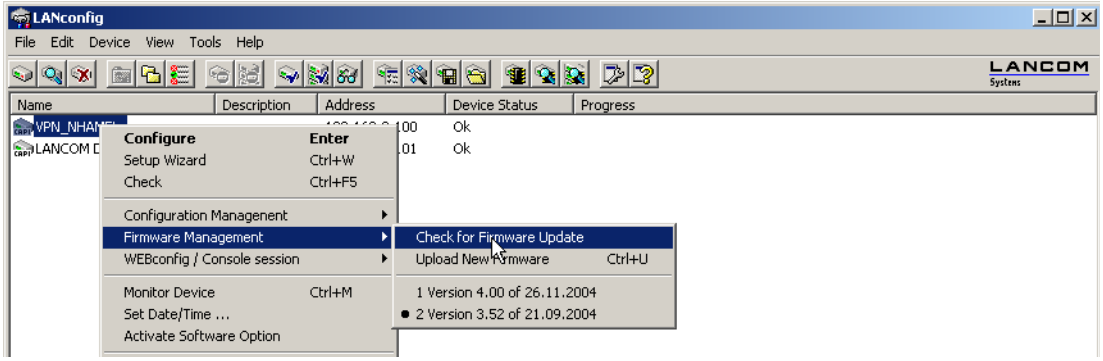
Automatic search for firmware updates

The directory where LANconfig is to search for the updates is set under **Tools** ▶ **Options** ▶ **Extras**. It is also possible to set up LANconfig to search the firmware archive and to check if any of the devices found require an update. With this option activated, starting LANconfig automatically displays all of the devices for which new updates are available.



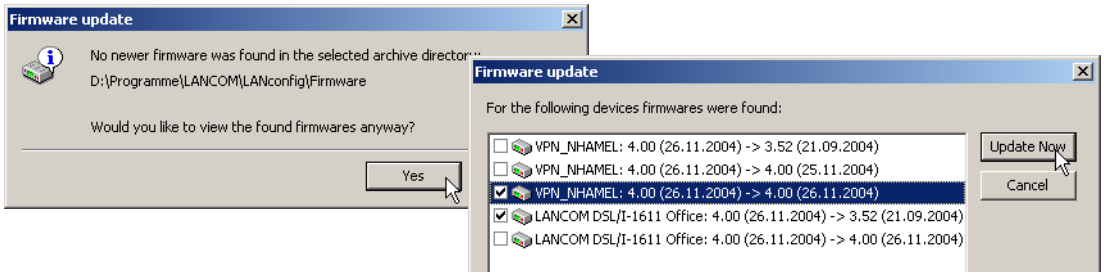
Manual search for firmware updates

To search manually for firmware updates, click with the right-hand mouse key on a device marked in the list and select the following point from the context menu: **Firmware management** ▶**Check for firmware update**. If you wish to update several devices simultaneously, the entry **Check for firmware updates** is displayed directly in the context menu.



View a full list of all firmware versions

If your search in the archive did not reveal a new firmware version, you can alternatively view a full list of all of the firmware files that have been found. You can, for example, switch back to an older version. LANconfig displays all versions found for the marked devices, including the version currently active in each device. For each device, you can select precisely one firmware version that will then be uploaded onto the device.

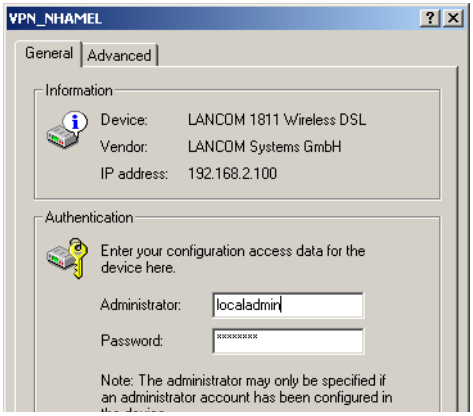


4.1.4 Password protection for SNMP read-only access.

The read-only access to a LANCOM device via SNMP—for example with LANmonitor--can be password protected. This uses the same user data as with access to LANconfig. Password protection of SNMP access means that the user data must be entered before information about the device status, etc. can be accessed over SNMP.

LANmonitor

User information can be entered in LANmonitor separately for each device. To do this, click with the right-hand mouse key on the required device, select the **Options** point from the context menu and enter your user data.



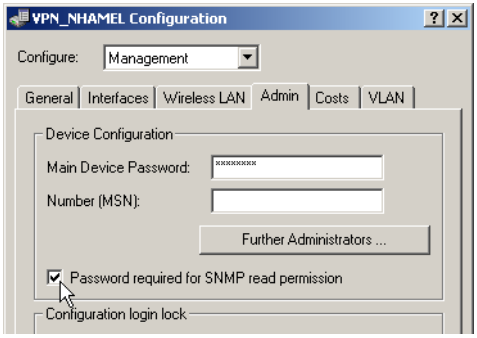
Access rights in LANmonitor depend on the rights possessed by the user:

- A supervisor has full access to the information in LANmonitor and can execute actions such as closing a connection, among others.

- A local administrator also has full access to the information in LANmonitor and can execute actions such as closing a connection, among others.
- A user with read-only rights can view the information in LANmonitor but cannot take any actions such as closing a connection.
- A user without rights has no SNMP access to the device's information.

LANconfig

For configuration with LANconfig, you will find the switch for SNMP access in the configuration area 'Management' on the 'General' tab.



WEBconfig, Telnet or terminal program

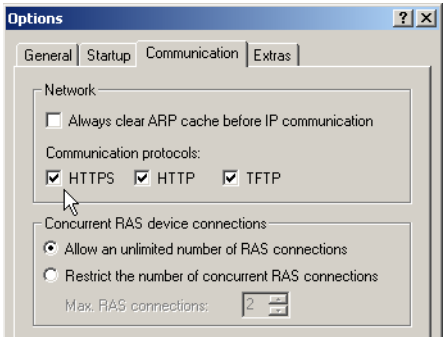
Under WEBconfig, Telnet or a terminal program, you will find the settings for the SNMP read access under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ Config ▶ Password-required-for-SNMP-read-access
Terminal/Telnet	`Setup/Config/Password-required-for-SNMP-read-access`

4.1.5 Device communication over HTTP and HTTPS

On occasion, extremely large files are transmitted for communicating with devices using LANconfig. In addition to its advantages, one disadvantage of the TFTP protocol that has been used up to now is that it enables data to be transmitted slowly. In particular with larger network installations with many routers at different locations, it is desirable for data to be exchanged with the devices more quickly.

The HTTP and HTTPS protocols are also offered to accelerate uploading firmware and scripts and uploading and downloading configurations. You can select the protocol that is used in LANconfig by selecting the menu option **Options** on the 'Communication' tab page. All other processes not mentioned here are realized using TFTP.



Using HTTP improves the transmission speed; HTTPS can also offer additional security mechanisms. The use of HTTPS is especially recommended for remote management over unsecured WAN connections (such as DYNDNS services).

Select here at least one of the protocols on offer. If several protocols are activated, LANconfig tries first of all to establish the transmission using the best protocol. If the attempt fails using this protocol, the next attempt is made using the next-best protocol.

As the name of the certificate does not match the name of the issuing site, the HTTPS check expects confirmation from the user before accessing the device.

4.2 Scripting

Installations with multiple LANCOM devices often profit from the automatic execution of certain configuration tasks. The scripting function in LANCOM enables entire sets of commands for device configuration to be stored in a single file—a script—for transfer to one or more devices in one step.

4.2.1 Applications

Scripting provides users with a powerful tool for the centralized configuration of LANCOM devices, and thus a wide range of potential applications:

- Read-out device configurations in a form that is easy to read and save

  The configuration files generated by LANconfig are not intended for processing with other tools; users will only get an overview of the complete configuration from a print-out of the configuration file. The scripting functions can output the configuration as ASCII text to be saved as a text file.

- Edit the configuration with a simple text editor

  If offline configuration with LANconfig is not possible or not desired, a configuration file generated by scripting can be edited with a text editor and then uploaded to the device again.

- Edit sections of the configuration

  Instead of the entire configuration, smaller sections of it can be read out from a device instead (e.g. just the firewall settings). Just as with complete configurations, sections can be edited and transferred to one or more

devices. This allows the particular settings in a device to be uploaded to other models or devices with a different version of the firmware.

- Automized configuration updates

  The centralized storage of configuration scripts in combination with scheduled LCOS commands (cron jobs) can be used to keep vital sections of the configuration in multiple devices up to date, e.g. the encryption settings for a WLAN.

- Convenient roll-out for larger installations

  The installation of multiple devices at different locations can be very easily controlled from a central location. Even employees without administrator rights can then set up the devices with a single command.

- Storage of configuration to volatile memory only

  Scripting commands can store configuration changes in RAM only, whereby storage of configuration information to the non-volatile flash memory is prevented. This ensures that the configuration is available only until the next system boot, so that in case of theft, for example, sensitive elements of the configuration cannot fall into the wrong hands.

- Configuration changes in test mode

  The same mechanism allows changes to the configuration in test mode. A script triggers a time-delayed system boot; the intervening time period can be used to change and test the device's configuration without risk. Should the changes lead to a failure, the device automatically reboots after the time delay and is reset to its original configuration.

  Comparable to the FirmSafe function, this variation is a type of "ConfSafe". Changes to the configuration after a firmware update can, on occasion, be impossible to edit in the case of a later downgrade to an older firmware version. If, however, the configuration subsequent to the firmware upgrade is stored in test mode only, then downgrading and subsequently re-booting the system will result in the restoration of the original firmware **and** its configuration.

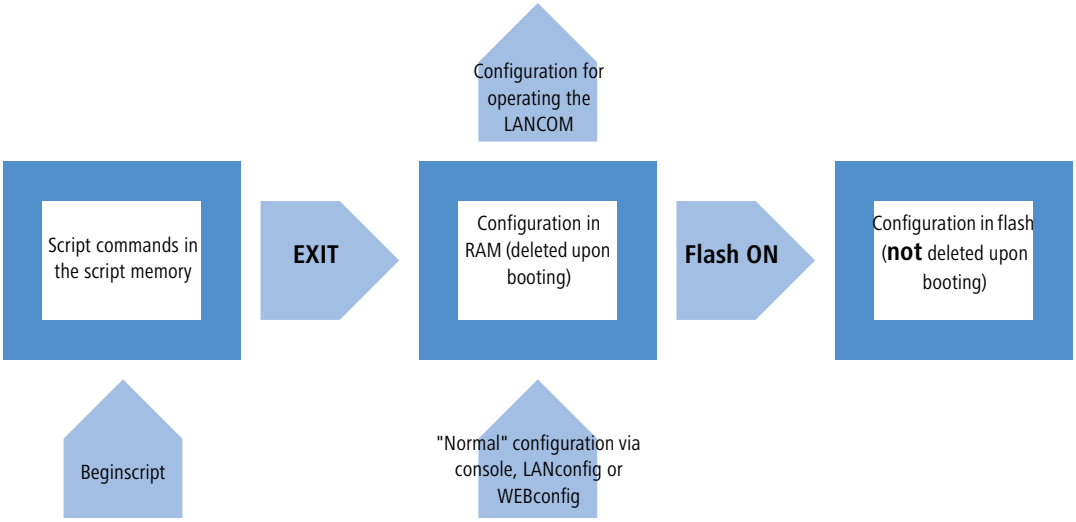
4.2.2 Scripting function

Scripting involves the collective transmission of a series of configuration commands to a LANCOM device just as if they were entered at a Telnet console (or similar). There are two variants of the collective transfer of configuration commands:

- The device is set to script mode by entering the command `beginscript` at the console. In this mode, the commands are not executed individually but are stored in an intermediate memory in the LANCOM. These commands are only executed after the command `exit` has been entered.
- Alternatively, the configuration commands are written offline to a script file (text file) and uploaded to the device as a complete script.

The configuration commands in the script file initially effect the configuration that is stored in the device's RAM only. The flash mode then determines whether or not the changes are to be made to the flash memory as well.

- In Flash Yes mode (standard), the configuration commands are directly written to the device's flash memory and are thus non-volatile (i.e. boot resistant). Since the flash mode is always ON with the other methods of configuration (console without script, LANconfig or WEBconfig), the configuration changes are written first to the RAM memory and then immediately to the flash memory.



- In Flash No mode the data are written to RAM only and are thus available only until the next boot.
  - During the boot process, the device reads the configuration data from the flash memory.
  - The configuration in the RAM can be written to the flash memory at any time with the command "Flash Yes".

While operating, LANCOM devices work with the information stored in the RAM configuration. The script commands stored in the intermediate memory are, just like the configuration in the flash memory, of no relevance to the real-time operations of a LANCOM.

4.2.3 Generating script files

A script for a LANCOM configuration exists in the form of a conventional text file. These include any necessary comments and of the all of the commands as used e.g. with a Telnet console to set the configuration. There are two different ways to generate a script file:

- The script can be generated entirely with a text editor.
- The configuration, or a section of it, is read out of a device, stored as a script file and then altered with a suitable text editor.

Read out the configuration via the console

① Log on to the console with Supervisor rights.

② Switch to the branch of the configuration tree that you wish to read out.

③ At the command prompt, execute the command `readscript`. Observe the optional command extensions ('Scripting commands' → page 63).

④ Using the Clipboard, copy and paste the required text section into a text editor and adapt the script to your requirements.

Via TFTP from the command line interface (DOS box)

The configuration commands can be read out directly from the command-line interface via TFTP.

① To do this, open up a DOS box, for example.

② Enter the following command at the prompt:

```
C:\>tftp IP address get "PASSWORDreadscript path" script.lcs
```

- IP address is the address of the device containing the configuration commands you wish to read out.
- PASSWORD is the appropriate password for the device.
- Path defines the branch of the configuration menu tree that is to be read out. If no path is entered then the entire configuration will be read out.
- script.lcs is the name of the script file in the current directory where the commands will be written to.

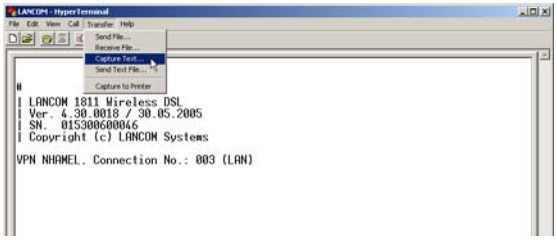
Please be aware that device passwords will be clearly visible as plain text while entering this command!

Via Hyperterminal

Terminal programs such as Hyperterminal provide an option of storing the text displayed by the console directly to a text file. This method is especially advantageous when dealing with larger configuration files as it avoids the potentially confusing method of using the Clipboard.

① Set up a connection to the device with Hyperterminal.

② Select the menu item **Transfer ▶ Capture Text** and select the desired storage location and file name for the script.



③ At the command prompt, execute the command `readscript`. Observe the optional command extensions ('Scripting commands' → page 63).

④ As soon as you have called up all of the required sections of the configuration, stop the recording with the menu item **Transfer ▶ Capture Text ▶ Stop**.

The configuration commands are now available as a script file and can be altered as required.

4.2.4 Uploading configuration commands and script files

There are two basic methods of uploading the script commands to the intermediate memory of the LANCOM:

- The commands can be manually entered at a console in script mode (with the command "beginscript"). In this way the commands are written directly from the console to the intermediate memory. After all of the commands are ready, they are processed by entering the command "exit" and are then transferred to the RAM.
- The required command sequence can be saved to a text file. This text file is then sent to the intermediate memory by using an appropriate tool (LANconfig, terminal program, TFTP). If the necessary commands are included in the file, the transfer of the configuration to the RAM will be started automatically.

There are various ways to upload script files to LANCOM devices, the choice of which depends upon the configuration tool that you prefer to use.

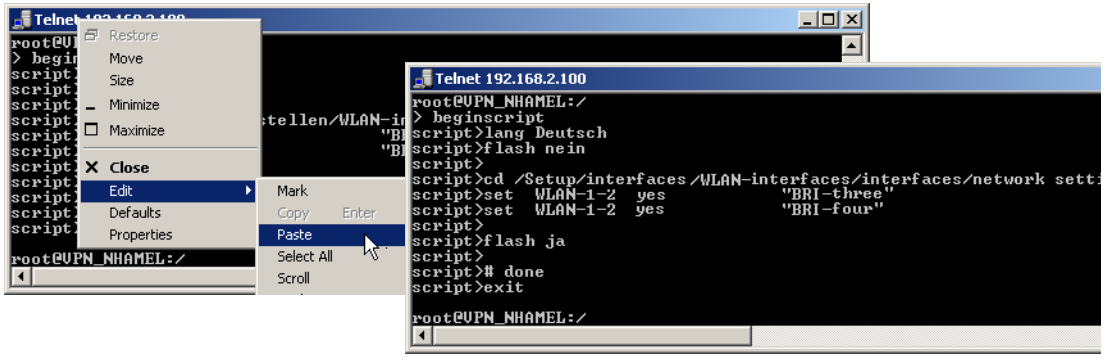
Command input via console session (Telnet, SSH)

In a console session, a script can be uploaded to the device via the Clipboard:

① Open your script with any text editor and transfer the configuration commands to the Clipboard.

② Log on to the console with Supervisor rights.

③ Start the script mode with the command `beginscript`.



④ Paste the commands from the Clipboard following the script prompt (`script>`). In Telnet, for example, with a right mouse-click on the upper frame of the window.

⑤ Entering the command `exit` executes of the configuration commands.

If the command `exit` is already included in the commands after pasting, the execution of the configuration will be carried out automatically immediately after pasting!

Upload script with TFTP client

During a console session (e.g. via Telnet or SSH), TFTP commands can be used to upload script files to the device directly from a TFTP server.

① Log on to the console with Supervisor rights.

② Enter the following command at the prompt:

```
>loadscript -s IP address -f script.lcs
```

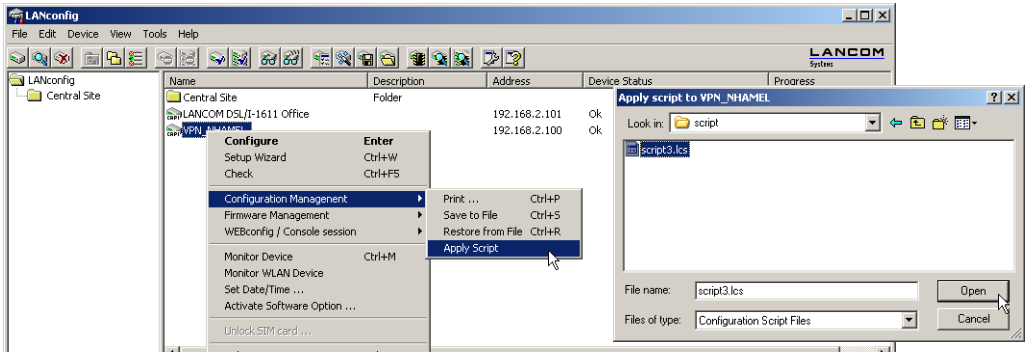
- IP address is the address of the TFCTP server where the script file is stored.
- script.lcs is the name of the script file on the TFTP server

Upload script with LANconfig

LANconfig has the option to upload a script either to a single device or to multiple devices simultaneously.

① Click on a device with the right mouse key and use the context menu to select the entry **Configuration Management** ▶ **Apply Script**. If multiple devices are marked, the entry **Apply Script** appears directly in the context menu.

② In the following dialog, select the required script file (*.lcs) for upload.



The upload of the script starts automatically. Status and error messages are either displayed directly by LANconfig or the can be viewed in a console session with the command `show script`.

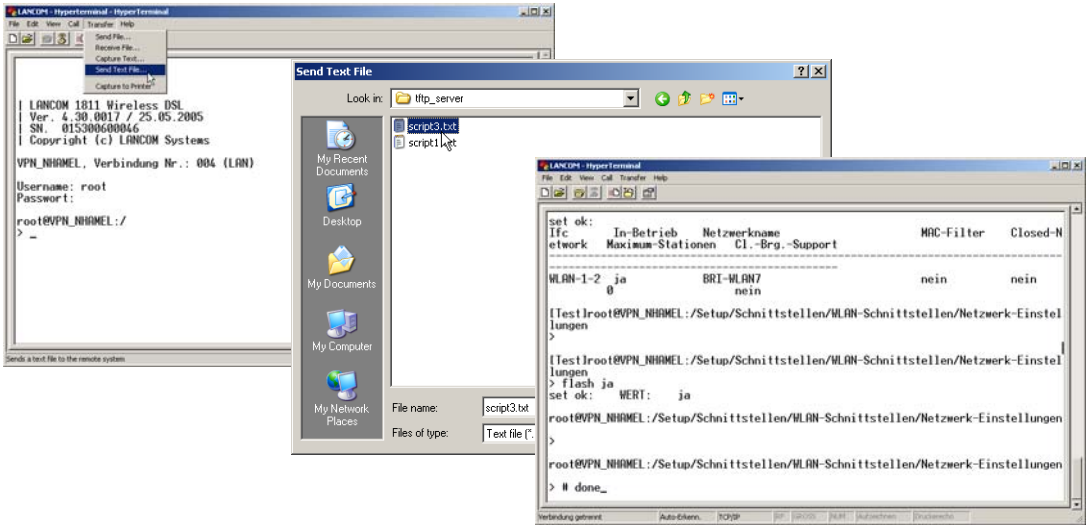
Upload script with Hyperterminal

A further way to upload scripts to a LANCOM is to use a terminal program such as Hyperterminal as supplied with Windows.

① Set up a connection to the device with Hyperterminal.

② Select the menu item **Transfer ▶Capture Text**.

③ Choose the required script file and start the transfer.



Following the successful completion of the transfer, the script is started automatically.

4.2.5 Multiple parallel script sessions

The LANCOM can manage multiple simultaneous script sessions. Just as multiple console sessions can be run simultaneously on a single device, different scripts can also access the LANCOM at the same time. Parallel script sessions are especially useful in the following scenarios:

- Script ① initiates a time-delayed reboot of the device after 30 minutes, for example. A second script ② is active during the device's run time and changes its configuration for test purposes; the flash mode is deactivated for this. If the changes in configuration from script ② make the device unattainable, then the restart prompted by script ① 30 minutes later causes these changes to be rejected.
- When using different scripts for partial configurations, multiple scripts can started simultaneously, for example with cron jobs. The individual configuration tasks do not need to be delayed until the previous script has completed its processing.

4.2.6 Scripting commands

- `readscript`

  In a console session, the command readscript generates a text dump of all commands and parameters that are required for the configuration of the LANCOM in its current state. In the simplest case, the LANCOM lists only commands that are relevant to those parameters that no longer have the factory settings.

Syntax: `readscript [-n][-d][-c] [-m] [PATH]`

Supervisor rights are necessary to execute this command.

Example: For a LANCOM that is set up only for Internet-by-call via ISDN, the command readscript will produce the following console output (assuming that there are no further restrictions):

From this example it is possible to recognize the behavior or the script that was generated with the command `readscript`.

- First of all the parameters with values different from the default settings are displayed.
- The values in the tables are deleted (`del *`) and replaced with the current values in the configuration (`add *`).
- Only those table entries or values which cannot be left empty are directly changed with the `Set` command.

The table lines or strings containing passwords are displayed in plain text as this is the format required by the Telnet user interface.

This script can be used to program other LANCOMs with exactly the same configuration as the original device.

As these scripts can be very long in some cases, it is possible to generate scripts that focus only on parts of the configuration. To do this, you first change to the directory with the configuration that is to be recorded (e.g. `cd set/ip-router/firewall` for the firewall settings) and then execute the `readscript` command. Alternatively, enter the path directly with the `readscript` command as a path parameter (e.g. `readscript set/ip-router/firewall`). In both cases, only the firewall settings that have been changed will be recorded in the script.

The following options can be used with the readscript command:

- `-d (default)`: The commands for modifying parameters that are set to the factory settings will be listed as well. These long scripts are useful for transferring configurations between different types of devices or between devices with different firmware versions as the factory settings can vary.
- `-n (numeric)`: This suffix causes the paths to be output in the numeric form of the SNMP description instead of plain text. This also facilitates the transfer of scripts between devices with different firmware versions as the path names may change but the SNMP tree generally does not.
- `-c (comment)`: In combination with `-d` and `-n`, this parameter generates additional comments which make the script easier to read. For the parameter `-d`, every command combination that sets a default value is marked with `# default value`. With `-n`, each numeric path is supplemented with its plain text equivalent.
- `-m (minimize)`: This parameter removes any gaps in the script, so making it more compact.

■ #

The # character followed by a space at the start of a line are the first characters of a comment. Subsequent characters to the end of the line will be ignored.

The space after the # is obligatory.

■ `del *`

This command deletes the table in the branch of the menu tree defined with `Path`.

Syntax: `del [PATH]*`

■ `default`

This command enables individual parameters, tables or entire menu trees to be reset to their factory settings.

Syntax: `default [-r] [PATH]`

This command returns the parameters addressed by the `PATH` to their factory settings. If `PATH` indicates a branch of the menu tree, then the option `-r` (recursive) must be entered.

Supervisor rights are necessary to execute this command.

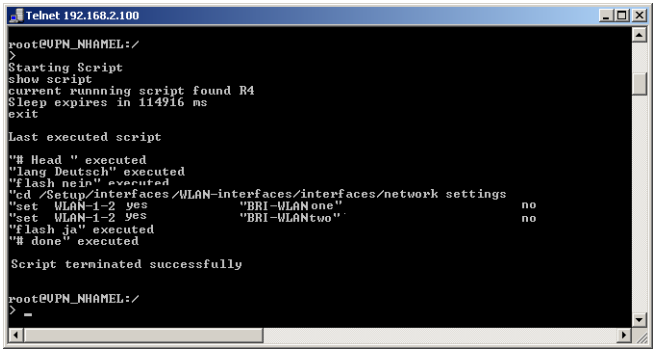
- `beginscript`

  The command `beginscript` switches a console session into script mode. In this state, commands entered are not transferred directly to the LANCOM's configuration RAM but initially to the device's script memory. The commands will only be transferred to and started in the configuration RAM via a script session by executing the command exit.

Supervisor rights are necessary to execute this command.

- `show script`

  The command `show script` displays the content of the most recently executed script and an overview of the currently running scripts. The names displayed in this output can be used to interruption scripts early ('killscript' → page 66).



Supervisor rights are necessary to execute this command.

- `killscript`

  The command killscript deletes the content of a script session that has not yet been executed. The script session is selected by its name ('show script' → page 66).

Supervisor rights are necessary to execute this command.

- `flash Yes/No`

  When configuring a device with scripts, any add-, set- or del- command can lead to an (unintentional) update of the configuration in flash; to prevent this, the update to flash function can be deactivated. After concluding

the configuration, this function can be activated again with `flash Yes`. Changes in the RAM configuration are then written to flash. The status `flash Yes/No` is stored globally.

Supervisor rights are necessary to execute this command.

- `sleep`

  The sleep command allows the processing of configuration commands to be delayed for a certain time period or to be scheduled for a certain time.

  Syntax: `sleep [-u] value[suffix]`

  Permissible suffixes are `s`, `m`, or `h` for seconds, minutes, or hours; if no suffix is defined, the units are milliseconds.

  With the option switch `-u`, the sleep command accepts times in the format `MM/DD/YYYY hh:mm:ss` (English) or in the format `TT.MM.JJJJ hh:mm:ss` (German).

Times will only be accepted if the system time has been set.

The sleep function is useful for a time-delayed reboot when testing an altered configuration or for a scheduled firmware update for large-scale roll-outs with multiple devices.

4.3 Group configuration with LANconfig

When managing multiple devices it can be very helpful to upload a selection of configuration parameters into a group of devices at once, as opposed to setting each and every parameter manually in the individual devices, e.g. with identical client rights in WLAN access points. Importing complete configuration files is not a viable alternative since device-specific parameters such as the IP address are uploaded as well. Group configuration with LANconfig enables the easy import of partial configuration files and thus makes the simultaneous administration of multiple devices a reality.

The partial configuration files with the common parameters for a group of LANCOM devices are, just like the full configuration files, stored on hard disk or on a server. To aid the configuration of entire groups of devices, links to the partial configuration files are created under LANconfig to provide a convenient connection between the device entries in LANconfig and these partial configuration files.

Group configuration is supported only by LANCOM devices with a firmware version LCOS 5.00 or higher.

LCOS version 5.00 initially support the group configuration of WLAN devices. Later firmware versions will also support further types of group configuration, such as the VPN parameters. Refer to the LANCOM web site www.lancom.de for more information about the latest firmware versions and the additional possibilities of group configuration.

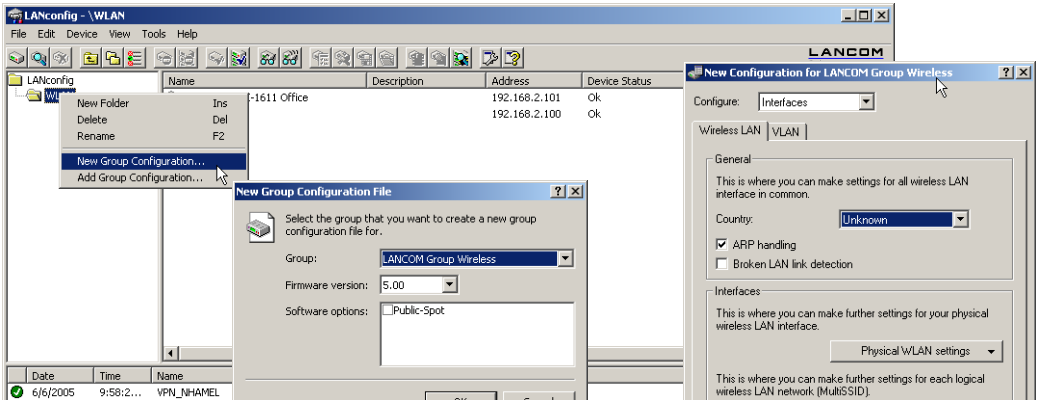
4.3.1 Create a group configuration

A requirement for working with group configuration to the grouping of devices within folders. These LANconfig folders contain those device entries which are effectively managed by common partial configurations, and the group configurations as links to the partial configuration files.

Group configuration with a new partial configuration file

① Create a new folder and move the devices that are to be grouped into it with the mouse.

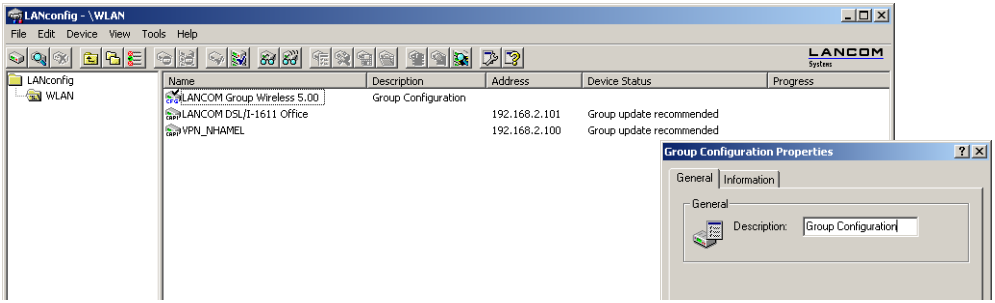
② Then click on the folder with the right-hand mouse key and select the entry **New group configuration...** from the context menu. After selecting the group type and the firmware version, the LANconfig configuration dialogue opens up with a reduced selection of configuration options.



③ The parameters here should be set as required for the entire group. When the configuration dialogue is closed, LANconfig will request that you save the partial configuration file to a location of your choice.

The group configuration then saves all parameters to a partial configuration file. Those parameters which were not changed are also set to the standard values. Use the scripting function ('Scripting' → page 57) to read out non-standard settings from a device and transfer them to other devices, if required.

④ The link to the partial configuration file appears in the list of entries and has the description 'Group Configuration'. The name of the group configuration can be changed via the Properties. To do this, click on the entry with the right-hand mouse key and select **Properties** from the context menu.



The group configuration is a link to the partial configuration file. Please note that changes to the partial configuration file will lead to changes in that group configuration.

Use an existing partial configuration file

There are cases where it is more effective to use a different folder structure in LANconfig than that required for group configuration. Devices in location-specific folders can indeed be set up with the same group configurations. To avoid having to create the same partial configuration for every folder, links to a common partial configuration file can be created in multiple folders.

① To use an existing partial configuration file for a group configuration, click on the appropriate folder with the right-hand mouse key and select **Add group configuration...** from the context menu.

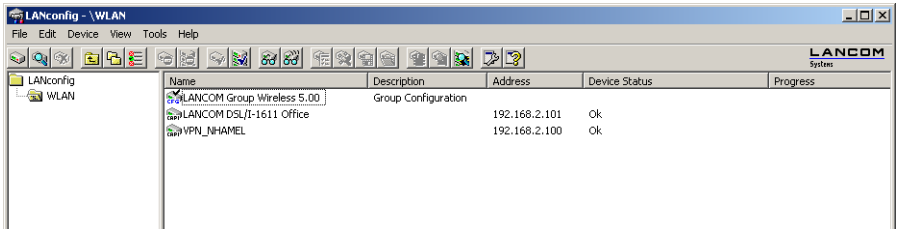
② In the subsequent dialog, select the existing partial configuration file to create a link to this file in the folder.

Please note that changes to the partial configuration file will lead to changes in that group configuration in various folders.

4.3.2 Update device configurations

By selecting or updating a folder, LANconfig checks the configuration of the devices in this folder for agreement with the settings in the active group configuration. In case of discrepancy from the group configuration, the device status informs that 'Group update recommended'.

To load the group configuration into the WLAN device, drag the group configuration entry onto the appropriate device entry. After successfully transferring the parameters, the device status will change to 'OK'.



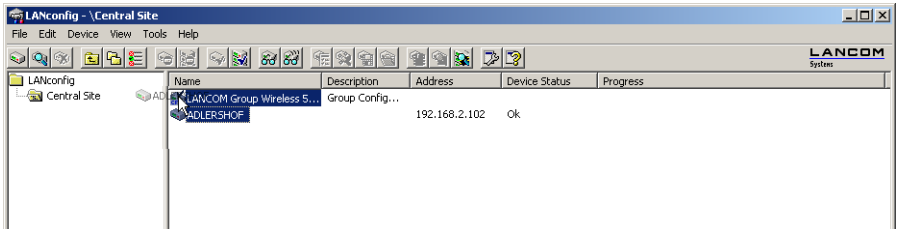
It is also possible to use the partial configuration for a device as a group configuration. Simply drag the device entry onto the group configuration entry.

4.3.3 Update group configurations

Apart from manually changing the parameters in a group configuration, the current configuration of a device can be used as the basis for a group configuration. One device is thus declared as "Master" for all other devices in the same file.

To take over the values from a current device configuration for a group configuration, simply drag the entry for this device onto the desired group configuration. All of the parameters defined in the group configuration are then overwritten by the values in the device configuration.

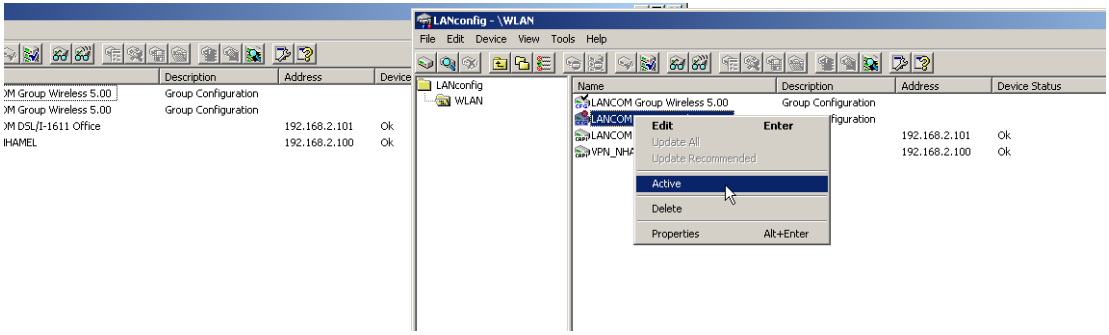
The next time that LANconfig checks the devices, it will find that the configurations in the other devices no longer agrees with the new group configuration; this will be displayed by the device status.



4.3.4 Using multiple group configurations

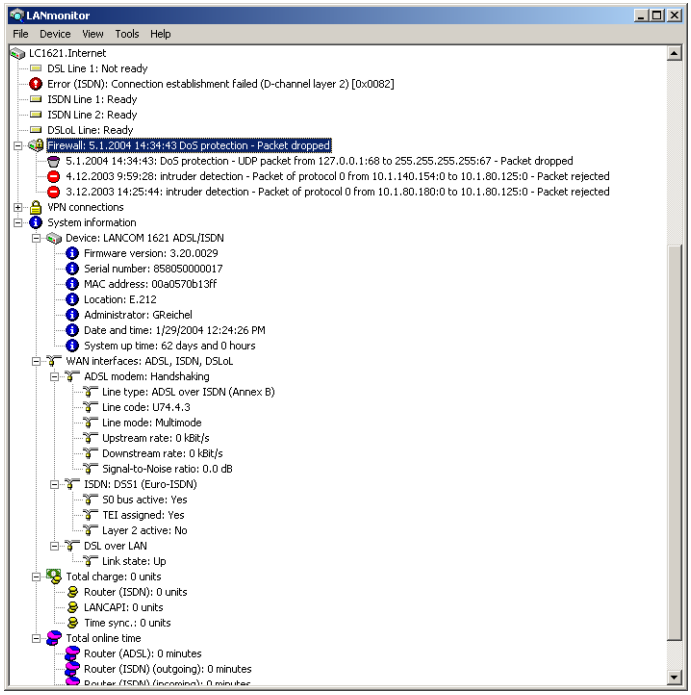
Multiple group configurations can be created within a single folder. Only one of these group configurations may be active at a time since the device status only relates to **one** group configuration. Active group configurations are indicated by a blue tick, inactive group configurations are indicated by a red cross. To activate a group configuration, click on the entry with the right-hand mouse key and select **Active** from the context menu. All other group configurations are then deactivated automatically.

Different group configurations in one folder may not be linked to the same partial configuration file.



4.4 Display functions in LANmonitor

LANmonitor supports the administration of the LANCOM applications by offering a range of functions that simplify the surveillance of devices at widely dispersed locations. The overview of devices monitored by LANmonitor already shows the most important information about the status of the devices:

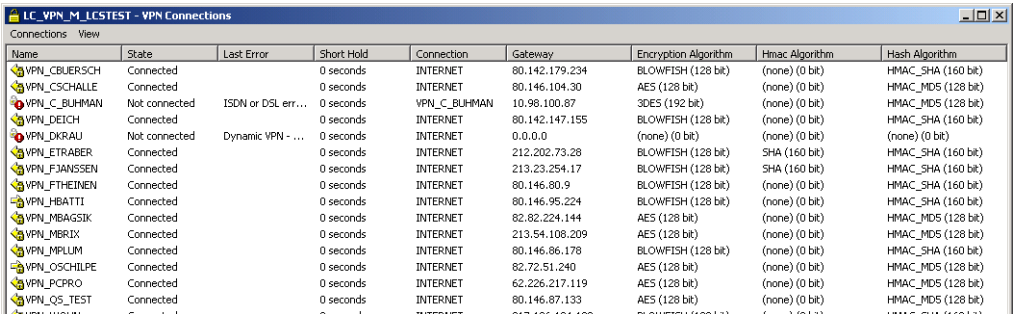


The information that can be taken from the overview includes, among others, details about active WAN connections, the five most recent firewall messages, the current VPN connections and system information about charges and online times.

Right-clicking with the mouse on a device in LANmonitor opens up a context menu with further information:

- VPN connections

  The list of VPN connections is a log of the 100 most recent VPN connections. The detailed recorded information includes

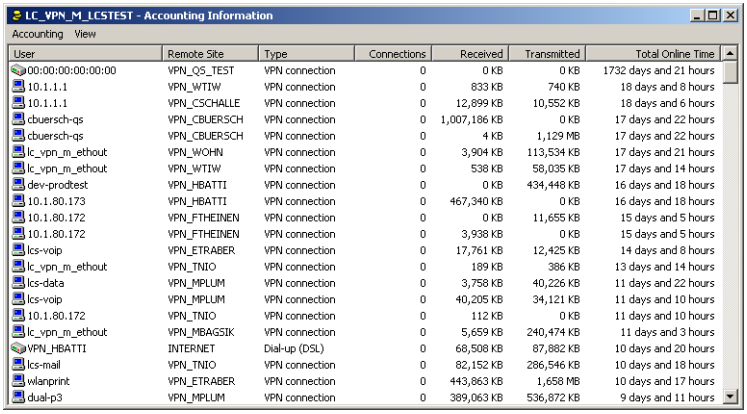


Name	State	Last Error	Short Hold	Connection	Gateway	Encryption Algorithm	Hmac Algorithm	Hash Algorithm
VPN_CBUERSCH	Connected		0 seconds	INTERNET	80.142.179.234	BLOWFISH (128 bit)	(none) (0 bit)	HMAC_SHA (160 bit)
VPN_CSCHALLE	Connected		0 seconds	INTERNET	80.146.104.30	AES (128 bit)	(none) (0 bit)	HMAC_MD5 (128 bit)
VPN_C_BUHMAN	Not connected	ISDN or DSL err...	0 seconds	VPN_C_BUHMAN	10.98.100.87	3DES (192 bit)	(none) (0 bit)	HMAC_MD5 (128 bit)
VPN_DEICH	Connected		0 seconds	INTERNET	80.142.147.155	BLOWFISH (128 bit)	(none) (0 bit)	HMAC_SHA (160 bit)
VPN_DKRAU	Not connected	Dynamic VPN - ...	0 seconds	INTERNET	0.0.0.0	(none) (0 bit)	(none) (0 bit)	(none) (0 bit)
VPN_ETRABER	Connected		0 seconds	INTERNET	212.202.73.28	BLOWFISH (128 bit)	SHA (160 bit)	HMAC_SHA (160 bit)
VPN_FJANSSEN	Connected		0 seconds	INTERNET	213.23.254.17	BLOWFISH (128 bit)	SHA (160 bit)	HMAC_SHA (160 bit)
VPN_FTHEINEN	Connected		0 seconds	INTERNET	80.146.80.9	BLOWFISH (128 bit)	(none) (0 bit)	HMAC_SHA (160 bit)
VPN_HBATTI	Connected		0 seconds	INTERNET	80.146.95.224	BLOWFISH (128 bit)	(none) (0 bit)	HMAC_SHA (160 bit)
VPN_MBAGSIK	Connected		0 seconds	INTERNET	82.82.224.144	AES (128 bit)	(none) (0 bit)	HMAC_MD5 (128 bit)
VPN_MBRIX	Connected		0 seconds	INTERNET	213.54.108.209	AES (128 bit)	(none) (0 bit)	HMAC_MD5 (128 bit)
VPN_MPLUM	Connected		0 seconds	INTERNET	80.146.86.178	BLOWFISH (128 bit)	(none) (0 bit)	HMAC_SHA (160 bit)
VPN_OSCHILPE	Connected		0 seconds	INTERNET	82.72.51.240	AES (128 bit)	(none) (0 bit)	HMAC_MD5 (128 bit)
VPN_PCPRO	Connected		0 seconds	INTERNET	62.226.217.119	AES (128 bit)	(none) (0 bit)	HMAC_MD5 (128 bit)
VPN_QS_TEST	Connected		0 seconds	INTERNET	80.146.87.133	AES (128 bit)	(none) (0 bit)	HMAC_MD5 (128 bit)

  - Name of the remote device
  - Current status
  - Last error message
  - IP address of the gateway
  - Encryption information

- Accounting information

  The accounting information is a protocol of the connections from each station in the LAN to remote sites in the WAN. The detailed information recorded includes

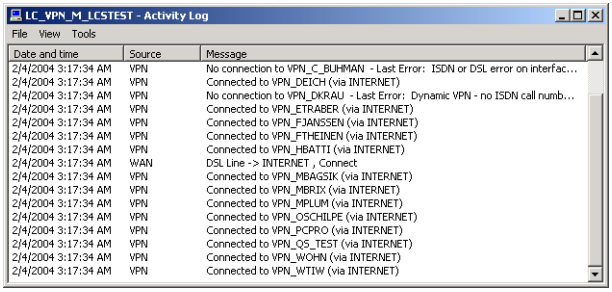


User	Remote Site	Type	Connections	Received	Transmitted	Total Online Time
00:00:00:00:00:00	VPN_QS_TEST	VPN connection	0	0 KB	0 KB	1732 days and 21 hours
10.1.1.1	VPN_WTIW	VPN connection	0	833 KB	740 KB	18 days and 8 hours
10.1.1.1	VPN_CSCHALLE	VPN connection	0	12,899 KB	10,552 KB	18 days and 6 hours
cbuersch-qs	VPN_CBUERSCH	VPN connection	0	1,007,186 KB	0 KB	17 days and 22 hours
cbuersch-qs	VPN_CBUERSCH	VPN connection	0	4 KB	1,129 MB	17 days and 22 hours
lc_vpn_m_ethout	VPN_WOHN	VPN connection	0	3,904 KB	113,534 KB	17 days and 21 hours
lc_vpn_m_ethout	VPN_WTIW	VPN connection	0	538 KB	58,035 KB	17 days and 14 hours
dev-prodtest	VPN_HBATTI	VPN connection	0	0 KB	434,448 KB	16 days and 18 hours
10.1.80.173	VPN_HBATTI	VPN connection	0	467,340 KB	0 KB	16 days and 18 hours
10.1.80.172	VPN_FTHEINEN	VPN connection	0	0 KB	11,655 KB	15 days and 5 hours
10.1.80.172	VPN_FTHEINEN	VPN connection	0	3,938 KB	0 KB	15 days and 5 hours
lcs-voip	VPN_ETRABER	VPN connection	0	17,761 KB	12,425 KB	14 days and 8 hours
lc_vpn_m_ethout	VPN_TNIO	VPN connection	0	189 KB	386 KB	13 days and 14 hours
lcs-data	VPN_MPLUM	VPN connection	0	3,758 KB	40,226 KB	11 days and 22 hours
lcs-voip	VPN_MPLUM	VPN connection	0	40,205 KB	34,121 KB	11 days and 10 hours
10.1.80.172	VPN_TNIO	VPN connection	0	112 KB	0 KB	11 days and 10 hours
lc_vpn_m_ethout	VPN_MBAGSIK	VPN connection	0	5,659 KB	240,474 KB	11 days and 3 hours
VPN_HBATTI	INTERNET	Dial-up (DSL)	0	68,508 KB	87,882 KB	10 days and 20 hours
lcs-mail	VPN_TNIO	VPN connection	0	82,152 KB	286,546 KB	10 days and 18 hours
wlanprint	VPN_ETRABER	VPN connection	0	443,863 KB	1,658 MB	10 days and 17 hours
dual-p3	VPN_MPLUM	VPN connection	0	389,063 KB	536,872 KB	9 days and 11 hours

- □ Name or IP address of the station
- □ Remote station used to establish the connection
- □ Type of connection, e.g. DSL or VPN
- □ Number of connections
- □ Data volume sent and received
- □ Online time

■ Activity log

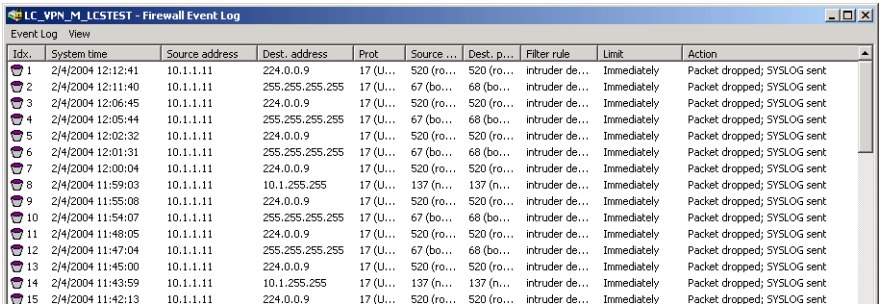
The activity log is a detailed list of the connections via WAN, WLAN, VPN, LANCAPI and a/b port, and a list of firewall activities. The detailed information recorded includes



- □ Date and time
- □ Source
- □ Message

■ Firewall actions log

The firewall actions log lists the last 100 actions taken by the firewall. The detailed information recorded includes



- □ Time
- □ Source and destination address
- □ Protocol with source and destination port

- □ Activated filter rule and exceeded limit
- □ Action carried out

4.5 LANmonitor—know what's going on

The LANmonitor includes a monitoring tool with which you can view the most important information on the status of your routers on your monitor at any time under Windows operating systems—of all of the LANCOM routers in the network.

Many of the internal messages generated by the devices are converted to plain text, thereby helping you to troubleshoot.

Explanations about the LANmonitor messages and helpful tips can be found in the appendix under 'Error messages in LANmonitor' → page 577.

You can also use LANmonitor to monitor the traffic on the router's various interfaces to collect important information on the settings you can use to optimize data traffic.

In addition to the device statistics that can also be read out during a Telnet or terminal session or using WEBconfig, a variety of other useful functions are also available in LANmonitor, such as the enabling of an additional charge limit.

With LANmonitor you can only monitor those devices that you can access via IP (local or remote). With this program you cannot access a router via the serial interface.

4.5.1 Extended display options

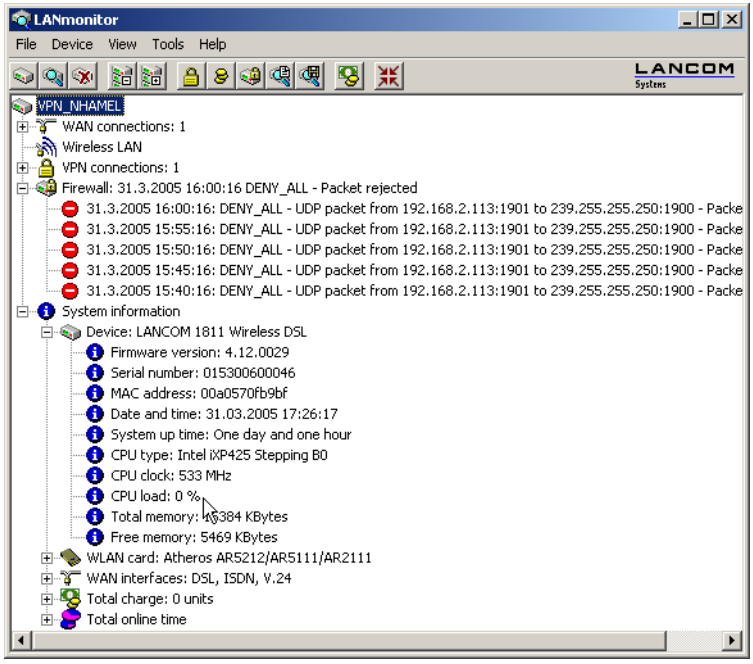
Under **View** ▶ **Show Details** you can activate and deactivate the following display options:

- ■ Error messages
- ■ Diagnostic messages
- ■ System information

Many important details on the status of the LANCOM are not displayed until the display of the system information is activated. These include, for example, the ports and the charge management. Therefore, we recommend that interested users activate the display of the system information.

4.5.2 Enquiry of the CPU and Memory utilization over SNMP

The load on CPU and memory in the LANCOM can be queried with SNMP or displayed in LANmonitor.



4.5.3 Monitor Internet connection

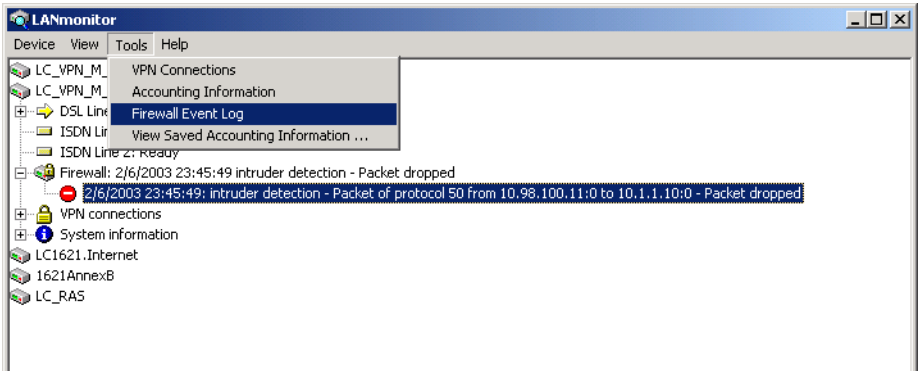
To demonstrate the functions of LANmonitor we will first show you the types of information LANmonitor provides about connections being established to your Internet provider.

① To start LANmonitor, go to **Start** ▶ **Programs** ▶ **LANCOM** ▶ **LANmonitor**. Use **File** ▶ **Add Device** to set up a new device and in the following window, enter the IP address of the router that you would like to monitor. If the configuration of the device is protected by password, enter the password too.

Alternatively, you can select the device via the LANconfig and monitor it using **Device** ▶ **Monitor Device**.

② LANmonitor automatically creates a new entry in the device list and initially displays the status of the transfer channels. Start your Web browser and enter any web page you like. LANmonitor now shows a connection being established on one channel and the name of the remote site being called. As soon as the connection is established, a plus sign against the communication channel entry indicates that further information on this channel is available. Click on the plus sign or double-click the appropriate entry to open a tree structure in which you can view various information

.

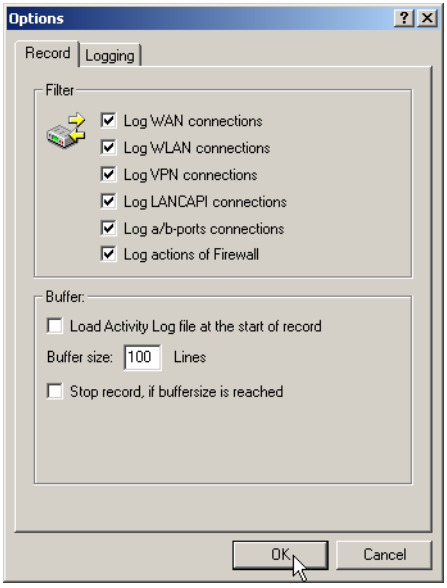


In this example, you can determine from the PPP protocol information the IP address assigned to your router by the provider for the duration of the connection and the addresses transmitted for the DNS and NBNS server.

Under the general information you can watch the transmission rates at which data is currently being exchanged with the Internet.

③ To break the connection manually, click on the active channel with the right mouse button. You may be required to enter a configuration password.

④ If you would like a log of the LANmonitor output in file form, select **Device** ▶ **Device Activities Logging** and go to the 'Logging' tab. Open the dialog for the settings for the activity protocol, click on Tools ▶ Options.



On the 'Protocol' tab you can define whether the following activities should be protocolled:

- WAN connections
- WLAN connections
- VPN connections
- LANCAPI connections
- a/b port connections
- Firewall actions

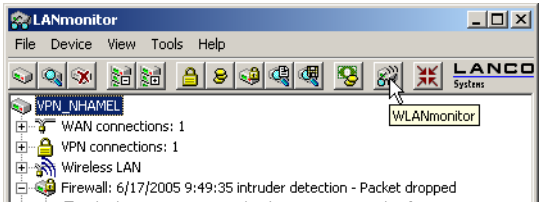
You can also specify whether LANmonitor should create a log file daily, monthly, or on an ongoing basis.

4.6 Visualization of larger WLANs with WLANmonitor

With LANCOM WLANmonitor you can centrally monitor the status of a wireless network(WLAN). It presents information about the entire network in general and detailed information about individual access points and logged-in clients. LANCOM WLANmonitor can also collect access points into groups. These groups may consist of access points gathered in buildings, departments, or at particular locations. In particular with large WLAN infrastructures, this helps to keep an overview of the entire network.

4.6.1 Start the LANCOM WLANmonitor

WLANmonitor is a component of LANmonitor. Start WLANmonitor from LANmonitor using the menu item **Tools ▶WLANmonitor**, by using the corresponding button in the LANmonitor button bar or directly with **Start ▶ Programs ▶ LANCOM ▶ WLANmonitor**.



Alternatively, WLANmonitor can be started from the console with the command

```
[installation path]lanmon -wlan
```

4.6.2 Search for access points

After starting WLANmonitor, commence a search for available access points via the menu item **File ▶ Find access points**. The access points found are listed in the middle column. Also shown here is the main information for each access point such as the name, number of registered clients, the frequency band and channels being used.

- Name of the access point
- Number of the connected clients
- Used frequency band
- Used channel
- IP address of the access point

The right-hand column (client list) lists the clients that are logged in to the selected access point. The following information is shown for each client:

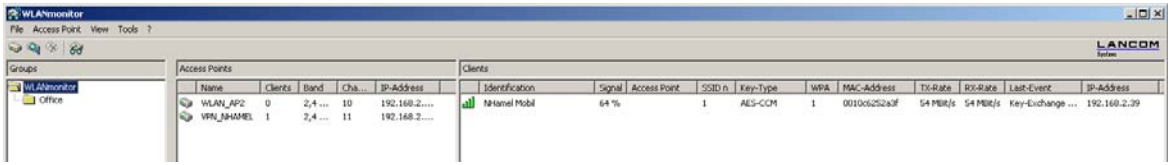
- Connection quality as a bar chart
- Identification: The name of the logged-in client in as far as this is entered into the access list or a RADIUS server.

  LANconfig: WLAN Security ▶ Stations ▶ Stations

  Telnet: Setup/WLAN/Access-List

  WEBconfig: Expert Configuration ▶ Setup ▶ WLAN ▶ Access-List
- Signal: Connection signal strength
- Access point: Name of the access point that the client is logged on to
- SSID: Identifier for the WLAN network
- Encryption: Type of encryption used for the wireless connection
- WPA version (WPA-1 or WPA-2)
- MAC address: Hardware address of the WLAN client

- TX rate: Transmission data rate
- RX rate: Reception data rate
- Last event, e.g. 'Authentification successful', 'RADIUS successful'
- IP addresss of the WLAN clients



4.6.3 Add access points

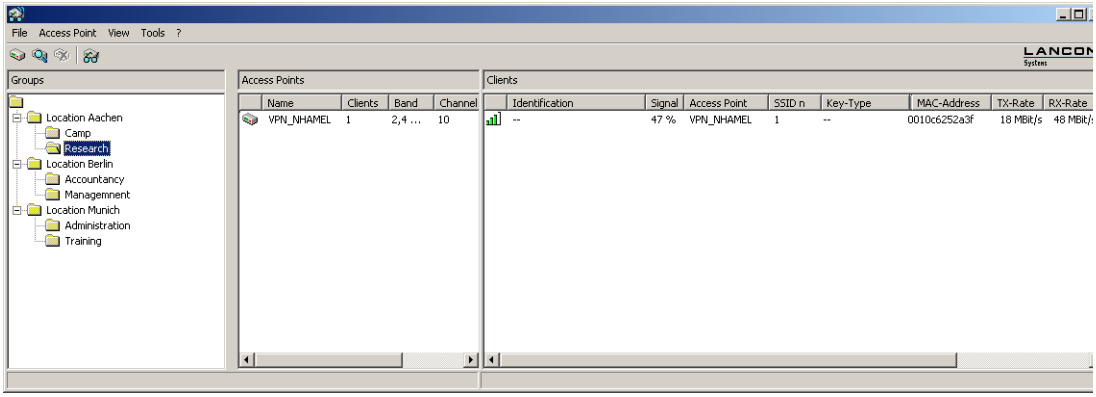
If an access point was not recognized automatically, it can be added to the list manually with the menu item **File ▶ Add access point**. In the following window, enter the IP address or the name of the access point, the administrator name, and the corresponding password.

4.6.4 Organize access points

The LANCOM WLANmonitor lets you organize all of the available access points in a manner that is independent of their physical location. This helps to maintain an overview of the network and is particularly useful when localizing problems. Further, WLAN information can be called up according to the groups. You can group your access points according to their departments, locations or applications (e.g. public hotspot), for example.

The groups are shown in the left column in WLANmonitor. Starting from the top group 'WLANmonitor', you can use the menu item **File ▶ Add group** to create new sub-groups and so build up a structure. Access points found during

a search are assigned to the currently selected group in the group tree. Access points that have been recognized already can be moved to the another group with drag and drop.



To aid the allocation of access points and clients, you can mark a device with the mouse. The counterpart(s) will then be marked in the list as well:

- If an access point is marked in the access point list, all of the clients logged in to this device will also be marked in the client list.
- If a client is marked in the client list, the access point that it is registered with will be marked in the access point list.

5 Diagnosis

5.1 Trace information—for advanced users

Trace outputs may be used to monitor the internal processes in the router during or after configuration. One such trace can be used to display the individual steps involved in negotiating the PPP. Experienced users may interpret these outputs to trace any errors occurring in the establishment of a connection. A particular advantage of this is: The errors being tracked may stem from the configuration of your own router or that of the remote site.

The trace outputs are slightly delayed after the actual event, but are always in the correct sequence. This will not usually hamper interpretation of the displays but should be taken into consideration if making precise analyses.

5.1.1 How to start a trace

Trace output can be started in a Telnet session. Set up a Telnet connection to your device. The command to call up a trace follows this syntax:

```
trace [code] [parameters]
```

The trace command, the code, the parameters and the combination commands are all separated from each other by spaces.

5.1.2 Overview of the keys

This code...	... in combination with the trace causes the following:
?	displays a help text
+	switches on a trace output
-	switches off a trace output
#	switches between different trace outputs (toggle)
no code	displays the current status of the trace

5.1.3 Overview of the parameters

The available traces depend individually on the particular model and can be listed by entering `trace` with no arguments on the command line.

This parameter...	... brings up the following display for the trace:
Status	status messages for the connection
Error	error messages for the connection
LANCOM	LANCOM protocol negotiation
IPX-router	IPX routing
PPP	PPP protocol negotiation
SAP	IPX Service Advertising Protocol
IPX-watchdog	IPX watchdog spoofing
SPX-watchdog	SPX watchdog spoofing
LCR	Least-Cost Router
Script	script processing
RIP	IPX Routing Information Protocol
IP-router	IP routing
IP-RIP	IP Routing Information Protocol
ARP	Address Resolution Protocol
ICMP	Internet Control Message Protocol
IP masquerading	processes in the masquerading module
DHCP	Dynamic Host Configuration Protocol
NetBIOS	NetBIOS management
DNS	Domain Name Service Protocol

This parameter...	... brings up the following display for the trace:
Packet dump	display of the first 64 bytes of a package in hexadecimal form
D-channel-dump	trace on the D channel of the connected ISDN bus
ATM	spoofing at the ATM packet level
ADSL	ADSL connections status
VPN-Status	IPSec and IKE negotiation
VPN-Packet	IPSec and IKE packets
SMTP-Client	E-mail processing of the integrated mail client
SNTP	Simple Network Time Protocol information

5.1.4 Combination commands

This combination command...	... brings up the following display for the trace:
All	all trace outputs
Display	status and error outputs
Protocol	LANCOM and PPP outputs
TCP-IP	IP-Rt., IP-RIP, ICMP and ARP outputs
IPX-SPX	IPX-Rt., RIP, SAP, IPX-Wd., SPX-Wd., and NetBIOS outputs
Time	displays the system time in front of the actual trace output
Source	includes a display of the protocol that has initiated the output in front of the trace

Any appended parameters are processed from left to right. This means that it is possible to call a parameter and then restrict it.

5.1.5 Trace filters

Some traces, such as the IP router trace or the VPN trace, produce a large number of outputs. The amount of output can become unmanageable. The trace filters allow you to sift out the information that is important to you.

A trace filter is activated by adding the parameter "@" that induces the following filter description. In filter description uses of the following perators:

Operator	Beschreibung
(space)	OR: The filter applies if one of the operator occurs in the trace output
+	AND: The filter applies if the operator occurs in the trace output
-	Not: The filter applies if the operator does not occur in the trace output
"	the output must match the search string exactly

An operator can be entered as any string of characters, such as the name of a remote station, protocols or ports. The trace filter then processes the output according to the operator rules, much like an Internet search engine. Examples of the application of filters can be seen under 'Examples of traces' → page 85.

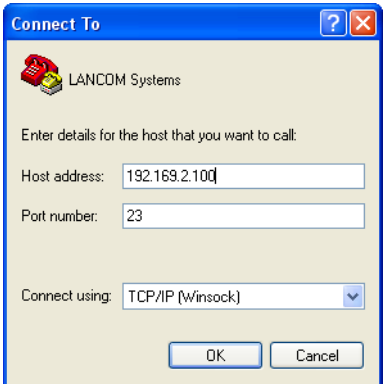
5.1.6 Examples of traces

This code...	... in combination with the trace causes the following:
trace	displays all protocols that can generate outputs during the configuration, and the status of each output (ON or OFF)
trace + all	switches on all trace outputs
trace - all	switches off all trace outputs
trace + protocol display	switches on the output for all connection protocols together with the status and error messages
trace + all - icmp	switches on all trace outputs with the exception of the ICMP protocol
trace ppp	displays the status of the PPP
trace # ipx-rt display	toggles between the trace outputs for the IPX router and the display outputs
trace + ip-router @ GEGENSTELLE-A GEGENSTELLE-B	switches on all trace outputs for IP routers related to remote site A or B
trace + ip-router @+GEGENSTELLE-A -ICMP	switches on all trace outputs for IP routers related to remote site A or B that do not use ICMP
trace + ip-router @ GEGENSTELLE-A GEGENSTELLE-B +ICMP	switches on all trace outputs for IP routers related to remote site A or B that use ICMP
trace + ip-router @+TCP +"port: 80"	switches on all trace outputs from the IP router wiht TCP/IP and port 80. “port: 80” is in quotes so that the space is recognised as a part of the string.

5.1.7 Recording traces

Traces can be conveniently recorded under Windows (e.g. as an aid to Support), and we recommend you do this as follows:

Start the program HyperTerminal under **Start ▶ Programs ▶ Accessories ▶ Communications ▶ Hyper Terminal**. Enter a name of your choice when prompted to do so.



In the window 'Connect to' use the pulldown menu 'Connect using' and select the entry 'TCP/IP'. As 'Host address' enter the local/official IPaddress or the FQDN of the device. After confirmation, HyperTerminal dipslays a request to log in. Enter the configuration password .

You record the traces by clicking on **Transmit ▶ Capture text**. Enter the path of the directory where the text file is to be saved. Now change back to the dialog window and enter the required trace command.

To stop the trace, click on the HyperTerminal menus **Transmit ▶ Stop text capture**.

5.2 SYSLOG storage in the device

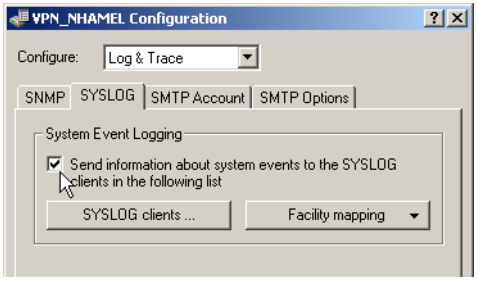
SYSLOG protocols the activities of a LANCOM device. To extend the output of the SYSLOG information over an appropriate SYSLOG client, the 100 most recent SYSLOG messages are stored in the device's RAM. This means that the SYSLOG messages can be viewed directly on the device to help with diagnosis.

5.2.1 Activate SYSLOG module

The SYSLOG module must first be activated for the protocol to be recorded. Additionally an appropriate SYSLOG client must be configured ('Configuring the SYSLOG client' → page 86).

LANconfig

For configuration with LANconfig you will find the SYSLOG module under the configuration area 'Log & Trace' on the 'SYSLOG' tab.



WEBconfig, Telnet or terminal program

Under WEBconfig, Telnet or a terminal program, you will find the SYSLOG module under the following paths:

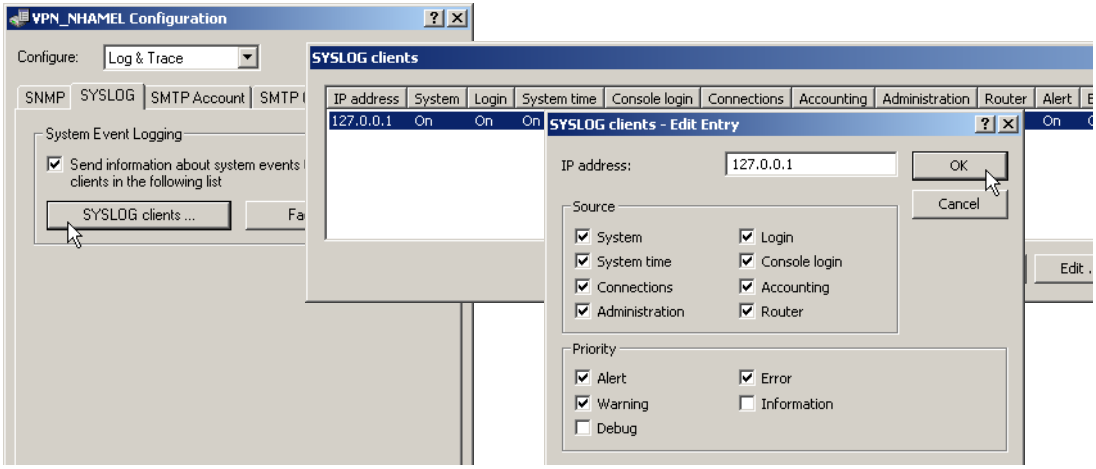
Configuration tool	Call/Table
WEBconfig	Expert-Configuration ▶ Setup ▶ SYSLOG
Terminal/Telnet	`/Setup/SYSLOG`

5.2.2 Configuring the SYSLOG client

The SYSLOG module can write different messages to the memory in the device. If there are messages that you do not require (e.g. debug and information messages), you can reduce the scope of the messages by entering a local loopback address of you LANCOM device in the IP area 127.x.x.x (e.g. 127.0.0.1) as the SYSLOG client; for this client, you then activate only certain sources and/ or priorities.

LANconfig

For configuration with LANconfig you can open the list of SYSLOG clients under the configuration area 'Log & Trace' on the 'SYSLOG' tab using the **SYSLOG clients** button.



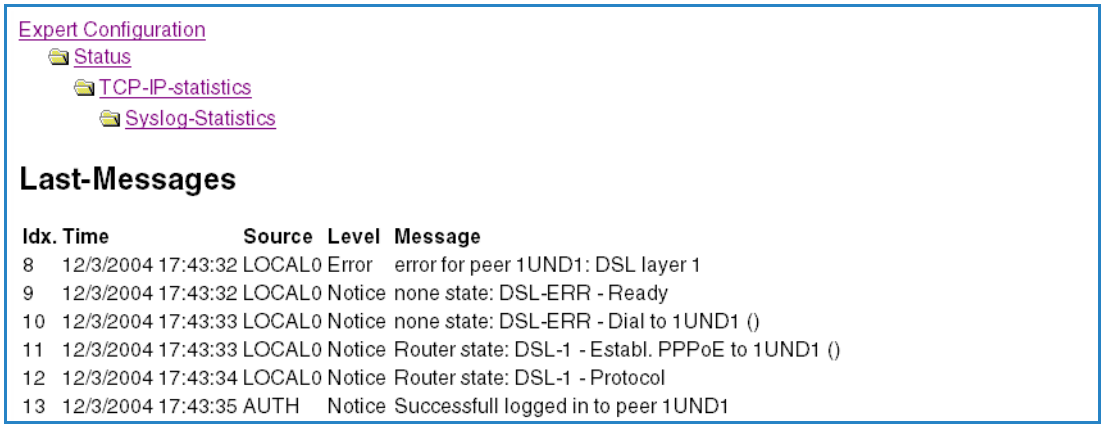
WEBconfig, Telnet or terminal program

Under WEBconfig, Telnet or a terminal program, you will find the list of SYSLOG clients under the following paths:

Configuration tool	Call/Table
WEBconfig	Expert-Configuration ▶ Setup ▶ SYSLOG ▶ Table-SYSLOG
Terminal/Telnet	`/Setup/SYSLOG/Table-SYSLOG`

5.2.3 Read-out SYSLOG messages

To read the SYSLOG messages, access the statistics under WEBconfig or Telnet. The SYSLOG output can be accessed under **Status ▶ TCP-IP-statistics ▶ Syslog-statistics**:



5.3 The ping command

With the ping command in Telnet or in a terminal connection an „ICMP Echo Request" is sent to the addressed host. As long as the recipient provides the protocol and the request is not filtered by the firewall, the addressed host answers with an „ICMP Echo Reply". In case the host is not available, the last router before the host answers with „Network unreachable" or „Host unreachable".

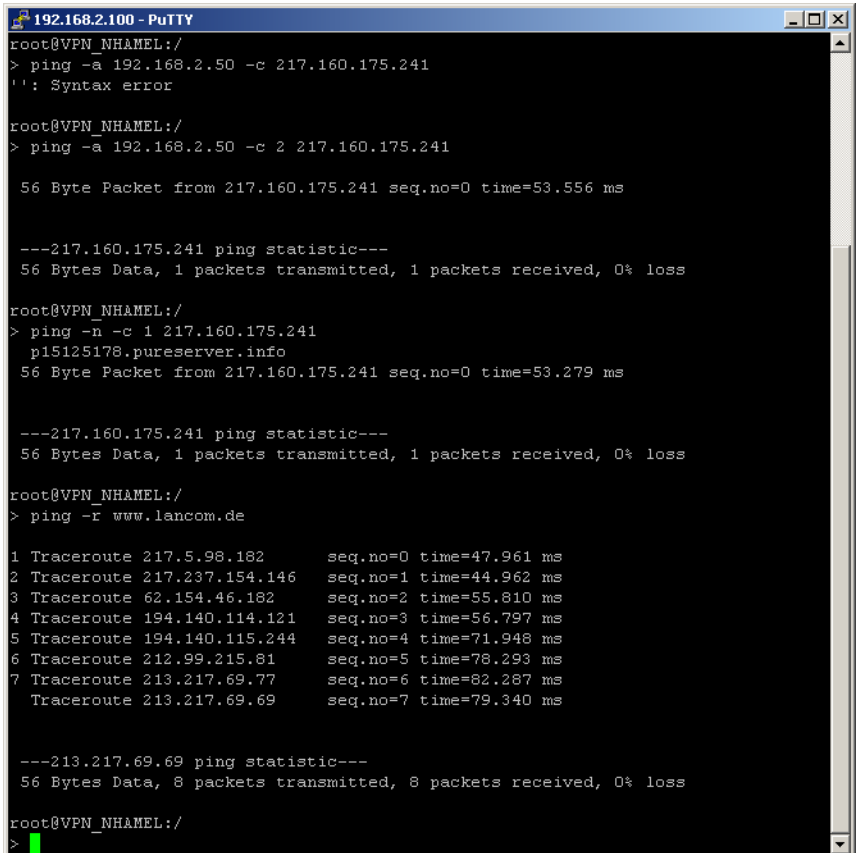
The syntax of the ping commando is:

- `ping [-fnqr] [-s n] [-i n] [-c n] [-a a.b.c.d] hostaddress`

The meaning of the optional parameters are listed in the following table:

Parameter	Meaning
-a a.b.c.d	Sets the sender address of the ping (standard: IP Adresse of the router)
-a INT	Sets the intranet address of the router as sender address
-a DMZ	Sets the DMZ address of the router as sender address
- a LBx	Sets one of the 16 Lancom Loopback addresses as sender address. Valid for x are the hexadecimal values 0-f
-f	flood ping: Sends many ping signals in a small amount of time. Can be used e. g. to test the broadband of the network. ATTENTION: flood ping can easily be interpretated as a DoS attack.
-n	Sends the computer name back zu the given IP address
-q	Ping command does not give an output on the panel
-r	Change to traceroute mode: every interstation passed by the data package is listed
-s n	Sets the package size to n Byte (max. 1472)
-i n	Time between the packages in seconds

Parameter	Meaning
-c n	Send n ping signals
hostaddress	Address or hostname of the recipient
stop /<RETURN>	Entering "stop" or pressing the RETURN button terminates the ping command



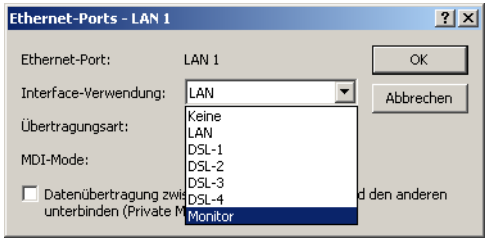
5.4 Monitoring the switch

The data transmission over the switch of LANCOM devices only takes place on the port the target computer is attached to. Therefore the connections on the other ports are not visible.

For monitoring data traffic between ports, the ports must be set to monitor mode. In this state all data is issued, that is transmitted over the switch of the devices between stations of the LAN and WAN.

LANconfig

For the configuration with LANconfig open the Ethernet switch settings in the configuration area 'Interfaces' on the register 'LAN' with the button **Ethernet Ports**.



WEBconfig, Telnet or terminal program

Under WEBconfig or Telnet resp. a terminal program you can find the ethernet switch settings with the following directories.

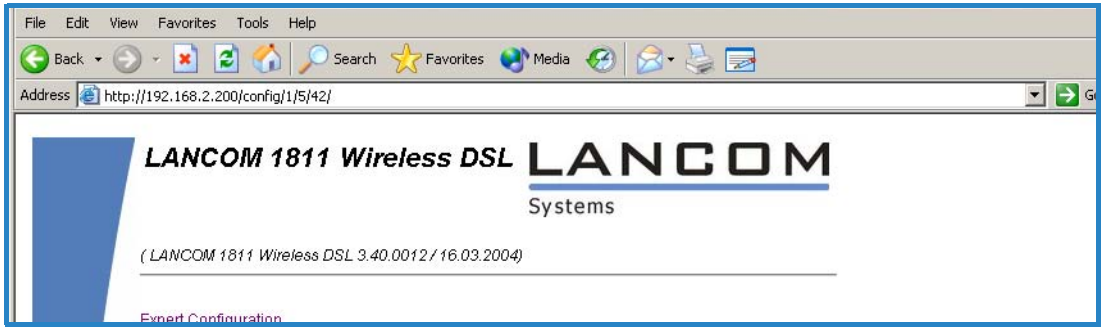
Configuration tool	Directory/Table
WEBconfig	Expert Configuration ▶ Setup ▶ Interfaces ▶ Ethernet-Ports
Terminal/Telnet	`/Setup/Interfaces/Ethernet-Ports`

5.5 Cable testing

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

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

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



The following results can occur:

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

6 Security

You certainly would not like any outsider to have easy access to or to be able to modify the data on your computer. Therefore this chapter covers an important topic: safety. The description of the security settings is divided into the following sections:

- Protection for the configuration
  - Password protection
  - Login barring
  - Access verification
- Securing ISDN access

At the end of the chapter you will find the most important security settings as a checklist. It ensures that your LANCOM is excellently protected.

Some further LCOS features to enhance the data security are described in separate chapters:

- 'Firewall' → page 171
- 'IP masquerading' → page 120
- 'Virtual LANs (VLANs)' → page 326

6.1 Protection for the configuration

A number of important parameters for the exchange of data are established in the configuration of the device. These include the security of your network, monitoring of costs and the authorizations for the individual network users.

Needless to say, the parameters that you have set should not be modified by unauthorized persons. The LANCOM thus offers a variety of options to protect the configuration.

6.1.1 Password protection

The simplest option for the protection of the configuration is the establishment of a password.

As long as a password hasn't been set, anyone can change the configuration of the device. For example, your Internet account information could be stolen, or the device could be reconfigured in a way that the protection-mechanisms could by bypassed.

Note: If a password has not been set, the Power LED flashes, until the devices have been configured correctly.

Tips for proper use of passwords

We would like to give you a few tips here for using passwords:

- **Keep a password as secret as possible.**
  Never write down a password. For example, the following are popular but completely unsuitable: Notebooks, wallets and text files in computers. It sounds trivial, but it can't be repeated often enough: don't tell anyone your password. The most secure systems surrender to talkativeness.
- **Only transmit passwords in a secure manner.**
  A selected password must be reported to the other side. To do this, select the most secure method possible. Avoid: Non-secure e-mail, letter, or fax. Informing people one-on-one is preferable. The maximum security is achieved when you personally enter the password at both ends.
- **Select a secure password.**
  Use random strings of letters and numbers. Passwords from common language usage are not secure. Special characters such as '&"?#-*+_:;,!°' make it difficult for potential attackers to guess your password and increase the security of the password.

Capital and small letters are distinguished in the configuration password.

- **Never use a password twice.**
  If you use the same password for several purposes, you reduce its security effect. If the other end is not secure, you also endanger all other connections for which you use this password at once.
- **Change the password regularly.**
  Passwords should be changed as frequently as possible. This requires effort, however considerably increases the security of the password.
- **Change the password immediately if you suspect someone else knows it.**
  If an employee with access to a password leaves the company, it is high time to change this password. A password should also always be changed when there is the slightest suspicion of a leak.

If you comply with these simple rules, you will achieve the highest possible degree of security.

Entering the password

You will find the box to enter the password in LANconfig in the configuration area 'Management' on the 'Admin' tab. Under WEBconfig you run the wizard **Security Settings**. In a terminal or Telnet session you set or change the password with the command `passwd`.

Configuration tool	Run
LANconfig	Management ▶ Admin ▶ Main device password
WEBconfig	Security settings
Terminal/Telnet	`passwd`

Protecting the SNMP access

At the same time you should also protect the SNMP read access with a password. For SNMP the general configuration password is used.

Configuration tool	Run
LANconfig	Management ▶ Admin ▶ Password required for SNMP read permission
WEBconfig	Expert Configuration ▶ Setup ▶ SNMP ▶ Password- required-for-SNMP-read-access
Terminal/Telnet	`setup/SNMP/password-required`

6.1.2 Login barring

The configuration in the LANCOM is protected against "brute force attacks" by barring logins. A brute-force attack is the attempt by an unauthorized person to crack a password to gain access to a network, a computer or another device. To achieve this, a computer can, for example, go through all the possible combinations of letters and numbers until the right password is found.

As a measure of protection against such attacks, the maximum allowed number of unsuccessful attempts to login can be set. If this limit is reached, access will be barred for a certain length of time.

If barring is activated on one port all other ports are automatically barred too.

The following entries are available in the configuration tools to configure login barring:

- Lock configuration after (`Login-errors`)
- Lock configuration for (`Lock-minutes`)

Configuration tool	Run
LANconfig	Management ▶ Admin
WEBconfig	Expert Configuration ▶ Setup ▶ Config
Terminal/Telnet	`Setup/Config`

6.1.3 Restriction of the access rights on the configuration

Access to the internal functions of the devices can be restricted separately for each access method as follows:

- ISDN administrative account
- LAN
- Wireless LAN (WLAN)
- WAN e.g. ISDN, DSL or ADSL)

For network-based configuration access further restrictions can be made, e.g. that solely specified IP addresses or dedicated LANCAPI clients are allowed to do so. Additionally, all following internal functions are separately selectable.

- LANconfig (TFTP)
- WEBconfig (HTTP, HTTPS)
- SNMP
- Terminal/Telnet

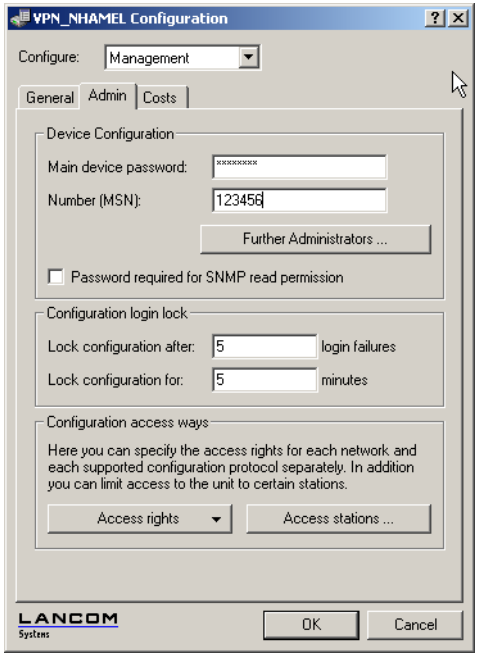
The use of the internal functions with a WAN interface of devices with VPN can be restricted merely for the VPN connection.

Restrictions on the ISDN administrative account

As long as no MSN-configuration is entered a non-configured LANCOM accepts the calls on all MSNs. As soon as the first change in the configuration ist saved the device only accepts calls on the configuration MSN.

If no configuration MSN ist entered when configuring the first time, the remote configuration ist switched off and the device ist protected from the access over the ISDN line.

① Change to the register card 'Admin' in the 'Management' configuration area:



② Enter as call number within 'Device configuration' a call number of your connection, which is not used for other purposes.

Enter alternatively the following instruction:

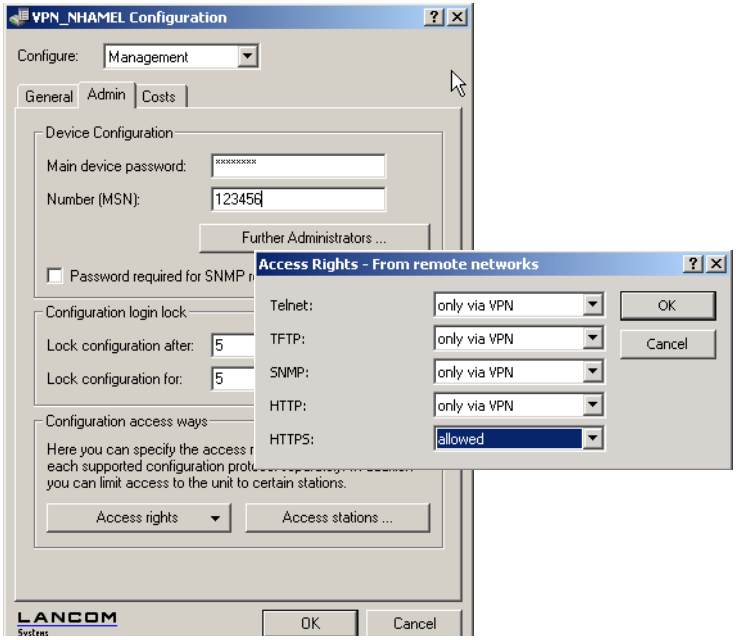
```
set /setup/config/farconfig-(EAZ-MSN) 123456
```

The ISDN administrative account is excluded as only configuration method from in the following described restrictions of network access methods. I.e. all on the Admin MSN incoming connections are not limited by the access restrictions of remote networks.

If you want to completely switch off the ISDN remote management, leave the field with Admin MSN empty.

Limit the network configuration access

The access to the internal functions can be controlled separately for accesses from the local or from remote networks - for all configuration services separately. The configuration access can generally be permitted or forbidden, a pure read access or - if your model is equipped with VPN - also can be permitted only over VPN.



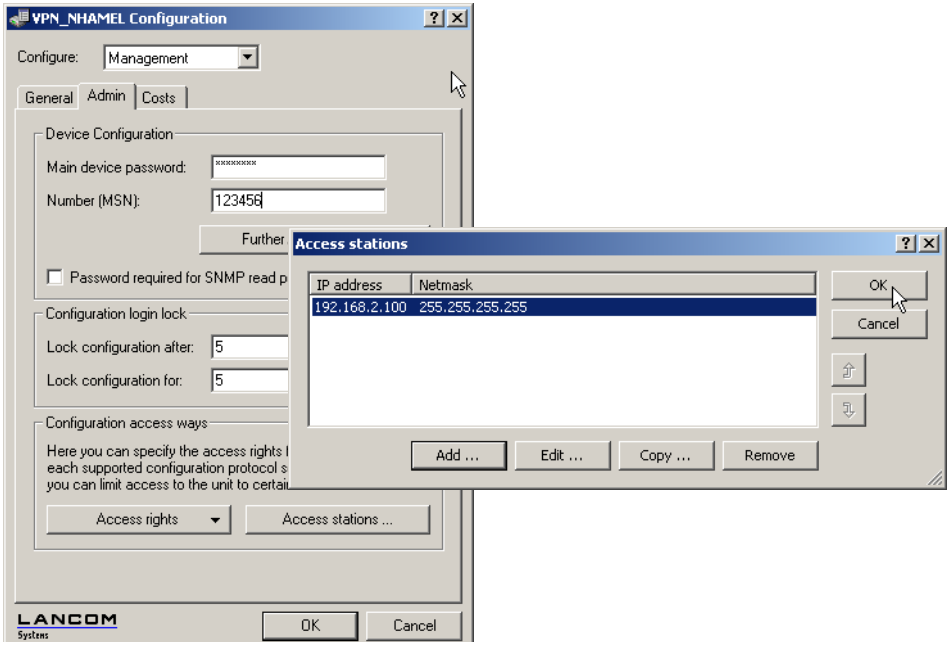
If you want to remove the network access to the router over the WAN completely, set the configuration access from distant nets for all methods to 'denied'.

You can reach the configuration of the access-list of WEBconfig or Telnet with the following runs:

Configuration tool	Run
WEBconfig	Expert Configuration ▶ Setup ▶ Config ▶ Access-list
Terminal/Telnet	`/Setup/Config-Modul/access-list`

Restriction of the network configuration access to certain IP addresses

With a special filter list the access to the internal functions of the devices can be limited to certain IP addresses. The configuration dialog with the access rights from local or distant networks can be opened with the Button **Access stations**.



By default, this table does not contain entries. Thus the device can be accessed over TCP/IP from computers with arbitrary IP addresses. With the first entry of a IP address (as well as the associated net mask) the filter is activated, and solely the IP addresses contained in this entry are entitled to use the internal functions then. With further entries, the number of the entitled ones can be extended. The filter entries can designate both individual computers and whole networks.

With WEBconfig for Telnet you reach the configuration of the access list with the following runs:

Configuration tool	Run
WEBconfig	Expert Configuration ▶ Setup ▶ / TCP-IP Access-list
Terminal/Telnet	`/setup/TCP-IP/access-list`

6.2 Protecting the ISDN connection

For a device with an ISDN connection basically any ISDN subscriber can dial into your LANCOM. To prevent undesired intruders, you must therefore pay particular attention to the protection of the ISDN connection.

The protection functions of the ISDN connection can be divided into two groups:

- Identification control
  - Access protection using name and password
  - Access protection via caller ID
- Callback to defined call numbers

6.2.1 Identification control

For identification monitoring either the name of the remote site or the so-called caller ID can be used. The caller ID is the telephone number of the caller that is normally transmitted to the remote site with the call with ISDN.

Which "Identifier" is to be used to identify the caller is set in the following list:

Configuration Tool	Run
LANconfig	Communication ▶ Call Management
WEBconfig	Expert Configuration ▶ Setup ▶ WAN ▶ Protect
Terminal/Telnet	`setup/WAN/protect`

You have a choice of the following:

- all: Calls are accepted from any remote station.
- by number: Only calls from those remote stations whose Calling Line Identification number (CLIP) is entered in the number list are accepted.
- by approved number: Only calls from those remote stations whose Calling Line Identification number (CLIP) is entered in the peer list **and** whose number is approved by the Central Office.

It is an obvious requirement for identification that the corresponding information is sent by the caller.

Verification of name and password

In the case of PPP, a user name (and in conjunction with PAP, CHAP or MS-CHAP, a password) is sent to the remote station during connection establishment. When a computer dials into the LANCOM, the communications software, for example Windows Dial-Up Network, prompts the user for the user name and password to be transferred.

If the router establishes the connection itself, for instance, to an ISP, it is using the user name and password from the PPP list. If no user name is listed there, the device name is used in its place.

The PPP list can be found as follows:

Configuration tool	Run
LANconfig	Communication ▶ Protocols ▶ PPP list
WEBconfig	Expert Configuration ▶ Setup ▶ WAN ▶ PPP-list
Terminal/Telnet	`/setup/WAN/PPP-list`

In addition, the PPP protocol also permits the caller to require an authentication from the remote station. The caller then requests a user or device name and password from the remote station.

Of course you will not need to use the PAP, CHAP or MS CHAP security procedures if you are using the LANCOM to dial up an Internet service provider yourself, for example.You will probably not be able to persuade the ISP to respond to a request for a password...

Checking the number

When a call is placed over an ISDN line, the caller's number is normally sent over the D channel before a connection is even made (CLI – Calling Line **Identifier**).

Access to your own network is granted if the call number appears in the number list, or the caller is called back if the callback option is activated. If the LANCOM is set to provide security using the telephone number, any calls from remote stations with unknown numbers are denied access.

You can use call numbers as a security measure with any B-channel protocol (layers).

6.2.2 Callback

The callback function offers a special form of access privilege: This requires the 'Callback' option to be activated in the peer list for the desired caller and the call number to be specified, if required.

Configuration tool	Run
LANconfig	Communications ▶ Remote site ▶ Remote Sites (ISDN/serial)
WEBconfig	Expert configuration ▶ Setup ▶ WAN ▶ dialup-peers
Terminal/Telnet	`/Setup/WAN/dialup-peers`

Using the settings in the name and number list and the selection of the protocol (LANCOM or PPP), you can control the callback behaviour of your router :

- The router can refuse to call back.
- It can call back using a preset call number.
- First the name can be checked and then a preset telephone number can be called back.
- The caller can opt to specify the call number to be used for callback.

And all the while you can use the settings to dictate how the cost of the connection is to be apportioned. The router accepts all unit charges, except for the unit required to send the name, if call back 'With name' is set in the peer list. The caller also accepts a unit if the caller is not identified via CLIP (**C**alling **L**ine **I**dentifier **P**rotocol). On the other hand, the caller incurs no costs if identification of the caller's number is possible and is accepted (callback via the D channel).

An especially effective callback method is the fast-callback procedure (patent pending). This speeds up the callback procedure considerably. The procedure only works if it is supported by both stations. All current LANCOM routers are capable of fast callback.

Additional information on callback can be found in section 'Callback functions' → page 151.

6.3 Anti-Theft Protection with the ISDN Location Check

In larger installations with partly unattended routers and access points the threat is high that the device is stolen and set up in other places. If RAS accounts, LAN coupling or VPN connections are configured on these routers, the thief can access the protected network from a diffenrent location.

You can inhibit the abuse of your router with a location check: The router will therefore initiate an ISDN selfcall after each switch-on, to check if it is installed in the correct place. The router will first start operating (routing, connection establishment) as soon as the number of the incomming call corresponds to the configured one.

Precondition for the successful ISDN location check:

- The device must be reachable on the public ISDN network.
- During the selfcall the device requires two vacant B channels. As long as only one channel is available the device cannot call itself over ISDN, e.g. because a device is engaging a B channel for phoning.

6.3.1 Configuration of the ISDN Location Check

LANconfig

The parameters for the ISDN Location Check can be found in the configuration area 'Management' on the register card 'Location'.

With the Option 'Enable ISDN location check' you can activate the ISDN Location Check.

For the configuration the following items must be entered:

- The 'Destination number' is the number, which is dailed by the router for the check call.

The destination number must always be entered so that the router can initiate a ISDN selfcall.

- The 'Calling number (MSN)' determines which number is transmitted to the remote station as an incoming call.

  This entry is optional. If the outgoing number is not defined, the device uses the 'Destination number'. The entry of the outgoing number is mostly only then required, when the router is connected to a telephone switchboard. In this case the definition of the calling number is considered by the telephone switchboard.

- The 'Calling party number' is used by the router to verificate the ISDN selfcall. The device compares this number with the number of the incoming call. It will not start operating until these numbers are identical.

  This Entry ist optional. If the incoming calling number is not defined, the device uses the 'Destination number'. The definition of the incoming call is required, to consider that by telephone switchboards may change the outgoing number. In this case the replaced number must be entered instead of the destination number.

  In case you are not certain, which calling number is transmitted by your telephone switchboard, you can find it out with the following procedure:

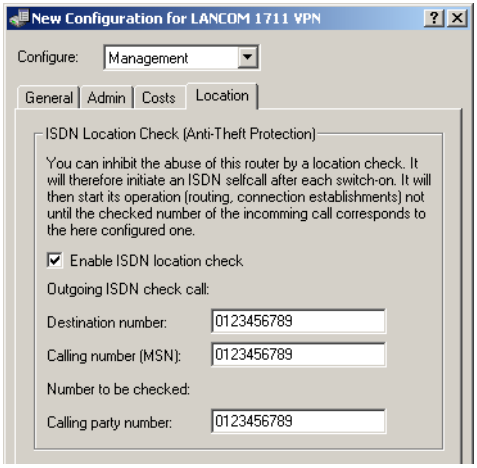
① First enter the 'Destination number' and activate the ISDN Location Check. The comparison of the incoming number and the expected calling party number will probably lead to a mismatch and the device is locked.

② In WEBconfig or Telnet you can look up which phone number was last perceived by the router.

③ Deactivate the ISDN Location Check and enter the reported 'last-seen-call-from' number as the 'Calling party number'.

④ Activate the ISDN Location Check again, the device will then retry an ISDN selfcall. The comparison of the incoming number and the expected calling party number will lead to a match, the router will then be accessble again.

Always enter the complete phone number, containing the outside line access number (if existent), the country dailling code and the area dailling code. In many cases public telephone switches supplement dailling codes when transmitting numbers. In case the dailling codes are not entered, the expected and transmitted number will differ and therefore the ISDN Location Check will fail. The prefixed zeros are not considered, but can be entered.



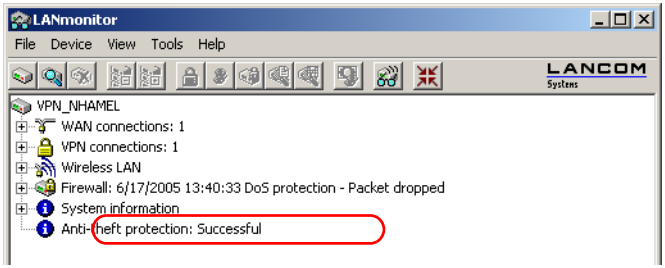
WEBconfig, Telnet or Terminal program

Under WEBconfig, Telnet resp. Terminal program you can configure the ISDN Location Check under following directories:

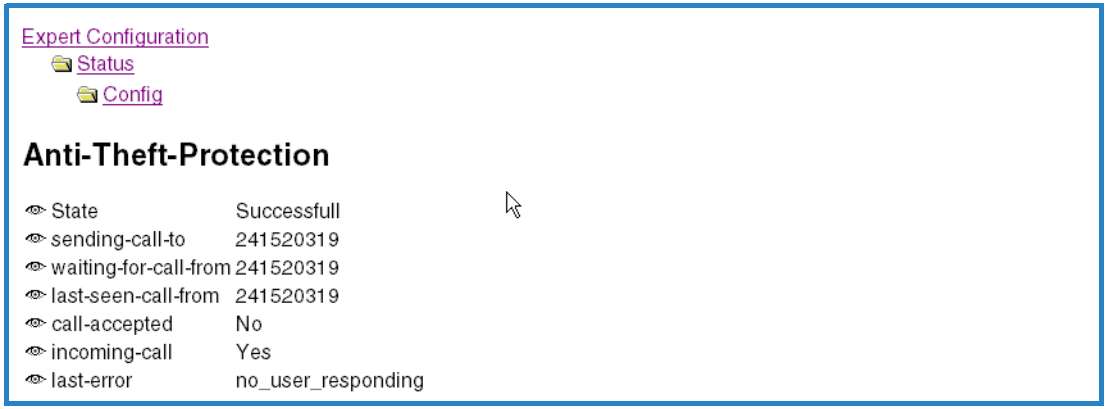
Configuration tool	Menu/Table
WEBconfig	Expert Configuration ▶ Setup ▶ Config ▶ Anti-Theft-Protection
Terminal/Telnet	`Setup/Config/Anti-Theft-Protection`

6.3.2 Status request of the ISDN Location Check

The status of the ISDN Location Check can be looked up with LANmonitor:



With WEBconfig (**Expert Configuration ▶ Status ▶ Config ▶ Anti-Theft-Protection**) or Telnet (`Status/Config/Anti-Theft-Protection`) you can also look up the ISDN Location Check.



Not until the Location Check is in the state 'Successful' the router can transmit data over the WAN interface. A Location Check is then successful, if the number 'waiting-for-call-from' corresponds to the number 'last-seen-call-from'. The call is not accepted by the router. The status also shows, if the router has recognized a call at all.

6.4 The security checklist

In the following checklist you will find an overview of the most important security functions. That way you can be quite sure not to have overlooked anything important during the security configuration of your LANCOM.

- **Have you assigned a password for the configuration?**

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

- **Have you permitted remote configuration?**

  If you do not require remote configuration, then deactivate it. If you require remote configuration, then be sure to assign a password protection for the configuration (see previous section). The field for deactivating the remote configuration is also contained in LANconfig in the 'Management' configuration area on the 'Security' tab. Under 'Access Rights' 'From remote networks' select for all configuration types 'denied'.

- **Have you permitted the configuration of wireless networks?**

  If you do not require the configuration from wireless networks switch it off. The field for switching off the configuration from wireless networks you can also find in LANconfig in the 'Management' configuration area on the 'Security' tab. Under 'Access Rights' 'From the wireless LAN' select for all configuration types 'denied'.

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

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

- **Have you allowed remote access?**

  If you do not require remote access, deactivate call acceptance by deactivating a call acceptance 'by number' and leaving the number list blank in LANconfig in the 'Communication' configuration area on the 'Call accepting' tab.

- **Have you activated the callback options for remote access and is CLI activated?**

  When a call is placed over an ISDN line, the caller's number is normally sent over the D channel before a connection is even made (CLI – **C**alling **L**ine **I**dentifier). Access to your own network is granted if the call number appears in the number list, or the caller is called back if the callback option is activated (this callback via the D channel is not supported by the Windows Dial-Up Network). If the LANCOM is set to provide security using the telephone number, any calls from remote stations with unknown numbers are denied access.

- **Have you activated the Firewall?**

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

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

  For maximum security and control you prevent at first any data transfer through the Firewall. Only those connections, which are explicitly desired have to allowed by the a dedicated Firewall rule then. Thus 'Trojans' and certain Email viruses loose their communication way back. The Firewall rules are summarized in LANconfig under 'Firewall/Qos' on the register card 'Rules'. A guidance can be found under 'Set-up of an explicit "Deny All" strategy' → page 200.

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

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

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

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

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

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

- **Have you encoded the radio network and secured it with an ACL?**

  With 802.11i, WPA or WEP you can encode your data in the radio network with different kinds of encoding methods as for AES, TKIP or WEP. LANCOM Systems recommends the most secure encoding with 802.11i and AES. If the used WLAN client adapter does not provide these, use the TKIP or at least WEP. Make sure that your device when using the encoding function has at least one passphrase or WEP key entered. To check the WEP settings select in the LANconfig in the configuration area 'Management' on the tab 'Interfaces' under 'Wireless LAN' the wireless LAN interface you would like to configure.

  With the Access Control List (ACL) you allow or prohibit the access of single radio LAN clients to your radio LAN. The access is regulated over the static MAC address of the wireless client adapter. To check the Access Control List select in LANconfig in the configuration area 'WLAN Security' the tab 'Stations'.

- **Have you configured 802.1x or IPsec over WLAN for especially sensitive data transfer?**

  For more security when transmitting sensitive data over your wireless LAN you can use the IEEE 802.1x technology. To check or activate the IEEE 802.1x settings select in the LANconfig the configuration area 'WLAN Security' the tab 'IEEE 802.1x'.

  If your base station provides VPN you can alternatively to IEEE 802.1x select IPsec over WLAN to protect your data between radio networks and local networks in a VPN tunnel.

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

  That confidential information about RAS access, LAN coupling or VPN connections could fall into the wrong hands if the device is stolen. The device's configuration can be protected by various means; for example, it will cease to function if there is an interruption to the power supply, or if the device is switched on in another location.

  - With the ISDN site verification, the device can only be operated at one particular ISDN connection. After being switched on, the device calls itself at the corresponding telephone number to check that it is still connected to the "proper" ISDN connection. ('Anti-Theft Protection with the ISDN Location Check' → page 100).
  - 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. ('Scripting' → page 57).

7 Routing and WAN connections

This chapter describes the most important protocols and configuration entries used for WAN connections. It also shows ways to optimize WAN connections.

7.1 General information on WAN connections

WAN connections are used for the following applications.

- Internet access
- LAN to LAN coupling
- Remote access

7.1.1 Bridges for standard protocols

WAN connections differ from direct connections (for example, via the LANCAPI) in that the data in the WAN are transmitted via standardized network protocols also used in the LAN. Direct connections, on the other hand, operate with proprietary processes that have been specially developed for point-to-point connections.

Via WAN connections a LAN is extended, and with direct connections only one individual PC establishes a connection to another PC. WAN connections form a kind of bridge for the communication between networks (or for connecting individual computers to the LAN).

Which protocols are used for WAN connections?

WAN connections over highspeed ports (e.g. DSL connections) use the IP standard for transmitting packets. Devices with an ISDN interface provide beside IP additionally IPX.

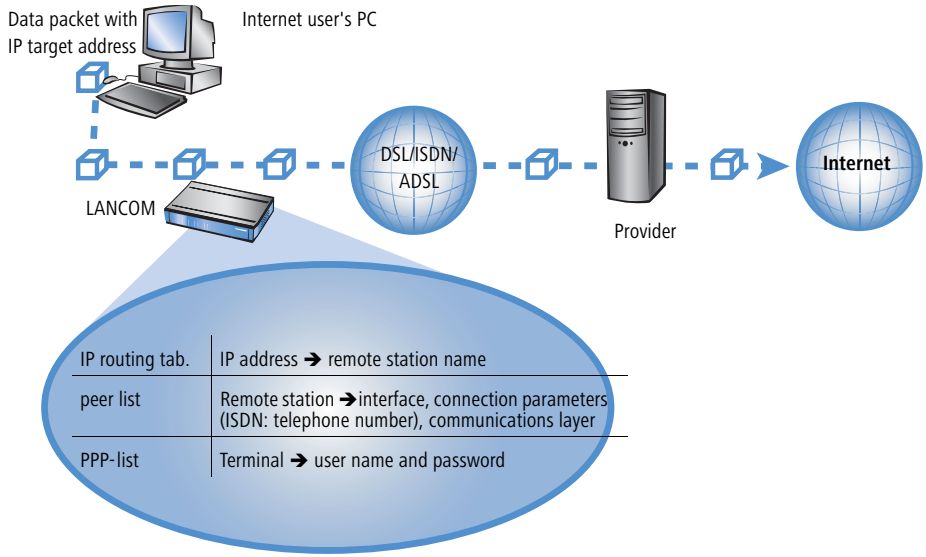
Close cooperation with router modules

Characteristic of WAN connections is the close cooperation with the router modules in the LANCOM. The router modules (IP and IPX) take care of connecting LAN and WAN. They make use of the WAN modules to fulfil requests from PCs within the LAN for external resources.

7.1.2 What happens in the case of a request from the LAN?

Initially the router modules only determine the remote station to which a data packet is to be sent. The various parameters for all required connections must be arranged so that a given connection can be selected and established as required. These parameters are stored in a variety of lists, the interaction of which permits the correct connections.

A simplified example will clarify this process. Here we assume that the IP address of the computer being searched for is known in the Internet.



① **Selecting the correct route**
A data packet from a computer initially finds the path to the Internet through the IP address of the receiver. The computer sends the packet with this address over the LAN to the router. The router determines the remote station in its IP routing table via which the target IP address can be reached, e.g. 'Provider_A'.

② **Connection data for the remote station**
Using these names, the router checks the names list and finds the necessary connection data for provider A. Included in these connection data are, for instance, the WAN interface (DSL, ISDN) through which the provider is connected to, protocol information, or the necessary number for an ISDN call connection. The router also obtains the user name and password required for login from the PPP list.

③ **Establishing the WAN connection**
The router can then establish a connection to provider via a WAN interface. It authenticates itself with a user name and password.

④ **Transmission of data packets**
As soon as the connection is established, the router can send the data packet to the Internet.

7.2 IP routing

An IP router works between networks which use TCP/IP as the network protocol. This only allows data transmissions to destination addresses entered in the routing table. This section explains the structure of the IP routing table of an LANCOM Systems router, as well as the additional functions available to support IP routing.

7.2.1 The IP routing table

The IP routing table is used to tell the router which remote station (which other router or computer) it should send the data for particular IP addresses or IP address ranges to. This type of entry is also known as a "route" since it is used to describe the path of the data packet. This procedure is also called "static routing" since you make these entries yourself and they remain unchanged until you either change or delete them yourself. Naturally, "dynamic routing" also exists. The routers use the routes in this way to exchange data between themselves and continually update it automatically. The IP router looks at the static and the dynamic routing table when the IP RIP is activated.

You also use the IP routing table to tell the router the length of this route's path so that it can select the most suitable route in conjunction with IP RIP where there are several routes to the same destination. The default setting for the distance to another router is 2, i.e. the router can be reached directly. All devices which can be reached locally, such as other routers in the same LAN or workstation computers connected via proxy ARP are entered with the distance 0. The "quality level" of this route will be reduced if the entry addressed has a higher distance (up to 14). "Unfavorable" routes like this will only be used if no other route to the remote station in question can be found.

Configuration of the routing table

Configuration tool	Run
LANconfig	IP router ▶ Routing ▶ Routing table
WEBconfig	Expert Configuration ▶ Setup ▶ IP-router ▶ IP-routing-table
Terminal/Telnet	`cd /setup/IP-router/IP-routing-table`

An IP routing table can, for example, look like this:

IP address	Netmask	Routing-Tag	Router	Distance	Masquerading	Active
192.168.120.0	255.255.255.0	0	MAIN	2	Off	yes
192.168.125.0	255.255.255.0	0	NODE1	3	Off	yes
192.168.130.0	255.255.255.0	0	191.168.140.123	0	Off	yes

What do the various entries on the list mean?

- IP addresses and netmasks

  This is the address of the destination network to which data packets may be sent and its associated network mask. The router uses the network mask and the destination IP address of the incoming data packets to check whether the packet belongs to the destination network in question.

  The route with the IP address '255.255.255.255' and the network mask '0.0.0.0' is the default route. All data packets that cannot be routed by other routing entries are sent over this route.

- Routing Tag

With the routing tag the selection of the target route can be controlled more easily. Therefore not only the target IP adress for the selection of the route is detected but also other information, which is joined to the data packets by the firewall. With the routing tag "0" the routing entry is valid for all packets.

- Router

  The router transmits the appropriate data packets to the IP address and network mask to this remote station.

  - If the remote station is a router in another network or an individual workstation computer the name of the remote station.
  - If the router on the network cannot address the remote station itself, then the IP address of another router which knows the path to the destination network is entered.

  The router name indicates what should happen with the data packets that match the IP address and network mask.

  - Routes with the entry '0.0.0.0' identify exclusion routes. Data packets for this "zero route" are rejected and are not routed any further. That way routes which are forbidden on the Internet (private address spaces, e.g. '10.0.0.0'), for example, are excluded from transmission.
  - If an IP address is input as router name, this is a locally available router, which is responsible for transfer of the relevant data packets.

- Distance

  Number of routers between your own and the destination router. This value is often equated with the cost of the transmission and used to distinguish between inexpensive and expensive call paths for wide-area connections. The distance values entered are propagated as follows:

  - All networks which can be reached while a connection exists to a destination network are propagated with a distance of 1.
  - All non-connected networks are propagated with the distance entered in the routing table (but with a minimum distance of 2) as long as a free transmitting channel is still available.
  - The remaining networks are propagated with a distance of 16 (= unreachable) if there are no longer any channels available.
  - Remote stations connected using proxy ARP are an exception to this. These "proxy hosts" are not propagated at all.

- Masquerading

  Use the 'Masquerade' option in the routing table to inform the router which IP addresses to use when transferring packets from local networks.

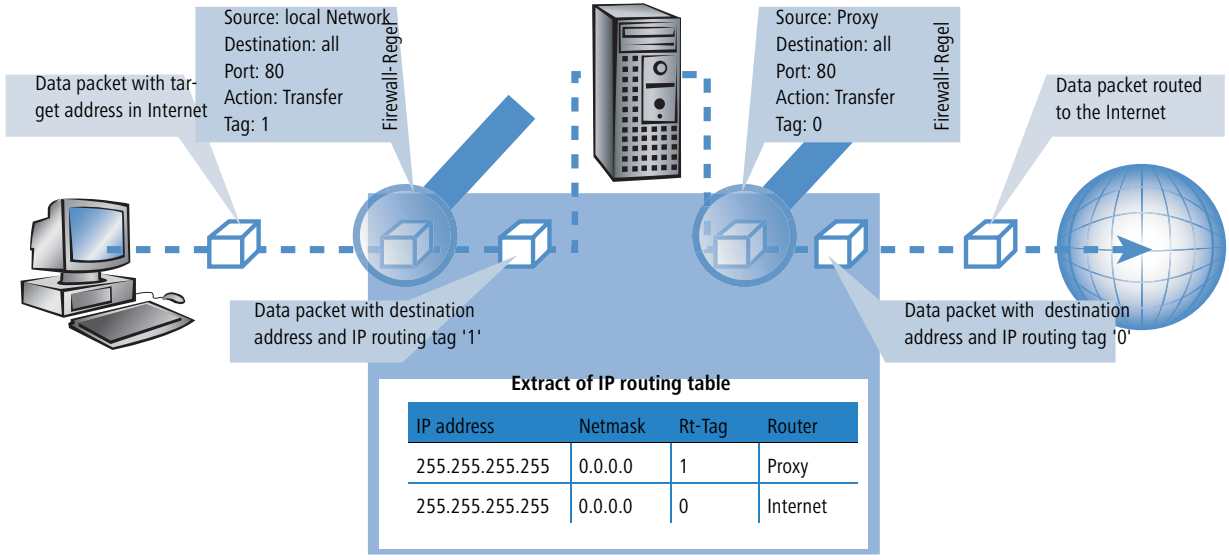
  For further information see the section 'IP masquerading' → page 120.

7.2.2 Policy-based routing

Policy-based routing does not rely exclusively upon the destination IP address to define the destination route (meaning the remote device that is to be used to transfer the data). Further information can be used-such as the service or the protocol used, sender addresses or the destination for the data packets-for the selection of the destination

route. Policy-based routing can be used to achieve a significantly finer-grained routing behavior, such as in the following application scenarios:

- The LAN's entire Internet traffic is diverted to a proxy without entering the proxy address into the browsers. As the users do not notice the proxy routing, the scenario is named "transparent" proxy.



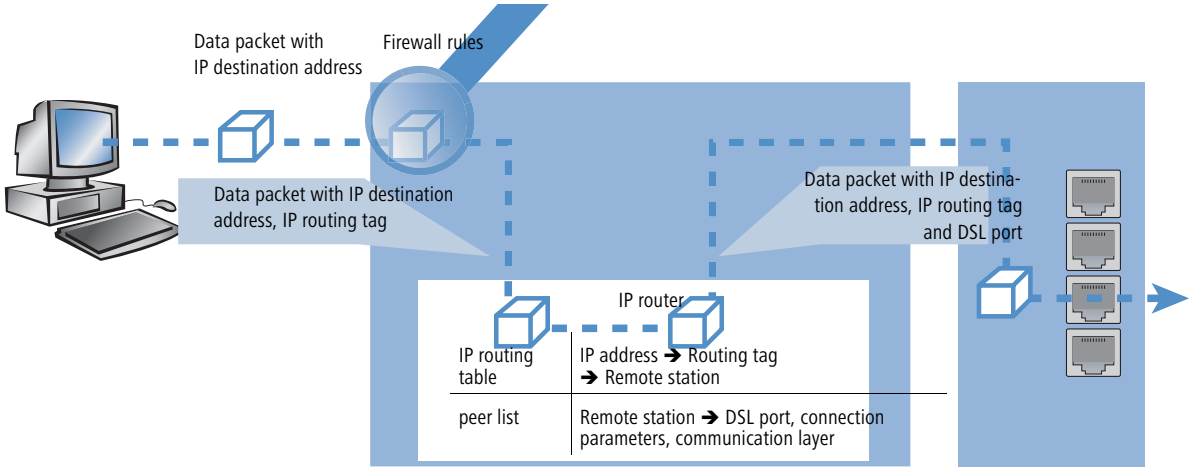
Extract of IP routing table

IP address	Netmask	Rt-Tag	Router
255.255.255.255	0.0.0.0	1	Proxy
255.255.255.255	0.0.0.0	0	Internet

- With load balancing, the data traffic for selected protocols is diverted over a certain DSL port that uses an additional external ADSL modem.
- A server in the local network is only supposed to be accessible from the WAN via a fixed IP address; this is routed via a certain WAN interface.
- VPN traffic is forwarded to a VPN tunnel with dynamic end points by using the routing tag '0'; the company's remaining Internet traffic is diverted to another firewall by means of another suitable routing tag.

Suitable entries can be made in the firewall to select channels according to information other than just the destination IP address. These entries are supplemented with a special routing tag that is used to control the channel selection with the routing table. For example, a rule adds the routing tag '2' to the entire data traffic for a local group of computers (defined by an IP address range). Alternatively, certain protocols receive a different supplementary routing tag.

The diagram demonstrates the application of policy-routing with load balancing:



- When establishing a connection, the firewall initially checks if the packets for transmission fit to a rule which contains a routing tag. The routing tag is entered into the data packet.
- The IP routing table combines the routing tag and destination IP address to determine the appropriate remote station. The IP routing table is processed from top down in the usual fashion.
- If an entry is found corresponding to the network, then the second step is to check the routing tag. The required remote station can be found with the help of the appropriate routing tag.

If the routing tag has a value of "0" (default) then the routing entry applies to all packets.

- Internal services implicitly use the default tag. If the user wishes to direct the default route through a VPN tunnel with a dynamic tunnel endpoint, for example, then the VPN module uses the default route with the routing tag "0" as standard.

  To direct the default route through the VPN tunnel anyway, create a second default route with routing tag "1" and the VPN remote station as router names. With the appropriate firewall rule you can transfer all services from all source stations to all destination stations with routing tag "1".
- Routing tags and RIP: The routing tag is also transmitted in RIP packets for processing upon reception, so that, for example, the change in distances in the proper route can be changed.

Routing tags for VPN and PPTP connections

Routing tags are used on the LANCOM in order to evaluate criteria relevant to the selection of the target route in addition to the IP address. In general, routing tags are added to the data packets using special firewall rules. However, in some cases, it is desirable to assign the tags directly.

- Routing tags for VPN connections

The VPN name list can be used to enter the routing tag for every VPN connection. The routing tag is used in order to determine the route to the remote gateway (default '0').

In addition, every gateway can be assigned a specific routing tag in the gateway table. The tag 0 has a special function in this table: If the tag is set at 0 on a gateway, then the tag from the VPN name list table is used.

The VPN routing tag parameters can be found under Setup/VPN/VPN Peers or Setup/VPN/Additional Gateways and under LANconfig in the configuration area 'VPN' on the 'General' tab by clicking on 'Connection List' and 'Other remote gateways' in the list.

- Routing tags for PPTP connections

In the PPTP table, a routing tag can be entered in addition to the IP address of the PPTP server. Using this routing tag, two or more DSL modems that use a single IP address can be operated on different DSL ports.

Peer	IP Address	Rtg tag	Port	SH time
PEER01	10.0.0.138	1	1723	9999
PEER02	10.0.0.138	2	1723	9999

In the IP routing table, two appropriately tagged routes are required:

IP address	IP netmask	Rtg tag	Peer or IP	distance	Masquerading
10.0.0.138	255.255.255.255	2	PEER02 PPTP	0	No
10.0.0.138	255.255.255.255	1	PEER01 PPTP	0	No
192.168.0.0	255.255.0.0	0	0.0.0.0	0	No
172.16.0.0	255.240.0.0	0	0.0.0.0	0	No
10.0.0.0	255.0.0.0	0	0.0.0.0	0	No
224.0.0.0	224.0.0.0	0	0.0.0.0	0	No
255.255.255.255	0.0.0.0	0	PEER LB	0	yes

Using these settings and the corresponding entry in the load balancing table, load balancing can be performed that would also work in Austria.

Peer	Bundle Peer 1	Bundle Peer 2	Bundle Peer 3
PEER LB	PEER01	PEER02	

7.2.3 Local routing

You know the following behavior of a workstation within a local network: The computer searches for a router to assist with transmitting a data packet to an IP address which is not on its own LAN. This router is normally introduced to

the operating system with an entry as standard router or standard gateway. It is often only possible to enter one default router which is supposed to be able to reach all the IP addresses which are unknown to the workstation computer if there are several routers in a network. Occasionally, however, this default router cannot reach the destination network itself but does know another router which can find this destination.

How can you assist the workstation computer now?

By default, the router sends the computer a response with the address of the router which knows the route to the destination network (this response is known as an ICMP redirect). The workstation computer then accepts this address and sends the data packet straight to the other router.

Certain computers, however, do not know how to handle ICMP redirects. To ensure that the data packets reach their destination anyway, use local routing. In this way you instruct the router itself in your device to send the data packet to other routers. In addition, in this case no more ICMP redirects will be sent. The setting is made under:

Configuration tool	Run
LANconfig	IP router ▶ General ▶ Forward packets within the local network
WEBconfig	Expert Configuration ▶ Setup ▶ IP-router ▶ Loc.-routing
Terminal/Telnet	`set /setup/IP-router/Loc. routing on`

Local routing can be very helpful in isolated cases, however, it should also only be used in isolated cases. For local routing leads to a doubling of all data packets to the desired target network. The data is first sent to the default router and is then sent on from here to the router which is actually responsible in the local network.

7.2.4 Dynamic routing with IP RIP

In addition to the static routing table, LANCOM Systems routers also have a dynamic routing table containing up to 128 entries. Unlike the static table, you do not fill this out yourself, but leave it to be dealt with by the router itself. It uses the Routing Information Protocol (RIP) for this purpose. All devices that support RIP use this protocol to exchange information on the available routes.

What information is propagated by IP RIP?

A router uses the IP RIP information to inform the other routers in the network of the routes it finds in its own static table. The following entries are ignored in this process:

- Rejected routes with the '0.0.0.0' router setting.
- Routes referring to other routers in the local network.
- Routes linking individual computers to the LAN by proxy ARP.

Although the entries in the static routing table are set manually, this information changes according to the connection status of the router and so do the RIP packets transmitted.

- If the router has established a connection to a remote station, it propagates all the networks which can be reached via this route in the RIPs with the distance '1'. Other routers in the LAN are thus informed by these means that a connection to the remote station has been established on this router which they can use. The establishment of additional connections by routers with dial-up connections can be prevented, thus reducing connection costs.
- If this router cannot establish a further connection to another remote station, all other routes are propagated with the distance '16' in the RIPs. The '16' stands for "This route is not available at the moment". A router may be prevented from establishing a connection in addition to the present one may be due to one of the following causes:
  - Another connection has already been established on all the other channels (also via the LANCAPI).
  - Y connections for the S_0 port have been explicitly excluded in the interface table.
  - The existing connection is using all B channels (channel bundling).
  - The existing connection is a leased-line connection. Only a few ISDN providers enable a dial-up connection to be established on the second B channel in addition to a permanent connection on the first B channel.

Which information does the router take from received IP RIP packets?

When the router receives such IP RIP packets, it incorporates them in its dynamic routing table, which looks something like this:

IP address	IP netmask	Time	Distance	Router
192.168.120.0	255.255.255.0	1	2	192.168.110.1
192.168.130.0	255.255.255.0	5	3	192.168.110.2
192.168.140.0	255.255.255.0	1	5	192.168.110.3

What do the entries mean?

IP address and network mask identify the destination network, the distance shows the number of routers between the transmitter and receiver, the last column shows which router has revealed this route. This leaves the 'Time'. The dynamic table thus shows how old the relevant route is. The value in this column acts as a multiplier for the intervals at which the RIP packets arrive. A '1', therefore, stands for 30 seconds, a '5' for about 2.5 minutes and so on. New information arriving about a route is, of course, designated as directly reachable and is given the time setting '1'. The value in this column is automatically incremented when the corresponding amount of time has elapsed. The distance is set to '16' after 3.5 minutes (route not reachable) and the route is deleted after 5.5 minutes.

Now if the router receives an IP RIP packet, it must decide whether or not to incorporate the route contained into its dynamic table. This is done as follows:

- The route is incorporated if it is not yet listed in the table (as long as there is enough space in the table).
- The route exists in the table with a time of '5' or '6'. The new route is then used if it indicates the same or a better distance.

- The route exists in the table with a time of '7' to '10' and thus has the distance '16'. The new route will always be used.
- The route exists in the table. The new route comes from the same router which notified this route, but has a worse distance than the previous entry. If a device notifies the degradation of its own static routing table in this way (e.g. releasing a connection increases the distance from 1 to 2, see below), the router will believe this and include the poorer entry in its dynamic table.

RIP packets from the WAN will be ignored and will be rejected immediately. RIP packets from the LAN will be evaluated and will not be propagated in the LAN.

The interaction of static and dynamic tables

The router uses the static and dynamic tables to calculate the actual IP routing table it uses to determine the path for data packets. In doing so, it includes the routes from the dynamic table which it does not know itself or which indicate a shorter distance than its own (static) route with the routes from its own static table.

Scaling with IP RIP

If you use several routers in a local network with IP RIP, you can represent the routers outwardly as one large router. This procedure is also known as "scaling". As a result of the constant exchange of information between the routers, such a router theoretically has no limits to the transmission options available to it.

Configuration of IP-RIP function

Configuration tool	Menu/table
LANconfig	IP router ▶ General ▶ RIP options
WEBconfig	Expert Configuration ▶ Setup ▶ IP-router ▶ RIP-config
Terminal/Telnet	`setup/IP-router/RIP-config`

- In the field 'RIP support' (or 'RIP type') the following selection is possible:
  - 'off': IP-RIP is not used (default).
  - 'RIP-1': RIP-1 and RIP-2 packets are received but only RIP-1 packets are sent.
  - 'RIP-1 compatible': RIP-1 and RIP-2 packets are received. RIP-2 packets are sent as an IP broadcast.
  - 'RIP-2': Similar to 'RIP-1 compatible', except that all RIP packets are sent to the IP multicast address 224.0.0.9.
- The entry under 'RIP-1 mask' (or 'R1 mask') can be set to the following values:

- 'class' (default): The network mask used in the RIP packet is derived directly from the IP address class, i.e. the following network masks are used for the network classes:

Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

- 'address': The network mask is derived from the first bit that is set in the IP address entered. This and all high-order bits within the network mask are set. Thus, for example, the address 127.128.128.64 yields the IP network mask 255.255.255.192.
- 'class + address': The network mask is formed from the IP address class and a part attached after the address procedure. Thus, the above-mentioned address and the network mask 255.255.0.0 yield the IP network mask 255.128.0.0.

Routers with RIP capabilities dispatch the RIP packets approximately every 30 seconds.The router is only set up to send and receive RIPs if it has a unique IP address.The IP RIP module is deselected in the default setting using the IP address xxx.xxx.xxx.254.

7.2.5 SYN/ACK speedup

The SYN/ACK speedup method is used to accelerate IP data traffic. With SYN/ACK speedup IP check characters (SYN for synchronization and ACK for acknowledge) a given preference within the transmission buffer over simple data packets. This prevents the situation that check characters remain in the transmission queue for a longer time and the remote station stop sending data as a result.

The greatest effect occurs with SYN/ACK speedup with fast connections (e. g. ADSL) when data quantities are simultaneously transferred in both directions at high speed.

The SYN/ACK speedup is activated at the factory.

Switching off in case of problems

Due to the preferred handling of individual packets, the original packet order is changed. Although TCP/IP does not ensure a certain packet order, problems may result in a few isolated applications. This only concerns applications

that assume a certain order that differs from the protocol standard. In this case the SYN/ACK speedup can be deactivated:

Configuration tool	Menu/table
LANconfig	IP router ▶ General ▶ Pass on TCP SYN and ACK packets preferentially
WEBconfig	Expert Configuration ▶ Setup ▶ IP-router ▶ Routing-method ▶ SYN/ACK-speedup
Terminal/Telnet	`cd /setup/IP-router/routing-method set SYN/ACK-speedup OFF`

7.3 Configuration of remote stations

Remote stations are configured in two tables:

- In the peer list(s) all information is set that applies individually to only one remote station.
- Parameters for the lower protocol levels (below IP or IPX) are defined in the communication layer table.

The configuration of the authentication (protocol, user name, password) is not covered in this section.Information on authentication is contained in the section 'Establishing connection with PPP' → page 146.

7.3.1 Peer list

The available remote stations are created in the peer list with a suitable name and additional parameters. For every WAN interface exists a separate peer list. The peer list reached as follows:

Configuration tool	Menu/table
LANconfig	Communication ▶ Remote sites ▶ Remote Sites (DSL)
WEBconfig	Expert configuration ▶ Setup ▶ WAN ▶ DSL-Broadband-Peers

Terminal/Telnet	`cd /Setup/WAN`
	`set DSL-Broadband-Peers[...]`
	set Dialup-Peers

For the remote stations following parameters are required:

Peer list	Parameter	Meaning
DSL	Name	With this name the remote stations are identified in the router modules. As soon as the router module has detected the remote station (using the IP address of the destination), the connection parameters are located in the peer list.
	Short hold	This time indicates how long the connection is kept if no data is being transmitted anymore. If zero is entered, the connection does not terminate automatically. If 9999 seconds are entered a broken off connection is rebuild automatically. (see 'Extended connection for flat rates—Keep-alive' → page 151)
	Access concentrator	The Access concentrator (AC) is a server, which can be accessed by the remote station. If several ADSL providers are listed, select the provider that is responsible for the remote station (using the name of the AC). The value for the AC is advised to you by your provider. If no value is entered for the AC, every AC is accepted that provides the demanded service.
	Service	Enter the service you would like to use from your provider. The service can be e.g. internet surfing or even video downstream. The value for the service is advised to you by your provider. If no value is entered, every Service is accepted that is provided by the AC.
	Layer name	Select the layer name for the connection. The configuration of this layer is described in the following section.
	VPI	Virtual Path Identifier.
	VCI	Virtual Channel Identifier. The value for VCI and VPI are advised to you by your provider. Standard values for the combination of VPI and VCI are: 0/35, 0/38, 1/32, 8/35, 8/48.
Dialup-Peers	Name	See DSL-Broadband-Peers
	Phonenumber	A Phonenumber is only then required, if the remote station must be called. This field can remain empty if only incoming calls should be accepted. Several phonenumbers for the same remote station can be entered in the RoundRobin list.
	Short hold	See DSL-Broadband-Peers
	Short hold 2	The second B channel is cut down, if it is not used for the set duration.
	Layer name	See DSL-Broadband-Peers
	Callback	The automatic callback provides a secure connection and decreases the costs for the caller. Further information can be found in the next section 'Callback functions' → page 151.

Please note following points when editing the peer list:

- If two identical peer lists (e.g. DSL-Broadband-Peers list and Dialup-Peers list) are entered, the LANCOM when connecting to the remote station uses the "faster" interface. The other interface is then used as a backup.
- If nor the access concentrator neither the service is specified the router connects to the first AC that answers the query.

In the occasion of a DSLoL interface the same entries as for the DSL interface are valid. The entries are made in the Broadband-Peers list.

7.3.2 Layer list

With a layer, a collection of protocol settings are defined, which should be used when connecting to specific remote stations. The list of the communication layers can be found under:

Configuration tool	List
LANconfig	Communication ▶ General ▶ Communication layers
WEBconfig	Expert Configuration ▶ Setup ▶ WAN ▶ Layer-list
Terminal/Telnet	`cd /setup/WAN` `module/ set layer-list [...]`

In the communication layer list the common protocol combinations are already predefined. Changes or additions should only be made when remote stations are incompatible to the existing layers. The possible options are contained in the following list.

Please note that the parameters located in LANCOM depend upon the functionality of the unit. It is possible that your unit does not offer all of the options described here.

Parameter	Meaning	
Layer name	The layer is selected in the peer list under this name.	
Encapsulation	Additional encapsulations can be set for data packets.	
	'Transparent'	No additional encapsulations.
	'Ethernet'	Encapsulation in the form of ethernet frames.
	'LLC-MUX'	Multiplexing via ATM with LLC/SNAP encapsulation according to RFC 2684. Several protocols can be transmitted over the same VC (Virtual Channel).
	'VC-MUX'	Multiplexing with ATM by establishing additional VCs according to RFC 2684.
Layer-3	The following options are available for the switching layer or network layer:	
	'Transparent'	No additional header is inserted.
	'PPP'	The connection is established according to the PPP protocol (in the synchronous mode, i.e. bit-oriented). The configuration data are taken from the PPP table.
	'AsyncPPP'	Like 'PPP', only the asynchronous mode is used. This means that PPP functions character-oriented.
	'... with script'	All options can be run with their own script if desired. The script is specified in the script list.
	'DHCP'	Assignment of the network parameters via DHCP.

Parameter	Meaning	
Layer-2	In this field the upper section of the security layer (Data Link Layer) is configured. The following options are available:	
	'Transparent'	No additional header is inserted.
	'PPPoE'	Encapsulation of the PPP protocol information in ethernet frames.
	'PPPoE'	The PPP negotiation runs via Ethernet. The PPP packets are encapsulated in Ethernet frames for this purpose. This process is frequently used for DSL connections.
Options	Here you can activate the compression of the data to be transmitted and the bundling of channels. The selected option only becomes active when it is supported by both the ports used and the selected Layer-2 and Layer-3 protocols. For further information see section 'ISDN Channel bundling with MLPPP' → page 154.	
Layer-1	In this field the lower section of the security layer (Data Link Layer) is configured. The following options are available:	
	'AAL-5'	ATM adaptation layer
	'ETH-10'	Transparent Ethernet as per IEEE 802.3.
	'HDLC'	Securing and synchronization of the data transfer as per HDLC (in the 7 or 8-bit mode).
	'V.110'	Transmission as per V.110 with a maximum of 38,400 bps.
	Modem	Modem transmission (requires Fax Modem option)

7.4 IP masquerading

One of today's most common tasks for routers is connecting the numerous workstation computers in a LAN to the network of all networks, the Internet. Everyone should have the potential to access, for example, the WWW from his workstation and be able to fetch bang up-to-date information for his work. ´

So that not every single computer with it's IP address in known on the entire internet "IP masquerading" is used to hide all computers located in an intranet. IP masquerading demands two points from a router: On the one hand a valid IP address in the local network, on the other hand a valid and public IP address in the internet (static or assigned by the provider).

Because these two addresses are not allowed to exist in one logical net, the router must have two IP addresses:

- the intranet IP address to communicate with computers in the LAN
- the public IP address to communicate with remote stations in the Internet

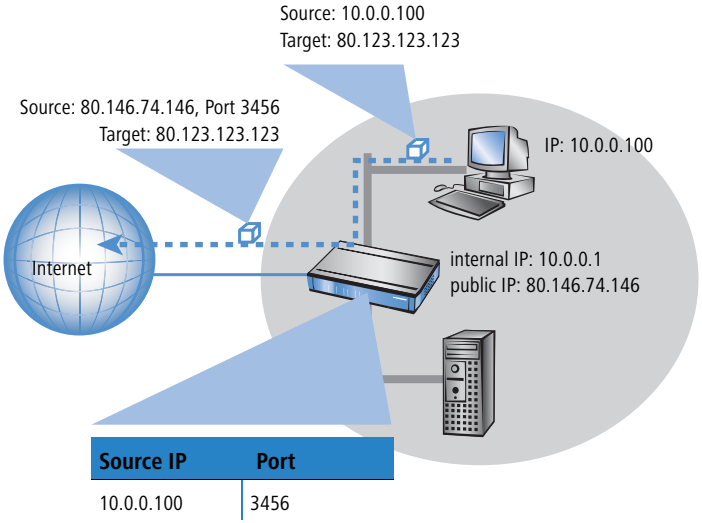
The computers in the LAN use the router as a gateway but are recognizable themselves. The router divides the intranet from the internet.

7.4.1 Simple masquerading

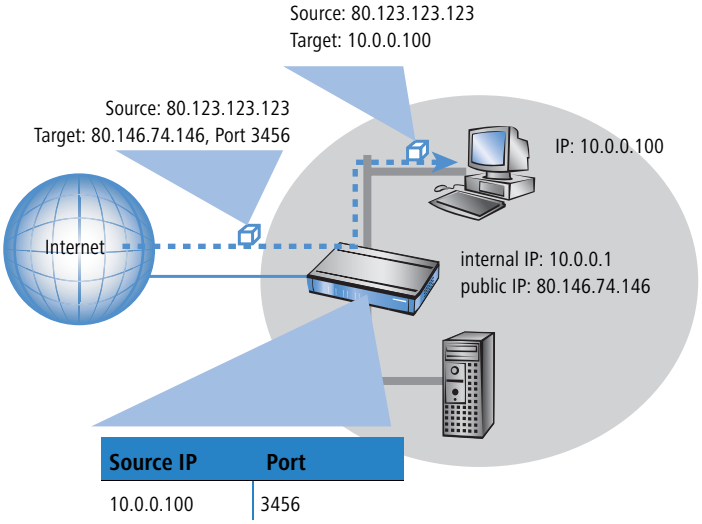
How does IP masquerading work?

Masquerading makes use of a characteristic of TCP/IP data transmission, which is to use port numbers for destination and source as well as the source and destination addresses. When the router receives a data packet for transfer it

now notes the IP address and the sender's port in an internal table. It then gives the packet its unique IP address and a new port number, which could be any number. It also enters this new port on the table and forwards the packet with the new information.



The response to this new packet is now sent to the IP address of the router with the new sender port number. The entry in the internal table allows the router to assign this response to the original sender again.



Which protocols can be transmitted using IP masquerading?

IP masquerading for all IP protocols that are based on TCP, UDP, or ICMP and communicate exclusively through ports. One example of this type of uncomplicated protocol is the one the World Wide Web is based on: HTTP.

Individual IP protocols do use TCP or UDP, but do not, however communicate exclusively through ports. This type of protocol calls for a corresponding special procedure for IP masquerading. Among the group of protocols supported by IP masquerading in the LANCOM are:

- FTP (using the standard ports)
- H.323 (to the same extent as used by Microsoft Netmeeting)
- PPTP
- IPSec
- IRC

Configuration of IP masquerading

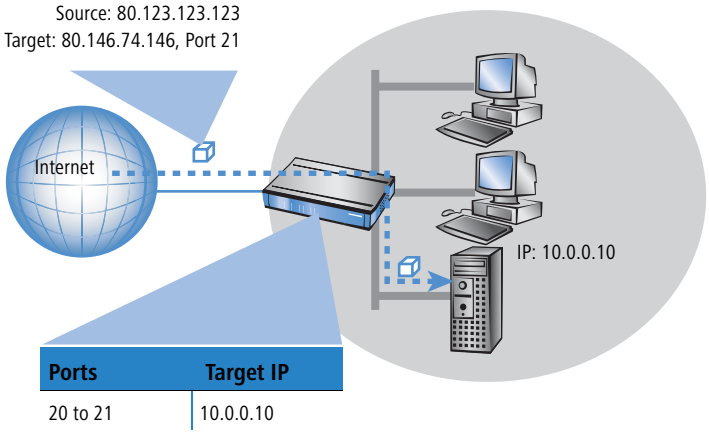
The use of IP masquerading is set individually for each route in the routing table. The routing table can be reached as follows:

Configuration tool	Run
LANconfig	IP router ▶ Routing ▶ Routing table
WEBconfig	Expert Configuration ▶ Setup ▶ IP-router IP-routing-table
Terminal/Telnet	`/setup/IP-router/IP-routing-table`

7.4.2 Inverse masquerading

(simple masquerading has the effect, that all IP addresses in the local network are masked behind the IP address of the router. But when using simple masquerading if a certain computer on the LAN is supposed to be available for stations on the internet (e.g. FTP server) the IP address of the FTP server is not visible either. A connection to this FTP server from the internet in not possible.

To enable the access to such a server ('exposed host') in the LAN, the IP address of the FTP server must be entered with all services that are also supposed to be available from outside the LAN. If a computer sends a packet from the Internet to, for example, an FTP server on the LAN , from the point of view of this computer the router appears to be the FTP server. The router reads the IP address of the FTP server in the LAN from the entry in the service table. The packet is forwarded to this computer. All packets that come from the FTP server in the LAN (answers from the server) are hidden behind the IP address of the router.



The only small difference is that:

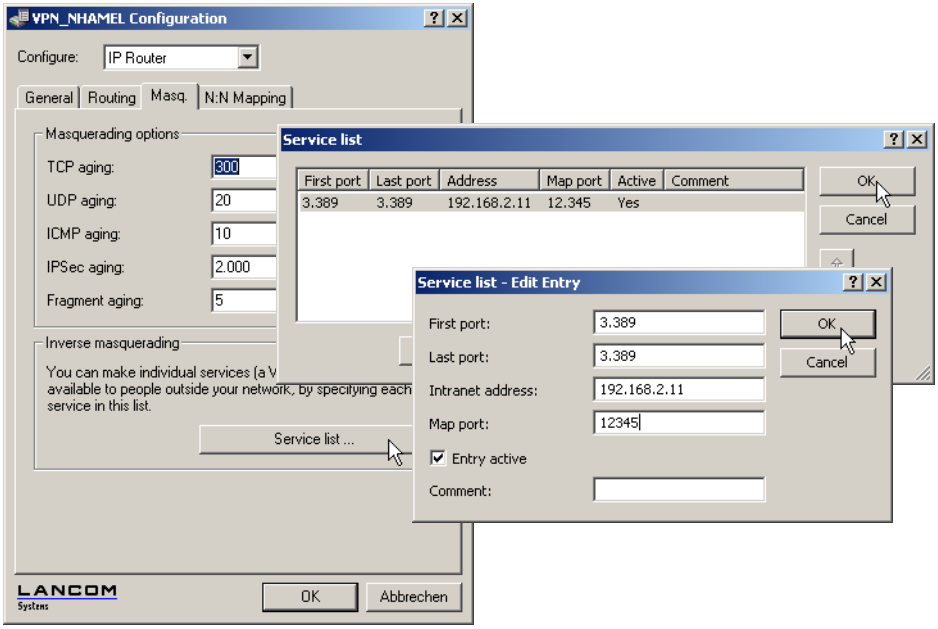
- Access to a service (port) in the intranet from outside must be defined in advance by specifying a port number. The destination port is specified with the intranet address of, for example, the FTP server, in a service table to achieve this.
- When accessing the Internet from the LAN, on the other hand, the router itself makes the entry in the port and IP address information table.

The table concerned can hold up to 2048 entries, that is it allows 2048 **simultaneous** transmissions between the masked and the unmasked network.

After a specified period of time, the router, however, assumes that the entry is no longer required and deletes it automatically from the table.

Configuration of the inverse masquerading

The service table for setting inverse masquerading can be reached in LANconfig in the configuration area 'IP Router' on the tab 'Masq.'.



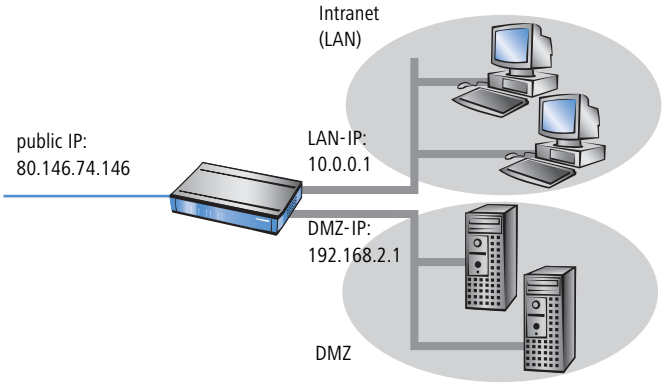
Under WEBconfig or Telnet the parameters for setting inverse masquerading can be found as follows.

Configuration tool	Run
WEBconfig	Expert Configuration ▶ Setup ▶ IP-router ▶ Masquerading ▶ Service-table
Terminal/Telnet	`/setup/IP-router/masquerading/ service-table`

Stateful Inspection and inverse masquerading: If in the Masquerading module a port is exposed (i.e. all packets received on this port should be forwarded to a server in the local area network), then this requires with a Deny All Firewall strategy an additional entry in the Stateful Inspection Firewall, which enables the access of all stations to the respective server.

7.4.3 De-Militarized Zone (DMZ)

Locally the router can manage two different IP address sections: the intranet (LAN) and the 'De-Militarized Zone' (DMZ). The DMZ has it's own area, which is used for reachable servers in the internet.



The option **Masq.** in the Service list informs the router, if the local intranet or DMZ addresses should be hidden behind the IP address of the router:

- **IP Masquerading switched off:** No masquerading is performed. This variation is for internet accesses with several static IP addresses (enter under DMZ IP address and DMZ netmask) to link only servers to the internet or e.g. to link two intranet subnets via VPN.
- **masking Intranet and DMZ (default):** This setting has the effect, that all local addresses are masked. Additionally to the Intranet (LAN) a second local net with private addresses can be linked to the Internet.
- **masking Intranet only:** This setting is especially for the internet access with several static IP addresses. The difference to the case 'IP Masquerading switched off' is that besides the DMZ the intranet address section with masked private IP addresses is available in the LAN.

The DMZ and the intranet addresses of the LANCOM are set as follows:

Configuration tool	Run
LANconfig	TCP/IP ▶ General
WEBconfig	Expert Configuration ▶ Setup ▶ TCP-IP
Terminal/Telnet	`/setup/TCP-IP`

7.4.4 Unmasked Internet access for server in the DMZ

While the inverse masquerading described in the proceeding paragraph allows to expose at least one service of each type (e.g. one Web, Mail and FTP server), this method is bound to some restrictions.

- The masquerading module must support and 'understand' the particular server service of the 'exposed host'. For instance, several VoIP servers use proprietary, non-standard ports for extended signalling. Thus such server could be used on unmasked connections solely.

- From a security point of view, it must be considered that the 'exposed host' resides within the LAN. When the host is under control of an attacker, it could be misused as a starting point for further attacks against machines in the local network.

In order to prevent attacks from a cracked server to the local network, some LANCOM provide a dedicated DMZ interface (LANCOM 7011 VPN) or are able to separate their LAN ports on Ethernet level by hardware (LANCOM 821 ADSL/ISDN, LANCOM 1511 DSL, LANCOM 1521 ADSL, LANCOM 1621 ADSL/ISDN, LANCOM 1711 VPN, LANCOM 1811 DSL and LANCOM 1821 ADSL).

Two local networks - operating servers in a DMZ

This feature requires an Internet access with multiple static IP addresses. Please contact you ISP for an appropriate offer.

Example: You are assigned the IP network address 123.45.67.0 with the netmask 255.255.255.248 by your provider. Then you can assign the IP addresses as follows:

DMZ IP address	Meaning/use
123.45.67.0	network address
123.45.67.1	LANCOM as a gateway for the **Intranet**
123.45.67.2	Device in the LAN which is to receive unmasked access to the Internet, e.g. web server connected at the **DMZ** port
123.45.67.3	broadcast address

All computers and devices in the Intranet have no public IP address, and therefore appear with the IP address of the LANCOM (123.45.67.1) on the Internet.

Separation of Intranet and DMZ

Although Intranet and DMZ may be already separated on a Ethernet level by distinct interfaces, an appropriate Firewall rules must be set up in any case so that the DMZ is being separated from the LAN on the IP level as well.
Thereby, the server service shall be available from the Internet and from the Intranet, but any IP traffic from the DMZ towards the Intranet must be prohibited. For the above example, this reads as follows:

- With a 'Allow All' strategy (default): Deny access from 123.45.67.2 to "All stations in local network"
- With a 'Deny All' strategy (see 'Set-up of an explicit "Deny All" strategy' → page 200): Allow access from "All stations in local network" to 123.45.67.2

7.5 Demilitarized Zone (DMZ)

A demilitarized zone (DMZ) makes certain routers in a network accessible from the Internet. These computers in the DMZ are generally used to offer Internet services such as e-mail or similar services. The rest of the network should of course be unaccessible for attackers on the Internet.

In order to allow this architecture, data traffic between the three zones Internet, DMZ and LAN must be analyzed by a firewall. The firewall's tasks can also be consolidated in a single device (router). For this, the router needs three interfaces that can be monitored separately from each other by the firewall:

- LAN interface
- WAN interface
- DMZ interface

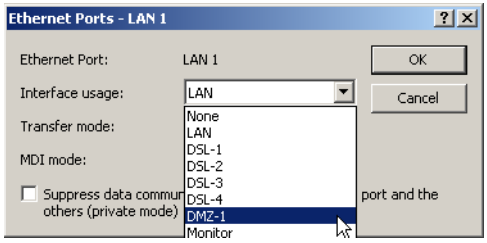
The 'Overview of functions by model and LCOS* versionn' → page 591 table lists which devices support this functionality.

7.5.1 Assigning interfaces to the DMZ

To configure the DMZ the corresponding interface is defined as the DMZ interface.

Configuration with LANconfig

Ethernet ports are defined in LANconfig in the configuration area 'Interfaces' on the 'LAN' tab under 'Ethernet ports'.



Configuration with WEBconfig, Telnet or SSH

Under WEBconfig, Telnet or SSH client you will find the settings for the Ethernet ports under the following paths:

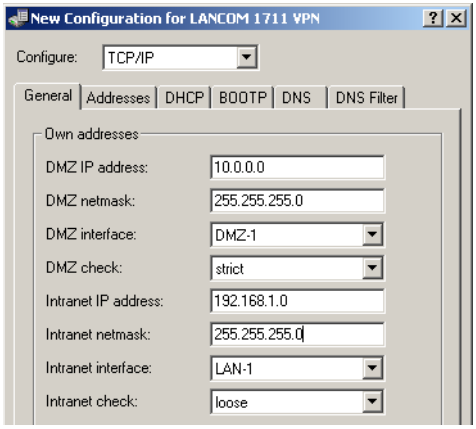
Configuration tool	Menu/Table
WEBconfig	Expert Configuration ▶ Setup ▶ Interfaces ▶ LAN
Terminal/Telnet	`Setup/Interfaces/LAN`

7.5.2 Assigning network zones to the DMZ

Various network zones (address ranges) are assigned to the DMZ and the LAN using the address settings. Depending on availability, WLAN interfaces can also be selected.

Configuration with LANconfig

Addresses can be defined in LANconfig in the configuration area 'TCP/IP' on the 'General' tab.



Configuration with WEBconfig, Telnet or SSH

Under WEBconfig, Telnet or SSH client you will find the settings for the Ethernet ports under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ TCP-IP
Terminal/Telnet	`Setup/TCP-IP`

7.5.3 Address check with DMZ and intranet interfaces

To shield the DMZ (demilitarized zone) and the Intranet from unauthorized attacks, you can activate an additional address check for each interface using the firewall's Intrusion Detection System (IDS).

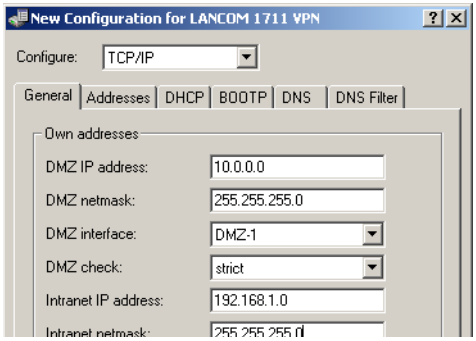
The relevant buttons are called 'DMZ check' or 'Intranet check' and can have the values 'loose' or 'strict':

- If the button is set to 'loose', then every source address is accepted if the LANCOM is addressed directly.
- If the switch is set to 'strict', then a return route has to be explicitly available so that no IDS alarm is triggered. This is usually the case if the data packet contains a sender address to which the relevant interface can also route data. Sender addresses from other networks to which the interface cannot route, or sender addresses from its own address range therefore lead to an IDS alarm.

For all devices, the default is 'loose'. The default is set to 'strict' for LANCOM 7011 VPN only, as a more precise address check has already already been used for this device.

Configuration with LANconfig

You will find the button for activating the DMZ and Intranet address check in LANconfig in the 'TCP-IP' configuration area on the 'General' tab page.



Configuration with WEBconfig, Telnet or SSH

Under WEBconfig, Telnet or SSH client you will find the settings for activating the DMZ and Intranet address check under the following paths:

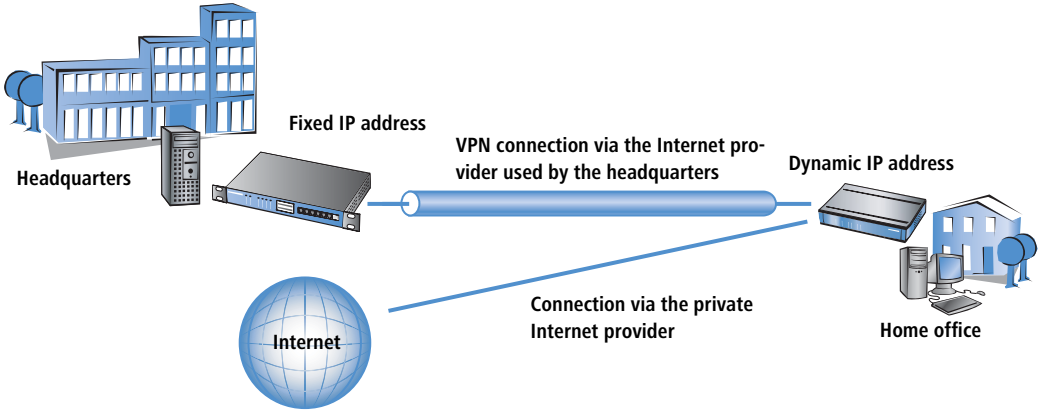
Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ TCP-IP
Terminal/Telnet	`Setup/TCP-IP`

7.6 Multi-PPPoE

In most cases just one connection at a time is established over a DSL or ADSL WAN interface. However, there are applications where it makes sense to use multiple parallel connections on the WAN interface. LANCOM devices with a DSL or ADSL interface can establish up to eight different channels in parallel in the WAN using the same physical interface.

7.6.1 Example application: Home office with private Internet access

One possible application is the home office used by sales personnel who need access to the network at the headquarters via a VPN connection. The company pays for the VPN connection, the employee in the home office pays for Internet access privately.



To ensure a clean separation of the data links, two Internet connections are established, one to each provider. In the IP routing table, the default route is assigned to the private provider; the network with the headquarters via the VPN connection is routed over the headquarters' provider.

7.6.2 Configuration

The configuration of this scenario involves the following steps with the home-office router:

- Configuration of the private Internet access, for example with the LANconfig Wizard or with WEBconfig.
- Configuration of the Internet access that is invoiced to the headquarters.
- Selection of the private provider for the default route in the IP routing table (e.g. manually with LANconfig or with the Wizard for selecting Internet providers in WEBconfig.
- Configuration of the VPN connection to the network at the headquarters.
- Allocation of the VPN connection to the headquarters' provider.

  To ensure that the data traffic for the headquarters is routed via the desired Internet provider, one more entry in the IP routing table is required. Here, the VPN gateway at the headquarters is entered along with its fixed IP address and appropriate netmask, and is forwarded to the remote site used by the headquarters' provider.

It is important that the route to the Internet provider used by the headquarters is masked; otherwise the LANCOM would apply the LAN address and not the WAN address, and the connection would never be established.

Further information about these steps in the configuration are to be found in the documentation for your LANCOM device.

Administrator rights for the employee in the home office: To avoid the employee making accidental changes to the settings for the Internet provider or VPN access, he should be assigned with the WEBconfig function rights for the "Internet connection" and "Selection of Internet provider" Wizards only. Information

about the configuration of special user rights can be found in this addendum under 'Managing rights for different administrators' → page 43.

Use the necessary filter rules in the area 'Firewall/QoS' to ensure that the Internet traffic is not accidentally directed via the network at the headquarters.

7.7 Load balancing

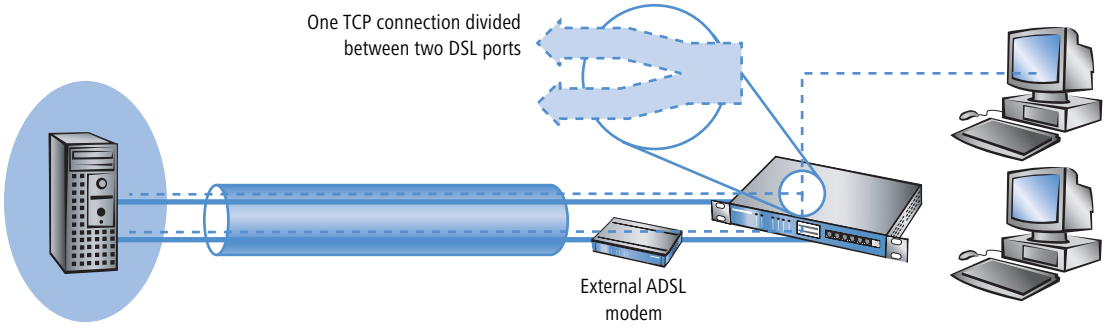
Despite the ever increasing bandwidth of DSL connections, they remain the communications bottle-neck. In some cases it can be advisable to combine multiple DSL connections. There are a number of possibilities to realize this, some of which need active support from the Internet provider:

- DSL channel bundling (Multilink-PPPoE – MLPPPoE)

  The availability of direct bundling depends on the Internet provider's product range. If available, the user has access to the sum of the bandwidths of all of the bundled channels. Multilink-PPPoE can also be used for bundling PPP connections.

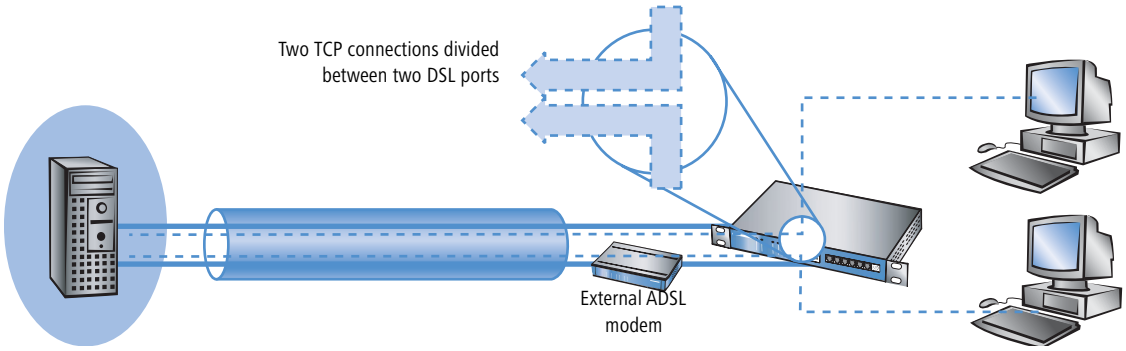
This version of channel bundling provides bandwidths that are a multiple of the smallest bundled channel. This means that it is especially efficient when channels are all of the same bandwidth. The direct bundling of different bandwidths means that the channels with the higher data rates suffer from a loss in effective bandwidth.

When bundling MLPPPoE for DSL channels behaves in the same way as the well known MLPPP for ISDN channel bundling ('ISDN Channel bundling with MLPPP' → page 154).



- Load balancing

  Load balancing involves the dynamic division of TCP connections between independent DSL connections. The user has access to the sum of the bandwidths of the bundled channels, but the individual TCP connections are limited to the bandwidth offered by the DSL connection allocated to it.



Unlike direct channel bundling, load balancing offers the true sum of all bundled bandwidths. This version is thus highly effective for combining different bandwidths.

7.7.1 DSL port mapping

A basic requirement for DSL channel bundling is the support of more than one DSL interface per device. This means that one or more external DSL modems are connected to the switch of a LANCOM router.

Please refer to the feature table in the appendix ('Overview of functions by model and LCOS* versionn' → page 591) to see if your device supports the connection of external DSL modems.

Allocation of switch ports to the DSL ports

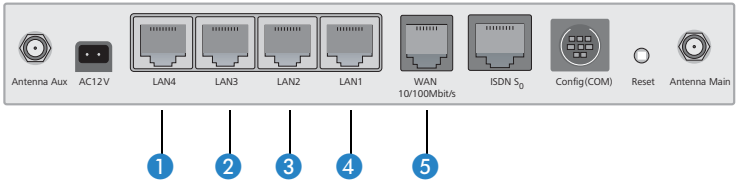
Depending on the mode ('Overview of functions by model and LCOS* versionn' → page 591), devices with an integrated switch can enable some of the LAN ports to be used as additional WAN ports for connecting to external DSL modems. These ports are listed in the interface table as separate DSL interfaces (DSL-1, DSL-2, etc.). The DSL ports are activated as DSL interfaces in teh WAN interfaces list, configured with the up- and downstream rates and allocated to the switch ports in the LAN interfaces list (example: LANCOM Wireless 1811DSL):

Port	Allocation	Connectors	MDI mode	Private mode
LAN -1	LAN -1	Auto	Auto	No
LAN -2	LAN -1	Auto	Auto	No
LAN -3	LAN -1	Auto	Auto	No
LAN -4	LAN -1	Auto	Auto	No
WAN	DSL-1	Auto	Auto	No

- The column 'Port' contains the description of the associated port as marked on the back cover of the device.
- The utilization of the port is listed In the column 'Allocation':

- □ None: The port is deactivated
- □ LAN-1: The port is allocated to the LAN
- □ DSL-1, DSL-2, ... : The port is allocated to one of the DSL interfaces
- □ Monitor: The port is a monitor port, i.e. everything received at the other ports is output via this port. A packet sniffer such as Ethereal can be connected to this port, for example.

The allocation of DSL ports to the Ethernet ports can be chosen freely. An effective solution is to allocate the DSL ports in the reverse order to the ports at the switch (for example: LANCOM Wireless 1811 DSL):



1. LAN4 ▷ DSL-2
2. LAN3 ▷ DSL-3
3. LAN2 ▷ DSL-4
4. LAN1 ▷ LAN-1: This port remains reserved for the LAN.
5. WAN ▷ DSL-1: (dedicated WAN port for the device)

If the device is equipped with more than one DSL port, the DSL port to be used is entered in the DSL-Broadband-Peers list:

- If no port is defined (or port "0"), the LANCOM selects the port after the one chosen for the connection's communication layer.
  - □ If Layer-1 is set with 'AAL-5', then the ADSL interface is chosen.
  - □ If Layer-1 is set with 'ETH', then the first DSL port (i.e. DSL-1) is chosen.
- If a particular port is defined (not "0"), then it will be used for the connection.

Observe that the communication layer set for the connection over this port in Layer 1 is set to 'ETH'.

- To enable channel bundling via multiple DSL interfaces, the appropriate ports are entered into the peer list for the remote station (as a comma-separated port list '1,2,3' or as a port range '1-3'). With a port list, the bundled channels will be established in the given order; only in case of error will the channels be tested in ascending order. With a port range, the channels are always established in ascending order.
  - □ In the list of Ethernet ports, the ports must be switched to DSL port.
  - □ In the layer used for the connection, a bundling method has to be activated that is also supported at the remote site.

- To configure channel bundling for an internal ADSL interface, the ADSL port '0' is entered into the list of ports **at the top of the list** (e.g. '0,1,2,3' as port list or '0-3' as port range). In the remote device, the communications layer must be set to Layer 1 'AAL-5'.

An entry in the peer list can contain various ports (e.g. ADSL and Ethernet), but it can only reference **one** communications layer in which just **one** layer-1 protocol can be defined. For bundled communications over ADSL and Ethernet ports, however, **two** different layer-1 protocols are required. For this reason, layer 1 is set to 'AAL-5' in these cases. As only one ADSL interface can exist in the devices, all of the interfaces bundled into this are automatically changed to layer 1 with 'ETH' for Ethernet DSL ports. This automatic change of the layer can only succeed if the ADSL interface is the first one to be selected for bundled connections.

- For devices with a built-in ADSL modem and an additional Ethernet interface (DSL or DSLoL), it is clear which ports are used for bundling. In this case it is not necessary to enter the ports into the peer list. These devices always internally assume a port list '0,1' so that the internal ADSL interface is the first one to be used for bundling.

For Multi-PPPoE ('Multi-PPPoE' → page 129), multiple PPPoE connections share one physical DSL connection. With Multi-DSL, several PPPoE connection are divided between the available DSL interfaces. The maximum possible number of parallel connections is limited to 8 channels.

Allocation of MAC addresses to the DSL ports

If a LANCOM uses switch ports to gain access to multiple DSL(WAN) interfaces, an appropriate number of MAC addresses must be used to differentiate the DSL ports. As there are cases where the required MAC address depends upon the remote station which, for example, uses the MAC address to determine the DSL access charge, the MAC addresses are defined for the logical DSL remote stations and not for the physical DSL ports.

The following options are available for setting the MAC address:

- Global: Global system MAC address
- Local: The unique, locally managed MAC address is calculated from the global address
- User defined: A MAC address that can be freely defined by the user

Every DSL connection contains its own MAC address. If two remote stations are configured with identical MAC addresses, the first connection uses the configured MAC address. For the second connection a "locally managed", unambiguous MAC address will be calculated from the user-defined MAC address.

When using channel bundling, the configured MAC address is used for the first connection, for all other bundle connections the locally managed MAC addresses based on the user-defined MAC address will be calculated.

If one of your connections is charged via the MAC address, configure this MAC address for the separately charged connection only. For all other connections you should use another address.

7.7.2 Direct DSL channel bundling

For the bundling of DSL connections, the DSL ports to be used are entered into the DSL-Broadband-Peers list. Only the number of DSL ports is entered, separated by commas if multiple ports are used (1,2,4) or as a range (1-4).

All that is required for PPPoE bundling is to activate bundling in the relevant layer and to use the port list to assign the relevant ports.

7.7.3 Dynamic load balancing

If the Internet provider does not directly support bundling, then multiple normal DSL connections can be coupled with a load balancer. First of all, the DSL accesses are set up for the necessary DSL ports. These are then coupled with a load-balancing table. This list assigns a virtual balancing connection (the connection that is entered into the routing table) to the other real DSL connections (bundle connections). Depending on the number of available DSL ports, several bundle connections can be assigned to one balancing connection.

The balancing connection is entered as a "virtual" connection. No access data or similar has to be entered for this connection. The entry merely serves as a "distributor" which uses the load-balancing table to assign several "real" bundled connections to an entry in the routing table.

DSL bundling is a static bundling. Any additional channels are **not** opened or closed according to the demand from data transfer volumes.

With load balancing, decisions about the routing of data packets can no longer be made simply based on the IP addresses because the individual bundled DSL connections all have different IP addresses. Thus load balancing also considers the information in the firewall connection list. This list has an entry for every established TCP connection, and for load balancing the list is supplemented with information about the DSL port used.

Connection establishment

A request for data transmission to a balancing remote station initially prompts the **first** bundle connection from the load balancing table to be established. Further progress depends upon the success of this connection establishment:

- If the connection is successfully established, the first step is the assignment of all pending TCP connections to this channel. Subsequently, all of the configured bundle connections will successively be established. As soon as at least two bundle connections are active, new TCP connections will be divided among the active bundle connections.
- Should establishment of the bundling connection fail, then attempts will be made to establish other bundle connections one after the other. As soon as one of the bundle connections is established, all of the pending TCP connections will be directed to this channel.

Spreading the data load

Two basic methods are available for balancing the data load:

- If the channel's bandwidth is known, then the connections will be assigned to the channel with the lowest workload (in percent).
- If the bandwidth is not known, then a differentiation is made according to the type of connection required; a TCP connection; or VPN or PPTP connections from the LANCOM.
  - If a TCP connection requests a channel, then the one with the lowest absolute workload will be chosen.
  - If a VPN or PPTP connection requests a channel, then the connections will be equally spread between all available channels.

For the most effective use of load balancing, the bandwidth should be entered into the list of WAN interfaces under LANconfig in the configuration area 'Interface' on the 'WAN' tab under the button **Interface settings** (Telnet: `/Setup/Interfaces/DSL`, WEBconfig: **Expert configuration ▶ Setup ▶ Interfaces ▶ DSL**).

7.7.4 Static load balancing

Apart from the dynamic choice of connection outlined in the previous section, there are possible scenarios where certain TCP connections should always make use of the same DSL connection. Two cases are to be considered here:

- A server with a fixed IP address can only be contacted via a dedicated connection. All that is required for the selection here is the destination IP address.
- A server uses a protocol that requires a control channel and other channels for data transfer (e.g. FTP, H.323, PPTP). In establishing the data channels, servers accept only the same IP address as that used by the control channel.

Destination-based channel selection

Destination-based channel selection is handled by an entry in the routing table that directly uses one of the bundle connections to reach the destination instead of using the virtual balancing connection.

Policy-based routing

Suitable entries can be made in the firewall to select channels according to the destination port or the source address. These entries are supplemented with a special routing tag that is used to control the channel selection with the routing table ('Policy-based routing' → page 109).

7.7.5 Configuration of load balancing

For the following configurations we assume that the remote devices are already set up with all necessary access data.

Direct channel bundling via PPPoE

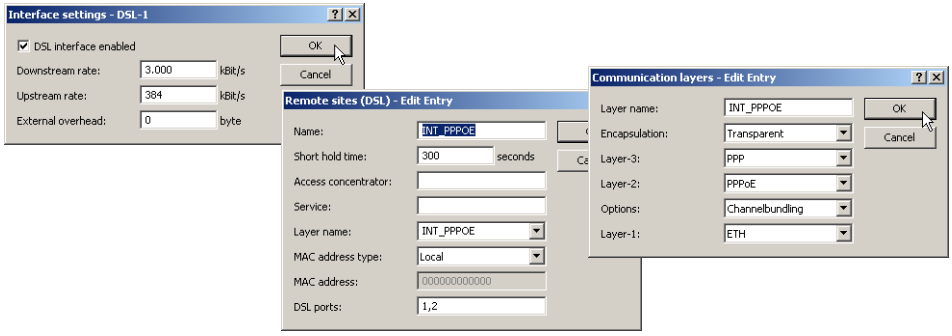
The following method is for the configuration of channel bundling via PPPoE:

① Assign the DSL ports to the required Ethernet ports, in LANconfig via **Interfaces ▶ LAN ▶ Ethernet-Ports**.
Telnet: `/Setup/Interfaces/Ethernet-ports`
WEBconfig: **Expert configuration ▶ Setup ▶ Interfaces ▶ Ethernet ports**

② Activate the additional DSL interfaces in LANconfig via **Interfaces ▶ WAN ▶ Interface settings**. Enter the data rates for up- and downstream.
Telnet: `/Setup/Interfaces/DSL`
WEBconfig: **Expert configuration ▶ Setup ▶ Interfaces ▶ DSL**

③ For the required remote station, enter the DSL ports that are to be used in LANconfig via **Communication ▶ Remote sites ▶ Remote sites (DSL)**.
Telnet: `/Setup/WAN/DSL-broadband-peers`
WEBconfig: **Expert configuration ▶ Setup ▶ WAN ▶ DSL-broadband-peers**

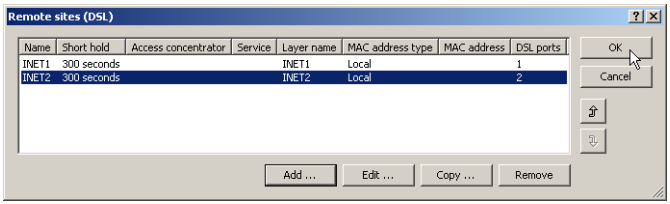
④ Actitivate channel bundling for the relevant layers in LANconfig via **Communication ▶ General ▶ Communication layers**.
Telnet: `/Setup/WAN/Layer`
WEBconfig: **Expert configuration ▶ Setup ▶ WAN ▶ Layer**



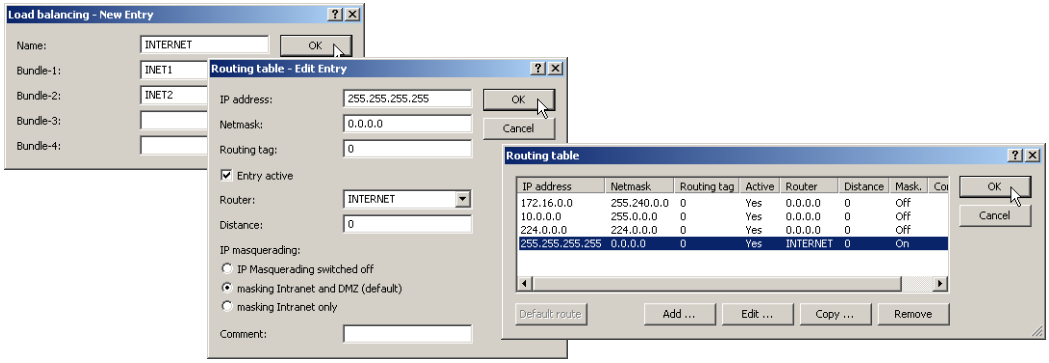
Dynamic load balancing with multiple DSL connections

The first step in setting up dynamic load balancing is to define the Internet accesses, e.g. 'INET1' and 'INET2', with the aid of the LANconfig Wizard.

① To distribute Internet traffic across different DSL interfaces, the individual remote stations are assigned to different DSL ports in LANconfig under **Communication ▶ Remote sites ▶ Remote sites (DSL)**.
Telnet: `/Setup/WAN/DSL-broadband-peers`
WEBconfig: **Expert configuration ▶ Setup ▶ WAN ▶ DSL-broadband-peers**



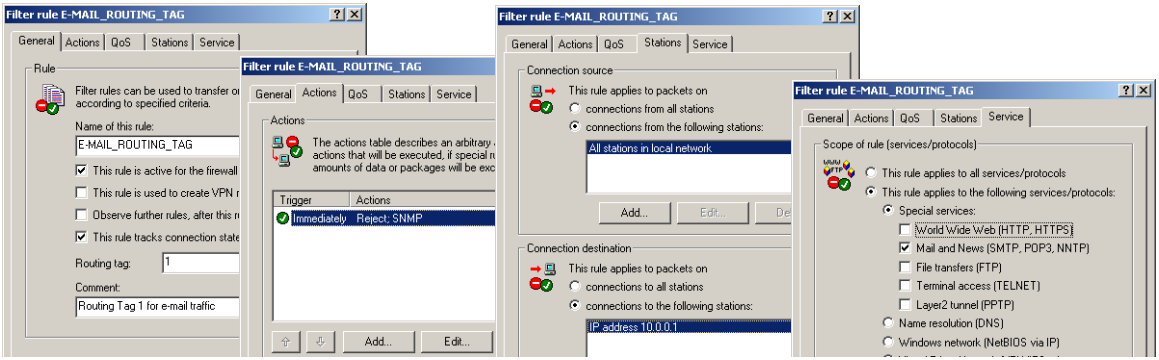
② The two DSL remotes are the assigned to a new virtual remote site 'INTERNET' in the load balancing list in LANconfig via **IP router ▶ Routing ▶ Load balancing**.
Telnet: `/Setup/IP-router/Load-balancer`
WEBconfig: **Expert configuration ▶ Setup ▶ IP router ▶ Load balancer**



③ The virtual remote site is entered into the routing table as the router for the default route in LANconfig via **IP router ▶ Routing ▶ Routing table**.
Telnet: `/Setup/IP-router/IP-routing-table`
WEBconfig: **Expert configuration ▶ Setup ▶ IP router ▶ IP routing table**

The virtual remote site 'INTERNET' is now to be used for Internet access. When data are routed over this connection, the load balancing table will cause the "real" DSL connections to be established and the data will be transmitted over the selected DSL ports.

④ Routing tags can be used for the application-dependent direction of data traffic to specific DSL ports. If, for example, outgoing e-mail traffic is to be routed over a certain DSL interface with a certain IP address, then the appropriate firewall rule must be created that transmits e-mail data traffic from all local stations to the mail server and sets the routing tag to '1'; do this with LANconfig via **Firewall/QoS ▶ Rules**.
Telnet: `/Setup/IP-router/Firewall/Rules`
WEBconfig: **Expert configuration ▶ Setup ▶ IP router ▶ Firewall▶ Rules**.



7.8 N:N mapping

Network Address Translation (NAT) can be used for several different matters:

- for better utilizing the IP4 addresses ever becoming scarcer
- for coupling of networks with same (private) address ranges
- for producing unique addresses for network management

In the first application the so-called N:1 NAT, also known as IP masquerading ('IP masquerading' → page 120) is used. All addresses ("N") of the local network are mapped to only one ("1") public address. This clear assignment of data streams to the respective internal PCs is generally made available by the ports of the TCP and UDP protocols. That's why this is also called NAT/PAT (Network Address Translation/Port Address Translation).

Due to the dynamic assignment of ports, N:1 masquerading enables only those connections, which have been initiated by the internal network. Exception: an internal IP address is statically exposed on a certain port, e.g. to make a LAN server accessible from the outside. This process is called "inverse masquerading" ('Inverse masquerading' → page 122).

A N:N mapping is used for network couplings with identical address ranges. This transforms unambiguously multiple addresses ("N") of the local network to multiple ("N") addresses of another network. Thereby, an address conflict can be resolved.

Rules for this address translation are defined in a static table in the LANCOM. Thereby new addresses are assigned to single stations, parts of the network, or the entire LAN, by which the stations can contact other networks then.

Some protocols (FTP, H.323) exchange parameters during their protocol negotiation, which can have influence on the address translation for the N:N mapping. For a correct functioning of the address translation, the connection information of these protocols are tracked appropriately by functions of the firewall in a dynamic table, and are additionally considered to the entries of the static table.

The address translation is made "outbound", i.e. the source address is translated for outgoing data packets and the destination address for incoming data packets, as long as the addresses are located within the

defined translation range. An "inbound" address mapping, whereby the source address is translated (instead of the destination address), needs to be realized by an appropriate "outbound" address translation on the remote side.

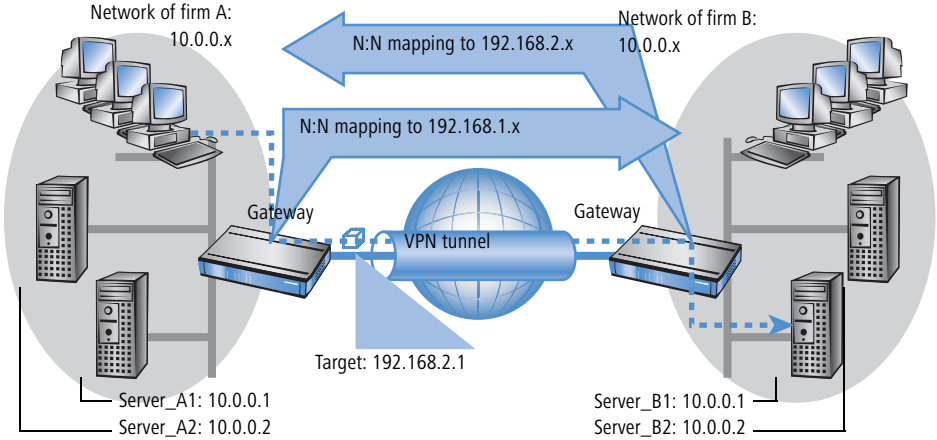
7.8.1 Application examples

The following typical applications are described in this section:

- Coupling of private networks utilizing the same address range
- Central remote monitoring by service providers

Network coupling

An often appearing scenario is the coupling of two company networks which internally use the same address range (e. g. 10.0.0.x). This is often the case, when one company should get access to one (or more) server(s) of the other one:

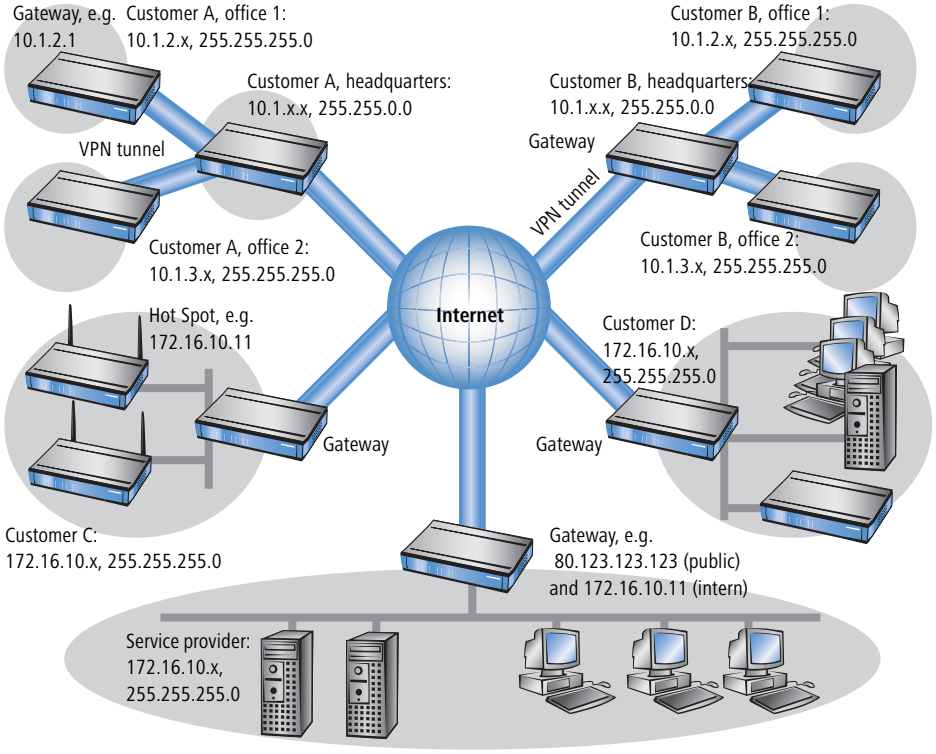


In this example network servers of company A and B should have access over a VPN tunnel to the respective other network. All stations of the LAN should have access to the server of the remote network. For the time being, there is no access possible to the other network, because both networks use the same address range. If one station of the network of company A wants to access server 1 of company B, the addressee (with an address from the 10.0.0.x network) will be searched within the own local network, and the inquiry even does not reach the gateway.

With the help of N:N mapping, all addresses of the LAN can be translated to a new address range for the coupling with the other network. The network of company A e. g. will be translated to 192.168.1.x, the network of company B to 192.168.2.x. Under these new addresses the two LANs are now reachable for the respective other network. The station from the network of company A is now addressing server 1 of company B under the address 192.168.2.1. The addressee does not reside any more within the own network, the inquiry is now passed on to the gateway, and the routing to the other network is working as desired.

Remote monitoring and remote control of networks

Remote maintenance and control of networks become more and more importance because of the possibilities given by VPN. With the use of the nearly ubiquitous broadband Internet connections, the administrator of such management scenarios is no longer dependent of the different data communication technologies or expensive leased lines.



In this example, a service provider monitors the networks of different clients out of a central control. For this purpose, the SNMP-capable devices should send the respective traps of important events automatically to the SNMP trap addressee (e. g. LANmonitor) of the network of the service provider. So the LAN administrator of the service provider has an up-to-date view of the state of the devices at any time.

The individual networks can be structured very differently: Clients A and B integrate their branches with own networks via VPN connections to their LAN, client C operates a network with several public WLAN base stations as hot spots, and client D has got an additional router for ISDN dial-up accesses in his LAN.

The networks of client A and B use different address ranges in the respective head office and the connected branches. A standard network coupling via VPN is therefore possible between these networks.

In order to avoid the effort to building up its own VPN tunnel to each individual subnetwork of the clients A and B, the service provider makes only one VPN connection to the head office, and uses the existing VPN lines between head office and branches for communication with the branches.

Traps from the networks report to the service provider whether e. g. a VPN tunnel has been build up or cut, if an user has been tried to log in three times with a wrong password, if an user has been applied for a hot spot, or if somewhere a LAN cable has been pulled out of a switch.

A complete list of all SNMP traps supported by LANCOM can be found in the appendix of this reference manual ('SNMP Traps' → page 581).

Routing of these different networks reaches very fast its limiting factors, if two or more clients use same address ranges. Additionally, if some clients use the same address range as the service provider as well, further address conflicts are added. In this example, one of the hot spots of client C has got the same address as the gateway of the service provider.

There are two different variants to resolve these address conflicts:

Loopback: decentralized 1:1 mapping

- In the decentralized variant, alternative IP addresses for communicating with the SNMP addressee are assigned to each of the monitored devices by means of an 1:1 mapping. This address is in technical language also known as “loopback address”, the method accordingly as “loopback method”.

The loopback addresses are valid only for communication with certain remote stations on the connections belonging to them. Thus a LANCOM is not generally accessible via this IP address.

Alternative: central N:N mapping

- Even more appealing is the solution of a central mapping: instead of configuring each single gateway in the branch networks, the administrator configures solely one central address translation in the gateway of the head office. On this occasion, also all subnetworks located “behind” the head office are supplied with the needed new IP addresses.

In this example, the administrator of the service provider selects 10.2.x.x as central address translation for the network of client B, so that both networks with actual same address range looks like two different networks for the gateway of the service provider.

The administrator selects the address ranges 192.168.2.x and 192.168.3.x for client C and D, so that the addresses of these networks do differ from the own network of the service provider.

In order to enable the gateway of the provider to monitor the networks of clients C and D, the administrator sets up an address translation to 192.168.1.x also for the own network.

7.8.2 Configuration

Setting up address translation

Configuration of N:N mapping succeeds with only few information. Since a LAN can be coupled with several other networks via N:N, different destinations can have also different address translations for a source IP range. The NAT table can contain 64 entries at maximum, including the following information:

- **Index**: Unambiguous index of the entry.
- **Source address**: IP address of the workstation or network that should get an alternative IP address.
- **Source mask**: Netmask of source range.
- **Remote station**: Name of the remote station over that the remote network is reachable.
- **New network address**: IP address or address range that should be used for the translation.

For the new network address, the same netmask will be used as the source address already uses. For assignment of source and mapping addresses the following hints apply:

- Source and mapping can be assigned arbitrarily for the translation of single addresses. Thus, for example, it is possible to assign the mapping address 192.168.1.88 to a LAN server with the IP address 10.1.1.99.
- For translation of entire address ranges, the station-related part of the IP address will be taken directly, only appended to the network-related part of the mapping address. Therefore, in an assignment of 10.0.0.0/255.255.255.0 to **192.168.1**.0, a server of the LAN with IP address 10.1.1.99 will get assigned the mapping address 192.168.**1.99**.

The address range for translation must be at minimum as large as the source address range.

Please notice that the N:N mapping functions are only effective when the firewall has been activated. ('Firewall/QoS enabled' → page 185)!

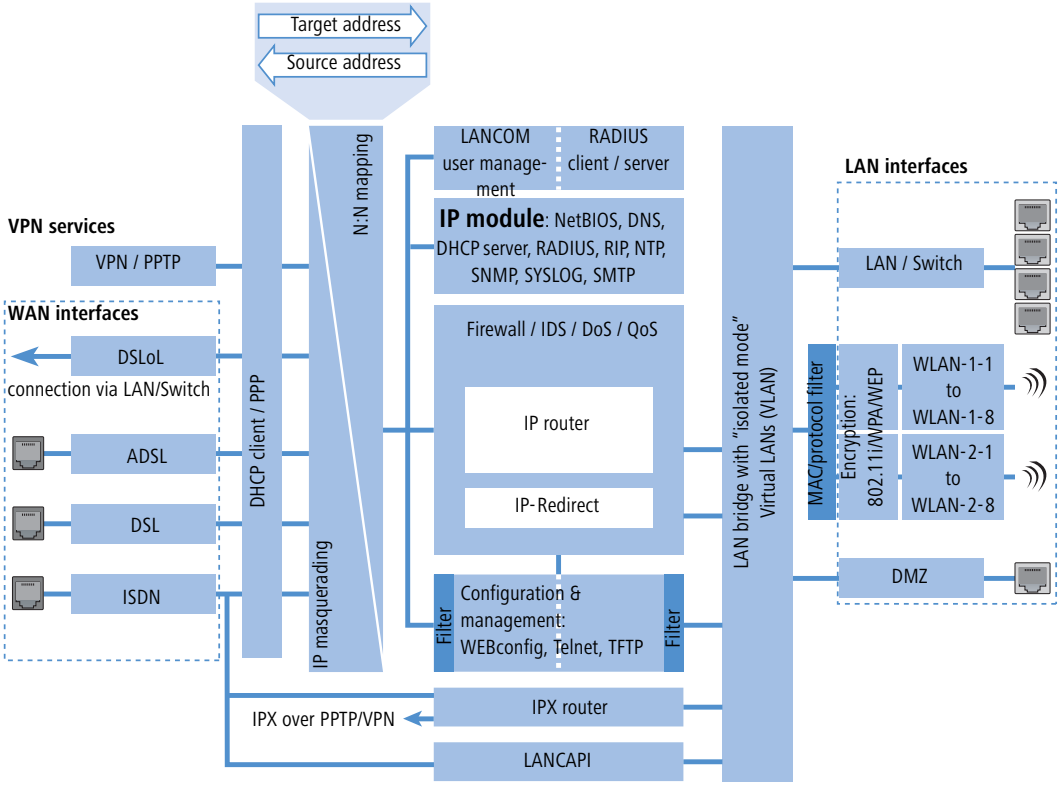
Additional configuration hints

By setting up address translation in the NAT table, the networks and workstations become only visible under another address at first in the higher network compound. But for a seamless routing of data between the networks some further settings are still necessary:

- Entries in the routing tables for packets with new addresses to find the way to their destination.
- DNS forwarding entries, in order that inquiries about certain devices in the respective other networks can be resolved into mapped IP addresses ('DNS forwarding' → page 536).
- The firewall rules of the gateways must be adjusted such that (if necessary) authorized stations resp. networks from the outside are permitted to set up connections.
- VPN rules for loopback addresses in order to transmit the newly assigned IP addresses through an according VPN tunnel.

The IP address translation takes place in the LANCOM between firewall and IP router on one hand, and the VPN module on the other hand. All rules related to the own network use therefore the "unmapped" original addresses. The entries of the remote network use the "mapped" addresses of the remote side, valid on the VPN connection.

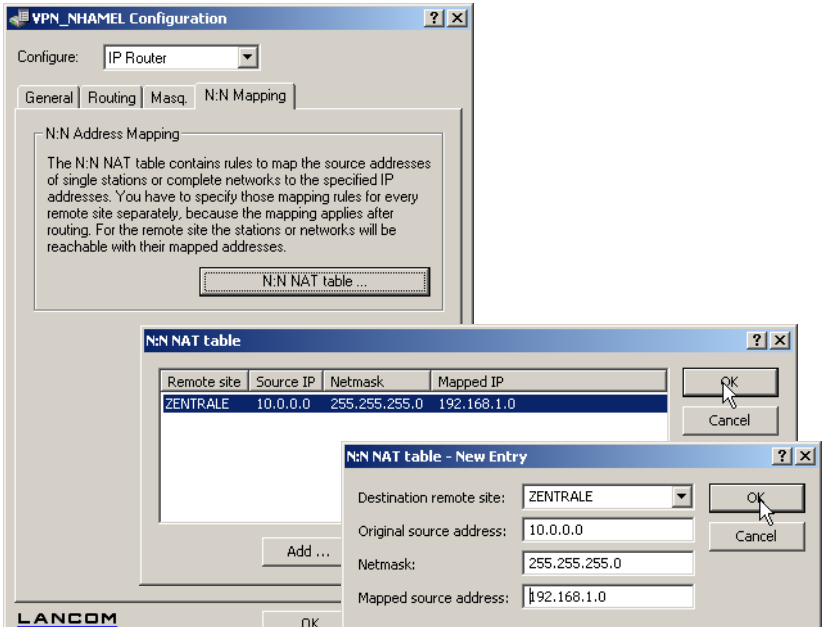
N:N mapping



Configuration with different tools

LANconfig

With LANconfig you adjust the address translation for the configuration range 'IP router' on register card 'N:N-Mapping':



WEBconfig, Telnet

Under WEBconfig and Telnet you find the NAT table for configuration of N:N mapping at the following positions of the menu tree:

Configuration tool	Run
WEBconfig	Expert configuration / Setup / IP router / NAT table
Terminal/Telnet	Setup / IP router / NAT table

When starting a new entry under WEBconfig, the NAT table shows up as follows:

7.9 Establishing connection with PPP

LANCOM Systems routers also support the point-to-point protocol (PPP). PPP is a generic term for a whole series of WAN protocols which enable the interaction of routers made by different manufacturers since this protocol is supported by practically all manufacturers.

Due to the increasing importance of this protocol family and the fact that PPP is not associated with any specific operating mode of the routers, we will be introducing the functions of the devices associated with the PPP here in a separate section.

7.9.1 The protocol

What is PPP?

The point-to-point protocol was developed specifically for network connections via serial channels and has asserted itself as the standard for connections between routers. It implements the following functions:

- Password protection according to PAP, CHAP or MS CHAP
- Callback functions
- Negotiation of the network protocol to be used over the connection established (IP or IPX, for example). Included in this are any parameters necessary for these protocols, for example IP addresses. This process is carried out using IPCP (IP Control Protocol).
- Negotiation of the connection parameters, e.g. the MTU (Maximum Transmission Unit, 'Manual definition of the MTU' → page 165).
- Verification of the connection through the LCP (Link Control Protocol)
- Combining several ISDN or DSL channels (MultiLink PPP resp. MultiLink PPPoE)

PPP is the standard used by router connections for communication between devices or the WAN connection software of different manufacturers. Connection parameters are negotiated and a common denominator is agreed using standardized control protocols (e.g. LCP, IPCP, CCP) which are contained in PPP, in order to ensure successful data transfer where possible.

What is PPP used for?

It is best to use the point-to-point protocol in the following applications:

- for reasons of compatibility when communicating with external routers, for example
- remote access from remote workstations with ISDN cards
- Internet access (when sending addresses)

The PPP which is implemented by LANCOM can be used synchronously or asynchronously not only via a transparent HDLC connection, but also via an X.75 connection.

The phases of PPP negotiation

Establishment of a connection using PPP always begins with a negotiation of the parameters to be used for the connection. This negotiation is carried out in four phases which should be understood for the sake of configuration and troubleshooting.

- Establish phase

  Once a connection has been made at the data communication level, negotiation of the connection parameters begins through the LCP.

  This ascertains whether the remote site is also ready to use PPP, and the packet sizes and authentication protocol (PAP, CHAP, MS-CHAP or none) are determined. The LCP then switches to the opened state.

- Authenticate phase

  Passwords will then be exchanged, if necessary. The password will only be sent once if PAP is being used for the authentication process. An encrypted password will be sent periodically at adjustable intervals if CHAP or MS CHAP is being used.

  Perhaps a callback is also negotiated in this phase via CBCP (Callback Control Protocol).

- Network phase

  LANCOM, supports the protocols IPCP and IPXCP.

  After the password has been successfully transmitted, the IPCP and/or IPXCP network layer can be established.

  IP and/or IPS packets can be transferred from the router modules to the opened line if the negotiation of parameters is successful for at least one of the network layers.

- Terminate phase

  In the final phase the line is cleared, when the logical connections for all protocols are cleared.

PPP negotiation in the LANCOM

The progress of a PPP negotiation is logged in the devices' PPP statistics and the protocol packets listed in detail there can be used for checking purposes in the event of an error.

The PPP trace outputs offer a further method of analysis. You can use the command

```
trace + ppp
```

to begin output of the PPP protocol frames exchanged during a terminal session. You can perform a detailed analysis once the connection has been broken if this terminal session has been logged in a log file.

7.9.2 Everything o.k.? Checking the line with LCP

The devices involved in the establishment of a connection through PPP negotiate a common behavior during data transfer. For example, they first decide whether a connection can be made at all using the security procedure, names and passwords specified.

The reliability of the line can be constantly monitored using the LCP once the connection has been established. This is achieved within the protocol by the LCP echo request and the associated LCP echo reply. The LCP echo request is a query in the form of a data packet which is transferred to the remote station along with the data. The connection is reliable and stable if a valid response to this request for information is returned (LCP echo reply). This request is repeated at defined intervals so that the connection can be continually monitored.

What happens when there is no reply? First a few retries will be initiated to exclude the possibility of any short-term line interference. The line will be dropped and an alternative route sought if all the retries remain unanswered. If, for example, the high-speed connection refuses to work, an existing ISDN port can open the way to the Internet as a backup.

During remote access of individual workstations with Windows operating systems, we recommend switching off the regular LCP requests since these operating systems do not reply to LCP echo requests.

The LCP request behavior is configured in the PPP list for each individual connection. The intervals at which LCP requests should be made are set by the entries in the 'Time' and 'Retr.' fields, along with the number of retries that should be initiated without a response before the line can be considered faulty. LCP requests can be switched off entirely by setting the time at '0' and the retries at '0'.

7.9.3 Assignment of IP addresses via PPP

In order to connect computers using TCP/IP as the network protocol, all participating computers require a valid and unique IP address. If a remote station does not have its own IP address (such as the individual workstation of a telecomputer), the LANCOM assigns it an IP address for the duration of the connection, enabling communications to take place.

This type of address assignment is carried out during PPP negotiation and implemented only for connections via WAN. In contrast, the assignment of addresses via DHCP is (normally) used within a local network.

Assignment of an IP address will only be possible if the LANCOM can identify the remote station by its call number or name when the call arrives, i.e. the authentication process has been successful.

Examples

- Remote access

  Address assignment is made possible by a special entry in the IP routing table. 255.255.255.255 is specified as the network mask as the IP address to be assigned to the remote site in the 'Router-name' field. In this case, the router name is the name, with which the remote site must identify itself to the LANCOM.

  In addition to the IP address, the addresses of the DNS and NBNS servers (Domain Name Server and NetBIOS Name Server) including the backup server from the entries in the TCP/IP module are transmitted to the remote station during this configuration.

So that everything functions properly, the remote site must also be adjusted in such a way that it can obtain the IP address and the name server from the LANCOM. This can be accomplished with Windows dial-up networking through the settings in the 'TCP settings' under 'IP address' and 'DNS configuration'. This is where the options 'IP address assigned by server' and 'Specify name server addresses' are activated.

- Internet access

  If Internet access for a local network is realized via the LANCOM, the assignment of IP addresses can occur in a reverse manner. Configurations are possible in which the LANCOM does not have a valid IP address in the Internet and is assigned one by the Internet provider for the duration of the connection. In addition to the IP address, the LANCOM also receives information via the DNS server of the provider during the PPP negotiation.

  In the local network, the LANCOM is only known by its internal valid intranet address. All workstations in the local network can then access the same Internet account and also reach e.g. the DNS server.

Windows users are able to view the assigned addresses via LANmonitor. In addition to the name of the remote station, the current IP address as well as the addresses of DNS and NBNS servers can be found there. Options such as channel bundling or the duration of the connection are also displayed.

7.9.4 Settings in the PPP list

You can specify a custom definition of the PPP negotiation for each of the remote sites that contact your net.

Configuration tool	List
LANconfig	Communication ▶ Protocols ▶ PPP list
WEBconfig	Expert Configuration ▶ Setup ▶ WAN ▶ PPP-list
Terminal/Telnet	`cd /setup/WAN` `set PPP-list [...]`

The PPP list may have up to 64 entries and contain the following values:

In this column of the PPP list...	...enter the following values:
Remote site (device name)	Name the remote site uses to identify itself to your router.
User name	The name with which your router logs onto the remote site. The device name of your router is used if nothing is specified here.
Password	Password transferred by your router to the remote site (if demanded). An asterisk (*) in the list indicates that an entry is present.
Auth.	Security method used on the PPP connection ('PAP', 'CHAP' or 'none'). Your own router demands that the remote site observes this procedure. Not the other way round. This means that 'PAP', 'CHAP' security is not useful when connecting to Internet service providers, who may not wish to provide a password. Select 'none' as the security attribute for connections such as these.

In this column of the PPP list...	...enter the following values:
Time	Time between two checks of the connection with LCP (see the following section). This is specified in multiples of 10 seconds (i.e. 2 for 20 seconds, for instance). The value is simultaneously the time between two verifications of the connection to CHAP. Enter this time in minutes. The time must be set to '0' for remote sites using a Windows operating system.
Retr.	Number of retries for the check attempt. You can eliminate the effect of short-term line interference by selecting multiple retries. The connection will only be dropped if all attempts are unsuccessful. The time interval between two retries is 1/10 of the time interval between two checks. Simultaneously the number of the "Configure requests" that the router maximum sends before it assumes a line error and clears the connection itself.
Conf, Fail, Term	These parameters are used to affect the way in which PPP is implemented. The parameters are defined in RFC 1661 and are not described in greater detail here. You will find troubleshooting instructions in this RFC in connection with the router's PPP statistics if you are unable to establish any PPP connections. The default settings should generally suffice. These parameters can only be modified via LANconfig, SNMP or TFTP!

7.10 DSL Connection with PPTP

Some DSL providers enable dial-in over PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) instead of PPPoE. PPTP is an extension of PPP, partly developed by Microsoft.

With PPTP it is possible to build up a "tunnel" over IP nets to a remote station. A tunnel is a logical shield connection, that protects the transferred data from unauthorized access. For this purpose the encoding algorithm RC4 is used.

Configuration of PPTP

As soon as the internet access over PPTP is selected the LANCOM enquires all needed PPTP parameters with the Internet Access Wizard. Additionally to the entries for PPPoE access the IP address of the gateway must be specified. A PPTP gateway is often a DSL modem. Detailed information is available from your DSL provider.

The PPTP list for editing the configuration can be reached as follows:

Configuration tool	List
LANconfig	Communication ▶ Protocols ▶ PPTP list
WEBconfig	Expert Configuration ▶ Setup ▶ WAN ▶ PPTP-Peers
Terminal/Telnet	`cd /Setup/WAN/set PPTP-Peers [...]`

The PPTP configuration consists of three parameters:

- 'Remote site'—the entry from the DSL-Broadband-Peers list.
- 'IP address'—IP address of the PPTP gateway, often the address of the DSL modem.
- 'Port'—IP port the PPTP protocol runs on. For conformity with the protocol standard enter the port '1.723'.

7.11 Extended connection for flat rates—Keep-alive

The term flat rate is used to refer to all-inclusive connection rates that are not billed according to connection times, but instead as a flat fee for fixed periods. With flat rates, there is no longer any reason to disconnect. On the contrary: New e-mails should be reported directly to the PC, the home workplace is to be continuously connected to the company network and users want to be able to reach friends and colleagues via Internet messenger services (ICQ etc.) without interruption. This means it is desirable to continuously maintain connections.

With the LANCOM the Keep-alive function ensures that connections are always established when the remote station has disconnected them.

Configuration of Keep-alive function

The keep alive procedure is configured in the peer list.

If the holding time is set to 0 seconds, a connection is not actively disconnected by the LANCOM. The automatic disconnection of connections over which no data has been transmitted for a longer time is deactivated with a holding time of 0 seconds then. However, connections interrupted by the remote site are not automatically re-established with this setting.

With a holding time of 9,999 seconds the connection is always re-established after any disconnection. Additionally, the connection is re-established after a reboot of the device ('auto reconnect').

7.12 Callback functions

The LANCOM supports automatic callback via its ISDN port.

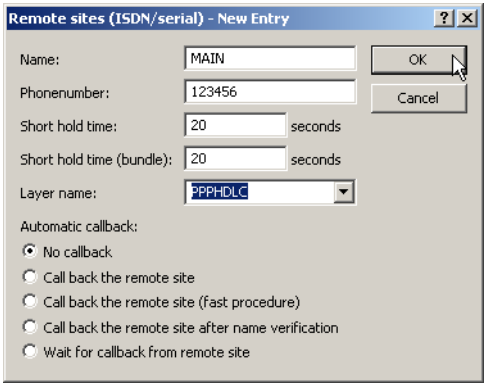
In addition to callback via the D channel, the CBCP (**C**allback **C**ontrol **P**rotocol) specified by Microsoft and callback via PPP as per RFC 1570 (PPP LCP extensions) are also offered. There is also the option of a particularly fast callback using a process developed by LANCOM. PCs with Windows operating system can be called back only via the CBCP.

7.12.1 Callback for Microsoft CBCP

With Microsoft CBCP, the callback number can be determined in various ways.

- The party called does not call back.
- The party called allows the caller to specify the callback number itself.
- The party called knows the callback numbers and **only** calls these back.

Via CBCP, it is possible to establish connection to the LANCOM from a PC with Windows operating system and also to be called back by this PC. Three possible settings are selected in the remote sites list via the callback entry as well as the calling number entry.



No callback

For this setting, the callback entry must be set to 'off' when configuring via WEBconfig or in the console.

Callback number specified by caller

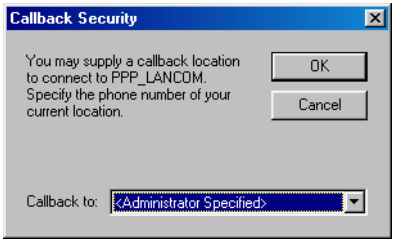
For this setting the callback entry must be set to 'Call back the remote site after name verification' (or must have the value 'Name' in WEBconfig or in the console). In the peer list **no** telephone number may be specified.

After the Authentication an input window appears on the caller's screen in Windows that requests the ISDN telephone number of the PC.

The calling number is determined in the LANCOM

For this setting the callback entry must be set to 'Call back the remote site after name verification' (or must be set to the value 'Name' in WEBconfig or in the console). In the peer list **one** telephone number must be specified.

Some Windows versions (especially Windows 98) prompt the user to confirm the callback to the telephone number stored in the LANCOM ('Administrator Specified') with an input window. Other Windows versions only inform the user that the PC is waiting for the callback from the LANCOM.



The callback to a Windows workstation occurs approx. 15 seconds after the first connection has been dropped. This time setting cannot be decreased since it is a Windows default setting.

7.12.2 Fast callback using the LANCOM Systems process

This fast, LANCOM Systems-specific process is ideal if two LANCOM are to communicate with one another via callback.

- The caller who may wish to be called back can activate the function 'Wait for callback from remote site' in the peer list (or 'Looser' when configuring via WEBconfig, terminal program or Telnet).
- The callback party selects 'Call back the remote site (fast procedure)' in the peer list and enters the calling number ('LANCOM' when configuring via WEBconfig, terminal program or Telnet).

For fast callback using the LANCOM Systems method, the number list for answering calls must be kept up to date at both ends.

7.12.3 Callback with RFC 1570 (PPP LCP extensions)

The callback as per 1570 is the standard method for calling back routers of other manufacturers. This protocol extension describes five possibilities for requesting a callback. All versions are recognized by LANCOM. All versions will be processed in the same way, however:

The LANCOM drops the connection after authenticating the remote station and then calls back the station a few seconds later.

Configuration

For callback as per PPP you select the option 'Call back the remote site' in LANconfig or 'Auto' with configuration via WEBconfig, terminal program or Telnet.

For callback as per PPP the number list for answering calls in the LANCOM must be up to date.

7.12.4 Overview of configuration of callback function

The following options are available in the peer list under WEBconfig and terminal program/telnet for the callback function:

With this entry ...	... you set up the callback in this manner:
'Off'	No callback occurs.
'Auto' (not for Windows operating systems, see below)	The remote station will be called back if so specified in the peer list. At first, the call is denied and as soon as the channel is clear again, it is called back (duration is approx. 8 seconds). If the remote station is not found in the numerical list, it is first accepted as the DEFAULT remote station, and the callback is negotiated during the protocol negotiation. A charge of one unit is incurred for this.

With this entry ...	... you set up the callback in this manner:
'Name'	Before a callback occurs, a protocol negotiation is always carried out even when the remote station was found in the numerical list (e.g. for computers with Windows having direct dialing on the device). Here only minor charges result.
'LANCOM'	When the remote station is found in the numerical list, a quick callback is carried out, i.e., the LANCOM sends a special signal to the remote station and calls back immediately when the channel is clear again. After approx. 2 seconds, the connection is established. If the remote station does not take back the call immediately after the signal, then after two seconds the situation reverts back to normal callback procedures (duration is once again approx. 8 seconds). This process is only available for DSS1 connections.
'Looser'	Use the 'Looser' option when a callback is expected from the remote station. This setting carries out two functions simultaneously. On the one hand, it ensures that a custom connection setup is taken back when there is an incoming call from the called remote station, and on the other hand, the function is activated with this setting to be able to react to the rapid callback procedure. In other words, in order to be able to use rapid callback, the caller must be in the 'Looser' mode while the party being called must discontinue callback with 'LANCOM'.

The setting 'Name' offers the greatest security when an entry is made into the number list as well as the PPP list. The setting 'LANCOM' offers the fastest callback method between two LANCOM Systems routers.

With Windows remote stations, the 'Name' setting **must** be selected.

7.13 ISDN Channel bundling with MLPPP

When establishing an ISDN connection to a remote station with PPP capability, you can transmit data more quickly. Data can be compressed and/or several B channels can be used for data transmission (channel bundling).

Connecting with cable bundling is distinguished from "normal" connections in that not only one, but rather several B channels are used parallel for data transmission.

MLPPP (**M**ultilink **PPP**) is used for channel bundling. This procedure is of course only available when PPP is used as the B-channel protocol. MLPPP is used e.g. for Internet access via Internet provider, which also operate remote stations with MLPPP capability from your direct dialing nodes.

Bundling over MLPPPoE can also be arranged for DSL channels ('DSL channel bundling (Multilink-PPPoE – MLPPPoE)' → page 131).

Two methods of channel bundling

- Static channel bundling

  If a connection is established with static channel bundling, the LANCOM tries to establish the second B channel immediately after setting up the first B channel. If this does not work because, for example, this channel is already taken by another device or a different connection within the LANCOM, the connection attempt is automatically and regularly repeated until the second channel is available for it.

■ Dynamic channel bundling

In the case of a connection with dynamic channel bundling, the LANCOM first only establishes one B channel and begins transmitting data. If, during this connection, it determines that the throughput rate lies above a certain threshold value, it tries to add the second channel.

If the second channel is established and the data throughput rate drops below the threshold value, the LANCOM waits for the set B2 timeout period and then automatically closes the channel again. In this way, the per minute charges are fully utilized so long as rate information is communicated during the connection. Therefore, the LANCOM only uses the second B channel if and as long as it really needs it.

Here's how to configure your system to combine channels

The configuration of channel bundling for a connection is made up of three settings.

① Select a communication layer for the remote station from the layer list that has bundling activated in the Layer-2 options. Select from the following Layer-2 options:

- **compr.** according to the LZS data compression procedure (Stac) reduces the amount of data if the data hasn't already been compressed. This procedure is also supported by routers of other manufacturers and by ISDN adapters under Windows operating systems.
- **bundle** uses two B channels per connection.
- **bnd+cmpr** uses both (compression and channel bundling) and provides the maximum possible data transmission performance.

② Now create a new entry in the peer list. When doing so, watch the holding times for the connection. Please observe the following rules:

- Depending on the type of application, the B1 hold time should be increased to such a level so that the connection is not dropped prematurely because of packets not being transmitted for a short time. Experience has shown that values between 60 and 180 seconds are a good basis which can be adapted as required during operation.
- The B2 holding time determines whether static or dynamic channel bundling will be used (see above). A B2 holding time of '0' or '9999' ensures that the bundling will be static; values in between permit dynamic channel bundling. The B2 holding time defines how long the data throughput may lie below the threshold for dynamic channel bundling without the second B channel automatically being disconnected.

③ Use the entry for the Y connection in the Router interface list to determine what should happen if a second connection to a different remote station is requested during an existing connection using channel bundling.

WEBconfig	Expert Configuration ▶ Setup▶ WAN ▶ Router-interface-list
Terminal/Telnet	`cd /setup/WAN` `set router-interface-list [...]`

- □ Y connection **On**: The router interrupts the bundled connection to establish a connection to the other remote station. When the second channel is free again, the originally bundled connection automatically takes the channel back (always in the case of static bundling, only as required when using dynamic bundling).
- □ Y connection **Off**: The router maintains the existing bundled connection; the establishment of the new connection must wait.

Please note that if channel bundling is used, the cost of two connections is charged.Here no additional connections via the LANCAPI are possible! So you should only use channel bundling if the double transmission capacity can really be used in full.

7.14 Operating a modem over the serial interface

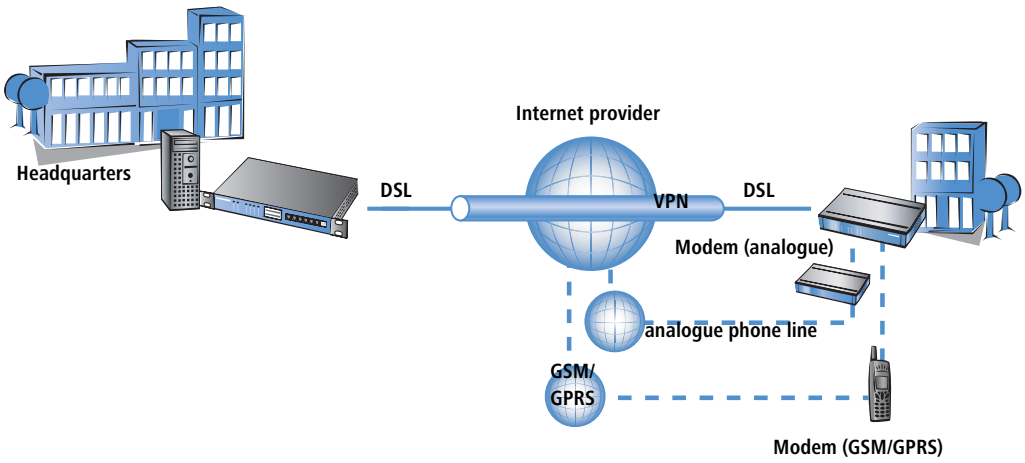
This section refers only to devices with a serial configuration interface.

7.14.1 Introduction

Internationally, analog telephone connections are just as common in the business world as the predominant ISDN connections in Germany. The operation of international networks thus places particular demands on remote maintenance options and for high-availability of the gateways and thus requires different interfaces than the ISDN common in Germany. Apart from conventional analog telephone lines, mobile telephone networks such as GSM or GPRS may, in certain cases, represent the only way of providing remote maintenance without broadband or other cabled access.

In response to these requirements, most LANCOM models with a serial interface can be extended with an additional WAN interface with the use of analog modems, GSM or GPRS. The following functions are available with a suitable modem in combination with the LANCOM Modem Adapter Kit:

- Internet access via modem with all of the router functions such as firewall, automatic connection establishment and termination, etc.
- Remote maintenance (e.g. dial-in to international sites)
- Backup connection (e.g. high-availability through GSM/GPRS modem connection)



7.14.2 System requirements

The following are required to set up a backup connection over the serial interface:

- LANCOM with serial configuration interface and support for LANCOM modem adapter kit. For devices with serial configuration interface please refer to the table 'Overview of functions by model and LCOS* versionn' → page 591 to see, whether your modell supports the modem operation at serial interface.
- LANconfig or alternatively a web browser or Telnet
- Serial configuration cable (supplied with the device)
- Analog modem, Hayes compatible, with access to a suitable analog telephone connection
- LANCOM modem adapter kit to connect the modem over the serial configuration cable

7.14.3 Installation

The installation simply involves the connection of the modem with the LANCOM Modem Adapter Kit with the serial configuration interface of the LANCOM.

Please do not use any other adapters than the original LANCOM Modem Adapter Kit! The contact assignment of the LANCOM Modem Adapter Kit differs from other commercial adapters like "null modem cables" or the like. The use of uncompliant accessories will cause serious damage on the LANCOM and/or the modem. For further details please refer to the 'Contact assignment of LANCOM modem adapter kit' → page 164.

7.14.4 Set the serial interface to modem operation

The operation of the serial interface requires the operating mode and bitrate to be set.

- Operating mode [default: outband]

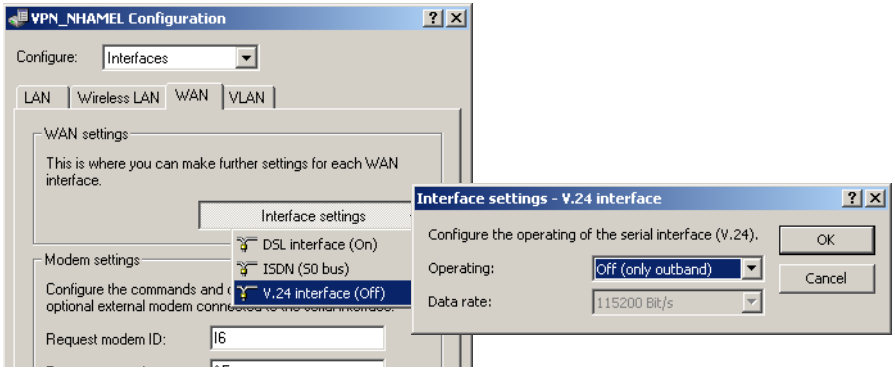
- □ Outband: In this mode, the serial interface is only used for configuration with a terminal program.
- □ Modem: In the 'Modem' setting, the device attempts to find a modem connected to the serial interface. If this is successful then the modem can be used as an additional WAN interface. If a computer running a terminal program is detected, then the device automatically switches the interface into outband mode.
- □ Interlink: Direct connection between two LANCOM devices

- Bitrate [default: 115,200 bps.]

  Set the maximum bitrate supported by your modem. The serial interfaces of LANCOM devices support data rates of 19,200 bps, 38,400 bps, 57,600 bps up to a maximum of 115,200 bps.

Configuration with LANconfig

The settings for the serial interface as a WAN interface can be found in the LANconfig configuration area 'Interfaces'. Select the 'V.24 interface' with the 'Interface settings' button on the 'WAN' tab.



Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you will find the settings for the serial interface under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert Configuration ▶ Setup ▶ Interfaces ▶ V24-Interface
Terminal/Telnet	`Setup/Interfaces/V24-Interface`

As long as the LANCOM is set to modem mode, a terminal program operating over the serial interface will display the AT commands that the LANCOM device transmits while attempting to identify a connected modem. In the terminal program, press the return key repeatedly until the modem identification is interrupted and start the configuration session.

7.14.5 Configuration of modem parameters

The operation of a modem at the serial interface requires the following settings:

- Request modem ID [Default: `ATI6`]
- Reset command [default: `AT&F`]

- Initialize command [default: ATL0M1X1S0=0]
  - L0: Loudspeaker quiet
  - M1: Loadspeaker on while connecting
  - X1: Operation at an extension
  - S0=0: Disable auto answering
- Deactivate modem echo [default: ATE0]
- AT polling cycle time [Default: 1 in seconds]
- AT polling count [Default: 5]
- Ring count [Default: 1]
- Initialize answer command
- Answer command [Default: ATA]
- Initialize dial command
- Dial command [default: ATDT]
- Escape sequence to terminate data phase resp. to return to command phase [Default: +++]
- Hold time after escape sequence [Default: 1000 in milli seconds]
- Disconnect: command to hang up during data phase [Default: ATH]

The modem parameters are set with values that should suit most modems. Thus changes are generally not necessary. Refer to the documentation for your modem for settings that vary from these.

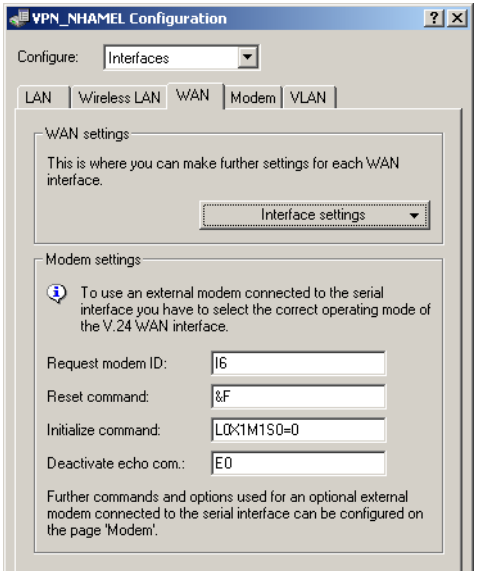
Setting up a GPRS backup connection

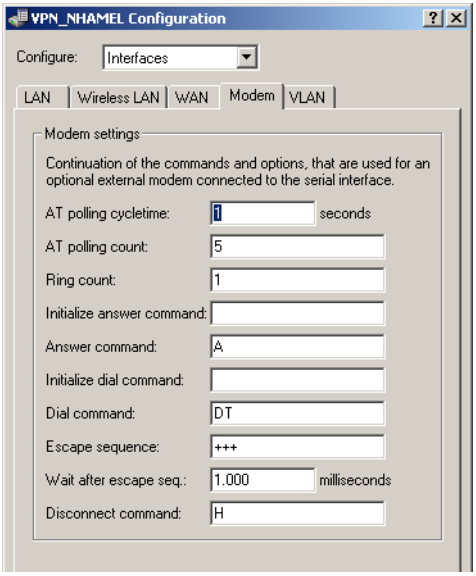
If the connection is to use a GPRS-capable modem at the serial interface, you will need the APN name and the dial-up telephone number. The following init-strings for the configuration apply to T-Mobile and Vodafone:

- T-Mobile
  - Init-string: L0X1M1S0=0+CGDCONT=1, "IP", "internet.t-d1.de"
  - Dial-up number: *99#
- Vodafone
  - Init-string: L0X1M1S0=0+CGDCONT=1, "IP", "web.vodafone.de"
  - Dial-up number: *99# or *99***1#

Configuration with LANconfig

The modem parameters can be found in the LANconfig configuration area 'Interfaces' on the 'WAN' and 'Modem' tab.





Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you will find the modem parameters under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert Configuration ▶ Setup ▶ Interfaces ▶ Modem-Parameters
Terminal/Telnet	`Setup/Interfaces/Modem-parameters`

Entering special characters in the console

For a GPRS dial-up, the initialisation strings require the entry of inverted commas and equal signs. Certain special characters can be correspondingly marked with a leading backslash:

- *
- "
- =
- space
- **Example:** `+cgdcont\=1,\"IP\",\"internet.t-d1.de\"`

As an alternative, the entire command sequence can be enclosed within inverted commas. In this case, those inverted commas which are inside the surrounding inverted commas must be preceded by a backslash.

- **Example:** `"+cgdcont=1,\"IP\",\"internet.t-d1.de\""`

7.14.6 Direct entry of AT commands

The command

- `sendserial "AT..."`

allows you to use Telnet to send a character string directly to a modem that is connected to the LANCOM. This function allows you to send any AT commands to the modem.

Sending AT commands ist possible in the internal modem state 'idle' or 'Modem ready' only. The responses can be found in the serial trace ('Trace output' → page 162).

7.14.7 Statistics

Statistics about activities of the serial interface can be accessed with a terminal program or Telnet under:

`Status/Modem Status`

The statistics show the following states:

- the type of modem identified
- the status of its last connection, e.g. the transfer rate, the transfer protocol used or the error-detection method used
- internal state of modem management, e.g.
  - device detection
  - interface deactivated

- □ modem initialization
- □ modem ready
- □ connection establishment
- □ modem in data mode

These messages may be very helpful for debugging purposes.

7.14.8 Trace output

The command

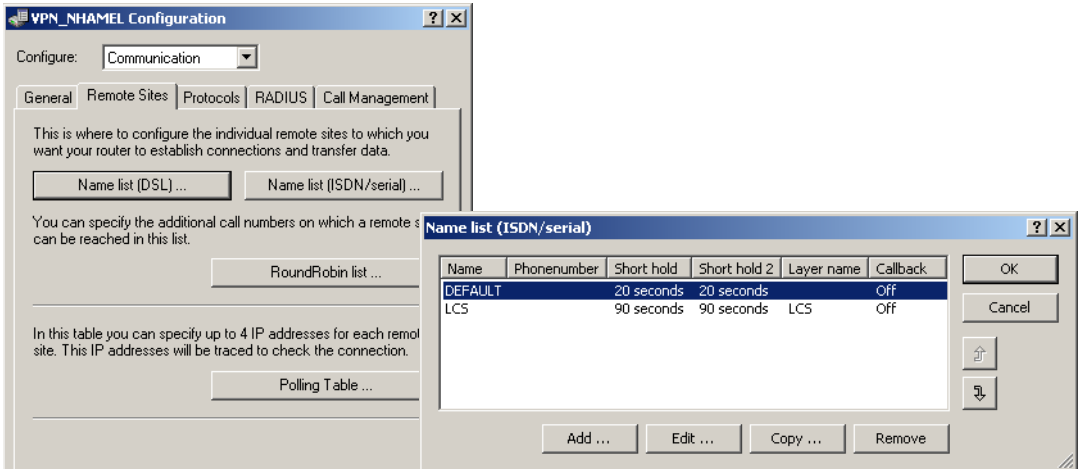
- `trace + serial`

allows you to start the trace output for the serial interface in a Telnet session when a LANCOM has a modem connected. The output shows all messages exchanged up until the establishment of data transfer between the modem and the LANCOM.

7.14.9 Configuration of remote sites for V.24 WAN interfaces

To establish a connection to a remote station via the modem connected to the serial interface, a corresponding entry in the remote site list (ISDN/serial) must be generated. The remote sites list (ISDN/serial contains the following information:

- Name: Name of the remote device
- Telephone number: Telephone number that reaches the remote site. The field can be left empty if calls are to be received only.
- Hold time: This time defines how long a connection is kept active even if no more data is being transferred. If a zero is entered, the connection will not be interrupted automatically. A hold time of "9999" means that the connection is permanently held open. If it is interrupted, then the connection will be actively opened up again. This behavior is known as **keep alive**.
- 2. Hold time: Is ignored.
- Layer name: The layer 'V.24_DEF' is selected for the connection over the serial WAN interface. The layer is preset and does not need further configuration. The layer 'V.24_DEF' uses the following settings:
  - □ Encapsulation: Transparent
  - □ Layer 3: APPP (asynchronous PPP)
  - □ Layer 2: Transparent
  - □ Options: none
  - □ Layer 1: SERIAL (shows that the serial interface is being used for connections via the layer 'V.24_DEF')



The remote site list with the remote sites for the modem at the serial interface can be found under the following paths:

Configuration tool	Menu/Table
LANconfig	Communication ▶ Remote sites ▶ Name list (ISDN)
WEBconfig	Expert configuration ▶ Setup ▶ WAN ▶ Dialup-Peers
Terminal/Telnet	`Setup/WAN/Dialup-Peers`

Once an entry in the remote site list has been generated for the WAN interface, this remote station can be used just like any other for routing and WAN connections.

7.14.10Configuration of a backup connection on the serial interface

The configuration of a backup connection via a modem at the serial interface requires first of all an entry in the Dialup-Peers list so that the required remote site can be reached. The following entries will also be required for the configuration of the LANCOM:

- Entry in the backup table

  In the backup table, generate an entry for the remote site that is to be used for the backup connection. This remote site is to be allocated to the remote site that is to be called by the modem at the serial interface.

The backup table is to be found under the following paths:

Configuration tool	Menu/Table
LANconfig	Communication ▶ Call Management ▶ Backup Table
WEBconfig	Expert configuration ▶ Setup ▶ WAN ▶ Backup table
Terminal/Telnet	`Setup/WAN/Backup-table`

- Entry in the polling table

  If the link to the remote station that is to be backed up cannot be checked by LCP polling (with PPP only) then an additional entry in the polling table is required. This involves assigning the remote site with an IP address that can be regularly tested with a ping command. The IP address should typically be a computer directly at the opposite end of the connection being tested, e.g. a DNS server in your provider's network.

  The polling table is to be found under the following paths:

Configuration tool	Menu/Table
LANconfig	Communication ▶ Remote Sites ▶ Polling Table
WEBconfig	Expert configuration ▶ Setup ▶ WAN ▶ Polling table
Terminal/Telnet	`Setup/WAN/Polling-table`

7.14.11 Contact assignment of LANCOM modem adapter kit

Contact assignment for LANCOM interlink or modem connection:

LANCOM signal	sub-d 9 plug	LANCOM or modem signal	sub-d 9 plug
TxD	3	RxD	2
RxD	2	TxD	3
RTS	7	CTS	8
CTS	8	RTS	7
DTR	4	DCD	1
DCD	1	DTR	4
GND	5	GND	5

7.15 Manual definition of the MTU

Many Internet providers operate their own backbone; however, their customers dial in to the network over the access nodes provided by third-party telecommunications providers. The two-stage dial-in procedure can lead to problems with the realized data rate:

- When dialing into the nodes of Deutsche Telekom, for example, a LANCOM negotiates a permissible maximum transmission unit (MTU), which defines the greatest possible size of unfragmented data packet. This MTU is then observed by the LANCOM.
- When the data packets are forwarded to the actual provider, an additional header is added which increases the size of the data packets again. For the data packets to meet with the permitted size, they must now be fragmented into smaller units. This additional fragmentation can cause losses in the data-transfer speeds.

This problem can be avoided by entering a fixed MTU for each remote site.

7.15.1 Configuration

WEBconfig, Telnet or terminal program

Under WEBconfig, Telnet or a terminal program, you will find the MTU list for a maximum of 16 entries under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ WAN ▶ MTU list
Terminal/Telnet	`Setup/WAN/MTU-list`

The table contains the following entries:

- Device name: Name of the remote device. It can be a physical or a virtual (PPTP/VPN) remote station
- MTU: MTU to be used for the connection

7.15.2 Statistics

Under **Status ▶ WAN-statistics** you will find the MTU statistics recorded for all current connections. The table is partially dynamic and begins with 16 entries. Like the MTU list under **Setup ▶ WAN** it contains two columns with the remote name and the MTU.

Remote site	MTU	Remark
INET	1200	The INET remote site is the Internet connection and a forced MTU of 1200 bytes.
MULTI	1492	MULTI is a PPPoE connection, for which the MTU was negotiated (and is consequently 1492 bytes).
TESTVPN	1100	TESTVPN is a VPN connection established via the Internet. An assumed overhead of 100 bytes is taken for VPN connections, and consequently the MTU here is 1100 bytes.
TESTVPN-PPTP	1060	TESTVPN-PPTP is a PPTP connection established over the VPN connection TESTVPN. The overhead for PPTP connections is 40 bytes, and consequently the MTU here is 1060 bytes.

MTU lists and MTU statistics are only available for devices with a DSL or ADSL interface.

7.16 ADSL 2+

Internet service providers are providing a new standard for data transfer with the current ADSL 2+ service. ADSL 2+ expands the frequency spectrum used from 1.1 MHz to 2.2 MHz, thereby enabling higher data rates with up to 24 MBps downstream. The higher data rates prove their worth particularly with broadband-intensive applications such as VoIP or video streaming over the Internet (such as HDTV).

Almost all current LANCOM devices with an integrated ADSL modem are ready for use with ADSL 2+:

- LANCOM 1821 wireless ADSL (from hardware release E)
- LANCOM 1721 VPN
- LANCOM 1521 wireless ADSL (ADSL 2 only)
- LANCOM 821+

The devices support the ADSL 2+ standard with the upgrade to the LCOS version 5.20. Please observe the following notes for the interface settings:

- If the device was previously set to 'multimode', this changes to 'automatic' when the firmware is updated.
- If a different protocol was configured previously, this setting remains unchanged.

In auto-mode, the protocol and wait time that were used for successful synchronization are saved in the flash memory. This can lead to problems if the line is converted or if the site changes. The values that are saved are deleted, however, as soon as a protocol other than 'auto' is set.

7.17 WAN RIP

In order for routes learned from RIP to be broadcast across the WAN, the respective remote stations can be entered into the WAN RIP table. The WAN RIP table contains the following values:

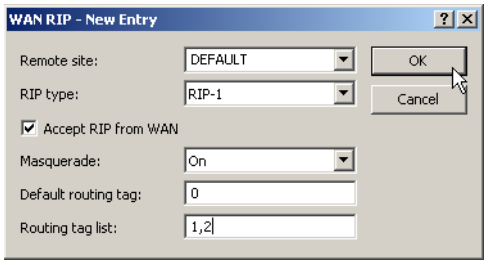
- **Remote site**: The name of the remote station is listed in the 'Remote site' column:
- **RIP type**: The column RIP type details the RIP version with which the local routes are propagated
- **RIP accept**: The column RIP accept lists whether RIP from the WAN is to be accepted. The RIP type must be set for this.
- **Masquerade**: The column Masquerade lists whether or not masquerading is performed on the connection and how it is carried out. This entry makes it possible to start WAN RIP even in an empty routing table. The following values are possible:
  - **Auto**: The masquerade type is taken from the routing table (value: 0). If there is no routing entry for the remote station, then masquerading is not performed.
  - **On**: All connections are masqueraded (value: 1).

  - □ **Intranet**: IP masquerading is used for connections from the intranet, connections from the DMZ pass through transparently (value: 2).
- **Default tag**: The column Default tag lists the valid "Default touting tag" for the WAN connection. All untagged routes are tagged with this tag when sent on the WAN.
- **Routing tags list**: The column Routing tags list details a comma-separated list of the tags that are accepted on the interface. If this list is empty, then all tags are accepted. If at least one tag is in the list, then only the tags in this list are accepted. When sending tagged routes on the WAN, only routes with valid tags are propagated.

  All learned routes from the WAN are treated internally as untagged routes and propagated on the LAN with the default tag (0). In the WAN, they are propagated with the tag with which they were learned.

Configuration with LANconfig

The WAN RIP table can be found in the LANconfig in the configuration area 'IP router' on the 'General' tab.



Configuration with WEBconfig, Telnet or SSH

Under WEBconfig, Telnet or SSH client you will find the WAN RIP table under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert Configuration ▶ Setup ▶ IP router ▶ RIP ▶ WAN sites
Terminal/Telnet	`Setup/IP router/RIP/WAN sites`

7.18 Spanning Tree Protocol

In networks with many switches and bridges, many physical connections can exist between two stations that are connected to the network. These redundant data paths are desirable because they can offer alternative paths to the desired destination in case individual network paths fail. On the other hand, these multiple connections can also lead to loops or cause network stations to receive multiple frames. Both occurrences negatively impact free data traffic performance in the network.

The Spanning Tree Protocol (STP) enables an analysis of the network at the layer 2 level and, as such, offers solutions for intelligent path selection between two network stations below the routing layer. By discovering redundant paths between network stations, STP builds a unique structure in which loops and double packets can be avoided. To this end, so-called Bridge Protocol Data Units (BPDUs) are sent as a multicast to a specific MAC address. The BPDUs allow redundant paths to be discovered as well as the distance and the data rate available on this connection. Using these

values, the Spanning Tree Protocol calculates a priority (also called route costs) with which the various connections are to be treated. The low-priority connections are disabled and are therefore no longer available for clients. Through the reduction of non-redundant connections between the clients, the protocol builds a tree which unambiguously defines all of the connections that arise from a central switch (root bridge).

The BPDUs are sent regularly in the network in order to check the availability of the connections. If a connection fails, then the network analysis is triggered again; the possible paths and the corresponding priorities are redefined.

7.18.1 Configuring the Spanning Tree Protocol

The following parameters are available for configuring STP functionality in LANCOM:

- **Spanning Tree Protocol**: When Spanning Tree is turned off, a LANCOM does not send any Spanning Tree packets and passes received packets along instead of processing them itself.
- **Bridge Priority**: This defines the priority of the bridge in the LAN. This can influence which bridge should preferably be made root bridge by the Spanning Tree Protocol. The bridge priority can assume a value between 0 and 65535, whereby a higher value means a lower priority.
- **Max Age**: This value defines the time (in seconds) after which a bridge drops messages received through Spanning Tree as 'outdated'. This parameter defines how quickly the Spanning Tree algorithm reacts to changes, for example due to failed bridges.
- **Hello Time**: This parameter defines (in seconds) in which intervals a device selected to be the root bridge sends Spanning Tree information into the LAN.
- **Forward Delay**: This time (in seconds) determines how much time must pass at a minimum before a Spanning Tree port can change the status (listening, learning, forwarding).

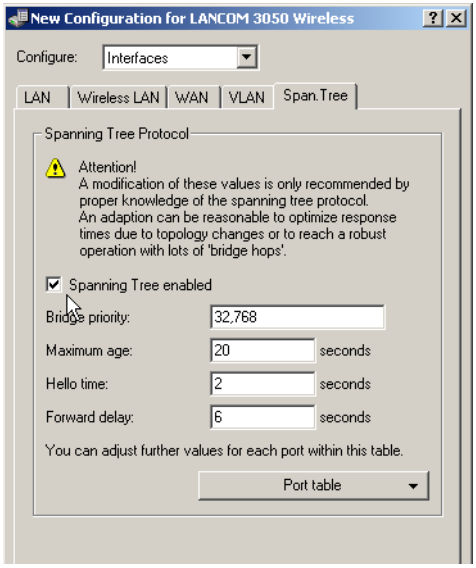
Modifying any of these three time values is only recommended for those with exact knowledge of the Spanning Tree protocol. An adjustment can be useful in order to optimize reaction times after topology changes or to achieve stable performance in networks with many 'bridge hops'.

- **Port Data**: Three values can be configured per port:
  - **Active**: This can be used to block a port completely, i.e. the port will always have the 'disabled' status.
  - **Isolated**: This can be used to define that STP packets from this port can never be forwarded to other ports or that STP packets coming from other ports can never be forwarded to this port. This feature is comparable to 'Private Mode' with Ethernet switch on LANCOM devices.
  - **Prio**: This can be used to define the preferred port to be enabled for redundant links. The value range extends from 0 to 255, whereby a lower value means a higher priority. If the values are equal, the Spanning Tree algorithm selects the port with low path costs or the port that is closer to the top of the list in the port table.

The parameters 'Active' and 'Isolated' retain their functionality even when Spanning Tree is disabled!

Configuration with LANconfig

Paramters for the Spanning Tree protocol are entered into LANconfig in the configuration area 'Interfaces' on the 'Span.Tree' tab.



Configuration with WEBconfig, Telnet or SSH

Under WEBconfig, Telnet or SSH client you will find the settings for the Spanning Tree parameters under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert-Configuration ▶ Setup ▶ LAN Bridge
Terminal/Telnet	`Setup/LAN-Bridge`

7.18.2 Status reports via the Spanning Tree Protocol

The current STP values can be viewed via Telnet in the LAN Bridge Status.

- **Bridge ID**: This is the ID for the device that is being used by the Spanning Tree algorithm. It is composed of the user-defined priority (upper 16 bits) and the device MAC address (lower 48 bits).
- **Root Bridge**: The ID for the device that is currently elected root bridge.
- **Root Port**: The port that can be used to reach the root bridge from this device. If the device itself is the root bridge, it is displayed with the special value '255'.
- **Root Path Cost**: The path costs of all hops added together in order to reach the root bridge from this device.
- **Port Data**
  - **Prio**: the priority of this port taken from the port configuration

- **State**: the current status of the port:

  Disabled: no packets can be sent or received through this port. This occurs when the port has either been disabled manually or when it has a negative link status.

  Listening: Intermediate state on the way to enabling. Only Spanning Tree packets are listened to, data packets are ignored and are also not forwarded to this port.

  Learning: Further intermediate state. As opposed to 'listening' additional MAC addresses from data packets entering this port are learned but data packets are still not forwarded.

  Forwarding: the port is completely active, data packets are received and forwarded in both directions.

  Blocking: Spanning Tree has identified this port to be redundant and disabled it for data traffic.
- **Root**: The ID for the root bridge that can be reached through this port.
- **Bridge**: This is the ID for the bridge through which the root bridge can be reached.
- **Path Cost**: This value defines the 'costs' for this port. The value is determined by the port technology (Ethernet, WLAN, etc.) and the bandwidth. Examples of values used are:

Transfer technology	Costs
Ethernet 10 MBit	100
Ethernet 100 MBit	19
Ethernet 1000 MBit	4
WLAN 2 MBit	500
WLAN 11 MBit	140
WLAN 54 MBit	35
WLAN 108 MBit	25

8 Firewall

For most companies and many private users a work without the Internet is no longer conceivable. E-mail and web are indispensable for communication and information search. But each connection of the workstations from the own, local network to the Internet represents however a potential danger: Unauthorized users can try to see your data via this Internet connection, to modify it or to manipulate your PCs.

Therefore this chapter covers an important topic: the firewall as defensive measure against unauthorized access. Besides a brief introduction to the topic of Internet security, we show you which protection a LANCOM is able to offer you by right configuration and how to make the needed specific settings.

8.1 Threat analysis

To plan and to realize suitable measures to guarantee security, it is advisable to know first all possible sources of danger:

- Which imminent dangers exist for the own LAN resp. the own data?
- Which are the ways intruders take for the access to your network?

We denote the intrusion into protected networks in the following as “attack” according to the general usage, and the intruder thus as “attacker”.

8.1.1 The dangers

The dangers in the Internet arise in principle from completely different motives. On the one hand the perpetrators try to enrich themselves personally or to damage the victims systematically. By the ever increasing know-how of the perpetrators, the “hacking” became already a kind of sports, in which young people often measure who takes at first the hurdles of Internet security.

Regardless of the individual motivation, the intention of the perpetrators mostly leads to the following aims:

- Inspect confidential information such as trade secrets, access information, passwords for bank accounts etc.
- Use of LAN workstations for purposes of the attackers, e. g. for the distribution of own contents, attacks to third workstations etc.
- Modify data of LAN workstations, e. g. to obtain even further ways for access.
- Destroy data on the workstations of the LAN.
- Paralyze workstations of the LAN or the connection to the Internet.

We restrict ourselves in this section to the attacks of local networks (LAN) resp. to workstations and servers in such LANs.

8.1.2 The ways of the perpetrators

In order to undertake their objectives, the perpetrators need at first a way to access your PCs and data. In principle, the following ways are open as long as they are neither blocked nor protected:

- Via the central Internet connection, e. g. via routers.
- Via decentral connections to the Internet, e. g. modems of single PCs or mobile phones on notebooks.
- Via wireless networks operating as a supplement to wired networks.

In this chapter we only deal with the ways via the central Internet connection, via the router.

For hints on the protection of wireless networks, please refer to the respective chapters of this reference manual resp. of the appropriate device documentation.

8.1.3 The methods

Normally strangers have of course no access to your local area network or to the workstations belonging to it. Without the appropriate access data or passwords nobody can thus access the protected area. If spying out of these access data is not possible, the attackers will try another way to achieve their goals.

A fundamental starting point is to smuggle data on one of the allowed ways for data exchange into the network, which opens from the inside the access for the attacker. Small programs can be transferred on a computer by appendices in e-mails or active contents on web pages, e.g., in order to lead afterwards to a crash. The program uses the crash to install a new administrator on the computer, which can then be used from distance for further actions in the LAN.

If the access via e-mail or www is not possible, the attacker can also look out for certain services of servers in the LAN, which are useful for his purposes. Because services of the servers are identified over certain ports of the TCP/IP protocol, the search for open ports is also called "port scanning". On the occasion, the attacker starts an inquiry for particular services with a certain program, either generally from the Internet, or, only on certain networks and unprotected workstations, which in turn will give the according answer.

A third possibility is to access an existing data connection and use it as a free-rider. The attacker observes here the Internet connection of the victim and analyses the connections. Then he uses e. g. an active FTP connection to smuggle his own data packets into the protected LAN.

A variant of this method is the "man-in-the-middle" attack. The attacker observes here first the communication of two workstations, and gets then in between.

8.1.4 The victims

The question about the degree of exposure for an attack influences to a considerable degree the expenditure one wants to or must meet for defending. In order to assess whether your network would be particularly interesting for an attacker as a potential victim, you can consult the following criteria:

- Particularly endangered are networks of common known enterprises or institutions, where valuable information is suspected. Such information would be e.g. the results of research departments, which are gladly seen by industrial spies. Or, on the other hand, bank servers, on which big money is distributed.
- Secondly, also networks of smaller organizations are endangered, which perhaps are only interesting to special groups. On the workstations of tax consultants, lawyers or doctors do slumber certainly some information quite interesting for third persons.
- Last but not least also workstations and networks are victims of attackers, which obviously offers no use for the attackers. Just the "script kiddies" testing out their possibilities by youthful ambition are sometimes just searching for defenceless victims in order to practise for higher tasks.

  The attack against an unprotected, apparently not interesting workstation of a private person can also serve the purpose to prepare a basis for further attacks against the real destination in a second step. The workstation of "no interest" becomes source of attacks in a second step, and he attacker can disguise his identity.

All things considered, we can resume that the statistical probability for an attack to the network of a global player of the industry may be higher than to a midget network of the home office. But probably it is only a matter of time that a defenceless workstation installed in the Internet will - perhaps even accidentally - become the victim of attacks.

8.2 What is a Firewall?

The term "Firewall" is interpreted very differently. We want to define at this point the meaning of "Firewall" within the boundaries of this reference manual.

A Firewall is a compilation of components, which monitors at a central place the data exchange between two networks. Mostly the Firewall monitors the data exchange between an internal, local network (LAN), and an external network like the Internet.

The Firewall can consist of hard and/or software components:

- In pure hardware systems the Firewall software often runs on a proprietary operating system.
- The Firewall software can also run on a conventional workstation, which is dedicated to this task under Linux, Unix or Windows.
- As a third and frequently used alternative, the Firewall software runs directly within the router, which connects the LAN to the Internet.

In the following sections we only look at the Firewall in a router.

The functions "Intrusion Detection" and "DoS protection" are part of the content of a Firewall in some applications. The LANCOM contains these functions also, but they are realised as separate modules beside the Firewall.

Further information can be found in the section 'Protection against break-in attempts: Intrusion Detection' → page 219 and 'Protection against "Denial of Service" attacks' → page 220.

8.2.1 Tasks of a Firewall

Checking data packets

How does the Firewall supervises the data traffic? The Firewall works in principle like a door keeper for data packets: Each packet will be checked, whether it may pass the door of the network (Firewall) in the desired direction or not. For such a checking different criteria are used, in common language of Firewalls called "rules" or "guidelines". Depending on the kind of information, which are used for creation of the rules and which are checked during the operation of the Firewall, one distinguishes different types of Firewalls.

Above all, the aspect of the "central" positioning is very Important: Only when the entire data traffic between "inside" and "outside" goes through the Firewall, it can fulfil its task reliably under any circumstances. Each alternative way can reduce or even turn off the security of the Firewall. This central position of the Firewall simplifies by the way also the maintenance: One Firewall as common passage between two networks is certainly easier to maintain than a "Personal Firewall" on each of the workstations belonging to the LAN.

In principle, Firewalls operate at the interconnection between two or more networks. For the following explanation, we only look as example at the passage between a local network of a company and the Internet. These explanations can be transferred however in a general manner also to other network constellations, e.g. for the protection of a subnetwork of the personnel department of a company against the remaining network users.

Logging and alerting

An important function of the Firewall is beside the checking of data packets and the right reaction to the results of this checking also the logging of all actions triggered by the Firewall. By analyzing these protocols, the administrator can draw conclusions from the occurred attacks and on the basis of this information he can, if necessary, go on to improve the configuration of the Firewall.

But sometimes, logging alone comes too late. Often, an immediate intervention of the administrator can prevent a major danger. That is why Firewalls have mostly an alerting function, by which the Firewall notifies the administrator e.g. by e-mail.

8.2.2 Different types of Firewalls

During the last years, the operating principles of Firewalls have more and more evolved. Under the generic term "Firewall", a whole range of different technical concepts is offered to protect the LAN. Here we introduce the most important ones.

Packet filters

One speaks about a packet filter-based Firewall, if the router only checks the details in the header of the data packets and decides on the basis of this information, whether the packet may pass or not. The following details belong to the analyzed information:

- IP address of source and destination

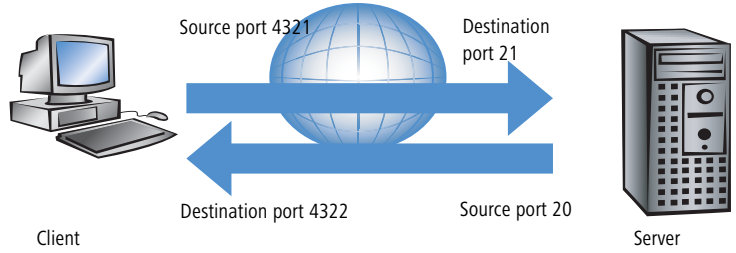
- Transfer protocol (TCP, UDP or ICMP)
- Port numbers of source and destination
- MAC address

The rules defined in a packet filter-orientated Firewall determine e.g., whether the packets may pass on by a special IP address range into the local network, or whether packets should be filtered for special services (i.e. with special port numbers). By these measures, the communication with certain workstations, entire networks or via special services can be reduced or even prevented. Besides, the rules are combinable, so that e.g. only workstations with special IP addresses get access to the Internet via the TCP port 80, while this services remains blocked for all other workstations.

The configuration of packet filtering Firewalls is quite simple, and the list with the permitted or forbidden packets can be extended very easily. Because also the performance requirements of a packet filter can be address with quite little means, the packet filters are often directly implemented in routers, which operate as interface between the networks anyway.

An unfavorable effect on the packet filters is, that the list of rules becomes uncomfortable after a while. Besides, for some services the connection ports are negotiated dynamically. To enable communication then, the administrator has to leave open all possibly used ports, which is contrary to the basic orientation of most security concepts.

One example for a process, which is quite problematical for simple packet filters, is the establishing of a FTP connection from a workstation of the own LAN to a FTP server in the Internet. By the generally used active FTP, the client (of the protected LAN) sends an inquiry from a port of the upper range (>1023) to port 21 of the server. The client informs the server, over which port it is expecting the connection. The server will establish as a result from its port 20 a connection to the desired port of the client.



To enable this process, the administrator of the packet filter must open all ports for incoming connections, because he does not know in advance for which port the client will inquire the FTP connection. An alternative is to use passive FTP. Thereby, the client establishes the connection itself to the server over a particular port, which was told to the server before. This process is, however, not supported by all clients/servers.

If we furthermore compare the Firewall with a porter, this door keeper only checks, whether he knows or not the courier with the packet at the door. If the courier is known and came ever into the building before, he has the permission to go in without hindrance and without being checked also for all following orders up to the workplace of the addressee.

Stateful Packet Inspection

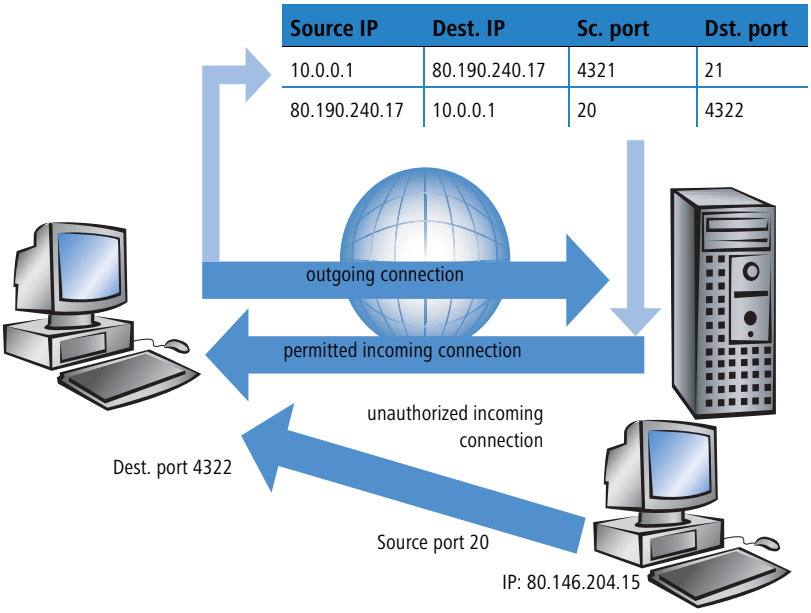
Stateful Packet Inspection (SPI), or briefly Stateful Inspection, enhances the packet filter approach by checking further connection state information. Beside the more static table with the permitted ports and address ranges, a dynamic table will be kept up in this variant, in which information about the connection state of the individual connections is held. This dynamic table enables to first block all endangered ports, and to selectively open only if required a port for a permitted connection (adjusted by source and destination address). The opening of ports is always made from the protected network to the unprotected one, that means mostly from LAN to WAN (Internet). Data packets that do not belong to one of the tracked session of the connection state table will be automatically discarded

Stateful Inspection: direction-dependent checking

The filter sets of a Stateful Inspection Firewall are - contrary to classical port filter Firewalls - dependent on their direction. Connections can only be established from source to their destination point. The other direction would require an explicit filter entry as well. Once a connection has been established, only the data packets belonging to this connection will be transmitted - in both directions, of course. So you can block in a reliable way all traffic not belonging to a known session, not coming from the local network.

Additionally, the Stateful Inspection is able to track from the connection set up, whether additional channels are negotiated for data exchange or not. Some protocols like e.g. FTP (for data transfer), T.120, H.225, H.245 and H.323 (for netmeeting or IP telephony), PPTP (for VPN tunnels) or IRC (for chatting) signalize when establishing the connection from the LAN to the Internet by a particular used source port whether they are negotiating further ports with the remote station. The Stateful Inspection dynamically adds also these additional ports into the connection state list, of course limited to the particular source and destination addresses only.

Let's have once again a look at the FTP download example. When starting the FTP session, the client establishes a connection from source port '4321' to the destination port '21' of the server. The Stateful Inspection allows this first set up, as long as FTP is allowed from local workstations to the outside. In the dynamic connection state table, the Firewall enters source and destination and the respective port. Simultaneously, the Stateful Inspection can inspect the control information, sent to port 21 of the server. These control signals indicate that the client requires a connection of the server from its port 20 to port 4322 of the client. The Firewall also enters these values into the dynamic table, because the connection to the LAN has been initiated from the client. Afterwards, the server can send so the desired data to the client.



But if another workstation from the Internet tries to use the just opened port 4322 of the LAN to file itself data from its port 20 on the protected client, the Firewall will stop this try, because the IP address of the attacker does not fit to the permitted connection!

After the successful data transfer, the entries disappear automatically from the dynamic table and the ports will be closed again.

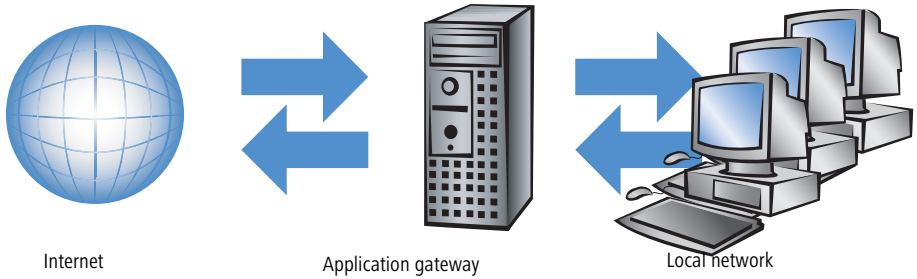
Moreover, a Firewall with Stateful Inspection is mostly able to re-assemble the received data packets, that means to buffer the individual parts and to assemble them again to an complete packet. Therefore, complete IP packets can be checked by the Firewall, rather than individual parts only.

This porter is making a definite better job. When somebody in this company orders a courier, he must also inform the porter that he is expecting a courier, when he will be arriving and what information should be found on the delivery note. Only when this information matches the logbook entries of the porter, the courier may pass. If the courier brings not only one packet, but rather two, only the one with the correct delivery note will pass. Likewise, a second courier demanding access to the employee will be rejected, too.

Application Gateway

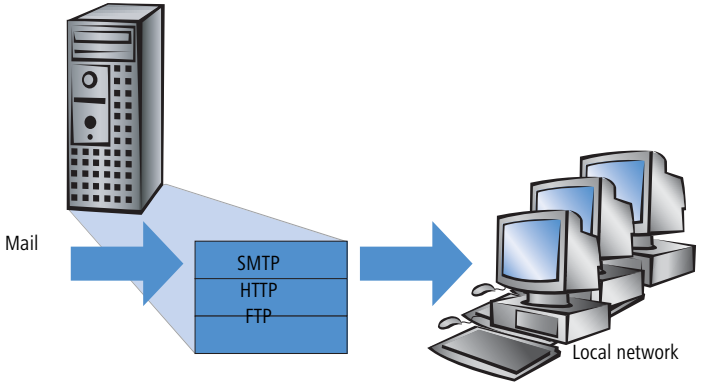
By checking of contents on application level, Application Gateways increase the address checking of the packet filters and the connection monitoring of the Stateful Packet Inspection. The Application Gateway runs mostly on a separate workstation, because of the high demands to the hardware performance. This workstation is between the local network and the Internet. Seen from both directions, this workstation is the only possibility to exchange data with

the respective other network. There doesn't exist any direct connection between these two networks, but just to the Application Gateway.



The Application Gateway is thus a kind of proxy for each of the two networks. Another term for this constellation is the "dualhomed gateway", because this workstation is so to speak at home in two networks.

For each application to be allowed through this gateway, an own service will be set up, e.g. SMTP for mail, HTTP for surfing the Internet or FTP for data downloads.



This service accepts data received by either one of the two sides and depicts it to the respective other side. What seems to be at first sight a needless mirroring of existing data, is on closer examination the far-reaching concept of Application Gateways: It never exists a direct connection e.g. between a client of the local network and a server of the Internet. The LAN workstations only see the proxy, the workstations of the Internet likewise. This physical separation of LAN and WAN, makes it quite difficult for attackers to intrude into the protected network.

Applied to the porter example, the packet will be left at the gate, the courier is not allowed to enter the company premises. The porter takes the packet, will open it after checking address and delivery note and will control also the content. When the packet has taken these hurdles successfully, then the company internal courier will bring it himself to the addressee of the company. He became proxy of the courier on company premises. The other way around, all

employees, wanting to send a packet, have to inform the porter, which has to collect the packet at the workstation place and which will hand over the packet to the ordered courier at the gate.

Functions of Application Gateways are not supported by the LANCOM, mainly because of the high hardware demands.

8.3 The LANCOM Firewall

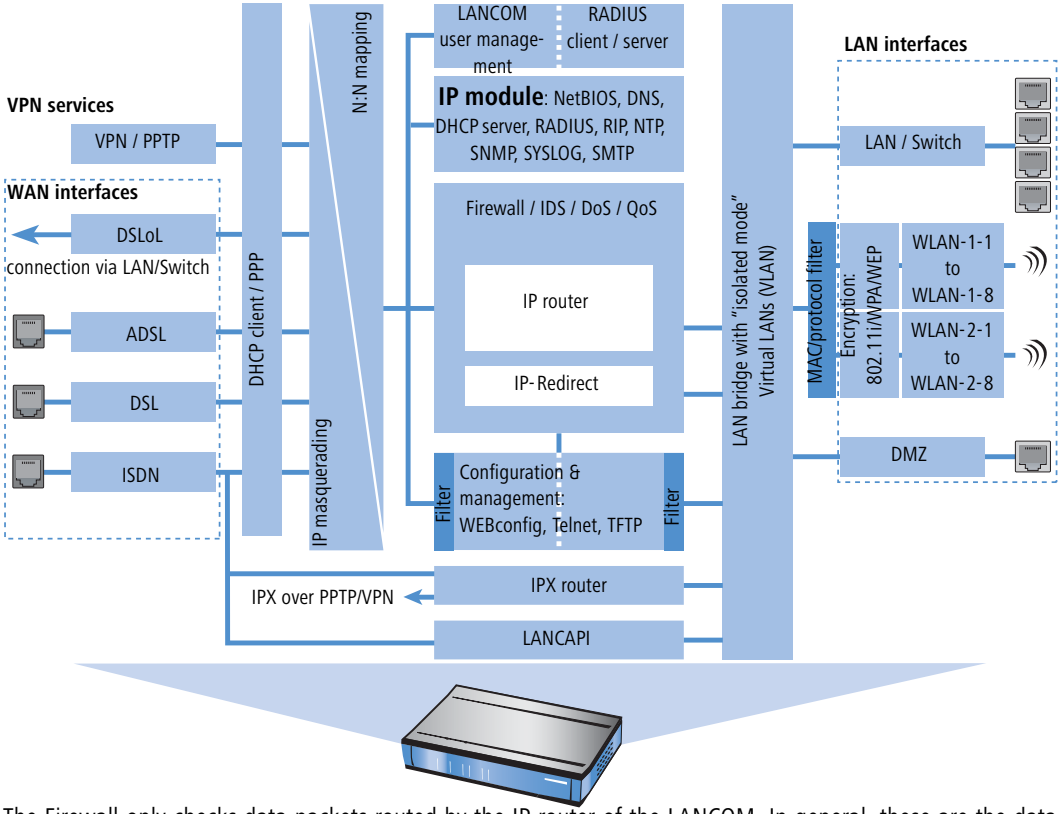
After general explanations concerning the dangers of the Internet and the tasks and types of Firewalls, this chapter describes special functions of the LANCOM Firewall and concrete configurations.

For LANCOM devices with VoIP functions that were already integrated or added in with a software option, the ports required for voice connections are activated automatically.

8.3.1 How the LANCOM Firewall inspects data packets

The Firewall filters only those data packets out of the entire data stream running through the IP router of the LANCOM, for which a special treatment has been defined.

The Firewall only checks routed data packets!



The Firewall only checks data packets routed by the IP router of the LANCOM. In general, these are the data packets, which are exchanged between one of the WAN interfaces and the internal networks (LAN, WLAN, DMZ).

For example, the communication between LAN and WLAN is normally not carried out by the router, as long as the LAN bridge allows a direct exchange. Thus the Firewall rules do not apply here. The same applies to the so-called "internal services" of the LANCOM like Telnet, TFTP, SNMP and the web server for the configuration with WEBconfig. The data packets of these services do not run through the router, and therefore aren't influenced by the Firewall.

Due to the positioning behind the masquerading module (seen from the WAN), the Firewall operates with the "real" internal IP addresses of the LAN stations, and not with the outside known Internet address of the LANCOM.

The LANCOM Firewall uses several lists for checking data packets, which are automatically generated from Firewall rules, resulting Firewall actions or by active data connections:

- Host block list
- Port block list
- Connection list
- Filter list

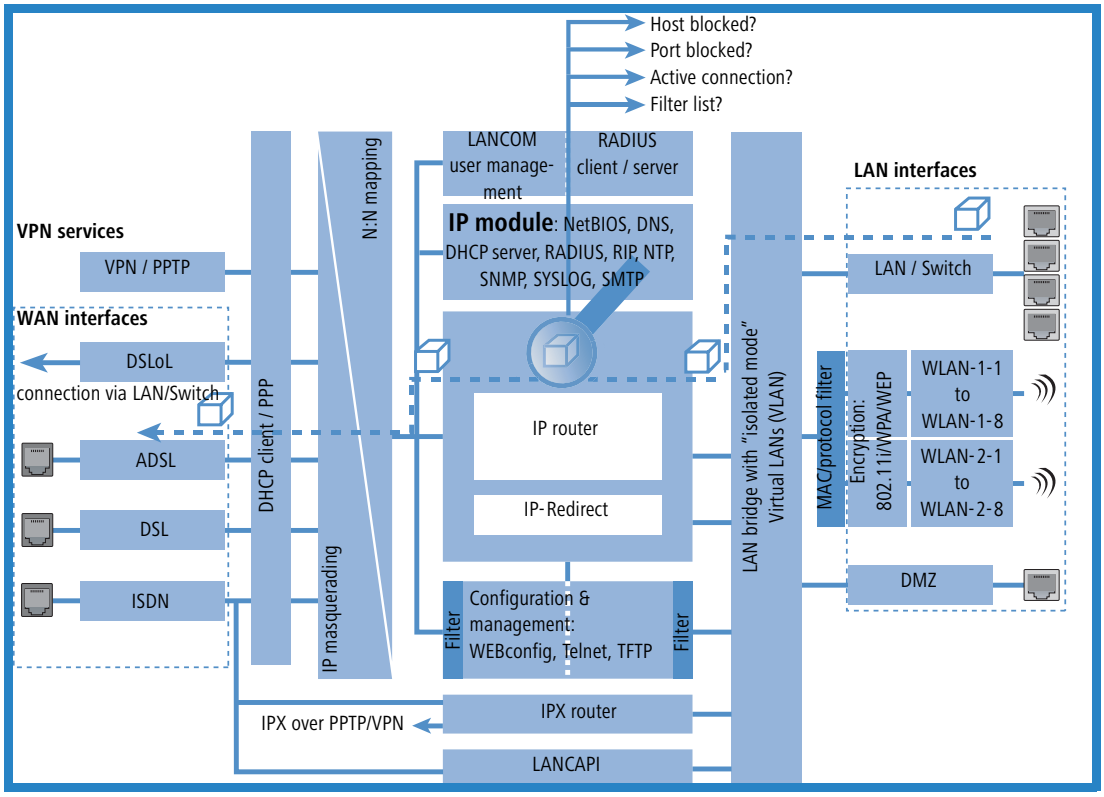
When a data packet should be routed via the IP router, the Firewall uses the lists as follows:

① The first check is, whether the packet was coming from a workstation belonging to the **host block list**. If the sender is blocked, the packet will be discarded.

② If the sender is not blocked in this list, the **port block list** will be checked, if the used port/protocol combination on the destination PC is closed. In this case the packet will be discarded.

③ If sender and destination are not blocked in the first two lists, then it will be checked whether a connection entry exists for this packet in the **connection list**. If such an entry exists, then the packet will be handled as noted in this list.

④ If no entry has been found for the packet, then the **filter list** will be searched, whether a suitable entry exists and the action indicated in this list will be carried out. If the action intends to accept the packet, then an entry is made in the connection list, as well as for any further actions.



If no explicit Firewall rule exists for a data packet, the packet will be accepted ('Allow-All'). That grants a backward-compatibility for existing installations. For maximum protection by the Stateful Inspection, please note the section 'Set-up of an explicit "Deny All" strategy' → page 200.

The four lists obtain their information as follows:

- In the **host block list** are all those stations listed, which are blocked for a certain time because of a Firewall action. The list is dynamic, new entries can be added continuously with appropriate actions of the Firewall. Entries automatically disappear after exceeding the timeout.
- In the **port block list** those protocols and services are filed, which are blocked for a certain time because of a Firewall action. This list is likewise a dynamic one, new entries can be added continuously with the appropriate Firewall actions. Entries automatically disappear after exceeding the timeout.
- For each established connection an entry is made in the **connection list**, if the checked packet has been accepted by the filter list. In the connection list is noted from which source to which destination, over which protocol and which port a connection is actually allowed. The list contains in addition, how long an entry will stay in the list and which Firewall rule is responsible for the entry. This list is very dynamic and permanently "moving".

- The **filter list** is made of the Firewall rules. The containing filters are static and only changed when Firewall rules are added, edited or deleted.

Thus all lists, which are consulted by the Firewall to check data packets, finally base on the Firewall rules ('Parameters of Firewall rules' → page 187).

8.3.2 Special protocols

One important point during the connection tracking is the treatment of protocols that dynamically negotiate ports and/or addresses, over which further communication is done. Examples of these kinds of protocols are FTP, H.323 or also many UDP-based protocols. Thereby it is necessary that further connections must be opened, additionally to the first connection. See also 'Different types of Firewalls' → page 174.

UDP connections

UDP is actually a stateless protocol, nevertheless one can speak regarding UDP-based protocols also of a (only short term) connection, since UDP mostly carries Request/Response based protocols, with which a client directs its requests to a well known port of a server (e.g. 53 for DNS), which in turn sends its responds to the source port selected by the client:

Client port	Connection	Server port
12345	Request →	53
12345	Response ←	53

However, if the server wants to send larger sets of data (e.g. TFTP) and would not like or can not differentiate on the well known port between requests and acknowledges, then it sends the response packets to the source port of the sender of the original request, but uses as its own source port a free port, on which it reacts now only to those packets, which belong to the data communication:

Client port	Connection	Server port
12345	Request →	69
12345	Response ←	54321
12345	Ack/Data →	54321
12345	Data/Ack ←	54321

While the data communication takes place now over the ports 12345 and 54321, the server on the well-known port (69) can accept further requests. If the LANCOM pursues a "Deny All" strategy, the answer packets of an entry of the port filter Firewall, which permits only a connection to port 69 of the server, would simply be discarded. In order to prevent this, when creating the entry in the connection state database, the destination port of the connection is kept free at first, and set only with the arrival of the first answer packet, whereby both possible cases of an UDP connection are covered.

TCP connections

TCP connections cannot be tracked only by examination of the ports. With some protocols (e.g. FTP, PPTP or H.323) examinations of the utilizable data are necessary to open all later negotiated connections, and to accept only those packets belonging really to the connections. This corresponds to a simplified version of IP masquerading, but without addresses or ports to be re-mapped here. It is sufficient to pursue the negotiation to open appropriate ports, and link them with the main connection, so that these ports are closed likewise with the closing of the main connection, and traffic on the secondary connection keeping open also the main connection.

ICMP connections

For ICMP two cases must be differentiated: The ICMP request/reply connections, like to be used with "ping", and the ICMP error messages, which can be received as an answer to any IP packet.

ICMP request/reply connections can be clearly assigned to the identifier used by the initiator, i.e. in the status database an entry will be provided with the sending of an ICMP request, which lets through only ICMP replies with the correct identifier. All other ICMP replies will get discarded silently.

In ICMP error messages, the IP header and the first 8 bytes of the IP packet (on behalf UDP or TCP headers) can be found within the ICMP packet. With the help of this information, the receipt of an ICMP error message triggers automatically the search for the accessory entry in the status database. The packet passes only if such an entry exists, otherwise it is discarded silently. Additionally, potentially dangerous ICMP error messages (redirect route) are filtered out.

Connections of other protocols

For all other protocols no related connections can be followed up, i.e. with them only a connection between involved hosts can occur in the status database. These can be initiated also only from one side, unless, in the port filter Firewall exists a dedicated entry for the "opposite direction".

8.3.3 General settings of the Firewall

Apart from individual Firewall rules, which ensure the entries in the filter, connection and block lists, some settings apply generally to the Firewall:

- Firewall/QoS enabled
- Administrator email (→ Page 185)
- Fragments (→ Page 185)

- Re-establishing of the session (→ Page 185)
- Ping blocking (→ Page 186)
- Stealth mode(→ Page 186)
- Mask authentication port (→ Page 187)

Firewall/QoS enabled

This option switches on or off the entire Firewall, including Quality of Service functions.

Please notice that the N:N mapping functions ('N:N mapping' → page 139) are only active when the Firewall has been switched on!

Administrator email

One of the actions a Firewall can trigger is alerting of an network administrator via email. The "administrator email" is the email account, to which the alerting mails are sent to.

Fragments

Some attacks from the Internet try to outsmart the Firewall by fragmented packets (packets split into several small units). One of the main features of a Stateful Inspection like in the LANCOM is the ability to re-assemble fragmented packets in order to check afterwards the entire IP packet.

You can centrally adjust the desired behavior of the Firewall. The following options are available:

- **Filter**: Fragmented packets are directly discarded by the Firewall.
- **Route**: Fragmented packets are passed on without any further checking by the Firewall, as long as permitted by valid filter settings.
- **Re-assemble**: Fragmented packets are buffered and re-assembled to complete IP packets. The re-assembled packets will then be checked and treated according to the valid filter settings.

Session recovery

The Firewall enters all actual permitted connections into the connection list. Entries disappear automatically from the connection list after a certain time (timeout), when no data has been transmitted over this connection any more re-triggering the timeout.

Sometimes connections are ended according to the general TCP aging settings, before data packets requested by an inquiry have been received by the remote station. In this case perhaps an entry for a permitted connection still exists in the connection list, but the connection itself is no more existing.

The parameter "Session recovery" determines the behavior of the Firewall for packets that indicate a former connection:

- **Always denied**: The Firewall re-establishes the session under no circumstances and discards the packet.
- **Denied for default route**: The Firewall re-establishes the session only if the packet wasn't received via the default route (e.g. Internet).

- **Denied for WAN**: The Firewall re-establishes the session only if the packet wasn't received over one of the WAN interfaces.
- **Always allowed**: The Firewall re-establishes the connection in principle if the packet belongs to a former connection of the connection list.

Ping blocking

One - not undisputed - method to increase security is hiding the router. Based loosely on the method: "Who doesn't see me neither tries to attack me...". Many attacks begin with the searching for workstations and/or open ports by actual harmless inquiries, e. g. with the help of the "ping" command or with a portscan. Each answer to these inquiries, even the answer "I'm not here" indicates to the attacker that he has found a potential destination. Because anybody who answers must be existing, too. In order to prevent this conclusion, the LANCOM is able to suppress the answers to these inquiries.

In order to achieve this, the LANCOM can be instructed not to answer ICMP echo requests any more. At the same time TTL-exceeded messages of a "trace route" are also suppressed, so that the LANCOM cannot be found, neither by "ping" nor by "trace route".

Possible settings are:

- **Off**: ICMP answers are not blocked.
- **Always**: ICMP answers are always blocked.
- **WAN only**: ICMP answers are blocked on all WAN connections.
- **Default route only**: ICMP answers are blocked on default route (usually Internet).

TCP Stealth mode

Apart from ICMP messages, also the behavior in case of TCP and UDP connections gives information on the existence or non-existence of the addressed workstation. Depending on the surrounding network it can be useful to simply reject TCP and UDP packets instead of answering with a TCP RESET resp. an ICMP message (port unreachable), if no listener for the respective port exists. The desired behavior can be adjusted in the LANCOM.

If ports without listener are hidden, this generates a problem on masked connections, since the "authenticate" - resp. "ident" service does no longer function properly (resp. do no longer correctly reject). The appropriate port can so be treated separately ('Mask authentication port' → page 187).

Possible settings are:

- **Off**: All ports are closed and TCP packets are answered with a TCP reset.
- **Always**: All ports are hidden and TCP packets are silently discarded.
- **WAN only**: On the WAN side all ports are hidden and on the LAN side closed.
- **Default route only**: Ports are hidden on the default route (usually Internet) and closed on all other routes.

Mask authentication port

When TCP or UDP ports are hidden, inquiries of mail servers to authenticate users can no more be answered correctly. Inquiries of the servers run into a timeout, and delivery of mails will be considerably delayed.

Also when the TCP Stealth mode is activated, the Firewall detects the intention of a station in the LAN to establish a connection to a mail server. As a result, the needed port will be opened for a short time (20 seconds) solely for the authentication inquiry.

This behavior of the Firewall in TCP Stealth mode can be suppressed specifically with the parameter "Always mask authentication port, too".

The activation of the option "Mask authentication port" can lead to considerable delays for the dispatch and receipt of e. g. emails or news!

A mail or a news server, which requests any additional information from the user with the help of this service, runs first into a disturbing timeout, before it begins to deliver the mails. This service needs thus its own switch to hide and/or to hold it "conformingly".

The problem thereby is however that a setting, which hides all ports, but rejects the ident port is unreasonable - alone by the fact that rejecting the ident port would make the LANCOM visible.

The LANCOM offers now the possibility to reject ident inquiries only by mail and news servers, and to discard those of all other PCs. For this, the ident inquiries of the respective servers are rejected for a short time (20 seconds) when a mail (SMTP, POP3 IMAP2) or a news server (NNTP) is calling up.

When the timeout is exceeded, the port will be hidden again.

8.3.4 Parameters of Firewall rules

In this section we describe the components of Firewall rules and the available options to set up the different parameters.

Information regarding definition of Firewall rules with the different kinds of configuration tools (LANconfig, WEBconfig or Telnet) can be found in chapter 'Configuration of Firewall rules' → page 202.

Components of a Firewall rule

A Firewall rule is at first defined by its name and some further options:

- **On/Off switch**: Is the rule active for the Firewall?
- **Priority**: Which is the priority of the rule? (→ Page 188)
- **Observe further rules**: Should further Firewall rules be observed when this rule applies to a data packet? (→ Page 188)
- **Create VPN rule**: Is this Firewall rule also used to create a VPN rule? (→ Page 189)

- **Routing Tag**: When applying the routing tag further information about for instance the used service or protocol can be used for selecting the target route. With this so called policy based routing a much better control of the routing behaviour is possible ('Policy-based routing' → page 109).

Priority

When setting up the filter list of the Firewall rules, the LANCOM will automatically sort the entries. Thereby the "grade of detail" will be considered: All specified rules are observed at first, after that the general ones (e. g. Deny All).

If after the automatic sorting the desired behavior of the Firewall does not turn out, it is possible to change the priority manually. The higher the priority of the Firewall rule, the earlier it will be placed in the according filter list.

For complex rule types please check the filter list as described in section 'Firewall diagnosis' → page 211.

Observe further rules

There are requirements to a Firewall, which cannot be covered by a single rule. If the Firewall is used to limit the Internet traffic of different departments (in own IP subnetworks), individual rules cannot e.g. illustrate the common upper limit at the same time. If to everyone of e.g. three departments should be granted a bandwidth of maximal 512 kbps, but the entire data rate of the three departments should not exceed a limit of 1024 kbps, then a multi-level checking of the data packets must be installed:

- In a first step it will be checked, if the actual data rate of the individual department does not exceed the limit of 512 kbps.
- In a second step it will be checked, if the data rate of all departments together does not exceed the overall limit of 1024 kbps.

Normally the list of the Firewall rules is applied sequentially to a received data packet. If a rule applies, the appropriate action will be carried out. The checking by the Firewall is terminated then, and no further rules will be applied to the packet.

In order to reach a two-stage or multi-level checking of a data packet, the "Observe further rules option" will be activated for the rules. If a Firewall rule with activated observation of further rules applies to a data packet, the appropriate action will be carried out at first, but then the checking in the Firewall will continue. If one of the further rules applies also to this data packet, the action being defined in this rule will also be carried out. If also for this following rule the observe further rules option is activated, the checking will be continued until

- either a rule applies to the packet, for which observe further rules is not activated.
- or the list of the Firewall rules has been completely worked through without applying a further rule to the packet.

To realize this aforementioned scenario it is necessary to install for each subnetwork a Firewall rule that rejects from a data rate of 512 kbps up additional packets of the protocols FTP and HTTP. For these rules the observe further rules option will be activated. Defined in an additional rule for all stations of the LAN, all packets will be rejected which exceed the 1024 kbps limit.

VPN rules

A VPN rule can receive its information about source and destination network from Firewall rules.

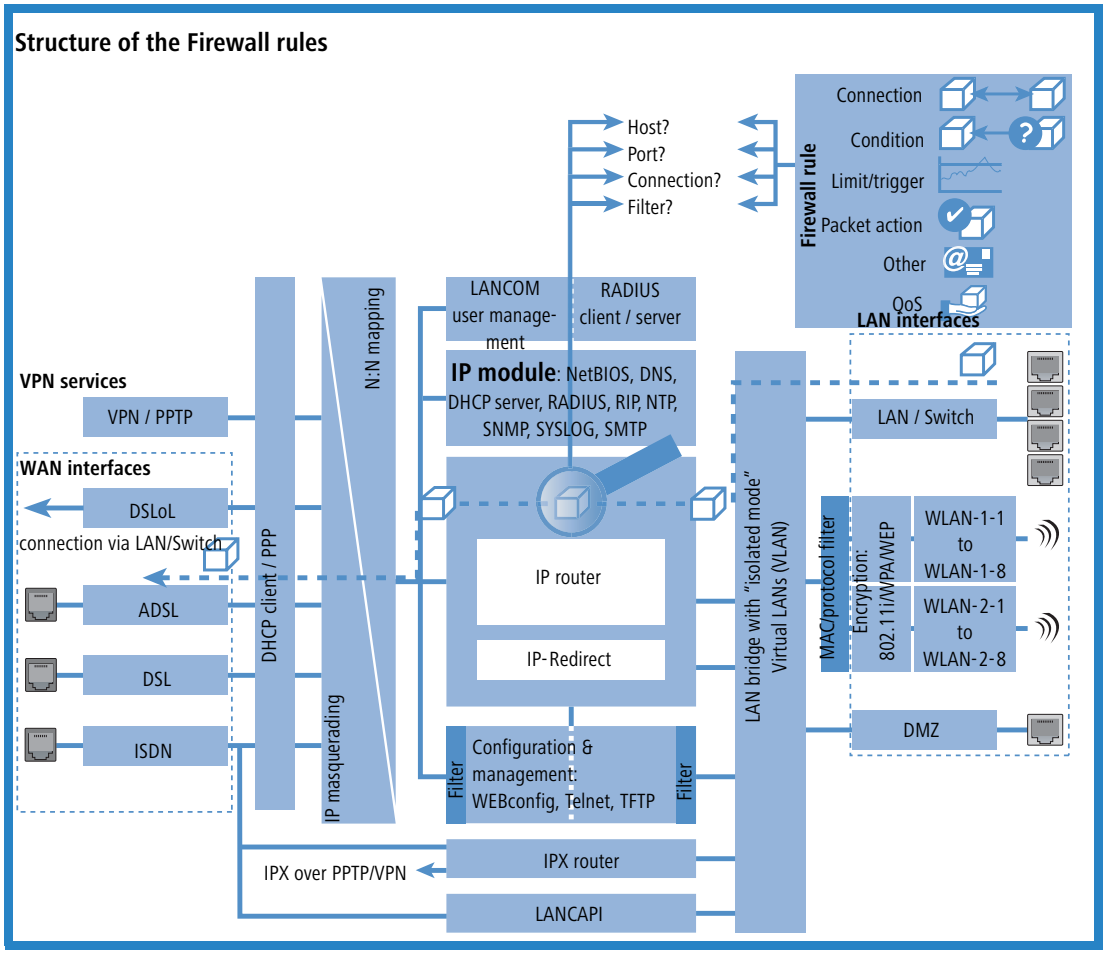
By activating the option "This rule is used to create VPN rules" for a Firewall rule, you determine that a VPN rule will be derived from this Firewall rule.

Apart from this basic information, a Firewall rule answers the question when and/or on what it should apply to and which actions should be executed:

- **Stations / Service**: To which stations/networks and services/protocols does the rule refer to? (→ Page 190)
- **Conditions**: Is the effectiveness of the rule reduced by other conditions? (→ Page 191)
- **Trigger**: On exceeding of which threshold shall the rule being triggered? (→ Page 191)
- **Action**: What should happen to the data packets when the condition applies and the limit is reached? (→ Page 192)
- **Further measures**: Should further measures be initiated apart from the packet action? (→ Page 192)
- **Quality of Service (QoS)**: Are data packets of certain applications or with the corresponding markings transferred preferentially by assurance of special Quality of Services? (→ Page 192)

Condition, limit, packet action and other measures form together a so-called "action set". Each Firewall rule can contain a number of action sets. If the same trigger is used for several action sets, the sequence of action sets can be adjusted.

In section 'How the LANCOM Firewall inspects data packets' → page 179 we have already described that in the end the lists for checking data packets are created from Firewall rules. Thus the extension of the block diagram looks like as follows:



Connection

The connection of a Firewall rule defines to which data packets the rule should refer to. A connection is defined by its source, its destination and the used services. The following details can be used to specify the source or destination:

- All stations
- The entire local network (LAN)
- Certain remote stations (described by the name of the remote site list)
- Certain stations of the LAN described by the host name)
- Certain MAC[1] addresses

- Ranges of IP addresses
- Complete IP networks

You can only operate with host names, when your LANCOM is able to transform the names into IP addresses. For that purpose the LANCOM must have learned the names via DHCP or NetBIOS, or the assignment must be entered statically in the DNS or IP routing table. An entry in the IP routing table can therefore assign a name to a whole network.

If the source or the destination for a Firewall rule has not been determined at greater detail, the rule applies generally to data packets "from all stations" resp. "to all stations".

The service is determined by the combination of an IP protocol with respective source and/or destination port. For frequently used services (www, mail, etc.) the appropriate combinations are already predefined in the LANCOM, others can be compiled additionally as required.

Condition

The effectiveness of a Firewall rule is also reduced with additional conditions. The following conditions are available:

- Only packets with certain ToS and/or DiffServ markings.
- Only, if the connection does not yet exist.
- Only for default route (Internet).
- Only for VPN routes.

Limit / Trigger

The limit or trigger describes a quantified threshold value that must be exceeded on the defined connection before the filter action gets executed for a data packet. A limit is composed by the following parameters:

- Unit (kbit, kbyte or packets)
- Amount, that means data rate or number.
- Reference value (per second, per minute, per hour or absolute)

Additionally, you can adjust for the limit whether it refers to a logical connection or to all connections together, which exist between the defined destination and source stations via the corresponding services. Thus it is controlled whether the filter takes effect, if e.g. all HTTP connections of the users in the LAN exceed the limit in sum, or whether it is sufficient that only one of the parallel established HTTP connections exceeds the threshold value.

For absolute values it is additionally possible to specify whether the counter belonging to it will be reset to zero when the limit has been reached.

1. MAC is the abbreviation for **M**edia **A**ccess **C**ontrol and it is the crucial factor for communication inside of a LAN. Every network device has its own MAC address. MAC addresses are worldwide unique, similar to serial numbers. MAC addresses allow distinguishing between the PCs in order to give or withdraw them dedicated rights on an IP level. MAC addresses can be found on most networking devices in a hexadecimal form (e.g. 00:A0:57:01:02:03).

In any case, data will be transferred if a limit has not been reached yet! With a trigger value of zero a rule becomes immediately active, as soon as data packets arrive for transmission on the specified connection.

Packet action

The Firewall has three possibilities to treat a filtered packet:

- **Transmit**: The packet will be transferred normally.
- **Drop**: The packet will be discarded silently.
- **Reject**: The packet will be rejected, the addressee receives an appropriate message via ICMP.

Further measures

The Firewall does not only serve to discard or accept the filtered data packets, but it can also take additional measures when a data packet has been registered by the filter. The measures here are divided into the fields “protocolling/notification” and “prevent further attacks”:

- **Send a Syslog message**: Sends a message via the SYSLOG module to a SYSLOG client, as defined in configuration field “Log & Trace”.
- **Send an email message**: Sends an email message to the administrator, using the account specified in the configuration field “Log & Trace”.
- **SNMP/LANmonitor**: Sends a SNMP trap, that will be analyzed e. g. by LANmonitor.

Each of these three message measures leads automatically to an entry in the Firewall event table.

- **Disconnect**: Cuts the connection, over which the filtered packet has been received.

On the occasion, the physical connection will be cut off (e. g. the Internet connection), not only the logical connection between the two involved PCs!

- **Lock source address**: Blocks the IP address from that the filtered packet has been received for a given time.
- **Lock target port**: Blocks the destination port to that the filtered packet has been sent for a given time.

Quality of Service (QoS)

Apart from the restrictions for the transfer of data packets, the Firewall can also concede a “special treatment” to certain applications. QoS settings use features of the Firewall to specifically identify data packets of certain connections or services.

For further information about QoS and the appropriate configuration please see chapter ’Quality of Service’ → page 226.

8.3.5 Alerting functions of the Firewall

This paragraph describes the Firewall alerts in detail that are sent on security-relevant events. The following message types are available:

- Email notification
- SYSLOG report
- SNMP trap

Alerts are triggered either separately by the intrusion detection system, by the denial of service protection or by arbitrary trigger conditions specified in the Firewall. The specific parameters for the different alerting types such as the relevant email account can be set at the following places:

Configuration tool	Run
LANconfig	Log & Trace ▶ SMTP Account ▶ SNMP ▶ SYSLOG
WEBconfig	Expert Configuration ▶ Setup ▶ SMTP ▶ SNMP Module SYSLOG Module
Terminal/Telnet	`/Setup/SMTP resp. SNMP Module or SYSLOG Module`

An example:

Let us assume a filter named 'BLOCKHTTP', which blocks all access to a HTTP server 192.168.200.10. In case some station would try to access the server nevertheless, the filter would block any traffic from and to this station, and inform the administrator via SYSLOG also.

SYSLOG notifications

If the Firewall drops an appropriate packet, a SYSLOG notification is created (see 'Setting up the SYSLOG module' → page 546) as follows:

```
PACKET_ALERT: Dst: 192.168.200.10:80 {}, Src: 10.0.0.37:4353 {} (TCP): port filter
```

Ports are printed only for port-based protocols. Station names are printed, if the LANCOM can resolve them directly (without external DNS request).

If the SYSLOG flag is set for a filter entry (`%s` action), then this notification becomes more detailed. Then the filter name, the exceeded limit and the filter action carried out are printed also. For the example above this should read as:

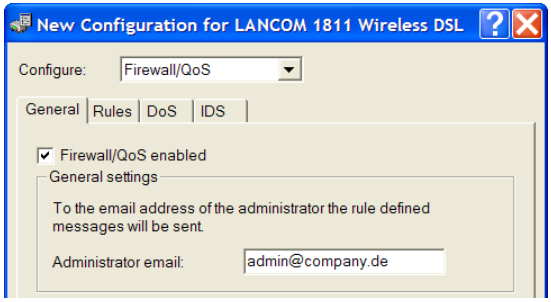
```
PACKET_ALERT: Dst: 192.168.200.10:80 {}, Src: 10.0.0.37:4353 {} (TCP): port filter
PACKET_INFO:
matched filter: BLOCKHTTP
exceeded limit: more than 0 packets transmitted or received on a connection
actions: drop; block source address for 1 minutes; send syslog message;
```

Notification by email

If the email system of the LANCOM is activated, then you can use the comfortable notification by email. The device sends an email to the administrator as soon as the firewall executes the appropriate action:

```
FROM: LANCOM_Firewall@MyCompany.com
TO: Administrator@MyCompany.com
SUBJECT: packet filtered

Date: 9/24/2002 15:06:46

The packet below

Src: 10.0.0.37:4353 {cs2} Dst: 192.168.200.10:80 {ntserver} (TCP)

45 00 00 2c ed 50 40 00 80 06 7a a3 0a 00 00 25 | E..,.P@. ..z....%
c0 a8 c8 0a 11 01 00 50 00 77 5e d4 00 00 00 00 | .......P .w^.....
60 02 20 00 74 b2 00 00 02 04 05 b4 | `. .t... ....

matched this filter rule: BLOCKHTTP
and exceeded this limit: more than 0 packets transmitted or received on a connection

because of this the actions below were performed:
drop
block source address for 1 minutes
send syslog message
send SNMP trap
send email to administrator
```

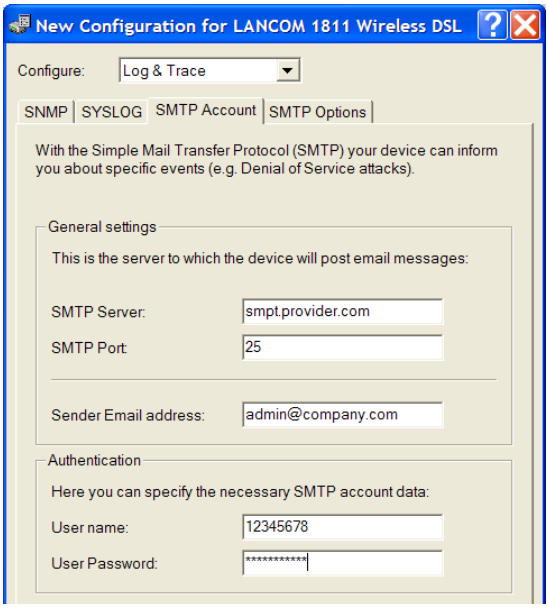
Sending the email from the LANCOM to the administrator only works if the right email address is entered. Under LANconfig you can enter the email address in the configuration area 'Firewall/QoS' under the tab 'General' .



Under WEBconfig or Telnet you can find the administrator email address as follows:

Configuration tool	Call
WEBconfig	Expert Configuration ▶ Setup ▶ IP Router ▶ Firewall
Terminal/Telnet	`/Setup/IP-Router/Firewall`

To send an email an the required settings must be entered under LANconfig in the configuration area 'Log & Trace' under the tab 'SMTP Account'.



Under WEBconfig or Telnet the SMTP settings can be reached as follows:

Configurations tool	Run
WEBconfig	Expert Configuration ▶ Setup ▶ SMTP
Terminal/Telnet	`/Setup/SMTP`

Notification by SNMP trap

If as notification method dispatching SNMP traps was activated (see also 'SNMP' → page 34), then the first line of the logging table is sent away as enterprise specific trap 26. This trap contains additionally the system descriptor and the system name from the MIB-2.

For the example the following trap is thus produced:

```
SNMP: SNMPv1; community = public; SNMPv1 Trap; Length = 443 (0x1BB)
SNMP: Message type = SNMPv1
SNMP: Version = 1 (0x0)
SNMP: Community = public
SNMP: PDU type = SNMPv1 Trap
```

```
SNMP: Enterprise = 1.3.6.1.4.1.2356.400.1.6021
SNMP: Agent IP address = 10.0.0.43
SNMP: Generic trap = enterpriseSpecific (6)
SNMP: Specific trap = 26 (0x1A)
SNMP: Time stamp = 1442 (0x5A2)
```

System descriptor

```
SNMP: OID = 1.3.6.1.2.1.1.1.0 1.
SNMP: String Value = LANCOM Business 6021 2.80.0001 / 23.09.2002 8699.000.036
```

Device string

```
SNMP: OID = 1.3.6.1.2.1.1.5.0 2. System-Name
SNMP: String Value = LANCOM Business 6021
```

Time stamp

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.2.1 3.
SNMP: String Value = 9/23/2002 17:56:57
```

Source address

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.3.1 3.
SNMP: IP Address = 10.0.0.37
```

Destination address

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.4.1 4.
SNMP: IP Address = 192.168.200.10
```

Protocol (6 = TCP)

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.5.1 5.
SNMP: Integer Value = 6 (0x6) TCP
```

Source port

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.6.1 6.
SNMP: Integer Value = 4353 (0x1101)
```

Destination port (80 = HTTP)

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.7.1 7.
SNMP: Integer Value = 80 (0x50)
```

Name of the filter rule

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.8.1 8.
SNMP: String Value = BLOCKHTTP
```

This trap and all different in the LANCOM generated traps are sent to all manually configured trap receivers, just like to each registered LANmonitor, which can evaluate this and possibly all other traps.

8.3.6 Strategies for Firewall settings

Firewalls are the interface between networks, and they restrict to a smaller or larger extent an unhindered data exchange. Thus Firewalls have opposite objectives than networks, although they are a part of them: networks should connect workstations, Firewalls should prevent the connection.

This contradiction shows the dilemma of the responsible administrators who have developed subsequently different strategies to solve this problem.

Allow All

The Allow All strategy favours unhindered communication of the employees compared over security. Any communication is allowed at first, the LAN is still open for attackers. The LAN becomes gradually more secured by configuration of the administrator, by settings of more and more new rules, which restrict or prevent parts of communication.

Deny All

The Deny All strategy proceeds at first according to the method "Block all!". The Firewall blocks completely the communication between the protected network and the rest of the world. In a second step, the administrator opens address ranges or ports, which are necessary e.g. for daily communication with the Internet.

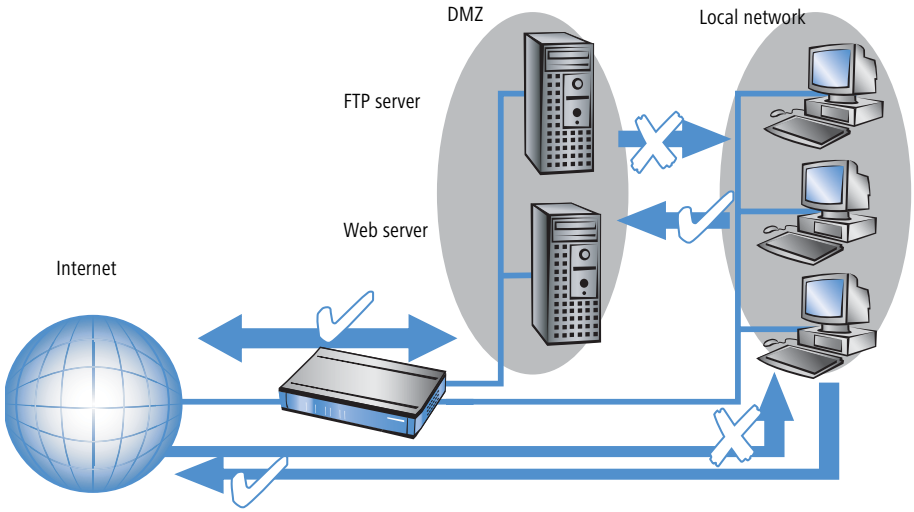
This approach ensures superior security for the LAN security compared to the Allow All strategy, but may lead especially in its initial stages to difficulties for the users. After activation of the Deny All strategy, some things just may behave differently than before, some stations may not reached any more etc.

Firewall with DMZ

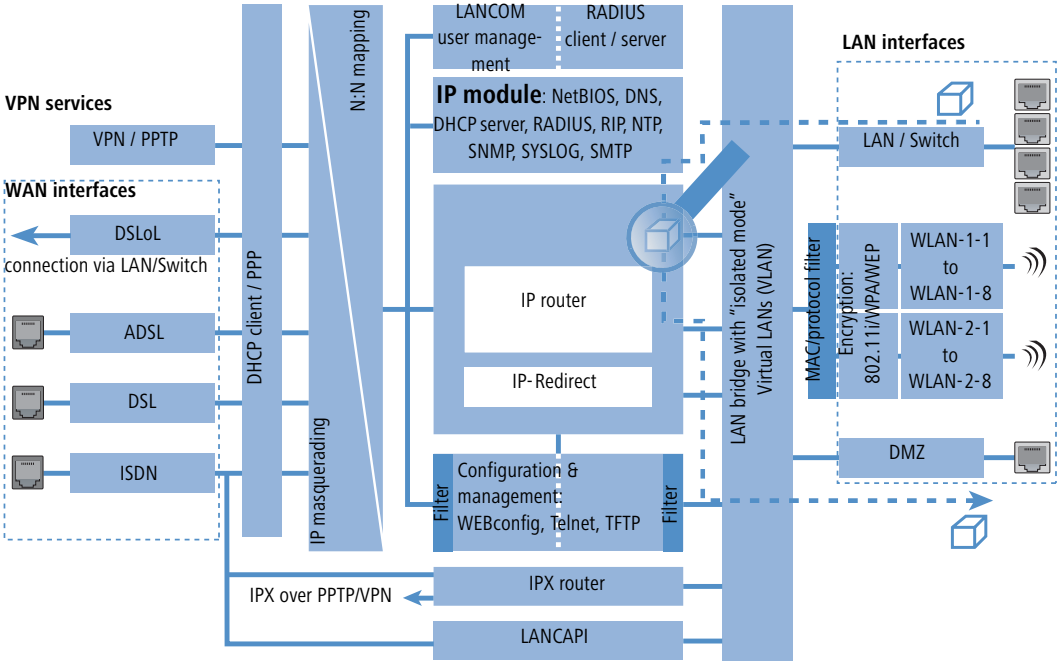
The demilitarized zone (DMZ) is a special range of the local network, which is shielded by a Firewall both against the Internet and against the normal LAN. All stations or servers that should be accessible from the unsecured network (Internet) should be placed into this network. These include for example own FTP and web servers.

The Firewall protects at first the DMZ against attacks from the Internet. Additionally, the Firewall protects also the LAN against the DMZ. To do so, the Firewall is configured in this way that only the following accesses are possible:

- Stations from the Internet can access to the servers in the DMZ, but no access from the Internet to the LAN is possible.
- The stations of the LAN can access the Internet, as well as servers in the DMZ.
- Servers of the DMZ have no access to the stations of the LAN. That guarantees that no "cracked" server of the DMZ becomes a security risk for the LAN.



Some LANCOM models support this structure by a separate LAN interface only used for the DMZ. Looking at the path of data through the LANCOM, then the function of the Firewall for shielding the LAN against the DMZ becomes visible.



A direct data exchange between LAN and DMZ via LAN bridge is not possible if a dedicated DMZ port is used. The path from LAN to DMZ and vice versa is therefore only possible through the router, and thus also only through the Firewall! This shields the LAN against inquiries from the DMZ, similar to the LAN against inquiries from the Internet.

The shielding of the DMZ against the Internet on one side and the LAN on the other is solved in many network structures with two separate Firewalls. When using a LANCOM with DMZ port, only one device for this setup is needed, which e.g. results in a clearly simplified configuration.

8.3.7 Hints for setting the Firewall

The LANCOM Firewall is an extremely flexible and powerful tool. In order to help you to creating individual Firewall rules, you'll find in the following some hints for your specific application

For LANCOM devices with VoIP functions that were already integrated or added in with a software option, the ports required for voice connections are activated automatically.

The default settings of the Firewall

On delivery there is exactly one entry in the Firewall rule table: “WINS”. This rule prevents unwanted connection set-ups on the default route (gen. to the Internet) by the NetBIOS protocol. Windows networks send inquiries in regular intervals into the network to find out if known stations are still available. This leads in case of a time-based account of a network coupling to unwanted connection set-ups.

The LANCOM can prevent this by the integrated NetBIOS proxy also for network couplings, by pretending an answer for the concerned resource, until a real access takes place.

Security by NAT and Stateful Inspection

If no further Firewall rule will be entered, the local area network is protected by the interaction of Network Address Translation and Stateful Inspection: Only connections from the local area network produce an entry in the NAT table, whereupon the LANCOM opens a communication port. The Stateful Inspection supervises communication via this port: Only packets, which belong exactly to this connection may communicate via this port. For accesses from the outside to the local network results thus an implicit "Deny All" strategy.

Transmitting firewall rules with scripts

With the help of scripts firewall rules can easily be transmitted to device and software (‘Scripting’ → page 57). Example scripts are saved in the LANCOM KnowledgeBase under www.lancom.de/support.

If you operate a web server in your LAN, that has been permitted access to this service from the outside (see 'IP masquerading' → page 120), stations from the Internet can establish from the outside connections to this server. The inverse masquerading has priority over the Firewall in this case, as long as no explicit "Deny All" rule has been set.

Set-up of an explicit "Deny All" strategy

For maximum protection and optimum control of the data traffic it is recommended to prevent first any data transfer by the Firewall. Then only the necessary functions and communication paths are allowed selectively. This offers e.g. protection against so-called "Trojans" and/or e-mail viruses, which set up actively an outgoing connection on certain ports.

Deny All: The most important Firewall rule!

The Deny All rule is by far the most important rule to protect local networks. By this rule the Firewall operates according to the principle: "All actions, which are not explicitly allowed, remain forbidden!" Only by this strategy the administrator can be sure not to have "forgotten" an access method, because only those accesses exist, which have been opened explicitly by himself.

We recommend to set up the Deny All rule before connecting the LAN via a LANCOM to the Internet. Then you can analyse in the logging table (to start e. g. via LANmonitor), which connection attempts have been blocked by the Firewall. With the help of this information the Firewall and the "Allow rules" can be gradually extended.

Some typical applications are shown in the following.

All filters described here can be installed very comfortably with the Firewall wizard, and if necessary be further refined with e.g. LANconfig.

- Example configuration "Basic Internet"

Rule name	Source	Destination	Action	Service (target port)
ALLOW_HTTP	Local network	All stations	transmit	HTTP, HTTPS
ALLOW_FTP	Local network	All stations	transmit	FTP
ALLOW_EMAIL	Local network	All stations	transmit	MAIL, NEWS
ALLOW_DNS_FORWARDING	IP address of LANOM (or: Local network)	transmit	transmit	DNS
DENY_ALL	All stations	reject	reject	ANY

- If you want to permit a VPN dial-in to a LANCOM acting as VPN gateway, then you need a Firewall rule allowing incoming communication from the client to the local network:

Rule	Source	Destination	Action	Service
ALLOW_VPN_DIAL_IN	remote site name	Local network	transmit	ANY

- In case a VPN is not terminated by the LANCOM itself (e.g. a VPN Client in the local area network, or LANCOM as Firewall in front of an additional VPN gateway), you'd have to allow IPSec and/or PPTP (for the "IPSec over PPTP" of the LANCOM VPN Client) ports additionally:

Rule	Source	Destination	Action	Service (target port)
ALLOW_VPN	VPN Client	VPN Server	transmit	IPSEC, PPTP

- For ISDN or V.110 dial-in (e.g. by HSCSD mobile phone) you have to allow the particular remote site (see also 'Configuration of remote stations' → page 117):

Rule	Source	Destination	Action	Service
ALLOW_DIAL_IN	remote site name	Local network	transmit	ANY

- For a network coupling you permit additionally the communication between the involved networks:

Rule	Source	Destination	Action	Service
ALLOW_LAN1_TO_LAN2	LAN1	LAN2	transmit	ANY
ALLOW_LAN2_TO_LAN1	LAN2	LAN1	transmit	ANY

- If you operate e.g. an own web server, you selectively allow access to the server:

Rule	Source	Destination	Action	Service (target port)
ALLOW_WEBSERVER	ANY	Webserver	transmit	HTTP, HTTPS

- For diagnostic purposes it is helpful to allow ICMP protocols (e.g. ping):

Rule	Source	Destination	Action	Service
ALLOW_PING	Local network	ANY	transmit	ICMP

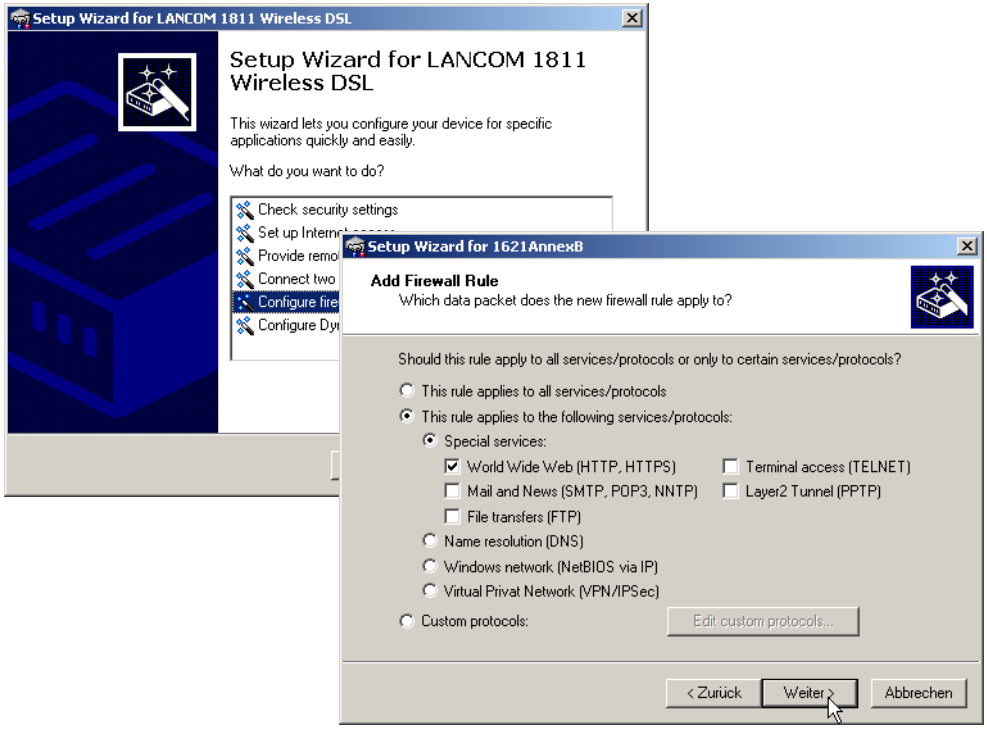
These rules can now be refined as needed - e.g. by the indication of minimum and maximum bandwidths for the server access, or by a finer restriction on certain services, stations or remote sites.

The LANCOM automatically sorts Firewall rules when creating the filter list. Thereby, the rules are sorted into the filter list on the basis of their level of detail. First all specific rules are considered, afterwards the general ones (e.g. Deny All). Examine the filter list in case of complex rule sets, as described in the following section.

8.3.8 Configuration of Firewall rules

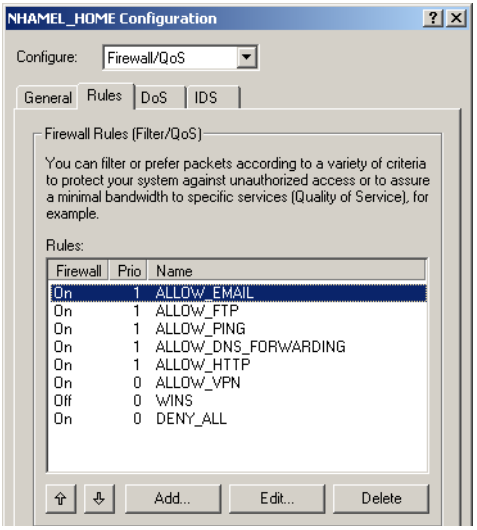
Firewall wizard

The fastest method to configure the Firewall is provided by the Firewall wizard in LANconfig:



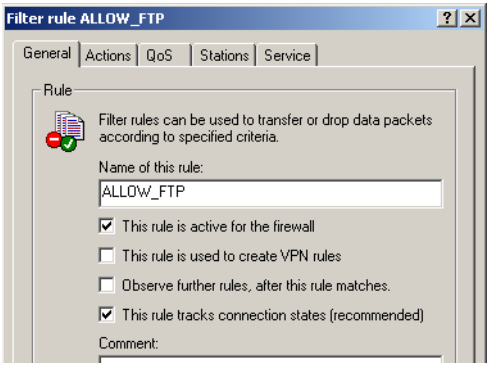
LANconfig

The filters can be installed very comfortably with LANconfig. Starting from the general register card "Firewall / QoS / Rules", you reach after "Add" or "Edit" the dialogue to define the Firewall rules:

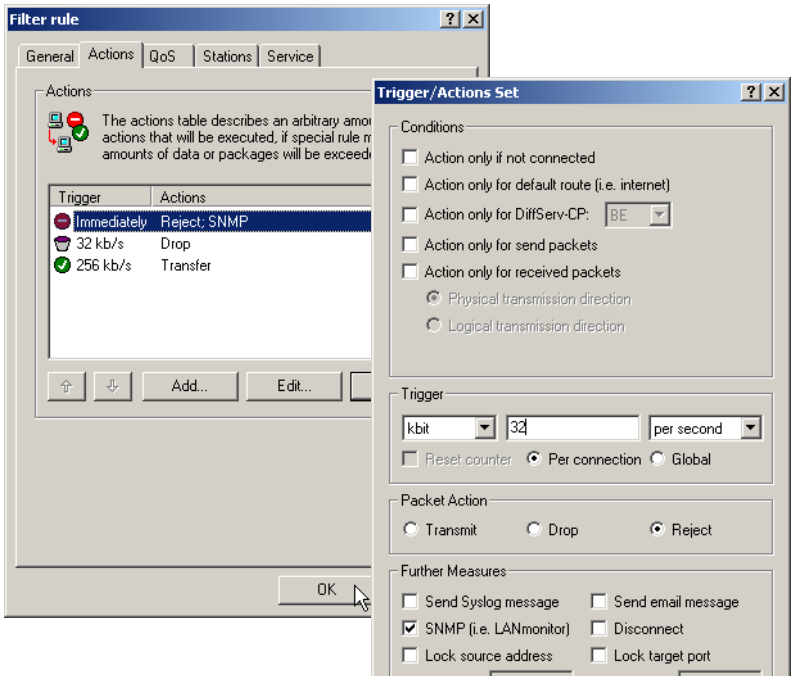


Within the dialogue for the definition of filter rules, the following options can be found on different index cards:

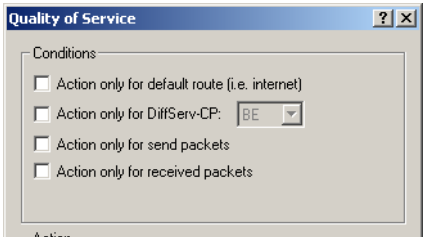
- **General**: Here the name of the Firewall rule is specified, as well as if further rules should be considered after this rule matched, and whether a VPN rule should be derived from this rule.



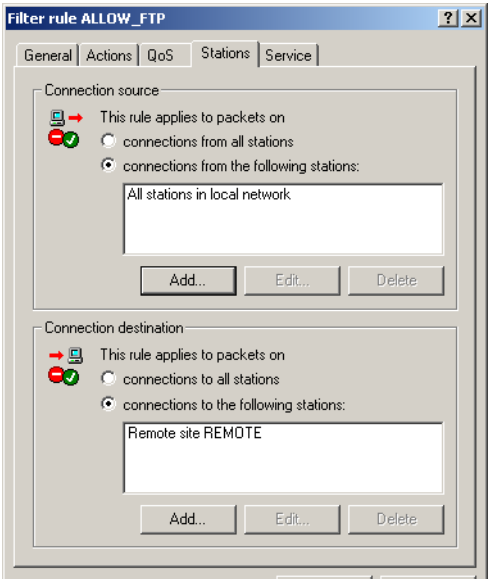
  - The option 'Observe further rules ...' can be used to create complex functions ensuring e.g. certain bandwidths with QoS (’Connection’ → page 190)
  - The option 'This rule is used to create VPN rules' enables to utilize the information about source and destination networks of this rule also to define VPN networks.
- **Actions**: Here the Firewall actions are defined, consisting of condition, trigger, packet action and further measures.



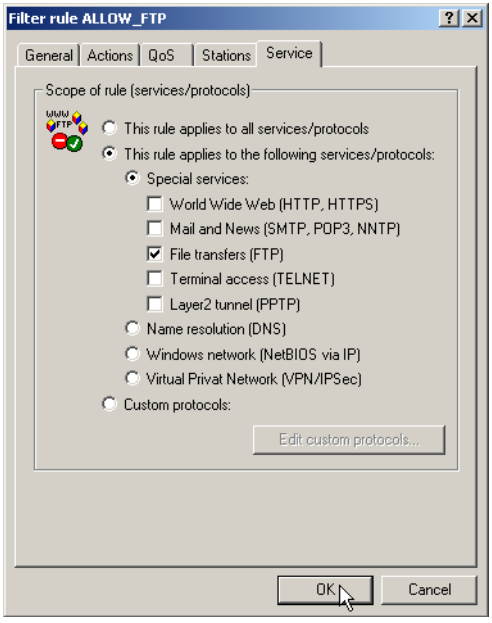
- **QoS**: Here you can assign minimum bandwidths for data packets specified by according Firewall rules (see also 'Defining minimum and maximum bandwidths' → page 240).



- **Stations**: Here the stations – as sender or addressee of the packets – are specified, for which the filter rule shall match.



- **Services**: Here the IP protocols, source and destination ports are specified for which the filter rule shall apply. For example, it can be specified here that only access to web pages and emails shall be permissible.



WEBconfig, Telnet

Under WEBconfig or Telnet the Firewall rules are configured in the following menus and lists:

Configuration tool	Run
WEBconfig	Expert Configuration / Setup / IP Router Module/ Firewall: Rule Table, Object Table, Actions Table
Terminal/Telnet	Setup / IP Router Module/ Firewall / Rule Table, Object Table, Actions Table

There is a special syntax in LCOS for the description of the Firewall rules. This syntax allows to describe also complex relations for checking and treatment of data packets within the Firewall just with a few characters.

Rules are defined in the rule table. Pre-defined objects can be saved in two additional tables in order to prevent entering frequently used objects each time again in LCOS syntax:

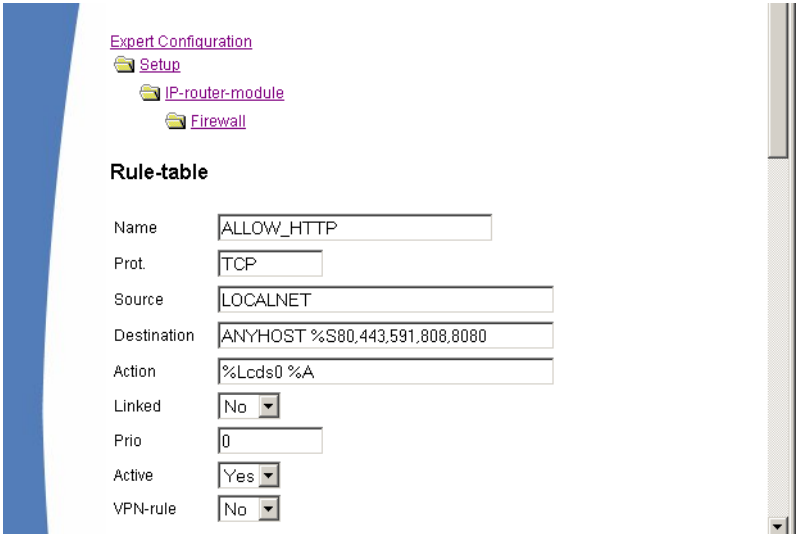
- The action table contains Firewall actions
- The object table contains stations and services

Objects from these tables can be used for rule definition, but this is not a must. They simply facilitate the use of frequently used objects.

Rule table

The rule table combines different information to a Firewall rule. The rule contains the protocol to be filtered, the source, the destination as well as the Firewall action to be executed. For each Firewall rule there is an additional on/off-switch, a priority, the option for a linkage with other rules and an activation of the rule for VPN connections. General information concerning these parameters can be found in section 'Parameters of Firewall rules' → page 187.

The definition of the Firewall rules can be composed of entries of the object table for protocols, services, stations (→ Page 207), and of entries of the action table for Firewall actions(→ Page 208). It can also contain direct descriptions in the appropriate LCOS syntax (e. g. %P6 for TCP).



For direct entering of rule parameters in LCOS syntax, the same guidelines apply as described in the following sections for protocols, source and destination, as well as for Firewall actions.

Object table

The object table defines elements and objects that apply to the rule table of the Firewall. Objects can be:

- Single PCs (MAC or IP address, host name)
- Entire networks
- Protocols
- Services (ports or port ranges, e. g. HTTP, Mail&News, FTP, ...)

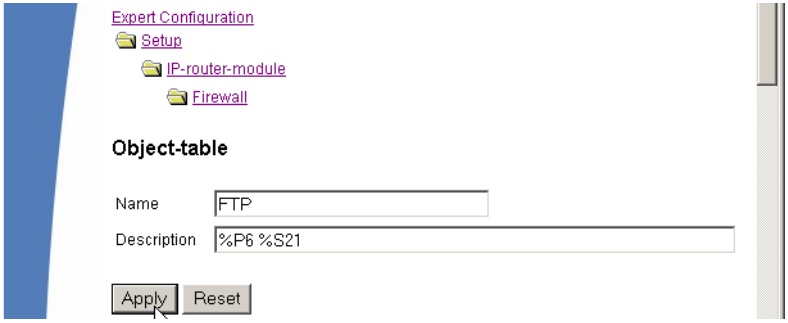
Any combination of these elements is possible. Furthermore, objects can be defined hierarchically. So one can first define objects for TCP and UDP protocols, then objects for e.g. FTP (= TCP + ports 20 and 21), HTTP (= TCP + port 80) and DNS (= TCP, UDP + port 53). All these single objects can be assembled subsequently into a new object, which contains all previously defined single objects then.

Stations and services can be described according to the following rules in the object table:

Description	Object ID	Examples and notes
Local network	%L	
Remote stations	%H	Name must be in DSL /ISDN /PPTP or VPN remote site list
Host name	%D	Note advice for host names (→ Page 191)
MAC address	%E	00:A0:57:01:02:03

Description	Object ID	Examples and notes
IP address	%A	%A10.0.0.1, 10.0.0.2; %A0 (all addresses)
Netmask	%M	%M255.255.255.0
Protocol (TCP/UDP/ICMP etc.)	%P	%P6 (for TCP)
Service (port)	%S	%S20-25 (for ports 20 to 25)

Equal identifier can generate comma-separated lists as for example host lists/address lists (%A10.0.0.1, 10.0.0.2), or hyphen-separated ranges like port ranges (%S20-25). The occurrence of a "0" or an empty string represents the 'any' object.



When configuring via console (Telnet or terminal program), the combined parameters (port, destination, source) must be embraced with inverted commas (character ").

Action table

As described above, a Firewall action consists of condition, limit, packet action and further measures. In the action table Firewall actions are composed as any combination of the following elements:

- Conditions

Condition	Description	Object ID
Connect filter	The filter is active when no physical connection to the packet destination exists.	@c
DiffServ filter	The filter is active when the packet contains the indicated Differentiated Services Code Point (DSCP) ('Evaluating ToS and DiffServ fields' → page 237.	@d (plus DSCP)
Internet filter	The filter is active when the packet is received or will be transmitted via default route.	@i
VPN filter	The filter is active when the packet is received or will be transmitted via VPN connection.	@v

If no further actions are specified in a "connect" or "Internet" filter, then implicitly a combination of these filters with the "reject" action is assumed.

- Limits/Trigger

  Each Firewall action can be tied together with a limit, whose excess leads to the triggering of the action. Also, several limits for a filter thereby can build action chains.

  Limit objects are generally introduced by %L, followed by:

  - Reference: per connection (c) or globally (g)
  - Kind: Data rate (d), number of packets (p) or packet rate (b)
  - Value of the limit
  - Further parameters (e. g. period and quantity)

  The following limitations are available:

Limit	Description	Object ID
Data (abs)	Absolute number of kilobytes on the connection after which the action is executed.	%lcd
Data (rel)	Number of kilobytes/second, minute, hour on the connection after which the action is executed.	%lcds %lcdm %lcdh
Packet (abs)	Absolute number of packets on the connection after which the action is executed.	%lcp
Packet (rel)	Number of packets/second, minute, hour on the connection after which the action is executed.	%lcps %lcpm %lcph
Global data (abs)	Global data (abs): Absolute number of kilobytes received from the destination station or sent to it, after which the action is executed.	%lgd
Global data (rel)	Number of kilobytes/second, minute or hour received from the destination station or sent to it, after which the action is executed.	%lgds %lgdm %lgdh
Global packet (abs)	Absolute number of packets received from the destination station or sent to it, after which the action is executed.	%lgp
Global packet (rel)	Number of packets/second, minute or hour received from the destination station or sent to it, after which the action is executed.	%lgps %lgpm %lgph
Receive option	Limit restriction to the direction of reception (this affects in the context with above limitations). In the ID object column, examples are indicated.	%lgdsr %lcdsr
Transmit option	Limit restriction to the sending direction (this affects in the context with above limitations). In the ID object column, examples are indicated.	%lgdst %lcdst

If an action is given without any associated limit, then implicitly a packet limit is assumed that is immediately exceeded with the first packet.

■ Packet action

Packet action	Description	Object ID
Accept	The packet will be accepted.	%a
Reject	The packet will be rejected with the corresponding error message.	%r
Drop	The packet will be discarded silently.	%d

These packet actions can be combined arbitrarily. If you choose absurd or ambiguous actions (e. g.: Accept + Drop), then the more secured action will be taken (here: “Drop”).

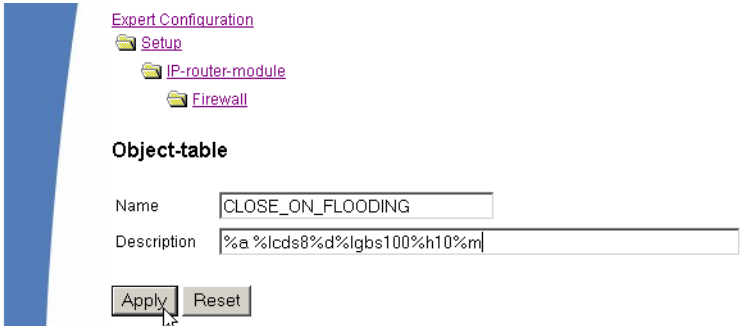
■ Further measures

Measure	Description	Object ID
Syslog	Gives a detailed notification via SYSLOG.	%s
Mail	Sends an email to the administrator.	%m
SNMP	Sends a SNMP trap.	%n
Close port	Closes the destination port for a given time.	%p
Deny host	Locks out the sender address for a given time.	%h
Disconnect	Disconnects the connection to the remote site from which the packet was received or sent.	%t
Zero limit	Resets the limit counter to 0 again upon exceeding of the trigger threshold.	%z
Fragmentation	Forces a fragmentation of all packets not matching to the rule.	%f

If the "close port" action is executed, an entry in a block list is made, by which all packets, which are sent at the respective computer and port, get rejected. For the "close port" object a timeout can be given in seconds, minutes or hours, which is inserted directly behind the object ID. This time value is composed of the designator of the time unit (h, m, s for hour, minute and second), and the actual time. Thus e.g. %pm10 closes a port for 10 minutes. If no time unit is provided, then implicitly "minutes" apply (and thus %p10 is equivalent to %pm10).

If the "Deny host" action is executed, then the sender of the packet is registered in a block list. Starting from this moment, all packets received from the blocked server will be rejected. Also the "Deny host" object can be provided with a time-out, which is formed similarly to the "CLOSE port" option.

If you want to limit e.g. the permissible data rate for a connection to 8 kbps and to lock out the aggressor committing a flooding attempt, and furthermore send at the same time an email to the administrator, then the description of the object for the action reads as follows:



- This description permits traffic (`%a`) at the beginning. A simple %a at the beginning of the description is equivalent to a %lp0%a (= accept, if the limit was exceeded on zero packets, i.e. with the first packet).
- If over the current connection now 8 kbit (`%lcds8`) is transferred in one second, then all further packets - up to the expiration of the second - will be silently discarded (`%d`), thus automatically creating a Traffic Shaping.
- If 100 packets for the server (destination address of the connection) arrive (`%lgbs100`) in one second, then the remote host (source address) is locked for 10 minutes (`%h10`), and an email is sent to the administrator (`%m`) .

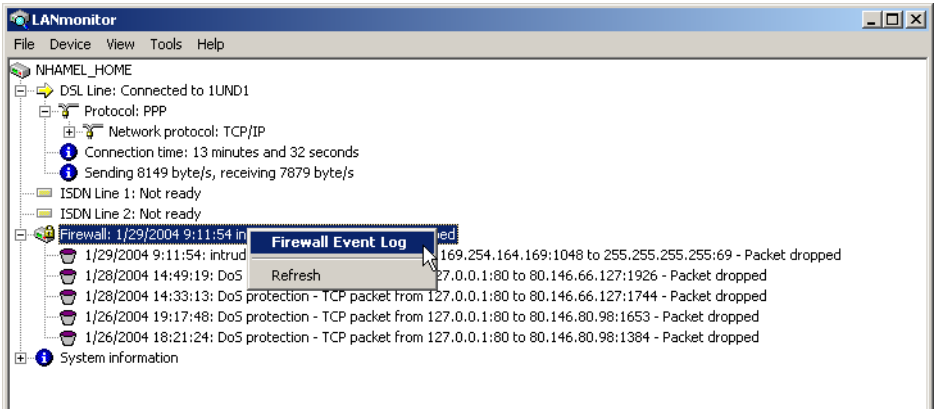
Similar to the address and service objects of the object table, action objects can be provided with a name, and can arbitrarily be combined recursively, whereby the maximum recursion depth is limited to 16. In addition, they can be entered directly into the action field of the rule table.

When building the actual filter table, action objects get minimized similarly to the address and service objects to the smallest necessary number, i.e. multiple definitions of an action get eliminated, and contradictory actions are turned into the "safest". Thus e.g. `%a` (accept) and `%d` (drop) becomes only `%d`, and `%r` (reject) and `%d` becomes `%r`.

8.3.9 Firewall diagnosis

All events, conditions and connections of the Firewall can be logged and monitored in detail.

The most comfortable inspection is accomplished by displaying the logging table (see below) with LANmonitor. LANmonitor displays under 'Firewall' the last five events, that were triggered either by a Firewall rule, the DoS, or the IDS system with activated 'SNMP/LANmonitor' option.



A new window with the complete logging table opens by clicking the right mouse button in the **Firewall Event Log** context menu. (→ Page 212).

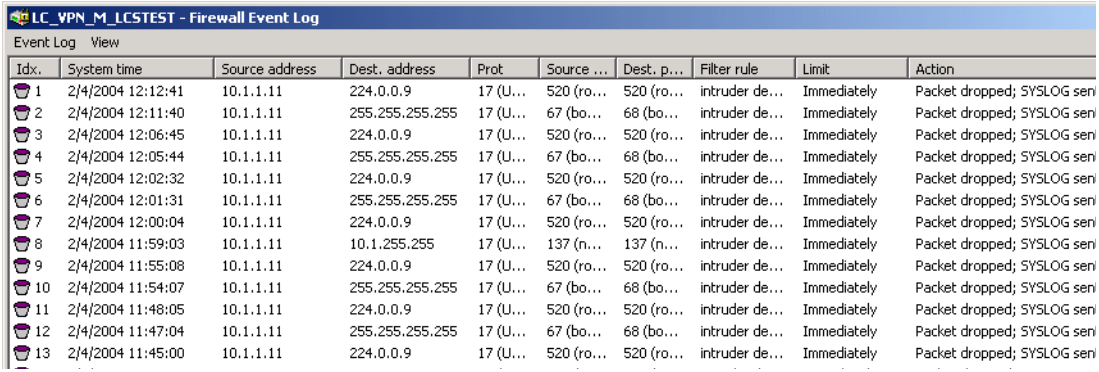
All lists and tables described in this section can be found under the following menu options:

Configuration tool	Run
WEBconfig	Expert Configuration Status IP-Router-Statistics
Terminal/Telnet	`/Status/IP-Router-Statistics`

The Firewall table

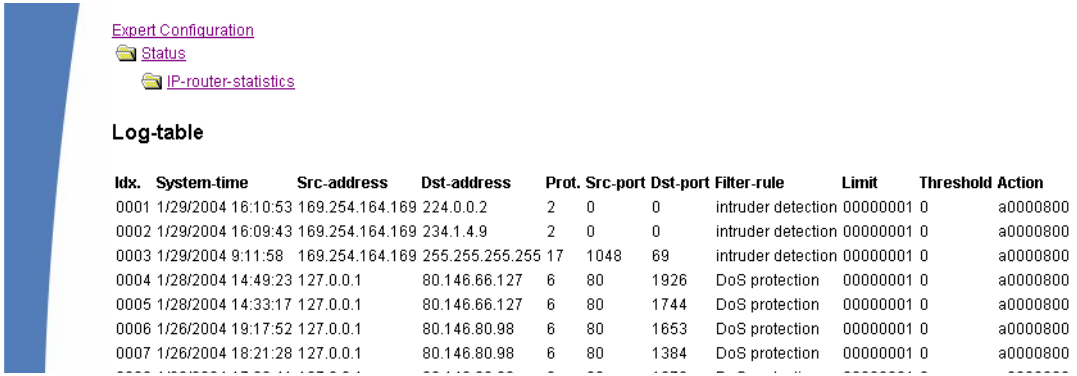
If an event occurred that had to be logged in either way, i.e. a log action was specified with the receipt of a packet, or a report by e-mail, Syslog or SNMP was generated, then this event is held in the logging table.

If you call up the logging table via LANmonitor, it looks like the following depiction:



Idx.	System time	Source address	Dest. address	Prot	Source ...	Dest. p...	Filter rule	Limit	Action
1	2/4/2004 12:12:41	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sen
2	2/4/2004 12:11:40	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sen
3	2/4/2004 12:06:45	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sen
4	2/4/2004 12:05:44	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sen
5	2/4/2004 12:02:32	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sen
6	2/4/2004 12:01:31	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sen
7	2/4/2004 12:00:04	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sen
8	2/4/2004 11:59:03	10.1.1.11	10.1.255.255	17 (U...	137 (n...	137 (n...	intruder de...	Immediately	Packet dropped; SYSLOG sen
9	2/4/2004 11:55:08	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sen
10	2/4/2004 11:54:07	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sen
11	2/4/2004 11:48:05	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sen
12	2/4/2004 11:47:04	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sen
13	2/4/2004 11:45:00	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sen

If you call up the logging table via WEBconfig, it looks like the following depiction:



The table contains the following values:

Element	Element meaning
Idx.	Current index (so that the table can be polled also via SNMP)
System time	System time in UTC codification (will be transformed on displaying of the table into clear text)
Src address	Source address of the filtered packet
Dst address	Destination address of the filtered packet
Prot.	Protocol (TCP, UDP etc.) of the filtered packet
Src-p	Source port of the filtered packet (only with port-related protocols)
Dst-p	Destination port of the filtered packet (only with port-related protocols)
Filter-Rule	Name of the rule, which has raised the entry.

Element	Element meaning
Limit	Bit field, which describes the crossed limit, which has filtered the packet. The following values are defined at present: 0x01 Absolute number 0x02 Number per second 0x04 Number per minute 0x08 Number per hour 0x10 Global limit 0x20 Byte limit (if not set, it concerns a packet-related limit) 0x40 Limit applies only in receiving direction 0x80 limit applies only in transmission direction
Threshold	Exceeded limit value of the trigger limit
Action	Bit field, which specifies all implemented actions. At present the following values are defined: 0x00000001 Accept 0x00000100 Reject 0x00000200 Connect filter 0x00000400 Internet- (Default route-) filter 0x00000800 Drop 0x00001000 Disconnect 0x00004000 Block source address 0x00020000 Block destination address and port 0x20000000 Send SYSLOG notification 0x40000000 Send SNMP trap 0x80000000 Send email

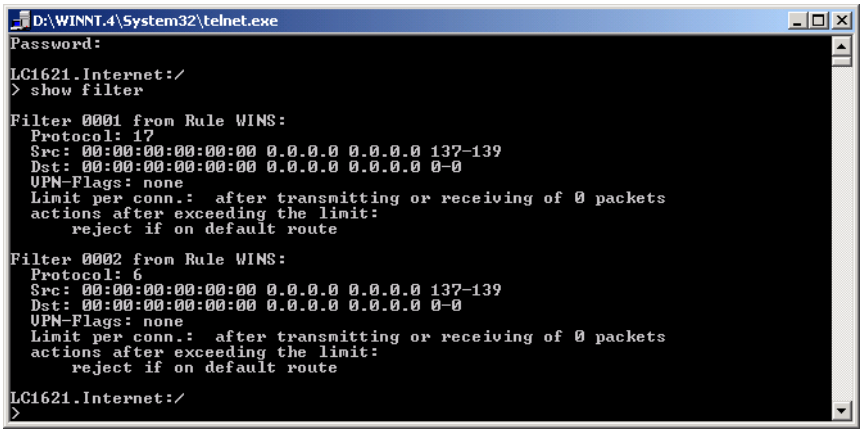
All Firewall actions are likewise displayed within the IP router trace ('How to start a trace' → page 81). Furthermore, some LANCOM models have a Firewall LED, which signals each filtered packet.

The filter list

The filter list allows to examine filters generated by rules defined in the action, object and rule table.

Please note that manually entered filter rules do not generate a fault indication and also no error message. If you configure filters manually, you should in each case examine on the basis of the filter list whether the desired filters were generated or not.

On Telnet level, the content of the filter list can be displayed with the command `show filter`:



Under WEBconfig the filter list has the following structure:

Expert Configuration

Status

IP-router-statistics

Filter-list

Idx.	Prot.	Src-MAC	Src-address	Src-netmask	S-st.	S-end	Dst-MAC	Dst-address	Dst-netmask	D-st.	D-end	Action
0001	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	995	995	limit: acce
0002	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	143	143	limit: acce
0003	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	119	119	limit: acce
0004	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	110	110	limit: acce
0005	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	25	25	limit: acce
0006	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	21	21	limit: acce
0007	1	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	0	0	limit: acce

The individual fields in the filter list have the following meaning:

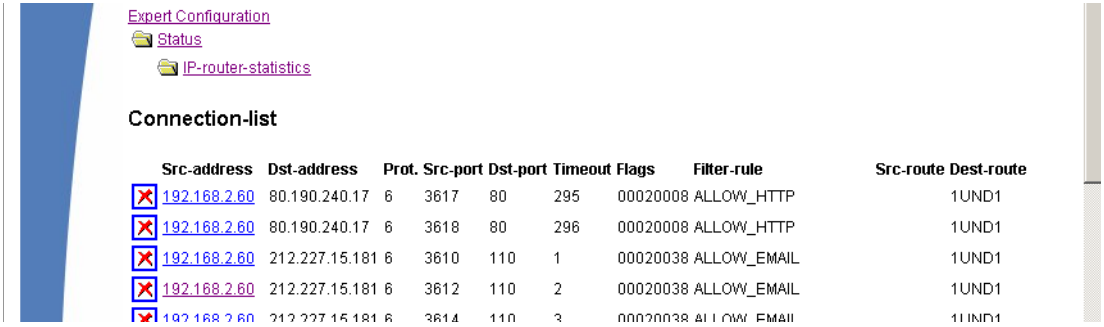
Entry	Description
Idx.	Current index
Prot	Protocol to be filtered, e.g. 6 for TCP or 17 for UDP.
Src MAC	Ethernet source address of the packet to be filtered or 000000000000, if the filter should apply to all packets.
Src address	Source IP address or 0.0.0.0, if the filter should apply to all packets.
Source mask	Source network mask, which determinates the source network together with the source IP address, or 0.0.0.0, if the filter should apply to packets from all networks.
Q start	Start source port of the packets to be filtered.
Q end	End source port of the packets to be filtered. Makes up the port range together with the start source port, in which the filter takes effect. If start and end port are 0, then the filter is valid for all source ports.

Entry	Description
Dst MAC	Ethernet destination address of the packet to be filtered or 000000000000, if the filter should apply to all packets.
Dst address	Destination address or 0.0.0.0, if the filter should apply to all packets.
Dst mask	Destination network mask, which determinates the destination network together with the destination IP address, or 0.0.0.0, if the filter should apply to packets to all networks.
Z start	Start destination port of the packets to be filtered.
Z end	Destination port of the packets to be filtered. Makes up the port range together with the start destination port, in which the filter takes effect. If start and end port are 0, so the filter is valid for all destination ports.
Action	Into this column, the "main action" is unveiled as a text, which will be executed when the first limit has been exceeded. The first limit can be also an implicit limit, e.g. if only one limit for the restriction of the throughput was configured. Then an implicit limit - linked with an "accept" action - is inserted. In this case, "accept" is unveiled as main action. You can see the complete actions under the command show filter.
Linked	Indicates whether it concerns a "first Match" rule (linked = no). Only with linked rules in the case of applying of this rule, also further rules are evaluated.
Prio	Priority of the rule having generated the entry.

The connection list

The connection table files source address, destination address, protocol, source port, destination port, etc. of a connection, as well as possible actions. This table is sorted according to source address, destination address, protocol, source port and destination port of the packet, which caused the entry in the table.

Under WEBconfig the filter list has the following structure:



The table contains the following elements:

Element	Element meaning
Src addr.	Source address of the connection
Dst addr.	Destination address of the connection
Protocol	Used protocol (TCP/UDP etc.). The protocol is decimally indicated.

Element	Element meaning
Src port	Source port of the connection. The port is only indicated with port-related protocols (TCP/UDP) or protocols, which own a comparable field (ICMP/GRE).
Dst port	Destination port of the connection (with UDP connections, this one is occupied only with the first answer).
Timeout	Each entry ages out with the time of this table, thus the table does not overflow with "died" connections.
Flags	In the flags the condition of the connection and further (internal) information are stored in a bit field.(→ Page 217) As conditions the following values are possible: **new, establish, open, closing, closed, rejected** (corresponding to the TCP flags: SYN, SYN ACK, ACK, FIN, FIN ACK and RST). UDP connections know the conditions **new, open** and **closing** (the last one only, if the UDP connection is linked with a condition-afflicted control path. This is e.g. the case with protocol H.323.).
Src route	Name of the remote station, over which the first packet has been received.
Dst route	Name of the remote station, where the first packet will be sent to.
Filter rule	Name of the rule, which has generated the entry (determines also the actions to be executed), when a suitable packet is received.

Meaning of the flags of the connection list

Flag	Flag meaning
00000001	TCP: SYN sent
00000002	TCP: SYN/ACK received
00000004	TCP: waiting for ACK of the server
00000008	all: open connection
00000010	TCP: FIN received
00000020	TCP: FIN sent
00000040	TCP: RST sent or received
00000080	TCP: session will be re-established
00000100	FTP: passive FTP connection will be established
00000400	H.323: belonging to T.120 connection
00000800	connection via loopback interface
00001000	checking concatenated rules
00002000	rule is catenated
00010000	destination is on "local route"
00020000	destination is on default route
00040000	destination is on VPN route
00080000	physical connection is not established
00100000	source is on default route

Flag	Flag meaning
00200000	source is on VPN route
00800000	no route for destination
01000000	contains global actions with condition

Port block list

Address, protocol and port of a destination station are filed in the port block list, if blocking of the destination port on the destination station was selected as a filter's packet action. This table is likewise a sorted semi-dynamic table. Sorting is done according to address, protocol and port. The table contains the following elements:

Element	Element meaning
Address	Address of the station, to which the blocking should apply.
Protocol	Used protocol (TCP/UDP etc.) The protocol is decimally indicated.
Port	Port to close at the station. If the respective protocol is not port related, then the entire protocol for this station becomes closed.
Timeout	Duration of the blocking in minutes.
Filter rule	Name of the rule, which has produced the entry (determines also the actions to be executed), when a suitable packet is received.

Host block list

The address of a station is filed in the host block list, if blocking of the sender was selected in a filter's packet action. This table is a sender address sorted semi-dynamic table and contains the following elements:

Element	Element meaning
Address	Address of the station, to which the blocking should apply.
Timeout	Duration of the blocking in minutes.
Filter rule	Name of the rule, which has generated the entry (determines also the actions to be executed), when a suitable packet is received.

8.3.10 Firewall limitations

Apart from understanding the functioning of Firewalls, it is also very important to discern their limitations and to extend them if necessary. The Firewall does not protect against malicious contents coming through the permitted ways into your local network. It is true that certain effects of some viruses and worms are stopped, because communication is blocked via the required ports, but no Firewall alone is a comprehensive protection against viruses.

Also monitoring of sensitive data in the Internet is not be prevented by a Firewall. If data once reaches the unsecured net beyond the Firewall, then it is exposed to well-known dangers. Despite using a Firewall, any confidential infor-

mation such as contracts, passwords, development information etc. should be transmitted only over protected connections, i.e. by using suitable data encryption and VPN connections.

8.4 Protection against break-in attempts: Intrusion Detection

A Firewall has the task to examine data traffic across borders between networks, and to reject those packets, which do not have a permission for transmission. Beside attempts to access directly a computer in the protected network, there are also attacks against the Firewall itself, or attempts to outwit a Firewall with falsified data packets.

Such break-in attempts are recognized, repelled and logged by the Intrusion Detection system (IDS). Thereby it can be selected between logging within the device, email notification, SNMP traps or SYSLOG alarms. IDS checks the data traffic for certain properties and detects in this way also new attacks proceeding with conspicuous patterns.

8.4.1 Examples for break-in attempts

Typical break-in attempts are falsified sender addresses ("IP Spoofing") and port scans, as well as the abuse of special protocols such as e.g. FTP in order to open a port on the attacked computer and the Firewall in front of it.

IP Spoofing

With IP Spoofing the sender of a packet poses itself as another computer. This happens either in order to trick the Firewall, which trusts packets from the own network more than packets from untrusted networks, or in order to hide the author of an attack (e.g. Smurf).

The LANCOM Firewall protects itself against spoofing by route examination, i.e. it examines, whether a packet was allowed to be received over a certain interface at all, from which it was received.

Portscan Detection

The Intrusion Detection system tries to recognize Portscans, to report and to react suitably on the attack. This happens similarly to the recognition of a 'SYN Flooding' attack (see 'SYN Flooding' → page 221): The "half-open" connections are counted also here, whereby a TCP RESET, which is sent by the scanned computer, leaves a "half-open" connection open again.

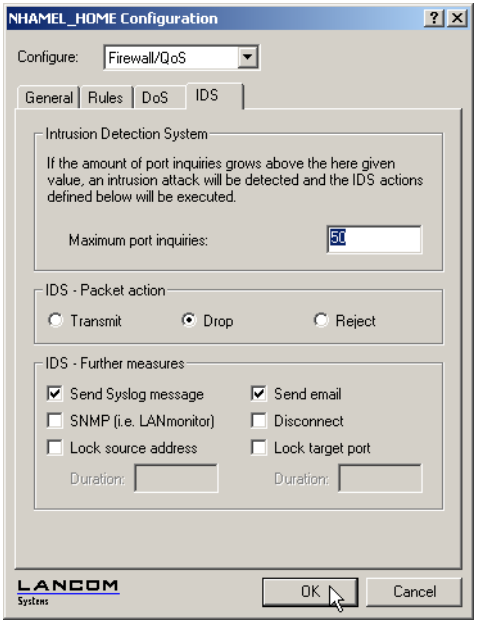
If a certain number of half-open connections between the scanned and the scanning computer exist, then this is reported as a port scan.

Likewise, the receipt of empty UDP packets is interpreted as an attempted port scan.

8.4.2 Configuration of the IDS

LANconfig

Parameters of the Intrusion Detection System are set in LANconfig in the configuration tool 'Firewall/QoS' on index card 'IDS':



Apart from the maximum number of port inquiries, fragment action and the possible registration mechanisms, also these reactions are possible:

- The connection will be cut off.
- The sender address will be blocked for an adjustable period of time.
- The destination port of the scan will be blocked for an adjustable period of time.

WEBconfig, Telnet

The behavior of the Intrusion Detection Systems can be configured here under WEBconfig or Telnet:

Configuration tool	Run
WEBconfig	Expert Configuration: Setup/IP Router Module/Firewall
Terminal/Telnet	Setup/IP Router Module/Firewall

8.5 Protection against "Denial of Service" attacks

Attacks from the Internet can be break-in attempts, as well as attacks aiming to block the accessibility and functionality of individual services. Therefore a LANCOM is equipped with appropriate protective mechanisms, which recognize well-known hacker attacks and which guarantee functionality.

8.5.1 Examples of Denial of Service Attacks

Denial of service attacks do profit from fundamental weaknesses of TCP/IP protocols, as well as from incorrect implementations of TCP/IP protocol stacks. Attacks, which profit from fundamental weaknesses are e.g. SYN Flood and Smurf. Attacks aiming at incorrect implementations are all attacks, which operate with incorrectly fragmented packets (e.g. Teardrop), or which work with falsified sender addresses (e. g. Land). In the following some of these attacks are described, their effects and possible countermeasures.

SYN Flooding

SYN Flooding means that the aggressor sends in short distances TCP packets with set SYN flag and with constantly changing source ports on open ports of its victim. The attacked computer establishes as a result a TCP connection, replies to the aggressor a packet with set SYN and ACK flags and waits now in vain for the confirmation of the connection establishment. Hundreds of "half-open" TCP connections are staying thereby, and just consume resources (e.g. memory) of the attacked computer. This procedure can go that far that the victim can accept no more TCP connection or crashes due to the lack of memory.

An appropriate countermeasure of a Firewall is to supervise the number of "half-open" TCP connections, which exists between two stations and to limit it. That means, if further TCP connections between these workstations were established, these connections would be blocked by the Firewall.

Smurf

The Smurf attack works in two stages and paralyzes two networks at once. In the first step a Ping (ICMP echo Request) packet with a falsified sender address is sent to the broadcast address of the first network, whereupon all workstations in this network answer with an ICMP echo Reply to the falsified sender address, which is located in the second network. If the rate of incoming echo requests is high enough, as well as the number of answering workstations, then the entire incoming traffic of the second network is blocked during the attack and, moreover, the owner of the falsified address cannot receive normal data any more during the attack. If the falsified sender address is the broadcast address of the second network, also all workstations are blocked in this network, too.

In this case the DoS recognition of the LANCOM blocks passing packets, which are addressed to the local broadcast address.

LAND

The land attack is a TCP packet that is sent with set SYN flag and falsified sender address to the victim workstation. The bottom line is that the falsified sender address is equal to the address of the victim. With an unfortunate implementation of TCP, the victim interprets the sent SYN-ACK again as SYN, and a new SYN-ACK is sent. This leads to a continuous loop, which lets the workstation freeze.

In a more up to date variant, the loopback address "127.0.0.1" is taken as sender address, but not the address of the attacked workstation. Sense of this deception is to outwit personal firewalls, which react in fact to the classical variant (sender address = destination address), but which pass through the new form without hindrance. This variant is also recognized and blocked by a LANCOM.

Ping of Death

The Ping of Death belongs to those attacks, which use errors when fragmented packets are reassembled. This functions as follows:

In the IP header there is a field "fragment offset" that indicates in which place the received fragment is to be assembled into the resulting IP packet. This field is 13 bits long and gives the offset in 8 byte steps, and can form an offset from 0 to 65528. With a MTU on the Ethernet of 1500 bytes, an IP packet can be made up to 65528 + 1500 - 20 = 67008 bytes. This can lead to an overrun of internal counters or to buffer overruns, and thus it can provoke the possibility to the aggressor of implementing own code on the victim workstation.

In this case, the Firewall offers two possibilities:

Either, the Firewall reassembles the entire incoming packet and examines its integrity, or solely the fragment which goes beyond the maximum packet size is rejected. In the first case, the Firewall itself can become the victim when its implementation was incorrect. In the second case "half" reassembled packets accumulate at the victim, which are only rejected after a certain time, whereby a new Denial of Service attack can result thereby if the memory of the victim is exhausted.

Teardrop

The Teardrop attack works with overlapping fragments. After the first fragment another one is sent, which overlaps completely within the first one, i.e. the end of the second fragment is located before the end of the first. If - due to the indolence of the IP stack programmer - it is simply counted "new end" - "old end" when determining the number of bytes to copy for the reassembly, then a negative value results, resp. a very large positive value, by which during the copy operation parts of the memory of the victim are overwritten and thereupon the workstation crashes.

The Firewall has again two possibilities:

Either the Firewall reassembles and rejects if necessary the entire packet, or it holds only minimum offset and maximum end of the packet and rejects all fragments, whose offset or end fall into this range. In the first case the implementation within the Firewall must be correct, so that the Firewall does not become the victim itself. In the other case "half" reassembled packets accumulate again at the victim.

Bonk/Fragrouter

Bonk is a variant of the Teardrop attack, which targets not at crashing the attacked computer, but to trick simple port filter Firewalls, which accept also fragmented packets and thus to penetrate into the network being protected. During this attack, the UDP or TCP Header of the first fragment is overwritten by skillful choice of the fragment offset. Thereby, simple port filter Firewalls accept the first packet and the appropriate fragments while overwriting the first packet's header by the second fragment. Thus suddenly a permissible packet is created, which rather actually should be blocked by the Firewall.

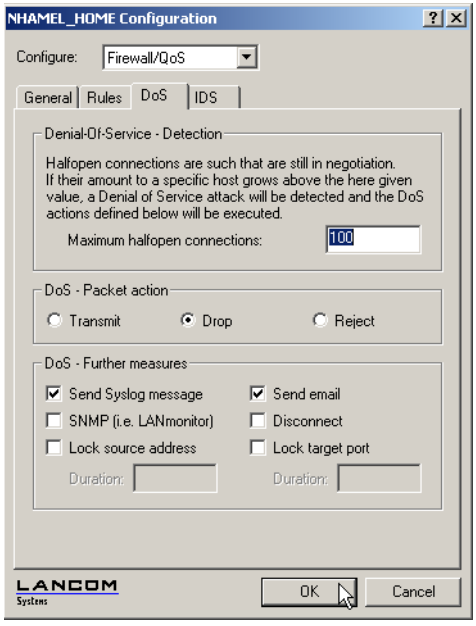
Concerning this occurrence, the Firewall can itself either reassemble or filter only the wrong fragment (and all following), leading to the problems already indicated by either one of the other solutions above.

By default installation all items are configured as "secure", i.e. maximal 100 permissible half-open connections by different workstations (see SYN Flooding), at most 50 half-open connections of a single computer (see Portscan) of fragmented packets to be reassembled.

8.5.2 Configuration of DoS blocking

LANconfig

Parameters against DoS attacks are set in the LANconfig in the configuration tool 'Firewall/QoS' on the register card 'DoS':



In order to drastically reduce the susceptibility of the network for DoS attacks in advance, packets from distant networks may be only accepted, if either a connection has been initiated from the internal network, or the incoming packets have been accepted by an explicit filter entry (source: distant network, destination: local area network). This measure already blocks a multitude of attacks.

For all permitted accesses explicitly connection state, source addresses and correctness of fragments are tracked in a LANCOM. This happens for incoming and for outgoing packets, since an attack could be started also from within the local area network.

This part is configured centrally in order not to open a gate for DoS attacks by incorrect configuration of the Firewall. Apart from specifying the maximum number of half-open connections, fragment action and possible notification mechanisms, also these more extensive possibilities of reaction exist:

- The connection will be cut off.

- The sender address will be blocked for an adjustable period of time.
- The destination port of the scan will be blocked for an adjustable period of time.

WEBconfig, Telnet

The behavior of the DoS detection and blocking can be configured here under WEBconfig or Telnet:

Configuration tool	Run
WEBconfig	Expert Configuration: Setup/IP Router Module/Firewall
Terminal/Telnet	Setup/IP Router Module/Firewall

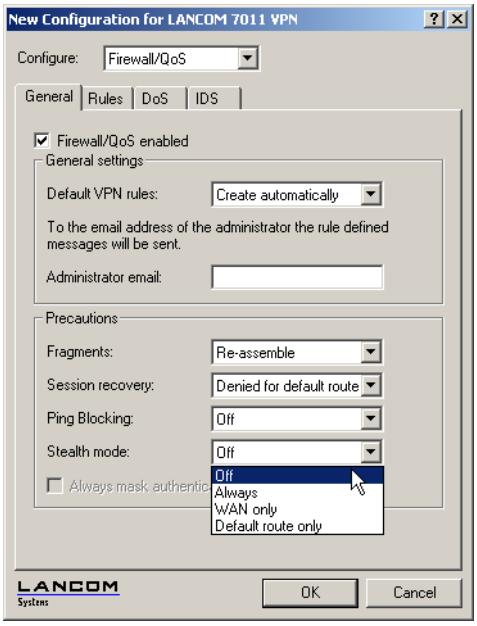
However, always active are the following protection mechanisms:

- Address examination (against IP Spoofing)
- Blocking of broadcasts into local area network (against Smurf and Co).

8.5.3 Configuration of ping blocking and Stealth mode

LANconfig

Parameters for ping blocking and Stealth mode can be set with LANconfig under 'Firewall/QoS' on register card 'General':



WEBconfig, Telnet

With WEBconfig or Telnet the suppression of responses can be configured here:

Configuration tool	Run
WEBconfig	Expert Configuration: Setup/IP Router Module/Firewall
Terminal/Telnet	Setup/IP Router Module/Firewall

9 Quality of Service

This chapter dedicates itself to quality: Under the generic term Quality of Service (short: QoS) those LCOS functions are summarized, which are concerned with the guarantee of certain service availabilities.

9.1 Why QoS?

The main objective of Quality of Service is to transfer certain data packets either particularly safe or as immediately as possible:

- It may happen during a data transfer that data packets are not delivered to the addressee. But for some applications it is very important that all sent packets really do arrive. An e-mail, for example, divided into several small data packets, can only be assembled together again, when all parts have arrived completely. Whether one or an other packet arrives with little time delay does not make any difference. These applications often count on the connection-orientated Transmission Control Protocol (TCP). This protocol ensures that data will be transferred correctly and chronologically via the net. It automatically adjusts the sending rate downwards if the confirmation of sent data packets is outstanding for longer times, and also takes care of repeated transmission in case of packet losses.
- In other applications, e.g. telephony via the Internet (Voice-over-IP, VoIP), it is - differently to the case above - very important that the data packets arrive at the addressee with only little time delay. But it really doesn't matter if once a data packet gets lost in this case. The participant at the other end of the connection will understand the caller, even if small parts of the speech got lost. This application aims at the fastest sending of data packets as possible. The connectionless User Datagram Protocol (UDP) is often used for this kind of application. Also this protocol has very little administrative overhead. But chronological delivery of packets is not guaranteed, data packets are simply sent out. Because no confirmation receipt exists, lost packets never get delivered again.

9.2 Which data packets to prefer?

The necessity of a QoS concept results only from the fact that the available bandwidth is not always sufficient for transferring all pending data packets reliably and on time. Load peaks result easily from running simultaneously large FTP downloads, while exchanging e-mails and using IP telephones over the data line. In order to meet also in these situations the demands of the desired data transfer, certain data packets must be treated preferentially. It is necessary for this, that at first a LANCOM recognizes which data packets should be preferred at all.

There are two possibilities to signal the need for a preferential treatment of data packets in the LANCOM:

- The application, as e.g. the software of certain IP telephones, is itself able to mark the data packets appropriately. This marking, the "tag", is set within the header of the IP packets. The two different variants of this marking "ToS" and "DiffServ" can simply described assume the following states:
  - ToS "Low Delay"
  - ToS "High Reliability"
  - DiffServ "Expedited Forwarding"

- □ DiffServ "Assured Forwarding"

The IP header bits of the ToS resp. DiffServ field are copied in case of a VPN route also into the enclosing IP header of the IPSec VPN packet. Thus QoS is available also for VPN routes over the Internet, as long as your provider treats according packets preferentially also in the WAN.

- When the application itself has no possibility to mark the data packets appropriately, the LANCOM can ensure the correct treatment. For this, it uses the existing functions of the firewall, which can classify e.g. data packets according to subnets or services (applications). Due to these functions it is e. g. possible to treat individually data packets of a FTP connection or those of a certain department (in a separate subnet).

  For treatment of data packets classified by the firewall the following two possibilities can be chosen:

  - □ Guaranteed minimum bandwidth
  - □ Limited maximum bandwidth

What is DiffServ?

DiffServ stands for "Differentiated Services" and is a quite recent model to signal the priority of data packets. DiffServ is based on the known Type-of-Service (ToS) field and uses the same byte within the IP header.

ToS is using the first three bits to describe the priorities (precedence) 0 to 7, as well as four further bits (the ToS bits) to optimize the data stream (e.g. "Low Delay" and "High Reliability"). This model is rather inflexible, and this is why it has been used quite rarely in the past.

The DiffServ model uses the first 6 bits to make distinctions of different classes. Up to 64 gradings are thus possible (Differentiated Services Code Point, DSCP) which enable a finer priorisation of the data stream:

- To ensure downward compatibility with ToS implementations, the previous precedence levels can be depicted with the "Class Selectors" (CS0 to CS7). Thereby, the level "CS0" denotes so-called "Best Effort" (BE) and stands for usual transfer of data packets without special treatment.
- The "Assured Forwarding" classes are used for a secured transfer of data packets. The first digit of the AF class describes each the priority of the transfer (1 to 4), the second digit the "drop probability" (1 to 3). Packets with AFxx marking are transferred in a secured way, and thus not dropped.

Finally, the class "Expedited Forwarding" marks those packets, that shall be transferred preferentially, before all other packets.

Code point	DSCP bits	Dec.
CS0 (BE)	000000	0
CS1	001000	8
CS2	010000	16
CS3	011000	24
CS4	100000	32

Code point	DSCP bits	Dec.
AF11	001010	10
AF12	001100	12
AF13	001110	14
AF21	010010	18
AF22	010100	20

Code point	DSCP bits	Dec.
AF33	011110	30
AF41	100010	34
AF42	100100	36
AF43	100110	38
EF	101110	46

Code point	DSCP bits	Dec.
CS5	101000	40
CS6	110000	48
CS7	111000	56

Code point	DSCP bits	Dec.
AF23	010110	22
AF31	011010	26
AF32	011100	28

Code point	DSCP bits	Dec.

9.2.1 Guaranteed minimum bandwidths

Hereby you give priority to enterprise-critical applications, e.g. Voice-over-IP (VoIP) PBX systems or certain user groups.

For LANCOM devices with VoIP functions that were already integrated or added in with a software option, the QoS settings for SIP calls are defined automatically.

Full dynamic bandwidth management for sending

Concerning the sending direction, the bandwidth management takes place dynamically. This means that e.g. a guaranteed minimum bandwidth is only available, as long as the corresponding data transfer really exists.

An example:

For the transmission of VoIP data of an appropriate VoIP gateway, a bandwidth of 256 Kbps is to be guaranteed always. Thereby, each individual VoIP connection consumes 32 Kbps.

As long as nobody telephones, the entire bandwidth is at the disposal to other services. Per adjacent VoIP connection 32 Kbps less is available to other applications, until 8 VoIP connections are active. As soon as a VoIP connection is terminated, the corresponding bandwidth is available again to all other applications.

For correct functioning of this mechanism, the sum of the configured minimum bandwidth must not exceed the effectively available transmission bandwidth.

Dynamic bandwidth management also for reception

For receiving bandwidth control, packets can be buffered and only belatedly confirmed. Thus TCP/IP connections regulate themselves automatically on a smaller bandwidth.

Each WAN interface is assigned a maximum reception bandwidth. This bandwidth will be accordingly degraded by every QoS rule that guarantees a minimum bandwidth of reception on this interface.

- If the QoS rule has been defined connection-related, the reserved bandwidth will be unblocked immediately after releasing the connection and the maximum available bandwidth will increase accordingly on the WAN interface.

- If the QoS rule has been defined globally, then the reserved bandwidth will be unblocked only after the ending of the last connection.

9.2.2 Limited maximum bandwidths

Hereby you limit e.g. the entire or connection-related maximum bandwidth for server accesses.

An example:

You operate both a Web server and a local network on a shared Internet access.

To prevent that your productive network (LAN) is paralyzed by many Internet accesses to your Web server, all server accesses are limited to half of the available bandwidth. Furthermore, in order to guarantee that your server services are available equally to many users at the same time, a certain maximum bandwidth per each server connection is set.

Combination possible

Minimum and maximum bandwidths can be used together in combination. Thus the available bandwidth can be distributed accordingly depending on your requirements, e.g. on certain user groups or applications.

9.3 The queue concept

9.3.1 Queues in transmission direction

Quality of Service requirements are realized in LCOS by using different queues for the data packets. For the transmission side, the following queues are utilized:

- Urgent queue I

  This queue is always processed at first before all others. The following data packets are handled here:

  - Packets with ToS "Low Delay"
  - Packets with DiffServ "Expedited Forwarding"
  - All packets that have been assigned a certain minimum bandwidth, as long as the guaranteed minimum bandwidth is not exceeded.
  - TCP control packets can be likewise dispatched by this queue preferentially (see 'SYN/ACK speedup' → page 116).

- Urgent queue II

  This is for all packets that have been assigned a guaranteed minimum bandwidth, but whose connection has exceeded this minimum bandwidth.

  As long as the interval for the minimum bandwidth is not exceeded (i.e. up to the end of the current second), all packets in this queue are treated without further special priority. All packets of this queue, of the "secured queue" and the "standard queue" share now the existing bandwidth. The packets are taken in order from the queues when sending in exactly the same sequence, in which they have been placed into these queues. If the

interval runs off, all blocks, which are at this time still in the "Urgent queue II" up to the exceeding of the in each case assigned minimum bandwidth, are placed again into the "Urgent queue I". The rest remains in the "Urgent queue II".

With this procedure it is guaranteed that prioritized connections do not crush the remaining data traffic.

- Secured queue

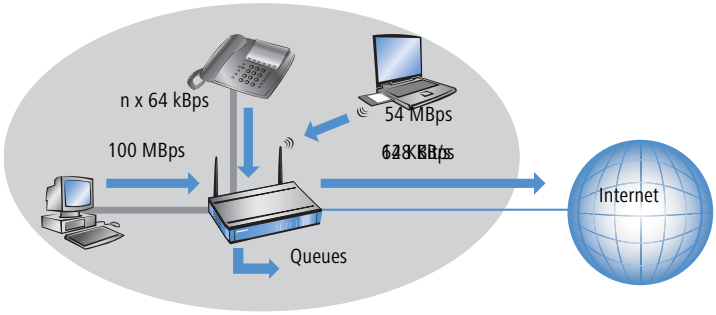
  This queue does not have a separate priority. However, packets in this queue are never dropped (transmission guaranteed).

  - Packets with ToS "High Reliability"
  - Packets with DiffServ "Assured Forwarding"

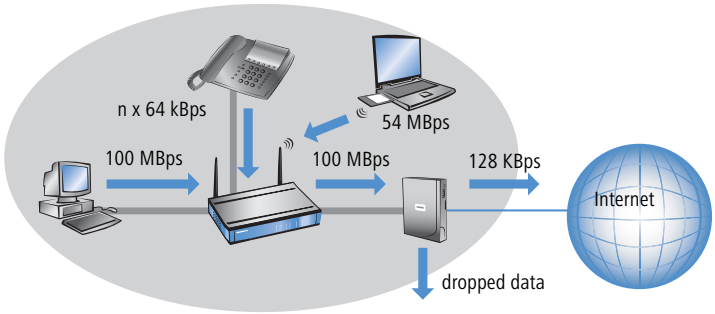
- Standard queue

  The standard queue contains all not classified data traffic. Packets in this queue are dropped at first when packets cannot be delivered fast enough.

The queue concept can, however, only work out when a "traffic congestion" of data packets has been accumulated at the interface from LAN to the WAN. Such a congestion is created when the interface within the LANCOM can submit fewer data to the WAN than data are delivered in peak periods from the LAN. This is e.g. the case, if the interface to the WAN is an integrated ADSL interface with comparatively low transmission speed ("upstream"). The integrated ADSL modem automatically reports back to the LANCOM how many data packets it is still able to receive, and thus brakes the data stream already within the router. As a result, the queues will automatically fill up.



Different is the case, if an Ethernet interface represents the connection to the WAN. From the LANCOM's point of view, the connection to the Internet via an external broadband modem looks like an Ethernet segment. On the distance from the LANCOM to the DSL modem, data will be transferred with full LAN speed of 10 or 100 Mbps. Because of an equal input and output speed, no natural congestion will be produced then. Furthermore, the Ethernet between the LANCOM and the broadband modem does not report anything about the capacity of the connection. The consequence: a congestion will only be happen within the broadband modem. But because no queues are deployed therein, surplus data will be lost. Thus a prioritization of "preferred" data is not possible!



To solve this problem, the transfer rate of the LANCOM's WAN interface will be reduced artificially. This interface will thereby be adjusted to the transfer rate that is available for the actual data transport towards the WAN. For a standard DSL connection, the DSL interface is thus adjusted in the LANCOM to the appropriate upstream rate (e.g. 128 kbps).

Data rates indicated by providers are mostly likely net rates. The gross data rate, which is available for the interface is a little bit higher than the net data rate guaranteed by the provider. If you know the gross data rate of your provider, you can enter this value for the interface and slightly increase in this way the data throughput. However, with entering the net data rate you play safe in any case!

9.3.2 Queues for receiving direction

Apart from the data transfer rate in transmission direction, the same consideration applies also to the receiving direction. Due to its 10 or 100 Mbps Ethernet interface, the LANCOM's WAN interface is fed by clearly fewer data from the broadband modem than would actually be receivable. All data packets received on the WAN interface are transferred to the LAN with equal rights.

In order to be able to prioritize incoming data as well, thus an artificial "brake" must be added also in this direction. Like already incorporated for the upstream direction, the data transfer rate of the interface is therefore adapted to the provider's offer in the downstream direction. For a standard DSL connection thus e.g. a downstream rate of 768 kbps applies. Again, the gross data rate can be entered here, if known.

Reducing the receiving bandwidth makes possible to treat received data packets suitably. Preferred data packets will be directly passed on to the LAN up to the guaranteed minimum bandwidth, all remaining data packets are running into congestion. This congestion produces generally a delayed confirmation of the packets. For a TCP connection, the sending server will react to this delay by reducing its sending frequency and adapting itself to the available bandwidth.

The following queues operate on the receiving side:

- Deferred Acknowledge Queue

  Each WAN interface contains additionally a QoS reception queue, which takes up those packets that should be „slowed down". The storage period of each individual packet depends on its length and on the actual permitted

reception bandwidth on the receiving side. Packets with a minimum reception bandwidth assigned by a QoS rule are passing through without any further delay, as long as the minimum bandwidth is not exceeded.

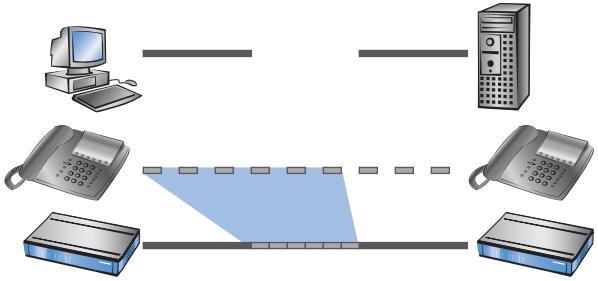
- Standard reception queue

  All packets that do not need special treatment because of an active QoS rule on the receiving side end up here. Packets of this queue are directly passed on resp. confirmed without consideration of maximum bandwidths.

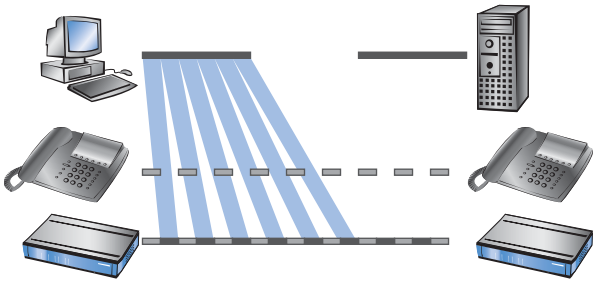
9.4 Reducing the packet length

The preferential treatment of data packets belonging to important applications can be endangered - depending on the situation - by very long data packets of other applications. This is the case e.g. when IP telephony and a FTP data transfer are simultaneously active on the WAN connection.

The FTP transfer uses quite large data packets of 1500 byte, whereas, the Voice over IP connection sends packets of e.g. 24 byte net in relatively short intervals. If FTP packets are in the sending queue of the LANCOM just at the moment when a VoIP packet is to be transferred, then the VoIP packet can only be sent after the line is free again. Depending on the transfer rate of the connection, this may cause a noticeable delay of the speech transmission.



This annoying behavior can be compensated if all data packets, which are not belonging to the connection preferred by QoS, do not exceed a certain packet length. While doing so, the data packets of the FTP connection will be divided into such small sections that the time-critical VoIP connection is able to deliver the packets without noticeable delay within the required time slots. A resulting delay has no disadvantageous effect to the TCP-secured FTP transfer.



Two different procedures exist to influence the packet length:

- The LANCOM can inform the peers of a data connection that they should only send data packets up to a certain length. Thereby, an appropriate PMTU (Path Maximum Transmission Unit) is enforced on the sending side. This procedure is called PMTU reduction".

  The PMTU reduction can be used for sending as well as for receiving direction. For the sending direction, the data source of the own LAN is adjusted with the PMTU reduction to a smaller packet size, for the receiving direction the data source of the WAN, e.g. web or FTP servers in the Internet.

  Provided that the data connection already exists when the VoIP connection is started, the senders regulate packet lengths very quickly to the permitted value. When setting up new data connections while a VoIP connection is already established, the maximum permitted packet length is negotiated directly during the connection phase.

The reduced packet length on the data connection still remains also after terminating the VoIP connection, as long as the sender checks the PMTU value again.

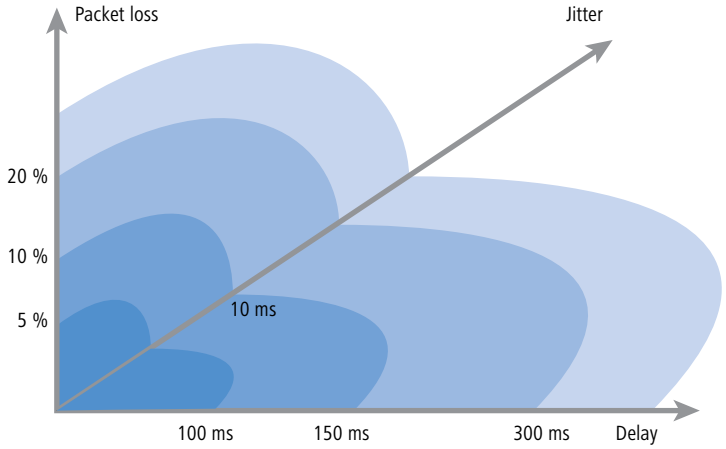
- The LANCOM is able to split packets to be sent above an adjustable maximum size (e.g. 256 byte) into smaller units itself. But such a procedure called "fragmentation" is not supported by all servers of the Internet, because dealing with fragmented packets is considered as a security risk, and therefore is turned off by many servers. That's why disturbances can occur e.g. while downloading or while transmitting web pages.

  Thus, this procedure is recommended only for connections without involving unknown servers, e.g. for a direct connection of branches to their head office via VPN connection, over which the Internet traffic is not running simultaneously.

9.5 QoS parameters for Voice over IP applications

An important task when configuring VoIP systems is to guarantee a sufficient voice quality. Two factors considerably influence the voice quality of a VoIP connection: The voice delay on its way from sender to addressee, as well as the loss of data packets, which do not arrive or do not arrive in time at the addressee. The "International Telecommunications Union" (ITU) has examined in extensive tests, what human beings perceive as sufficient voice quality, and has published as the result in the ITU G.114 recommendation.

For LANCOM devices with VoIP functions that were already integrated or added in with a software option, the QoS settings for SIP calls are defined automatically.



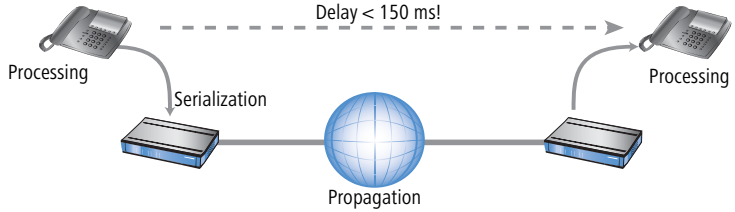
In case of a delay of not more than 100 ms, and a packet loss of less than 5%, the quality is felt like a "normal" telephone connection. In case of more than 150 ms delay and less than 10% packet loss, the telephone user perceives still a very good quality. Up to 300 ms and 20%, some listeners feel this quality like still suitable, beyond that the connection is considered as no more suitable for voice transmission.

Apart from the average delay time, also a variation in this delay is perceived by the human ear. Delay differences of the voice information from sender to addressee (jitter) are still tolerated up to 10 ms, and values beyond considered as irritating.

Accordingly, a VoIP connection should be configured such that the criteria for good speech quality are met: Packet loss up to 10%, delay up to 150 ms and jitter up to 10ms.

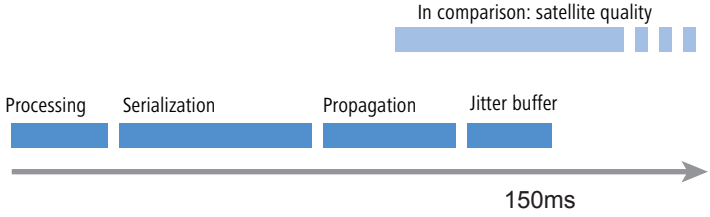
- Jitter can be removed in the receiving station by an appropriate buffer. In this buffer (jitter buffer) the packets are stored intermediately, and passed on at a constant rate to the addressee. By this intermediate buffering, the delay variations due to individual transmission times of the individual packets can be removed.
- The delay is influenced by several components:
  - Time of processing (packeting, coding and compression by the sender and the addressee), duration of handing over the packet from application to the interface (serialization), and the time for transmitting via the WAN distance (propagation) contribute to the fixed part of delay.
  - The variable part is determined by the jitter resp. by the setting of the jitter buffer.

  These two parts together compose a delay, which should ideally not exceed 150 ms.



- Apart from the general loss by network transmission, the packet loss is significantly influenced by the jitter buffer. If packets arrive with a larger delay than it can be balanced by the jitter buffer, the packets will be discarded and will increase the packet loss. The larger the jitter buffer, the smaller is the loss. Conversely, the entire delay will increase with the jitter buffer size. That means for configuration, that the jitter buffer should be selected as small as the quality can be considered still as sufficient.

In detail, delay is determined especially by the codec used, the resulting packet size and the available bandwidth:



- The time for processing is determined by the used codec. For a sampling time of 20 ms, exactly each 20 ms a new packet is generated. Times for compression can mostly be neglected.
- The time for handing over the packet to the interface is defined by the quotient of packet size and available bandwidth:

	Packet size in bytes						
	1	**64**	**128**	**256**	**512**	**1024**	**1500**
56 Kbps	0,14	9	18	36	73	146	215
64 Kbps	0,13	8	16	32	64	128	187
128 Kbps	0,06	4	8	16	32	64	93
256 Kbps	0,03	2	4	8	16	32	47
512 Kbps	0,016	1	2	4	8	16	23
768 Kbps	0,010	0,6	1,3	2,6	5	11	16
1536 Kbps	0,005	0,3	0,6	1,3	3	5	8

A 512 byte packet of an FTP connection occupies the line at 128 Kbps upstream for at least 32 ms.

Besides, the packets of the VoIP connection are often much larger than the pure net payload. The additional headers of the IP and Ethernet packets, as well eventual IPsec headers have to be added as well. The net load results from the product of net data rate and sampling time of the used codec. For all codecs, each 40 bytes UDP header and at least 20 bytes for the IPSec header must be added (RTP and IPSec headers can be larger, depending on the configuration).

Codec	Net data rate	Sampling	Packets per sec.	payload	IP packet	IPsec packet	Band-width
G.723.1	6,3 Kbit/s	30 ms	33,3	24 byte	64 byte	84 byte	22,3 Kbps
G.711	64 Kbit/s	20 ms	50	160 byte	200 byte	276 byte	110.4 Kbps

Since packets encrypted with DES, 3DES, or AES, are only able to grow in block sizes of 64 bytes, the IPSec packet for G.711 consists of 160 bytes payload + 96 bytes up to the next block limit + 20 bytes IPsec header = 276 bytes.

A similar "quote of loss" can also occur for the G.723 codec, if e.g. the RTP header is longer than 12 bytes. Then, the IP packet will grow up to the next block limit of 128 bytes; plus 20 bytes for the IPsec header creates packets of an overall length of 128 bytes, which means more than the sixfold net load!

The required bandwidth for transmission results finally from the quotient of packet size and sampling time.

- The time for transmission via Internet depends on the distance (about 1 ms per 200 km), and on the thereby passed routers (about 1 ms per hop). This time can be approximated by the half average ping time to the remote station.
- The jitter buffer can be adjusted directly at many IP telephones, e.g. as fixed number of packets, which should be used for buffering. The telephones load then up to 50% of the adjusted packets and begin afterwards to replay. The jitter buffer correspond therefore to half of the entered packets multiplied with the sampling time of the codec.
- Conclusion: The total delay is composed as follows for the according bandwidth, a ping time of 100 ms to the remote station and a jitter buffer of 4 packets for both codecs in this example:

Codec	Process-ing	Serializa-tion	Propaga-tion	Jitter buffer	Sum
G.723.1	30 ms	32 ms	50 ms	60 ms	172 ms
G.711	20 ms	32 ms	50 ms	40 ms	142 ms

The transfer time of the packets to the interface (serialization) assumes a PMTU of 512 bytes on a 128 Kbps connection. Therefore, for slower interfaces or other codecs it is eventually necessary to adjust jitter buffers and/or PMTU values.

Please notice that the bandwidths are required in the sending and receiving direction, as well as just for one single connection.

9.6 QoS in sending or receiving direction

For controlling data transfer by means of QoS one can select whether the according rule applies to the sending or to the receiving direction. But which direction refers to sending and receiving for a given a data transfer depends on the particular point of view. The following two variants apply:

- The direction corresponds to the logical connection setup
- The direction corresponds to the physical data transfer over the appropriate interface

The differences are unveiled by looking at a FTP transfer. A client of the LAN is connected to the Internet through a LANCOM.

- During an active FTP session, the client sends by the PORT command the information to the server, on which port the DATA connection is expected. As the result, the server establishes the connection to the client and sends the data in the same direction. In this case, the logical connection as well as the real data stream over the interface go from the server to the client, and the LANCOM takes both as the receiving direction.
- Different is the case of a passive FTP session. Here the client itself establishes the connection to the server. The logical connection setup thus is from client to server, but the data transmission over the physical interface flows in the reverse direction from server to client.

With standard settings, a LANCOM assumes the sending or receiving direction depending on the logical connection setup. Because such a point of view may not be easy to follow in certain application scenarios, the point of view can alternatively be changed to the flow of the physical data stream.

The differentiation between sending and receiving direction applies only to the installation of maximum bandwidths. For a guaranteed minimum bandwidth, as well as for fragmentation and PMTU reduction always the physical data transfer via the respective interface applies as the direction!

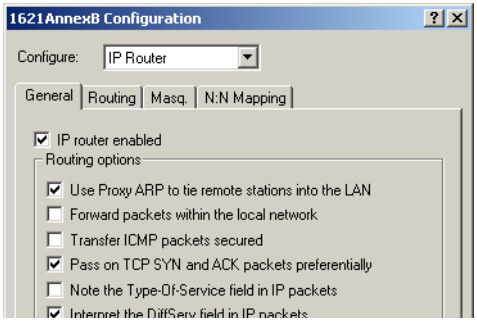
9.7 QoS configuration

9.7.1 Evaluating ToS and DiffServ fields

ToS or DiffServ?

LANconfig

For configuration with LANconfig, select the configuration field 'IP router'. Adjust on index card 'General' whether the 'Type of service field' or alternatively the 'DiffServ field' is to be observed for prioritization of data packets. When both options are turned off, the ToS/DiffServ field will be ignored.



WEBconfig, Telnet

For configuration with WEBconfig or Telnet, your decision for the evaluation of the ToS or DiffServ fields are entered at the following places:

Configuration tool	Run
WEBconfig	Setup/IP router/Routing method
Telnet	Setup/IP router/Routing method

Feature settings for routing method values are the following:

- **Standard**: The ToS/DiffServ field is ignored.
- **TOS**: The ToS/DiffServ field is considered as ToS field, the bits "Low delay" and "High reliability" will be evaluated.
- **DiffServ**: The ToS/DiffServ field is interpreted as DiffServ field and evaluated as follows:

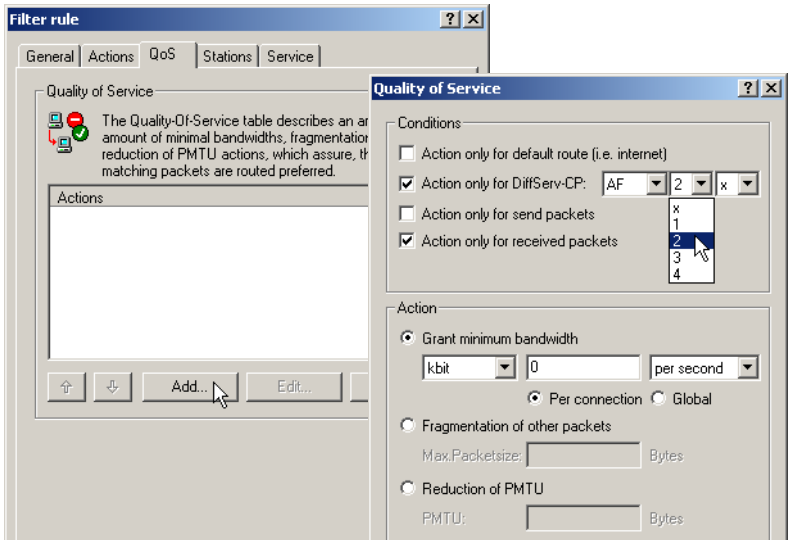
DSCP code points	Kind of transmission
CSx (including CS0 = BE)	normal transmission
AFxx	secured transmission
EF	preferred transmission

DiffServ in Firewall rules

The code points from the DiffServ field can be evaluated by Firewall rules for further control of QoS parameters such as minimum bandwidth or PMTU reduction.

LANconfig

The parameters for evaluating the DiffServ fields are adjusted when defining the QoS rule in LANconfig:



According to your selection of the DSCP type (BE, CS, AF, EF) the valid values can be adjusted in additional drop down lists. Alternatively, the DSCP decimal value can be entered directly. A table listing valid values can be found under 'What is DiffServ?' → page 227.

WEBconfig, Telnet

For configuration with WEBconfig or Telnet, the parameters are entered at the following places into a new Firewall rule:

Configuration tool	Run
WEBconfig	Setup/IP router/Firewall/Rule list
Telnet	Setup/IP router/Firewall/Rule list

The Firewall rule is extended by condition "@d" and the DSCP (Differentiated Services Code Point). The code point can either be indicated with its name (CS0 - CS7, AF11 to AF 43, EF or BE) or its decimal resp. hexadecimal depiction. "Expedited Forwarding" can therefore be indicated as "@dEF", "@d46" or "@d0x2e". Furthermore, collective names (CSx resp. AFxx) are possible.

Examples:

- **%Lcds0 @dAFxx %A**: Accept (secured transmission) on DiffServ "AF", limit "0"
- **%Qcds32 @dEF**: Minimum bandwidth for DiffServ "EF" of 32 kbps
- **%Fprw256 @dEF**: PMTU reduction for reception for DiffServ "EF" to 256 bytes

These examples reserve a desired bandwidth for Voice over IP phone calls. The first element "%Lcds0 @dAFxx %A" accepts DSCP "AFxx" marked packets of signalling calls. Voice data marked with "EF" is transferred preferentially by the entry "%Qcds32 @dEF", and a bandwidth of 32 Kbps is guaranteed thereby as well. In parallel, the PMTU is

reduced to 256 byte by "%Fprw256 @dEF", which enables ensuring the required bandwidth in receiving direction at all.

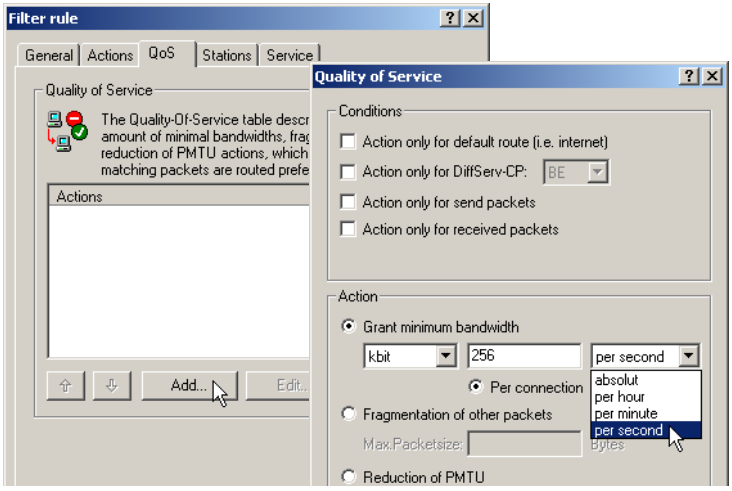
Further information about defining Firewall rules can be found in chapter 'Firewall' → page 171.

9.7.2 Defining minimum and maximum bandwidths

LANconfig

A minimum bandwidth for certain applications is defined in LANconfig by a Firewall rule according to the following conditions:

- The rule does not need an action, because QoS rules always implicitly assume "transfer" as action.
- The guaranteed bandwidth is defined on index card 'QoS'.



  - The option 'Action only for default route' limits the rule to those packets, which are sent or received via default route.
  - The option 'Action only for VPN route' limits the rule to those packets, which are sent or received via VPN tunnel.
  - The option 'Forced' defines a static reservation of bandwidth. Bandwidth reserved in this way cannot be used for any other connections, even while the preferred connection is inactive.
  - The option 'Per connection' resp. 'Globally' specifies, whether the minimum bandwidth set here is valid for each single connection corresponding to this rule ('per connection'), or, if this should be the upper limit for the sum of all connections together ('globally').
- Like for other Firewall rules, index cards 'Stations' and 'Services' determine for which stations in the LAN / WAN and for which protocols this rule applies.

WEBconfig, Telnet

For configuration with WEBconfig or Telnet, the minimum resp. maximum bandwidths are entered into a new Firewall rule at the following places:

Configuration tool	Run
WEBconfig	Setup/IP router/Firewall/Rule list
Telnet	Setup/IP router/Firewall/Rule list

A required minimum bandwidth is introduced by "%Q". Here it is implicitly assumed that the respective rule is an "Accept" action, and that the packets will thus be transmitted.

A maximum bandwidth is simply defined by a limit rule, which discards by a "Drop" action all packets, which exceed the defined bandwidth.

Examples:

- **%Qcds32**: Minimum bandwidth of 32 kbps for each connection
- **%Lgds256 %d**: Maximum bandwidth of 256 kbps for all connections (globally)

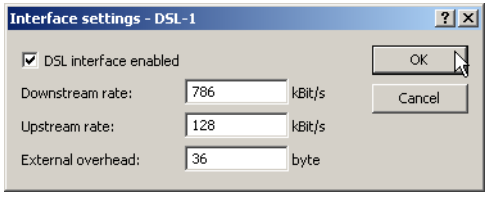
Further information about defining Firewall rules can be found in chapter 'Firewall' → page 171.

9.7.3 Adjusting transfer rates for interfaces

Devices with built-in ADSL/SDSL modem resp. with an ISDN adapter make these settings independently for the respective interface. For a LANCOM model with Ethernet **and** ISDN interface, these settings have to be made solely for the Ethernet interface.

LANconfig

Data rate restrictions for Ethernet, DSL and DSLoL interfaces are entered in LANconfig under configuration field 'Interfaces' on index card 'WAN' within the settings for the different WAN interfaces:



- An Ethernet WAN (DSL/cable) interface can be switched off completely in this dialogue.
- As upstream and downstream rate the gross data rates are entered, which are usually a little bit higher than the net data rates indicated by the provider as the guaranteed data rate (see also 'The queue concept' → page 229).

- The "external overhead" considers information added to the packets during the data transfer. Concerning applications with small data packets (e.g. Voice over IP), this extra overhead is quite noticeable. Examples for the external overhead:

Transfer	External overhead	Note
PPPoEoA	36 bytes	additional headers, loss by not completely used ATM cells
PPTP	24 bytes	additional headers, loss by not completely used ATM cells
IPoA (LLC)	22 bytes	additional headers, loss by not completely used ATM cells
IPoA (VC-MUX)	18 bytes	additional headers, loss by not completely used ATM cells
Cable modem	0	direct transfer of Ethernet packets

WEBconfig, Telnet

Under WEBconfig or Telnet the restrictions of data transfer rates for Ethernet, DSL and DSLoL interfaces are entered at the following places:

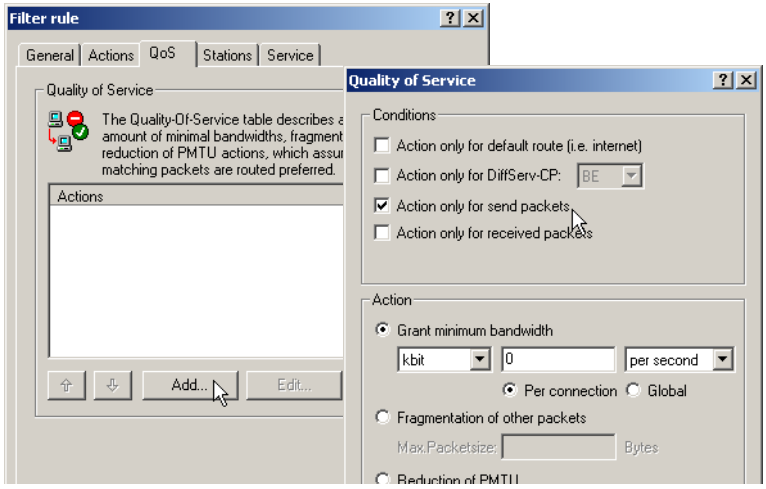
Configuration tool	Run
WEBconfig	Setup/Interfaces/DSL Interfaces
Telnet	Setup/Interfaces/DSL Interfaces

Only upstream and downstream rates are indicated by Kbps, external overhead in bytes/packet.

9.7.4 Sending and receiving direction

LANconfig

The interpretation of the data transfer direction can be adjusted in LANconfig when defining the QoS rule:



WEBconfig, Telnet

For configuration with WEBconfig or Telnet, the interpretation of the data transfer direction is specified at the following places in a new Firewall rule by parameters "R" for receive, "T" for transmit (send) and "W" for reference to the WAN interface:

Configuration tool	Run
WEBconfig	Setup/IP router/Firewall/Rule list
Telnet	Setup/IP router/Firewall/Rule list

A restriction of data transfer to 16 Kbps in sending direction applying to the physical WAN interface is e.g. made by the following Firewall rule:

- %Lcdstw16%d

9.7.5 Reducing the packet length

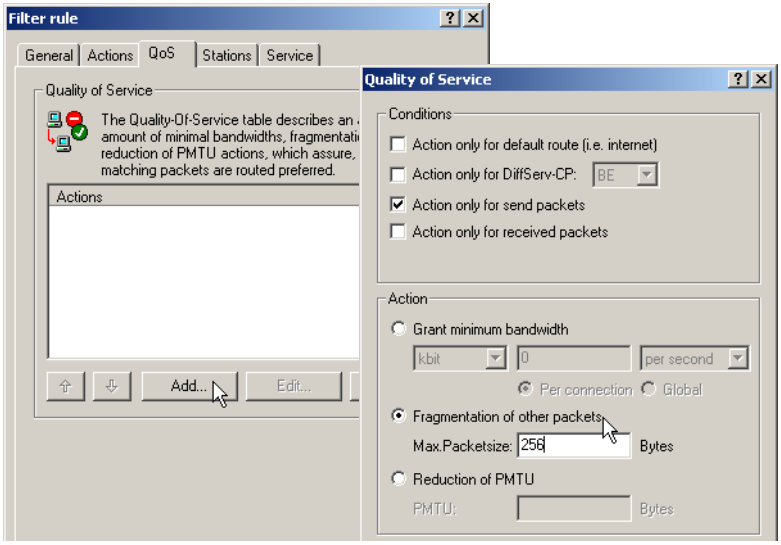
The length reduction of the data packets is defined by a Firewall rule according to the following conditions:

- The reduction refers to **all** packets, which will be sent to the interface and which do **not** correspond to the rule.
- Not packets of certain protocols are reduced, rather than all packets globally on that interface

For LANCOM devices with VoIP functions that were already integrated or added in with a software option, fragmentation and PMTU reduction can be set separately for SIP calls.

LANconfig

The length reduction of the data packets is set in LANconfig when defining the QoS rule:



WEBconfig, Telnet

For configuration with WEBconfig or Telnet, the reduction is entered at the following places in a new Firewall rule by parameter "P" for PMTU reduction (Path MTU, MTU = Maximum Transmission Unit) and "F" for the fragment size:

Configuration tool	Run
WEBconfig	Setup/IP router/Firewall/Rule list
Telnet	Setup/IP router/Firewall/Rule list

PMTU reduction and fragmentation refer always to the physical connection. Indicating parameter "W" for WAN sending direction is not required here and hence will be ignored if existing.

The following example shows a setting for Voice over IP telephony:

Rule	Source	Destination	Action	Protocol
VOIP	IP addresses of IP telephones in the LAN, all ports	IP addresses of IP telephones in the LAN, all ports	%Qcds32 %Prt256	UDP

This rule defines the minimum bandwidth for sending and receiving to 32 Kbps, forces and reduces the PMTU while sending and receiving to packets of 256 byte size. For the TCP connection, the maximum segment size of the local workstation is determined to 216, so that the server will send packets of maximum 256 byte (reduction of the PMTU in sending and receiving direction).

9.8 QoS for WLANs according to IEEE 802.11e (WMM/WME)

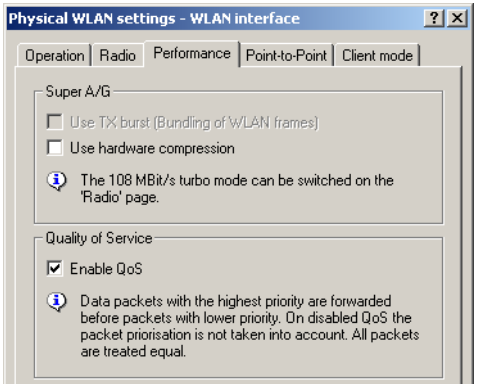
With the extension to the 802.11 standard, 802.11e, Quality of Service can be provided for transfers via WLAN. Among others, 802.11e supports the prioritization of certain data-packet types. Die Erweiterung stellt damit eine wichtige Basis für die Nutzung von Voice-Anwendungen im WLAN dar (Voice oder WLAN – VoWLAN).

The WiFi alliance certifies products that support Quality of Service according to 802.11e, and refer to WMM (WiFi Multimedia, formerly known as WME or Wireless Multimedia Extension). WMM defines four categories (voice, video, best effort and background) which make up separate queues to be used for prioritization.

The 802.11e standard sets priorities by referring to the VLAN tags or, in the absence of these, by the DiffServ fields of IP packets. Delay times (jitter) are kept below 2 milliseconds, a magnitude which is inaudible to the human ear. 802.11e controls access to the transfer medium with EDCF, the Enhanced Distributed Coordination Function.

Priorities can only be set if the WLAN client and the access point both support 802.11e or WMM, and also if the applications are able to mark the data packets with the corresponding priorities.

A LANCOM access point can activate 802.11e for each of its physical WLAN networks separately.



Configuration tool	Call
LANconfig	Interfaces ▶ Wireless LAN ▶ Physical WLAN settings ▶ Performance
WEBconfig, Telnet	Expert-Configuration > Setup > Interfaces > WLAN > Performance

10 Virtual Private Networks—VPN

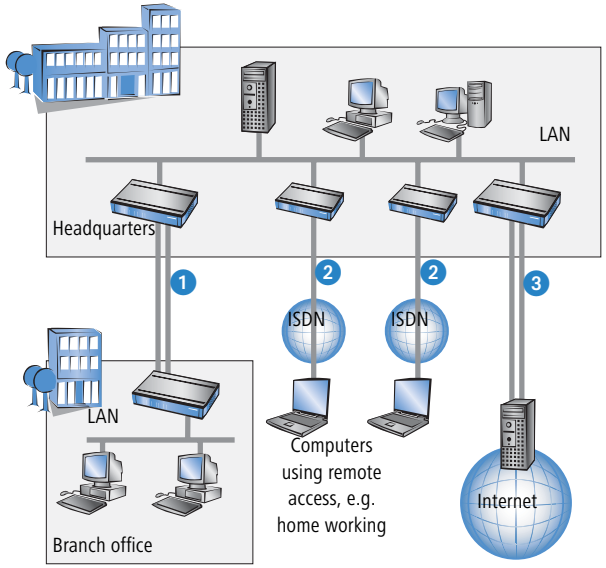
10.1 What does VPN offer?

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

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

Conventional network infrastructure

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



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

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

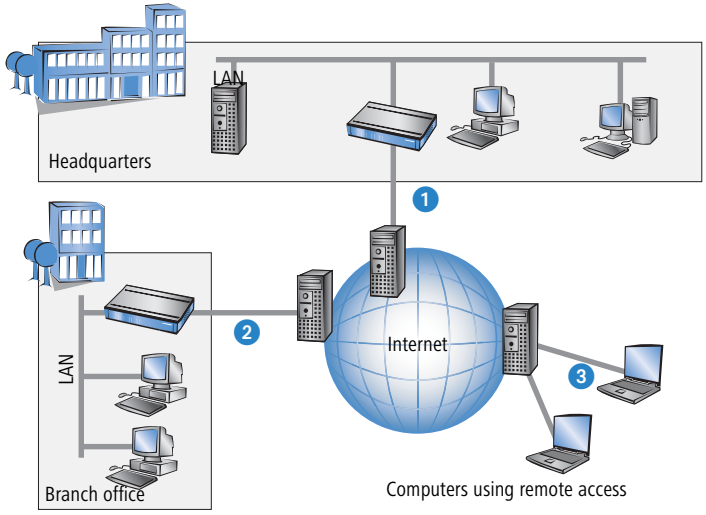
All connections to the outside world are based on dedicated lines, i.e. switched or leased lines. Dedicated lines are very reliable and secure. On the other hand, they involve high costs. In general, the costs for dedicated lines are

dependent on the distance. Especially in the case of long-distance connections, keeping an eye out of cost-effective alternatives can be worthwhile.

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

Networking via the Internet

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



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

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

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

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

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

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

Two technical properties of the IP standard speak against using the Internet as a part of a corporate network, however:

- The necessity of public IP addresses for all participants
- The lack of data security of unprotected data transfers

10.1.1 Private IP addresses on the Internet?

The IP standard defines two types of IP addresses: public and private. A public IP address is valid worldwide, while a private IP address only applies within a closed LAN.

Public IP addresses must be unique on a worldwide basis. Private IP addresses can occur any number of times worldwide; they must only be unique within their own closed network.

Normally, PCs in a LAN only have private IP addresses, while the router to the Internet also has a public address. All PCs behind this router have access to the Internet via its public IP address (IP masquerading). In such a case, only the router itself is responsive via the Internet. PCs behind the router are not responsive to the Internet without intervention by the router.

Routing at the IP level with VPN

IP connections must be established between routers with public IP addresses in order to link networks via the Internet. These routers provide the connections between multiple subnetworks. When a computer sends a packet to a private IP address in a remote network segment, the local router forwards the packet to the router of the remote network segment via the Internet.

The VPN gateway handles the conversion between private and public IP addresses. Without VPN, computers without public IP addresses would not be able to communicate with one another via the Internet.

10.1.2 Secure communications via the Internet?

The idea of using the Internet for corporate communications has been met with skepticism. The reason for this is that the Internet lies beyond a company's field of influence. Unlike dedicated connections, data on the Internet travels through the network structures of third parties that are frequently unknown to the company.

In addition, the Internet is based on a simple form of data transfer using unencrypted data packets. Third parties can monitor and perhaps even manipulate the contents of these packets. Anyone can access the Internet. As a result, third parties may gain unauthorized access to the transferred data.

VPN – Security through encryption

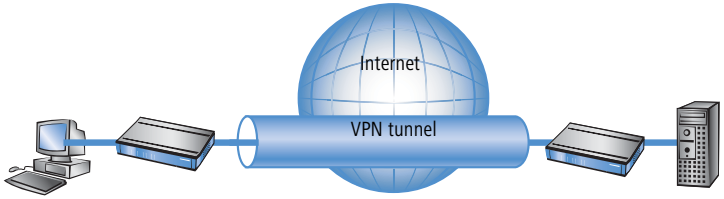
VPN was developed as a solution to this security problem. If necessary, it can encrypt the complete data communications between two participants. The packets are then unreadable for third parties.

The latest and most secure encryption technologies can be used for VPN. A very high level of security can thus be reached. VPN-protected data traffic via the Internet offers a degree of security that at least corresponds to that of dedicated lines.

Codes usually referred to as "keys" are agreed upon between the participants and used for data encryption. Only the participants in the VPN know these keys. Without a valid key, it is not possible to decrypt the data. They thus remain "private", inaccessible to unauthorized parties.

Send your data through the tunnel – for security's sake

This also explains the nature of a virtual private network: A fixed, physical connection between the devices of the type required for a direct connection does not exist at any time. Rather, the data flows via suitable routes through the Internet. With the proper technology, third parties can monitor and even record data traffic. As the packets are encrypted by VPN, the actual content of the packets is inaccessible. Experts compare this state to a tunnel: it's open at either end, but perfectly shielded in between. Secure connections within public IP networks are thus also referred to as "tunnels".

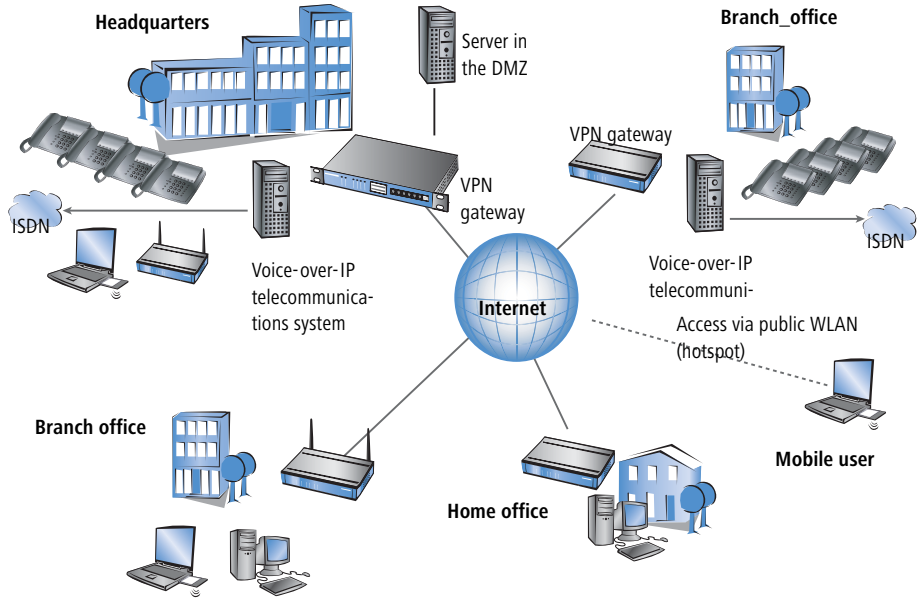


The goal of modern network structures has thus been achieved: secure connections via the largest and most low-cost public IP network: the Internet.

10.2 LANCOM VPN: an overview

10.2.1 VPN example application

VPN connections are used in many different fields of application. In most cases, a variety of communications technologies is used for transferring both data and audio, and VPN unites these systems into an integrated network. The following example illustrates a typical application that is often used in practice.



The principal components and features of these applications:

- The coupling of networks, for example between headquarters and a branch office
- Connecting external locations without fixed IP addresses via VPN router
- Connecting home offices without fixed IPs via ISDN or analog modems
- Connecting to Voice-over-IP telephone exchanges
- Connecting mobile users, for example when using public WLAN access

10.2.2 LANCOM VPN functions

This section lists all of the functions and properties of LANCOM VPN. This overview will provide a great deal of information for VPN experts. It is very compact, but contains a lot of complex, specialized terminology. Knowledge of the technical basics of VPN are required to understand this section. Don't worry: it's no problem if you skip this section. The information contained here is not required to set up and use LANCOM VPN.

- VPN in accordance with IPSec standard
- VPN tunnel via leased lines, switched connections and IP networks
- IPSec main and aggressive mode
- LANCOM Dynamic VPN: Public IP addresses can be static or dynamic (initiation of a connection towards remote sites with dynamic IP addresses requires ISDN)
- IPSec protocols AH, ESP and IPCOMP in transport and tunnel mode
- Hash algorithms:

  - □ HMAC-MD5-96, Hash length 128 bit
  - □ HMAC-SHA-1-96, Hash length 160 bit
- Symmetrical encryption methods
  - □ AES, key length 128, 192 and 256 bit
  - □ Triple-DES, key length 168 bit
  - □ Blowfish, key length 128 - 448 bit
  - □ CAST, key length 128 bit
  - □ DES, key length 56 bit
- IKE Config Mode
- IKE key exchange with Preshared Keys
- IKE with RSA signature and digital certificates (X.509)
- Key exchange via Oakley, Diffie-Hellman algorithm with key lengths 768 bit, 1024 bit or 1536 bit, well-known groups 1, 2 and 5
- Key management in accordance with ISAKMP
- Apart from conventional IPSec implementations, LANCOM devices offer extended functionality, such as the LANCOM Dynamic VPN that allows the use of the high-security IKE Main Mode even with dynamic IP addresses.
- In combination with the LANCOM Advanced VPN Client, a separate pre-shared key can be used for each connection even when using IKE Aggressive Mode connections.

10.3 VPN connections in detail

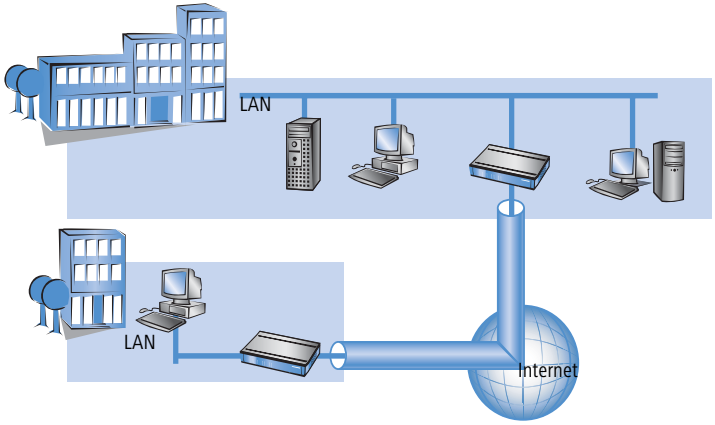
Two types of VPN connections are available:

- VPN connections linking two local networks. This type of connection is also known as a "LAN-LAN coupling".
- The connection of an individual computer with a network, generally via a dial-in connection (Remote Access Service – RAS).

10.3.1 LAN-LAN coupling

The coupling of two remote networks is known as a LAN-LAN coupling. With such a connection, the devices in one LAN can access those of the remote LAN (assuming they have the necessary access rights).

In practice, LAN-LAN couplings are frequently used between company headquarters and subsidiaries, or for connections to partner companies.



A VPN-enabled router (VPN gateway) is located at either end of the tunnel. The configuration of both VPN gateways must be matched to one another.

The connections are transparent for the remaining devices in the local networks, i.e., they appear to have a direct connection. Only the two gateways must be configured for the VPN connection.

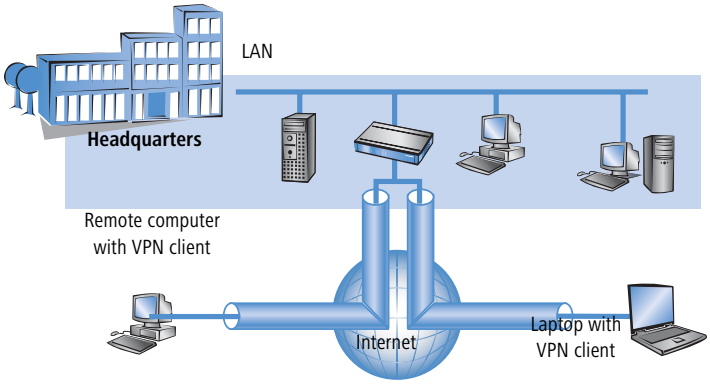
Internet access in parallel

The Internet access for VPN can be used simultaneously for other Internet applications, such as web-browsing or e-mail. For security reasons, the parallel Internet access may be unwanted in some cases. For instance, if a branch office should be enforced to access the Internet only via a central firewall. For such applications the parallel Internet access can be disabled as well.

10.3.2 Dial-in connections (Remote Access Service)

Individual remote computers (hosts) can access the resources of the LAN via dial-up connections. Practical examples of this are employees working from home or field staff that dial into the company network.

If the dial-up connection of an individual computer to a LAN is to be realized via VPN, that computer first connects to the Internet. A special VPN client software then sets up a tunnel to the VPN gateway of the LAN using this Internet connection.



The VPN gateway of the LAN must support the establishment of VPN tunnels with the VPN client software of the remote PC.

10.4 What is LANCOM Dynamic VPN?

LANCOM Dynamic VPN is a LANCOM Systems technology which permits VPN tunnels to be connected **to** remote stations that do not have a static, but only a dynamic IP address.

Who needs LANCOM Dynamic VPN and how does it work? We will answer this question in two steps: First, a look at the basics of IP addressing will show the problem of static IP addresses. The second step shows the solution thereof with LANCOM Dynamic VPN.

10.4.1 A look at IP addressing

Every participant on the Internet needs an IP address. Participants even need a special kind of IP address - a public one. The administration of public IP addresses is handled from central locations in the Internet. Each public IP address may only occur once on the entire Internet.

Local IP-based networks do not use public, but private IP addresses. For this reason, a number of address ranges within the entire IP address range have been reserved for private IP addresses.

A computer connected to both a local network and directly to the Internet therefore has two IP addresses: a public one for communication with the rest of the Internet and a private one by which the computer can be reached within the local network.

Static and dynamic IP addresses

Public IP addresses must be applied for and managed, which involves costs. There is also only a limited number of public IP addresses. For this reason, not every Internet user has his or her own fixed (static) IP address.

The alternative to static IP addresses are the so-called dynamic IP addresses. A dynamic IP address is assigned to an Internet user by the Internet Service Provider (ISP) upon dialling-in, and remains valid for the duration of the connection. The ISP takes an unused address selected at random from their pool of IP addresses. This IP address is only temporarily assigned to the user for the duration of a given connection. When the connection is ended, the IP address is once again free and the ISP can assign it to another user.

Many flatrate connections, too, are realised with via dynamic IP addresses. Every 24 hours or so, the connection is forcibly interrupted. The new connection is generally assigned with a new and different IP address.

Advantages and disadvantages of dynamic IP addresses

This process has a very important advantage for ISPs: they only need relatively small pools of IP addresses. Dynamic IP addresses are also favorable for users: it's not necessary for them to apply for static IP addresses in advance - they can connect to the Internet immediately. It's also not necessary for them to manage IP addresses. This saves trouble and costs. The other side of the coin: A user without a static IP address cannot be addressed directly from the Internet.

This is a major problem when setting up VPNs. If, for example, Computer A would like to communicate with Computer B using a VPN tunnel on the Internet, Computer A needs the remote computer's IP address. If B only has a dynamic address, A cannot know that address and therefore cannot contact B.

The LANCOM Dynamic VPN offers the answer here.

10.4.2 This is how LANCOM Dynamic VPN works

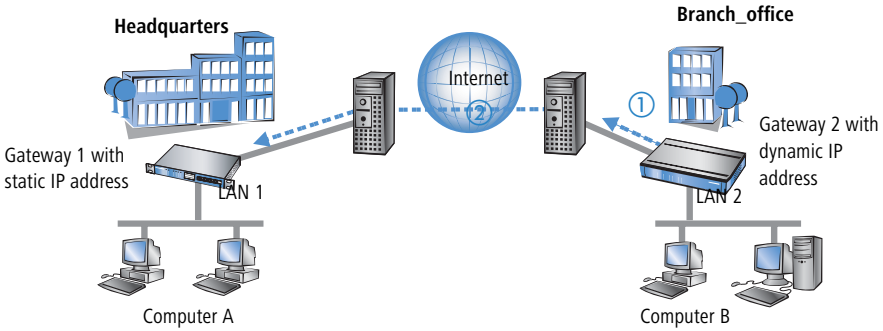
Let's use two examples to explain how LANCOM Dynamic VPN works (designations refer to the IP addressing type of the two VPN gateways):

- dynamic – static
- static – dynamic
- dynamic – dynamic

Dynamic – static

If a user on computer B in LAN 2 wishes to connect to computer A in LAN 1, then gateway 2 receives a request and tries to establish a VPN tunnel to gateway 1. Gateway 1 has a static IP address and can be directly contacted over the Internet.

A problem arises in that the IP address from gateway 2 is assigned dynamically, and gateway 2 must communicate its current IP address to gateway 1 when attempting to connect. In this case, LANCOM Dynamic VPN takes care of transmitting the IP address during connection establishment.



① Gateway 2 connects to the Internet and is assigned a dynamic IP address.

② Gateway 2 contacts Gateway 1 via its known public IP address. LANCOM Dynamic VPN enables the identification and transmission of the actual IP address of Gateway 2. Gateway 1 initiates the VPN tunnel then.

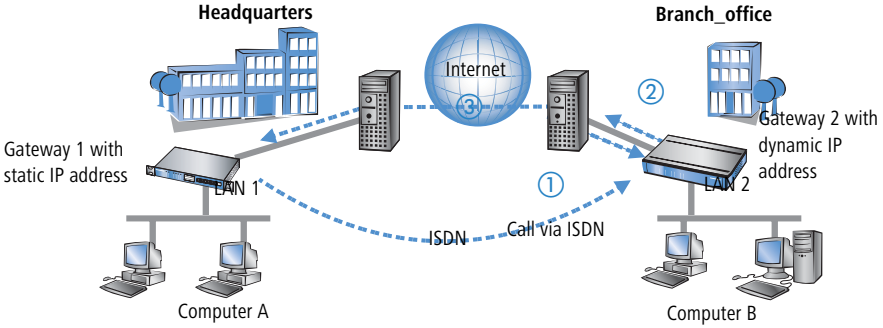
The great advantage of LANCOM devices with this application: Instead of the "Aggressive Mode" that is normally used when connecting VPN clients to the headquarters, the far more secure "Main Mode" can be applied. Although with Main Mode more unencrypted messages can be exchanged during the IKE handshake, the method is overall more secure than Aggressive Mode.

An ISDN line is not necessary for establishing this type of connection. The dynamic end communicates its IP address encrypted via the Internet protocol ICMP (or alternatively via UDP).

Static – dynamic

If, on the other hand, computer A in LAN 1 requires a connection to computer B in LAN 2, for example when headquarters carries out remote maintenance at the external locations, then gateway 1 receives the request and attempts to establish a VPN tunnel to gateway 2. Gateway 2 only has a dynamic IP address and cannot be directly contacted over the Internet.

With LANCOM Dynamic VPN, the VPN tunnel can be set up nevertheless. The connection is established in three steps:



① Gateway 1 calls Gateway 2 via ISDN. It takes advantage of the ISDN functionality of sending its own subscriber number via the D-channel free of charge. Gateway 2 determines the IP address of Gateway 1 from the preconfigured VPN remote stations using the received subscriber number.

If Gateway 2 does not receive a subscriber number via the D-channel (if that particular ISDN service feature is not available, for example) or an unknown number is transferred, the authentication will be performed via the B-channel. Once the negotiation was successful, Gateway 1 sends its IP address and closes the connection on the B-channel immediately.

② Now its Gateway 2's turn: It first connects to its ISP and is assigned a dynamic IP address.

③ Gateway 2 authenticates itself at Gateway 1. The static IP address of gateway 1 is known, of course.

④ Gateway 1 now knows the address of Gateway 2 and sets up the VPN tunnel to Gateway 2.

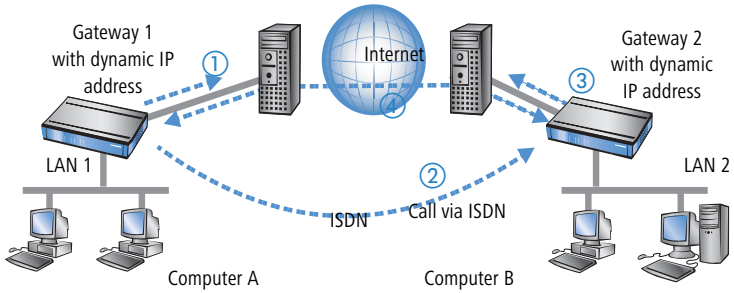
The advantage of LANCOM devices, for example when connecting from the headquarters to branch offices: The functions in LANCOM Dynamic VPN also allows access to networks without a flatrate, i.e. networks that are not always online. The ISDN connection and an associated MSN act to substitute the another address, such as a static IP address or the dynamic address translation via dynamic DNS services, a solution often used with flatrate connections.

The described connection set up requires an ISDN connection for both VPN gateways. But usually no charges will arise for this procedure.

Please note 'Information to the Dynamic VPN registration' → page 258.

Dynamic – dynamic

With LANCOM Dynamic VPN, VPN tunnels can also be set up between two gateways that both only have dynamic IP addresses. Let's modify the previous example so that in this case Gateway 1 also has a dynamic IP address. Once again, Computer A would like to connect to Computer B:



① Gateway 1 connects to its ISP and is assigned a public, dynamic IP address.

② It then calls Gateway 2 via ISDN to send this dynamic address. Three procedures are used to send the address:

- **As information in the LLC element of the D-channel.** In the D-channel protocol of Euro-ISDN (DSS-1), the so-called LLC (**L**ower **L**ayer **C**ompatibility) element can be used to send additional information to the remote station. This transfer takes place before the B-channel connection is established. Once the address has been sent successfully, the remote station rejects the call. Charges are thus not incurred for a B-channel connection. The IP address is sent nevertheless for free in this case.

The LLC element is generally available as a standard feature in Euro-ISDN that does not require registration or activation. It may be disabled by telephone companies or individual exchanges, however. The LLC element is not available in 1TR6, the German national ISDN. The procedure described above thus will not work with 1TR6.

- **As a subaddress via the D-channel.** If it is not possible to send the address via the LLC element, Gateway 1 will attempt to send the address as a so-called subaddress. Like the LLC element, the subaddress is an information element of the D-channel protocol that permits short items of information to be sent free of charge. In this case, the telephone company must enable the 'subaddressing' feature first; this is generally subject to a charge. As with the LLC element, the call is rejected by the remote station once the IP address has been transferred successfully. The connection thus remains free of charge.
- **Via the B-channel.** If both attempts to send the IP address via the D-channel fail, then a conventional connection via the B-channel must be established to send the IP address. The connection is dropped immediately after the IP address has been sent. This connection is subject to the usual charges.

③ Gateway 2 connects to the ISP and receives a dynamic IP address.

④ Gateway 2 authenticates itself at Gateway 1. The static IP address of gateway 1 is known, of course.

⑤ Gateway 1 now knows the address of Gateway 2 and sets up the VPN tunnel to Gateway 2.

Dynamic VPN works only between LANCOM that each feature at least one ISDN port that can be used for the ISDN connection.

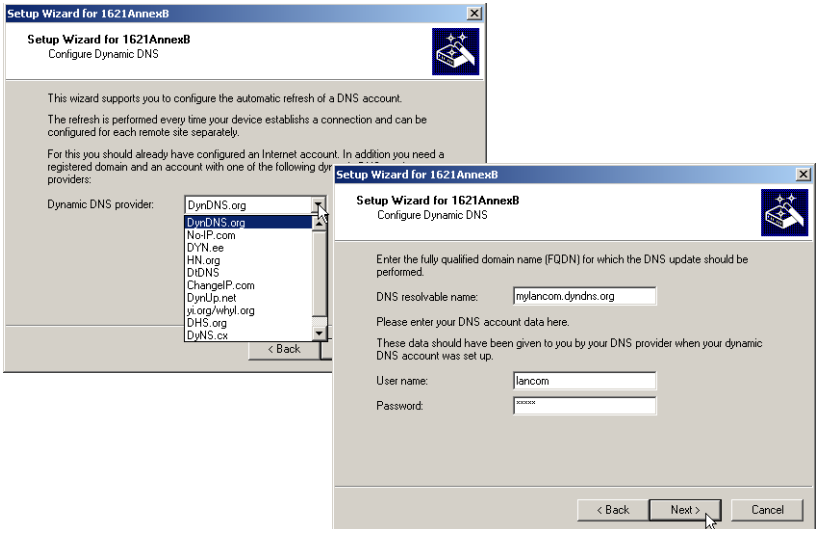
Please note 'Information to the Dynamic VPN registration' → page 258..

Dynamic IP addresses and DynDNS

It is also possible to establish a connection between two stations using dynamic IP addresses by using so-called dynamic DNS services (DynDNS). The address of the tunnel end-point is not defined as an IP number (which is, of course, dynamic and subject to frequent change) but as a static name instead (e.g. MyLANCOM@DynDNS.org).

Two things are needed for translating a name to its current IP address: A dynamic DNS server and a dynamic DNS client:

- The first, available from numerous providers in the Internet, is a server that is in communication with Internet DNS servers.
- The dynamic DNS client is integrated in the device. It can make contact to any one of a number of dynamic-DNS service providers and, assuming that a user account has been set up, automatically update its current IP address for the DNS name translation. This can be set up very conveniently with a Wizard under LANconfig (also see 'Dynamic DNS' on page 541):



For reasons of security and availability, LANCOM Systems recommends the use of Dynamic VPN in preference to dynamic DNS-based VPN solutions. Dynamic VPN is based on direct connections via the ISDN network and ensures a higher degree of availability than dynamic DNS services in the Internet.

10.4.3 Information to the Dynamic VPN registration

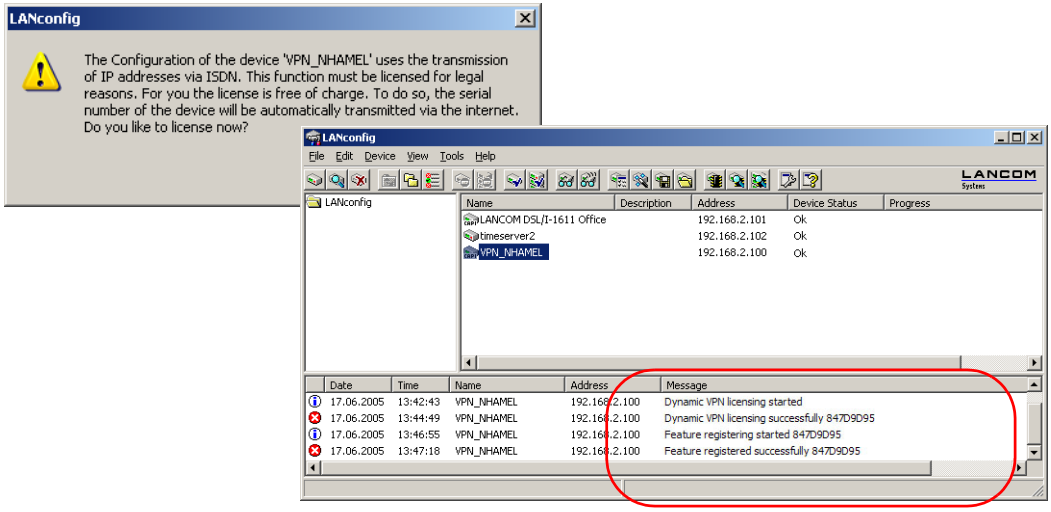
When using dynamic VPN with IP address transmission over ISDN you must activate this feature. This operating mode is usually then required, when you configure a VPN tunnel with dynamic IP addresses on both sides without dynamic DNS services. All other operation modes of dynamic VPN (for transmitting the IP address by ICMP, to provoke a call-back etc.) do **not** require a registration.

The registration is anonymous, i.e. no personal or firm data is transmitted.

The registration of the dynamic VPN option requires administrator rights.

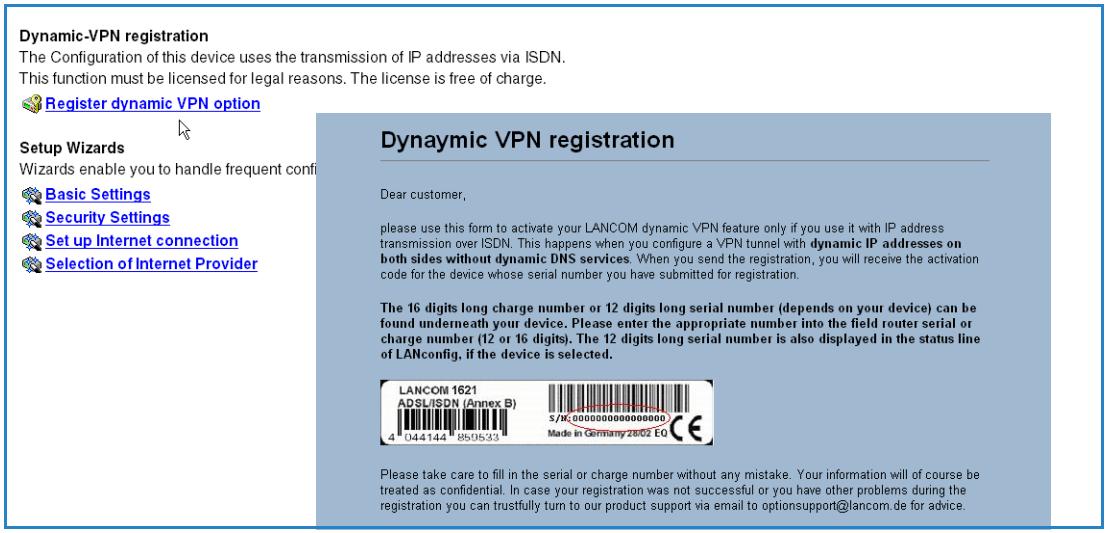
Registration with LANconfig

When scanning the device for instance right after the program start LANconfig automatically recognizes if the device must be activated. After confirming the arising hint the LANconfig automatically transmits the required data of the device to the registration server of LANCOM Systems. The release code ist automatically transmitted back to the device and activated. The state of this procedure is visible in LANconfig.



Registration with WEBconfig

For the registration with WEBconfig the serial number of the device ist required. You can find this information on the bottom side of your device.



When using WEBconfig you can find a link on the first page which leads you to the registrating server of LANCOM Systems. There you must enter the serial number of your device and your e-mail address. After transmitting the data you receive a release code for the device.

To load this release code into your router, please proceed as follows:

Log on with administrator rights on WEBconfig. Select **Enable Software Option**, which is placed on the entry page. On the following page enter the release code and confirm by clicking on **Apply**.

10.5 Configuration of VPN connections

Three questions are answered in the configuration of VPN connections:

- Between which VPN gateways (remote stations) is the connection established?
- What security parameters are used to secure the VPN tunnel between the two gateways?
- Which networks or computers can intercommunicate via these tunnels?

This section introduces the basic considerations for configuring VPN connections. Considered first of all is the simple connection of two local networks. Special cases such as dialling in to LANs with individual computers (RAS) or the connection of structured networks will be covered subsequently.

10.5.1 VPN tunnel: Connections between VPN gateways

Virtual Private Networks (VPNs) are used to interconnect local networks over the Internet. This involves the routing of the private LAN IP addresses via an Internet connection between two gateways with public IP addresses.

For the secure routing of private IP addresses over the Internet, a VPN connection, also known as a VPN tunnel, is established between the two LANs.

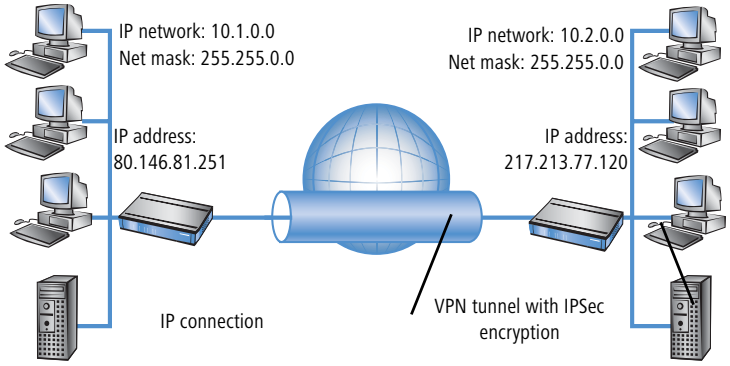
The VPN tunnel has two important tasks:

- To shield the transported data from unauthorized access
- To route private IP addresses via an Internet connection that can normally only be used to route public IP addresses.

The VPN connection between the two gateways is defined by the following parameters:

- The end-points of the tunnel, the VPN gateways, each of which are accessible via public IP addresses (static or dynamic)
- The IP connection between the two gateways
- The private IP address range that are to be routed between the VPN gateways
- Setting relevant to security, such as passwords, IPSec keys etc. to shield the VPN tunnel

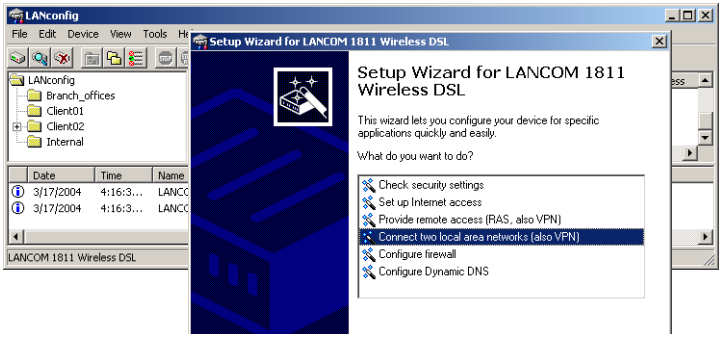
This information is contained in the so-called VPN rules.



10.5.2 Set up VPN connections with the Setup Wizard

If possible, make use of the Setup Wizard within LANconfig to set up VPN connections between local networks. The Wizard guides you through the configuration and makes all the necessary settings for you. Carry out the configuration on both routers, one after the other.

① Choose your device from the selection window in LANconfig and select the **Setup Wizard** button or use the menu bar **Tools** ▶ **Setup Wizard**.



② Follow the Wizard's instructions and enter the necessary data. 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 device should automatically connect to the remote station and make contact to the requested computer.

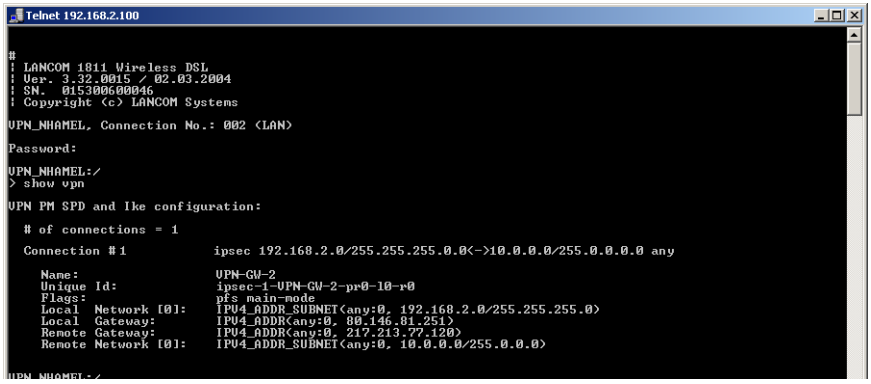
This Wizard automatically sets up the VPN connections essential for typical LAN-LAN coupling. In the following situations, the VPN connections will have to be configured manually:

- Where no Windows computer with LANconfig is available. In this case, the necessary parameters are set with WEBconfig or via the Telnet console.
- Where only selected portions of the LAN (intranet) are to communicate with other computers via the VPN connection. This is the case where, for example, the intranet is connected to further subnets with routers, or when only selected portions of the intranet should have access to the VPN connection. In such cases, additional parameters are defined supplementary to those entered in the Setup Wizard.
- Configuring VPN connections to third-party devices.

10.5.3 Inspect VPN rules

VPN rules represent a combination of various pieces of information and they are not directly defined in a LANCOM device; instead, they are compiled from a variety of sources. This is why it is not possible to inspect the VPN rules with LANconfig or any other configuration tool.

Information about the current VPN rules in the device can be retrieved with the Telnet console. Start a Telnet connection to the VPN gateway and enter the command **show vpn** in the console:



The output informs you of the network relationships that are relevant to VPN connections to other networks.

In this example, the local network at a branch office (network 192.168.2.0, netmask 255.255.255.0) is connected to the network at the headquarters (network 10.0.0.0, netmask 255.255.255.0). The public IP address of the local gateway is 80.146.81.251, and that of the remote VPN gateway is 217.213.77.120.

Entering "any:0" displays the protocols and ports that can be used over the connection.

Further output is displayed by the command "show vpn long". The information displayed here covers network relationships and also the parameters that are relevant to security, such as IKE and IPSec proposals.

10.5.4 Manually setting up VPN connections

Manually setting up VPN connections involves the tasks described previously:

- Definition of the tunnel endpoints

- Definition of the security-related parameters (IKE and IPSec)
- Definition of the VPN network relationships, i.e. the IP address ranges to be connected. Should the IP ranges overlap at both ends of the connection, please refer to the section 'N:N mapping' on page 139.
- When coupling Windows networks (NetBIOS/IP): Without WINS servers at both ends of the VPN connection (such as when linking a home office), the LANCOM can take over the necessary NetBIOS proxy functions. To this end, the NetBIOS module in the LANCOM must be activated, and the corresponding VPN remote site must be entered into the NetBIOS module as the remote site. Should WINS servers be present in both of the coupled networks, then the NetBIOS module should be deactivated so that the LANCOM does not perform NetBIOS proxy functions.

To use the LANCOM NetBIOX proxy either LANCOM Dynamic VPN must be applied, because it transmits the required addresses, or the IP address of the remote station as a primary NBNS must be entered in the IP parameter list (*LANconfig*: Communication / Protocols).

- When using LANCOM Dynamic VPN: Entry for the corresponding remote site in the PPP list with a suitable password for the Dynamic VPN handshake. The username entered here must correspond with the name entered in the remote device that describes the VPN connection to this local device. Activate "IP routing". If Windows networks are also to be coupled, then the NetBIOS entry should be activated here.

The tunnel endpoints, i.e. the local VPN gateway and each of the VPN remote stations, are entered into the VPN connection list.

Manually configuring the VPN connection involves the following steps:

① Create an entry for the remote VPN gateway in the connection list and enter its public IP address.

② The security parameters for the VPN connection are normally taken from the prepared list, and all that is required here is to define an IKE key.

③ For a Dynamic VPN connection, create a new entry in the PPP list with the name of the remote VPN gateway as the remote station, with the name of the local VPN gateway as the User Name, and set a suitable password. Be sure to activate the IP routing for this PPP connection and, if required, the routing of "NetBIOS over IP" as well. The remaining PPP parameters, such as the procedure for checking the remote station, can be defined in the same way as for other PPP connections.

④ The main task in setting up VPN connections is in defining the network relationships. Which IP address ranges at each end of the VPN tunnel should be included in the secured connection?

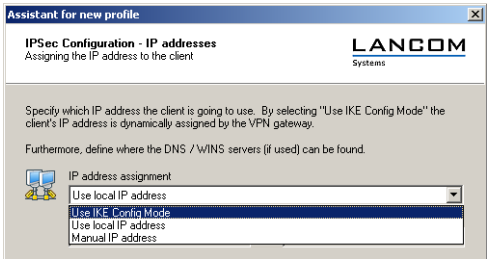
10.5.5 IKE config mode

When configuring VPN dial-in connections, there is as an alternative to fixed IP addresses for the remote stations that dial in, in that a pool of IP addresses can be made available to them. To this end, the "IKE-CFG" mode is additionally added to the entries in the connection list. This can assume the following values:

- **Server**: With this setting, the device functions as the server for this VPN connection. The assignment of an IP address to the client can take place in two ways:
  - If the remote site is entered in the routing table, the IP address defined here will be assigned to the client.

□ If the remote site is not entered in the routing table, an IP address which is available from the IP pool will be taken for the dial-in connections.

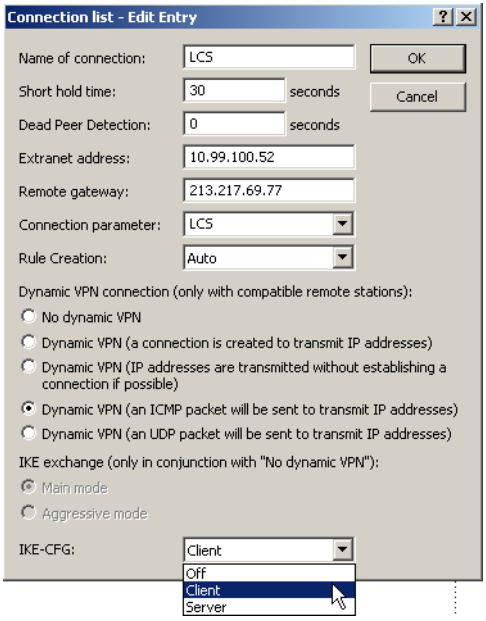
The remote site must be configured as IKE-CFG client in this case, and thus has to request an IP address from the server. To dial in with a LANCOM Advanced VPN Client, the option **Use IKE Config Mode** has to be activated in the connection profile.



- **Client**: With this setting, the device functions as the client for this VPN connection and requests an IP address from the remote site (server). The device acts in a similar manner to a VPN client.
- **Off**: If the IKE-CFG mode is switched off, no IP addresses will be assigned for the connection. Fixed IP addresses must be defined for both ends of the connection.

LANconfig

When using LANconfig for the configuration, you will find the VPN connection list in the configuration area 'VPN' on the 'General' tab under the button **Connection list**.



WEBconfig, Telnet or terminal program

Under WEBconfig, Telnet or a terminal program, you will find the settings for the IKE-CFG mode under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ VPN ▶ VPN-Peers
Terminal/Telnet	`Setup/VPN/VPN-Peers`

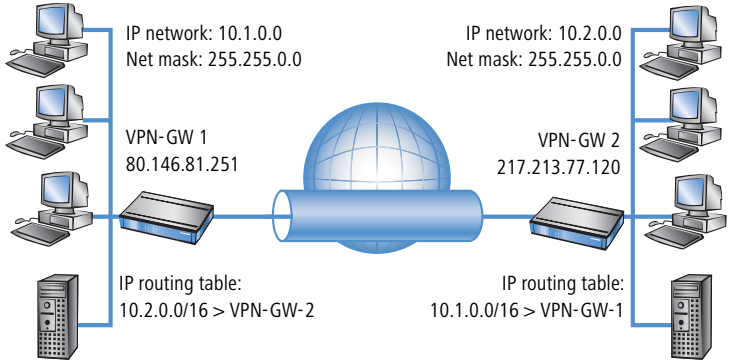
10.5.6 Prepare VPN network relationships

The firewall integrated into LANCOM routers is a powerful instrument for defining source and target address ranges between which data transfer (and limitations to it) can be enabled or prohibited. These functions are also used for setting up the network relationships for the VPN rules.

In the simplest case, the firewall can generate the VPN rules automatically.

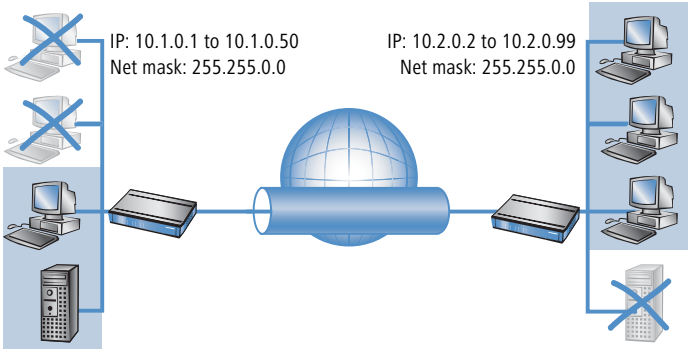
- The local intranet serves as the source network, i.e. the same private IP address range that the local VPN gateway itself belongs to.
- For automatically generated VPN rules, the target networks are those network ranges that have a remote VPN gateway set as their router.

To activate the automated rule generation, simply switch on the corresponding option in the firewall[1]. When coupling two simple local networks, the automatic VPN can interpret the necessary network relationships from the IP address range in its own LAN and from the entry for the remote LAN in the IP routing table.



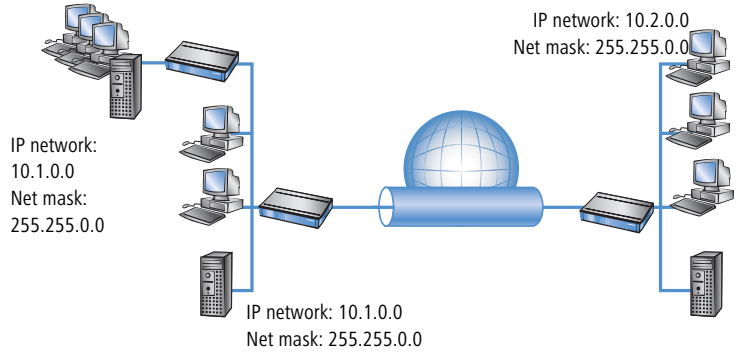
The description of the network relationships is more complicated if the source and target networks are not only represented by the intranet address ranges of the connected LANs:

- When only a portion of the local intranet is to be available to the remote network, then the automatic method is unsuited as the IP address range that is open to the VPN connection is too large.



- In many network structures, the local network is connected by further routers to sections of other networks with their own IP address ranges. Additional settings are required to include these address ranges in the network relationship.

1. automatic when using the VPN installation Wizard under LANconfig



In these cases, the network relationships that describe the source and target networks must be entered manually. Depending on the situation, the scope of the automatically generated VPN rules may be extended, although sometimes it is better to deactivate the automatic VPN system to prevent unwanted network relationships.

The necessary network relationships are defined by the appropriate firewall rules under the following circumstances:

- In the firewall rules, the option "Consider this rule when generating VPN rules" must be activated.

The firewall rules for generating VPN rules are active even when the actual firewall function in the LANCOM device is not required and is switched off!

- Make sure that the firewall action is set to "Transfer".
- Sources and targets for the connection can be entered as individual stations, certain IP address ranges, or whole IP networks.

It is vital that target networks are defined in the IP routing table so that the router in the LANCOM devices can forward the appropriate data packets to the other network. You can make use of the entries that already exist there and simply enter a higher-level network as the target. The intersecting portion of the target network defined by the firewall and the subordinate entries in the IP routing table is integrated into the network relationships for the VPN rules.

Example: The target networks 10.2.1.0/24, 10.2.2.0/24 and 10.2.3.0/24 are entered into the IP routing table and can be accessed via the router VPN-GW 2. An entry for the target network 10.2.0.0/16 is sufficient for these three subnets to be included in the VPN rules.

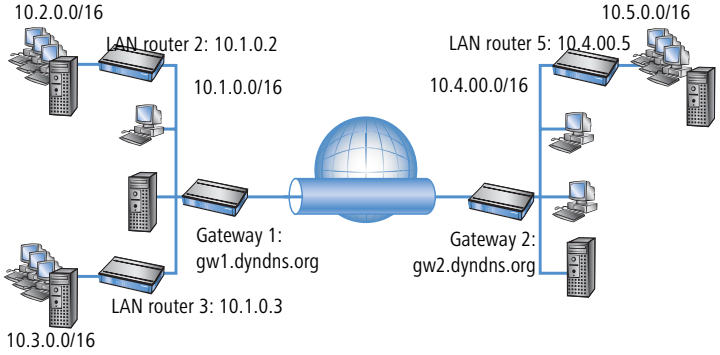
The definition of source and target networks must agree at both ends of the VPN connection. It is not possible, for example, to map a larger target address range to a smaller source address range at the opposite end. Decisive here are the IP address ranges allowed by the VPN rules and not the networks defined in the firewall rules. These can be very different from the network relationships in the VPN rules because of the intersecting ranges.

■ VPN connections can also be limited to certain services or protocols according to your requirements. This means that the VPN connection can be limited to use only with a Windows network, for example.

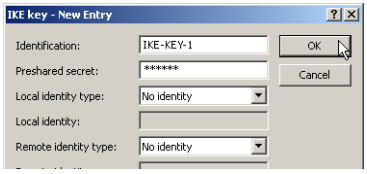
These limitation should be defined by a separate set of rules that applies only to the firewall and that will not be used in generating VPN rules. Combined firewall/VPN rules can very quickly become highly complex and difficult to comprehend.

10.5.7 Configuration with LANconfig

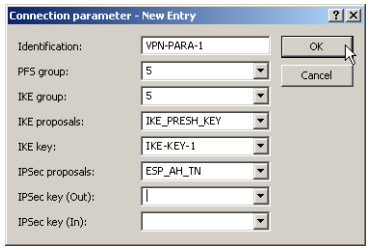
The section demonstrates how LANconfig can be used to configure a LAN-LAN coupling with additional subnets. In this section, VPN gateway 1 will be configured and then the configuration of gateway 2 with the help of WEBconfig will be demonstrated.



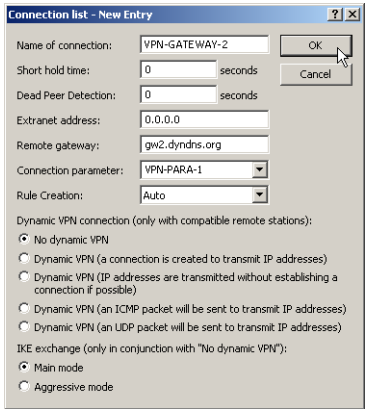
① When configuring VPN, access the "IKE param." tab and create a new IKE key for the connection:



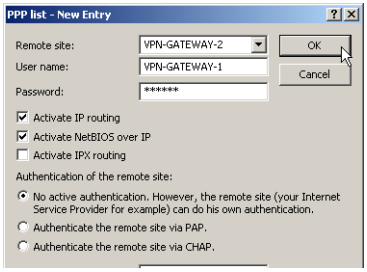
② Under the "General" tab, create a new entry in the list of Connection parameters. Select the IKE key created earlier for this. PFS and IKE groups can also be selected in the same way as IKE and IPSec proposals from the options prepared earlier.



③ You should then generate a new entry in the Connection list with the name of the remote gateway as "name for the connection". For LANCOM Dynamic VPN connections the entry "Remote gateway" must remain empty. Otherwise enter the public address of the remote station: either the fixed IP address or the name for translation by DNS.

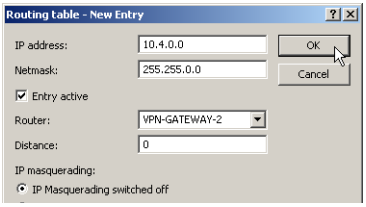


④ When using LANCOM Dynamic VPN: Change to the "Communication" configuration area. Using the "Protocols" tab, make a new entry in the PPP list. Select the remote VPN gateway as the remote site, enter the User Name as the name of the VPN connection that the remote VPN gateway uses to address the local device, and enter a suitable password that is identical at both locations, but for safety reasons should not be identical to the pre-shared key.



Be sure to activate "IP routing" and, if required, "NetBIOS over IP" (→ Seite 263).

⑤ Change to the "IP Router" configuration area. On the "Routing" tab, make a new entry in the routing table for those parts of networks that are to be accessible in the remote and in the local LAN. In each case, define the router as the remote VPN gateway and switch the IP masquerading off.



For the "VPN gateway 1", the following entries are necessary so that the remote network sections can be reached.

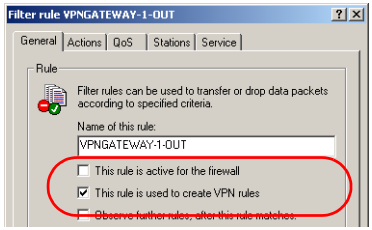
IP address	Net mask	Router	IP masquerading
10.4.00.0	255.255.0.0	VPN gateway 2	No
10.5.0.0	255.255.0.0	VPN gateway 2	No

For those subnetworks connected to your own LAN, define the router as the IP address for the appropriate LAN router.

IP address	Net mask	Router	IP masquerading
10.2.0.0	255.255.0.0	10.1.0.2	No
10.3.0.0	255.255.0.0	10.1.0.3	No

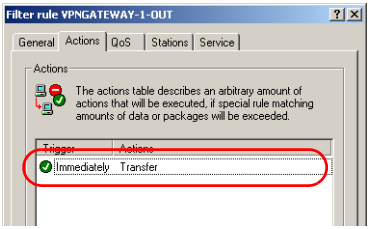
These entries enable VPN gateway 1 to forward packets arriving from the remote network to the correct sections of the local network.

⑥ Change to the "Firewall/QoS" configuration area. On the "Rules" tab, add a new firewall rule with the name "VPN GATEWAY 1 OUT" and activate the option "This rule is used to create VPN rules". This ensures that IP networks described in this rule will be used in establishing VPN network relationships.

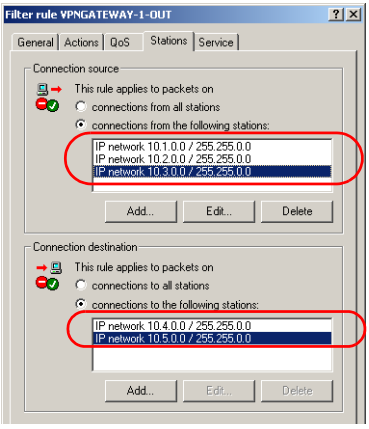


It is recommended to keep the rules used for making network relationships (source and target IP) separate from those firewall rules that for instance affect the services used in communications. Combining both aspects can leed to a higher number of internal managed VPN relationships and therefore to a loss of performance in the VPN tunnels.

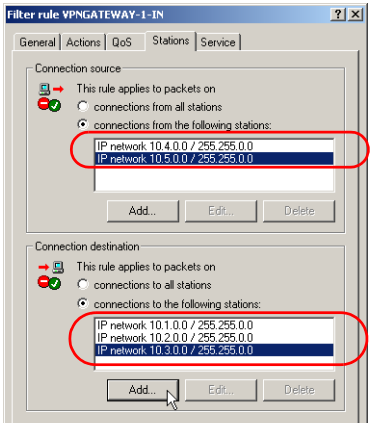
⑦ On the “Actions” tab for these firewall rules, set the “Packet Action” to “Transmit”.



⑧ On the “Stations” tab for these firewall rules, define the source of the data transfers as the subnets at the local site, and set the destination as all of the subnets at the remote site.



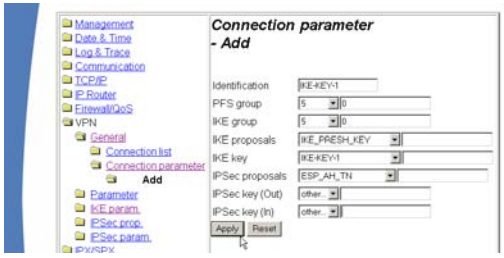
⑨ Now for the incoming data transmissions, generate a firewall rule named “VPN GATEWAY 1 IN” with the same parameters as the rule just described. The only difference is that the source and the destination networks are swapped.



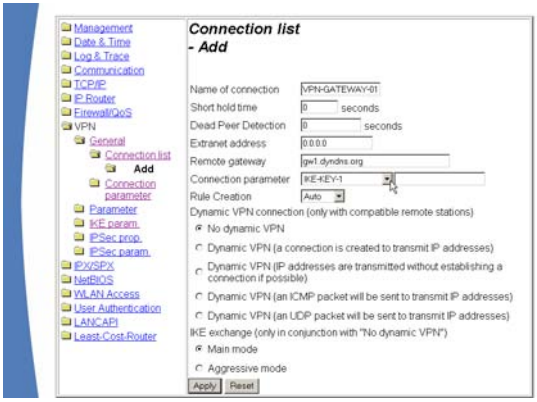
10.5.8 Configuration with WEBconfig

① Under **Configuration ▶ VPN ▶ IKE-Param. ▶ IKE key** set a new IKE key for the connection:

② Under **Configuration ▶ VPN ▶ General ▶ Connection parameters** define a new "VPN layer" for the connection parameters. Select the IKE key created earlier for this.



③ Under **Configuration ▶ VPN ▶ Connection list** generate a new entry with the name of the remote gateway set to "Name". For the "Remote gateway", enter the public address of the remote station: either the fixed IP address or the name for translation by DNS.



④ When using LANCOM Dynamic VPN: Under **Configuration** ▶ **Setup** ▶ **WAN module** ▶ **PPP list** make a new entry.
Select the remote VPN gateway as the remote site, enter the User Name as the name of the VPN connection that the remote VPN gateway uses to address the local device, and enter a suitable password that is identical at both locations.

Be sure to activate "IP routing" and, if required, "NetBIOS over IP" (→ Seite 263).

⑤ Under **Configuration** ▶ **Setup** ▶ **IP router module** ▶ **IP routing table** generate a new entry for each network portion that should be accessible in the remote and in the local LAN. In each case, define the router as the remote VPN gateway and switch the IP masquerading off.

For the "VPN gateway 2", the following entries are necessary so that the remote network sections can be reached.

IP address	Net mask	Router	IP masquerading
10.1.0.0	255.255.0.0	VPN gateway 1	No
10.2.0.0	255.255.0.0	VPN gateway 1	No
10.3.0.0	255.255.0.0	VPN gateway 1	No

For those subnetworks connected to your own LAN, define the router as the IP address for the appropriate LAN router.

IP address	Net mask	Router	IP masquerading
10.5.0.0	255.255.0.0	10.4.00.5	No

These entries enable VPN gateway 2 to forward packets arriving from the remote network to the correct sections of the local network.

⑥ Under **Configuration ▶ Firewall/QoS ▶ Object table** make an entry for each part of the network that should be used as a source or destination for the VPN connection via "VPN GATEWAY 1" ("VPN-GW1-LOCAL" and "VPN-GW1-REMOTE"). Enter each subnet in the form "%A10.1.0.0 %M255.255.0.0".

⑦ Under **Configuration ▶ Firewall/QoS ▶ Rules table** define a new firewall rule named "VPN-GW1-OUT". Set the objects to "CPN-GW1-LOCAL" and "VPN-GW1-REMOTE", the protocol to "ANY" and the action to "ACCEPT". Activate the option "VPN rule" so that the IP networks described in this rule will be used in establishing VPN network relationships.

As a rule, it is recommended that you keep the rules used for making network relationships separate from those firewall rules that affect the services used in communications, for example.

⑧ Now for the incoming data transmissions, generate a firewall rule named "VPN-GWY1-IN" with the same parameters as the rule just described. The only difference is that the source and the destination networks are swapped.

10.5.9 Diagnosis of VPN connections

If the VPN connections fail to work after the configuration of the parameters, the following diagnostic methods can be applied:

- The command **show vpn spd** on the Telnet console calls the "Security Policy Definitions".
- Use the command **show vpn sadb** to access information about the negotiated "Security Associations" (SAs).
- The command **trace + vpn** [status, packet] calls up the status and error messages for the current VPN negotiations.
  - The error message "No proposal chosen" indicates a fault in the configuration at the remote site.
  - The error message "No rule matched", on the other hand, indicates a fault in the configuration of the local gateway.

10.6 Working with digital certificates

The security of communications via VPN fulfils three core requirements:

- **Confidentiality**: The transmitted data cannot be read by unauthorized persons (via encryption).
- **Integrity**: The data cannot be changed during transmission (via authentication).
- **Authenticity**: The receiver can be certain that received data has genuinely been sent by the supposed sender (via authentication).

A number of encryption and authentication methods exist which provide satisfactory solutions for the first two aspects, confidentiality and integrity. The use of digital certificates aims to provide assurance about the authenticity of the communications partner.

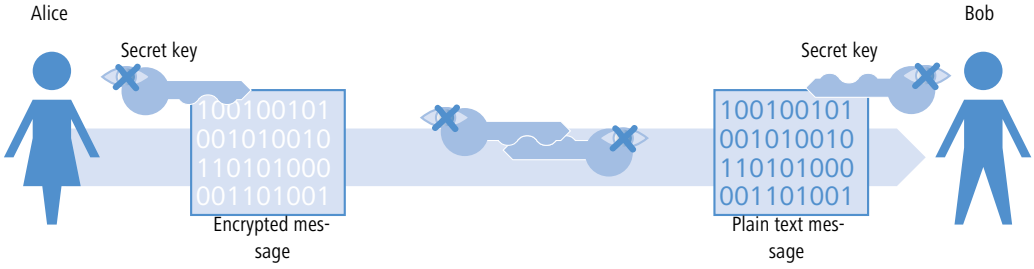
10.6.1 Basics

Encryption methods can be divided into two categories: Symmetrical and the asymmetrical encryption.

Symmetrical encryption

This is a method known for thousands of years and is based on the fact that the sender and the recipient both have access to a message by knowing a secret shared key. This key can take on a wide variety of forms: The Romans used a stick of a certain diameter for encryption and decryption.

Today's digital communications rely in the main upon a password as the key. Using this password and an encryption algorithm, the data from the sender are changed. The recipient uses the same key and the fitting encryption algorithm so that the data become legible again. Other persons who do not know the key cannot read the data. A common symmetrical method of encryption is 3DES, for example.



Example:

- Alice wants to send a confidential message to Bob. To do this, she encrypts the message with a secret key and a suitable method, e.g. 3DES. She sends the encrypted message to Bob informing him of the encryption method she used.
- Bob has the same key as Alice. Since he knows which encryption method was used, he can decrypt the message and transform it back into plain text.

Symmetrical encryption is simple and efficient but has two serious disadvantages:

- A different key is required for every secret communications relationship. If Alice and Bob are joined by Carol, three keys are necessary for secure data communications between all parties; with four participants, the number of keys required is six; with 12 participants, 66 keys are required and with 1000 participants, almost 500,000

keys are necessary! In a worldwide network with ever increasing demands for secure communications and higher numbers of participants, the serious nature of this problem is obvious.

- While this first disadvantage could be solved with technology, the second problem that is the core problem for symmetrical encryption: The secret key must be known at both ends of the communication and must not fall into the hands of unauthorized persons. Thus it is not possible for Alice simply to send the key to Bob per e-mail before the data connection has been secured sufficiently—which is the whole point of the encryption. She has to give the key to Bob in person, or at least make use of a communications method which is safe from eavesdroppers. This is a task which is almost impossible to handle in these times of worldwide dynamic communications.

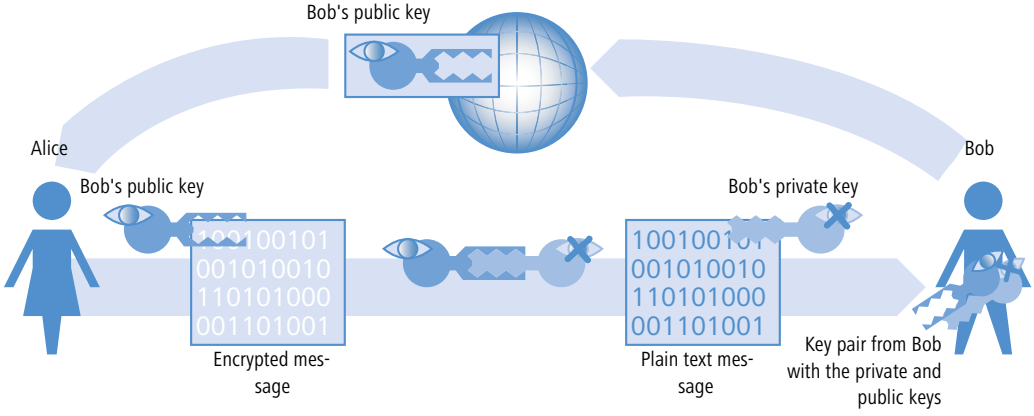
Asymmetric encryption

A totally new approach was developed in the 1970s; that of asymmetric encryption. This method no longer relies on a secret key that is known at both ends, but on a pair of keys instead:

- The first part of the key pair is used to **en**crypt the data that are to be sent to the key owner. This key, subsequently called the public key, can be made publicly available to anybody interested in communication.
- The second part of the key pair is the private key that is only used to **de**crypt the received message. This key is secret and may not fall into the hands of unauthorized persons.

The main difference to symmetrical methods: A publicly available key is used in this so-called "public key method". An example of an asymmetrical encryption method is RSA.

Let's take another look at the example with Alice and Bob:



- For secure communications, Bob first of all generates a key pair with a private key and a public key that belong together. The method used for generating this key ensures that the private key cannot be backwardly computed with knowledge of the public key. Bob can now publicize the public key without worry. He can send it to Alice per e-mail or simply publish it on a web server.

- Alice now encrypts the message for Bob with his public key. This now illegible message can only be decrypted by using Bob's private key. Even if the data are intercepted on the way from Alice to Bob, no-one but Bob can regenerate the plain text message.

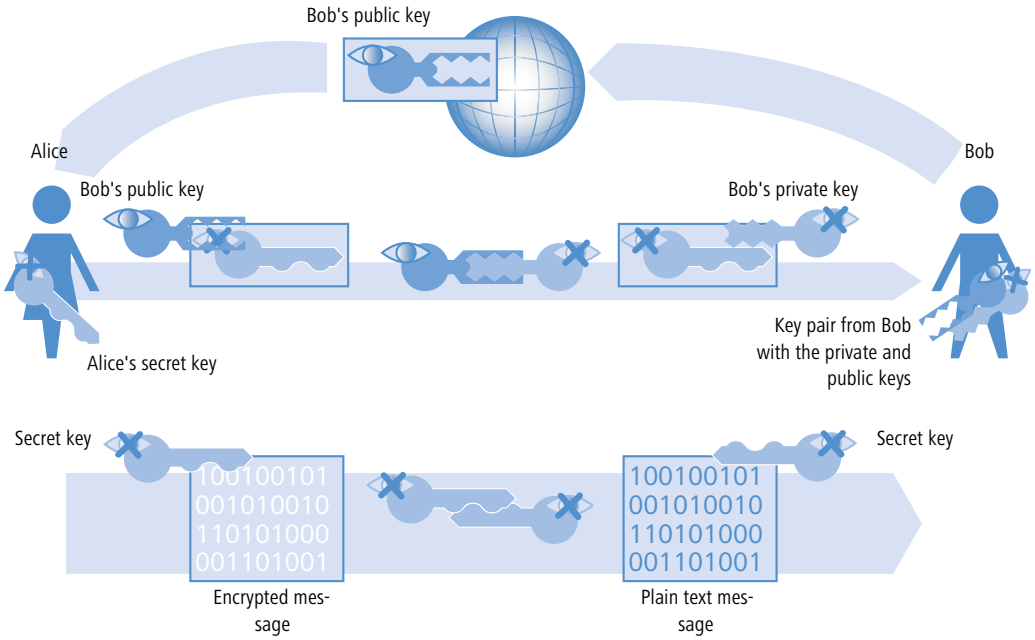
The asymmetrical encryption offers the following advantages over symmetrical variants:

- A key pair is not required for every communications relationship, but for each participant only. Even with 1000 participants, each user needs only his/her personal key pair, of which only the public key is publicly available. Instead of 500,000 secret keys, the public key method requires just 1000 key pairs.
- The risky transmission of a secret key to the communications partner is simply not necessary as knowledge is only required of the public key on the other side of the communications relationship. This is the solution to a significant problem in the dynamic encryption of data between multiple participants.

Combination of symmetrical and asymmetrical encryption

Asymmetrical encryption methods have quickly become established due to the security they offer. However, security has its price: Asymmetrical encryption methods are slow. The mathematics involved in the encryption and decryption of messages is far more complex that with symmetrical encryption methods and thus require more computing time—a critical factor when transmitting larger quantities of data.

The advantages of symmetrical and asymmetrical encryption can be used in suitable combinations of these methods. In this way, the higher security of the asymmetrical encryption is used to protect the transmission of the secret key. The actual data for transmission are then encrypted with the faster symmetrical method.



- First of all, Bob generates a key pair and publicizes the public key.
- Alice uses the public key to **en**crypt a secret symmetrical key and sends this to Bob. For each transmission, this secret key is newly defined according to a random procedure.
- Bob is the only one who can **de**crypt this secret key by using his private key.
- Alice and Bob then use this secret key to **en**crypt and **de**crypt the clearly much larger volume of the payload data.

Public key infrastructure

The combination of symmetrical and asymmetrical encryption methods enable initially unsecured connections to be used to establish secure data communications. Until now, the aspect of authenticity has been ignored. How should Alice know that the public key really does come from Bob? The use of public keys thus depends directly on the trust in the authenticity of the communications partner.

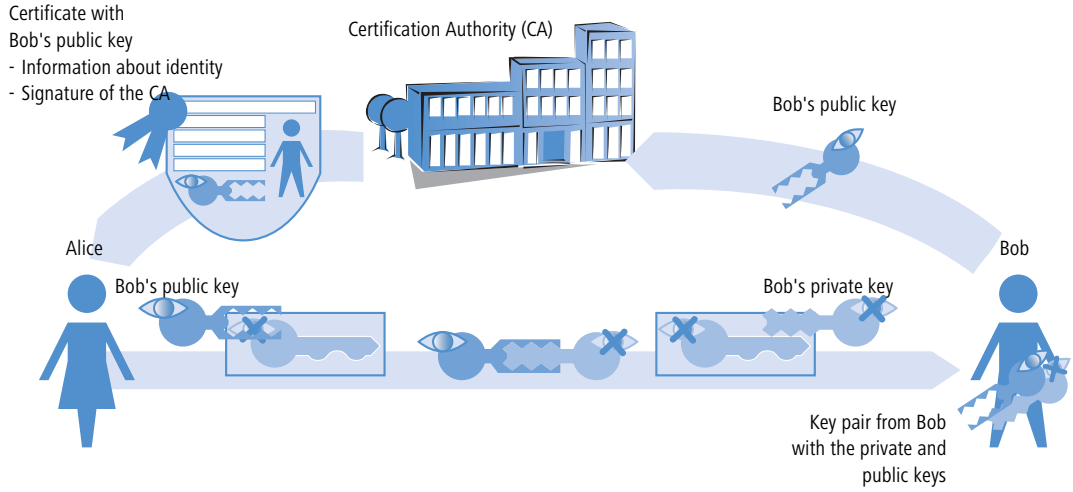
To secure this trust, a confirmation of the key pairs for use with asymmetrical encryption can be issued by publicly recognized and trustworthy authorities. In Germany, for example, the highest authority for the confirmation of digital keys is the Regulatory Authority for Telecommunications and Post (RegTP). The RegTP in turn issues accreditations to suitable service providers who are viewed as equally trustworthy.

The RegTP web site (www.regtp.de) features up-to-date lists of accredited certification service providers and notification of revoked accreditations. Accredited service providers include numerous tax advisers and legal associations.

The task of this organization is to attribute a public key to just one person or organization. This attribution is recorded and officially publicized in a certificate. Consequently these providers are known as Certification Authorities, or CAs for short. The uppermost certification authority is known as the Root CA.

Bob can now approach a CA to have his public key certified as belonging to him. He submits his public key to the CA who then confirm that the key belongs to Bob.

The CA issues a certificate which lists the public key and further information about Bob, such as his identity, among other things.



The certificate carries the signature of the CA to show that the confirmation itself is genuine. The certificate takes up just a small amount of data and is suitable for exchange with an asymmetric method. With a signature, however, the asymmetric method is used in the opposite direction:

- The CA, too, has a key pair consisting of private and public keys. Since this is a trustworthy authority, their key pair can be considered as reliable.
- The CA calculates a hash value for the certificate, encrypts this and uses it in the signature in Bob's certificate. This acts to confirm the attribution of Bob's public key to his identity.

  This procedure behaves in the opposite manner to the normal asymmetrical encryption. In this case, the encryption does not fulfil the task of protecting the data from unauthorized persons, but confirms the signature of the CA instead.
- Any data communications participant anywhere in the world with the public key from the CA is now in a position to check the signed certificate.

  Only the CA is in a position to use their private key to generate signatures that can be decrypted again by using the CA's public key. This signature guarantees that the certificate is genuinely sourced from the issuing CA.

10.6.2 Advantages of certificates

In some cases the use of certificates for securing VPN connections can be an alternative to the otherwise widespread preshared key (PSK) method:

- Increase security of VPN client connections (with IKE Main Mode)

  Main Mode cannot be used when using PSK connections between peers that use dynamic IP addresses. In these cases, the aggressive mode must be used with its lower degree of security. Using certificates allows peers with

dynamic IP addresses, such as dial-in computers with LANCOM Advanced VPN Client, to use the Main Mode and thus to increase the level of security.

- Higher security of the used keys and passwords

  Preshared keys are just as susceptible as other passwords, too. The way that users treat these passwords is a major factor in the securing of connections. With a certificate-based VPN establishment, the keys in the certificates are automatically generated with the desired key length. What's more, the random keys generated by computers offer more security from attack than the preshared keys of the same key length thought up by people.

- Possibility of authenicating remote sites

  When connecting with certificates oth remote stations must authenticate themselves. Further information can be contained in the certificates, which can be used for testing remote sites. The time limit of the certificates provide an additional protection, e.g. for users, who are only supposed to have access for a limited period of time.

- Providing tokens and smartcards

  When saving certificates on external data media the integration of "Strong Security" environments, the readout of passwords from computers of networks is inhibited.

The advantages of certificates have to be considered in relation to the considerable increase in effort of introducing and maintaining a public key infrastructure (PKI).

10.6.3 Structure of certificates

Contents

A certificate contains a variety of information which is important for it to fulfil its purpose. Some information is obligatory, some is optional. A certificate can also be stored in a variety of different formats. An X.509-standard certificate contains the following information, for example:

- Version: This is the relevant version of the X.509 standard. The current (06.2005) version is 'v3'.
- Serial number: This is a unique number that identifies the certificate.
- Signature algorithm: This identifies the algorithm that the issuer used to sign the certificate. The digital signature of the issuer is also to be found here.
- Validity: Certificates are valid for a limited period of time. This entry indicates the duration of the certificate's validity.
- Issuer: This identifies the issuer, for example by name, e-mail address, nationality, etc.
- Subject: This identifies the certificate's owner, for example by name, institution, e-mail address, nationality, city, etc.
- Subject public key: Information indicating the method used to generate the public key used by the certificate's owner. The owner's public key is also to be found under this item.

Target application

When the certificates are generated, the possible uses of the certificate usually have to be selected. Some certificates are intentionally designed for transfer with web browsers or e-mails only, and others are more generally applicable to any use.

When you generate certificates, make sure that you enter its intended purpose.

Formats

The ITU standard X.509 is a wide spread format for certificates. When displayed as text, this type of certificate looks like the following:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature algorithm: md5WithRSAEncryption
      Issuer: C=XY, ST=Austria, L=Graz, O=TrustMe Ltd, OU=Certificate Authority, CN=CA/
Email=ca@trustme.dom
        Validity
            Not Before: Oct 29 17:39:10 2000 GMT
            Not After : Oct 29 17:39:10 2001 GMT
          Subject: C=DE, ST=Austria, L=Vienna, O=Home, OU=Web Lab, CN=anywhere.com/
Email=xyz@anywhere.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
                    d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
                    9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
                    90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
                    1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
                    7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
                    50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
```

```
                8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
                f0:b4:95:f5:f9:34:9f:f8:43
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Alternative Name:
            email:xyz@anywhere.com
        Netscape Comment:
            mod_ssl generated test server certificate
        Netscape Cert Type:
            SSL Server
Signature Algorithm: md5WithRSAEncryption
    12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
    3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
    82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
    cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
    4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
    d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
    44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
    ff:8e
```

File types

There are various file types for digital certificates and private keys depending on the issuer. The following types are common:

- *.pfx and *.p12: PKCS#12 files
- *.pem, *.cer and *.crt: BASE-64-coded certificates
- *.cer, *.crt and *.der: DER coded certificates
- *.key: BASE64 or DER coded keys
- *.pvk: Microsoft-specific key format

Apart from the straightforward certificates, there is another file type that is of significance in the world of certificate-secured VPN connections: The PCK#12 files which can contain multiple components such as a certificate and a private key. To process the PKCS#12 file, a password has to be entered which was set when the certificate was exported.

BASE64-coded certificates have a header that typically features the following lines:
`----- BEGIN CERTIFICATE -----`

Validity

A further option is to refer to a certificate revocation list (CRL). CRLs list certificates that have lost their validity, for example if an employee has left the company and his certificate has been withdrawn. This information allows those who are checking certificates to refer to the appropriate CRL.

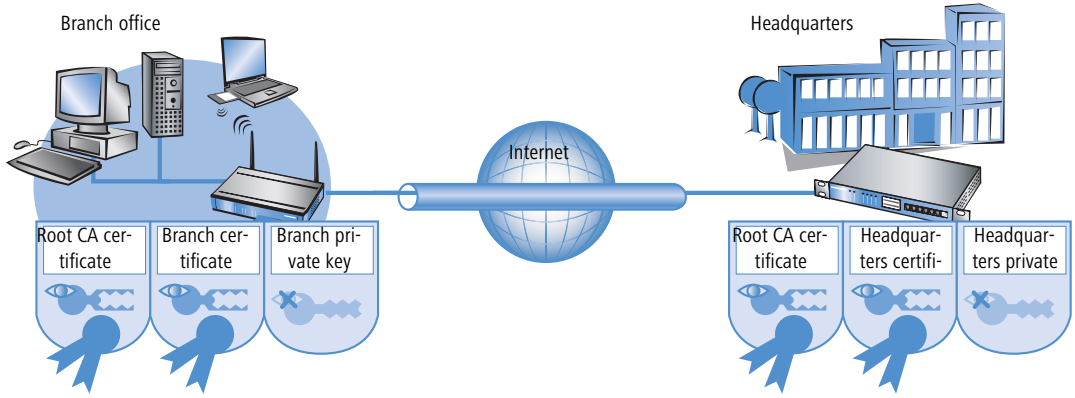
10.6.4 Security

Certain security aspects have to be observed even when dealing with certificates:

- Only ever transfer private keys via secure connections, e.g. with HTTPS.
- Passwords for keys or PKCS#12 files should be passphrases that are long enough and secure.

10.6.5 Certificates for establishing VPN connections

Along with basic information about certificates, this section now considers their concrete application in establishing VPN connections. For connection establishment with the support of certificates, certain information must be available at both ends of the connection (e.g. when connecting a branch office to the network at headquarters via LANCOM routers):



- The branch office has the following components:
  - The Root CA's certificate with the CA's public key
  - A certificate for its own device with its own public key and the confirmation of identity. The hash value of this certificate is signed with the CA's private key.
  - Its own private key
- The headquarters has the following components:
  - The Root CA's certificate with the CA's public key
  - A certificate for its own device with its own public key and the confirmation of identity. The hash value for this certificate is signed with the CA's private key.
  - Its own private key

Put simply, the following procedures are carried out during the VPN connection exchange in Main Mode (symmetrical in both directions):

① In an initial exchange of packets the peers negotiate, for example, the methods of encryption and authentication that are to be used. At this phase, both ends are not fully certain about who they are negotiating with, although this is not yet critical.

② At the next stage, common key material is negotiated for the continued communications, including among other things symmetrical keys and asymmetrical key pairs. At this phase, too, the two ends are not yet fully certain about who the keys are being negotiated with.

③ In the next stage, the certificate is used in a check to ensure that the peer involved in negotiating the key material really is the intended communication partner:

- The branch office uses the current negotiation's key material to calculate a checksum (hash value) that can only be calculated by the two peers involved (branch office and headquarters) and only so long as the connection exists.
- The branch office encrypts the hash with its own private key, generating a signature with it.
- The branch office then transmits this signature together with its own certificate to the peer at headquarters.
- The headquarters then checks the signature of the certificate received from the branch office. This can be done with the help of the public key at the Root CA, which is identical for both peers. If the signature in the branch office's certificate (generated with the CA's private key) can be decrypted with the CA's public key, then the signature is valid and the certificate is trustworthy.
- In the next stage, the headquarters checks the signature of the encrypted hash. The branch office's public key in the corresponding certificate was found to be valid at the previous stage. The headquarters can thus check if the signed hash can be decrypted with the branch office's public key. The headquarters can calculate the same hash as the branch office using the key material for the current connection. If this check is successful then the peer "branch office" can be considered as authentic.

10.6.6 Certificates from certificate service providers

Certificates on offer from public certifiers are available in various security classes. The higher security classes require more effort on behalf of the applicants to demonstrate the authenticity of their identity to the CA. The Trustcenter AG in Hamburg, for example, uses the following classes:

- Class 0: These certificates are issued without an identity check and serve only for customer tests.
- Class 1: For this class, the existence of an e-mail address is the only check. These certificates are useful for private users wishing to sign their e-mails, for example.
- Class 2: This level, too, does not involve any personal proof of identity. The submission of an application along with, for example, a certificate of company registration is sufficient. This level is suitable for communications between companies that already know each other.

- Class 3: This level involves a personal check of the person or company. The information in the issued certificates is compared with a passport or a notarized copy of the certificate of company registration. This level is suitable for advanced applications such as e-business or online banking.

In your dealings with public certificate service providers, be sure to check in detail the security class or the proof of identity. This is the only way to be sure that the certificates really do meet with your security requirements.

10.6.7 Establishing a proprietary CA

Referring to public CAs for secure enterprise communications can only be recommended under certain conditions.

- There is considerable effort involved in the issue of new certificates and this can be slow.
- The keys in use are transferred via connections which are inadequately secured.
- Communication is based upon the trust in the CA.

An alternative for company communications is to establish a proprietary CA. Suitable packages are the Microsoft CA on a Microsoft Windows 2003 server or, as an open source version, OpenSSL. A proprietary CA empowers you to issue and manage all of the necessary certificates for secure data exchange with complete independence from any external parties.

Companies are recommended to use a proprietary CA rather than public certifiers. There are, however, several important issues to be considered when planning a CA. For example, even as early as during the installation of a Windows CA, the validity period for the Root CAs has to be defined and cannot be altered subsequently. Other aspects of planning include:

- The certificate policy or the level of security that is to be achieved with certificates
- The available name space
- Key lengths
- The duration of certificate validity
- Managing blocking lists

Precise planning is strongly recommended since corrections at a later date often imply considerable amounts of effort.

10.6.8 Requesting a certificate with Stand-alone Windows CA

For operations with a LANCOM, a combination of PKCS#12 file with root certificate, a proprietary device certificate and the device's public key offer the best services.

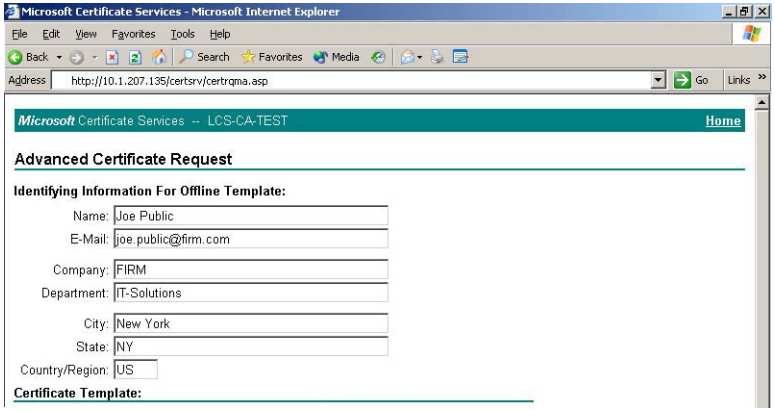
① Using your browser, access the start page of the Microsoft Certificate Services.

② For the certificate type, select 'Advance Certificate Request'.

③ The next step is to selection the option 'Generate and submit a certificate request '.

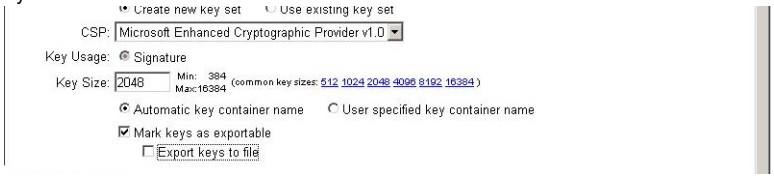
If, and only if, the root certificate is already available as a file, select the option 'BASE64'.

④ In the following step the information for identification is entered.



⑤ In the same dialog, select the certificate template as 'Other...' and then delete the value in 'Object ID'.

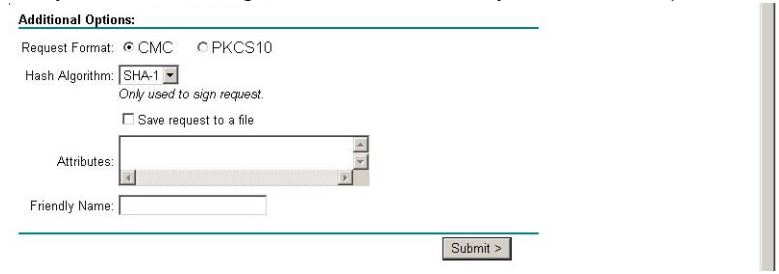
⑥ Mark 'Create new key set'. The public and private keys for the current user will now automatically be generated by the CA.



⑦ Select the key size according to certificate policy and activate the option to mark keys as exportable.

The key is not exported at this point and so a file name does not have to be specified. An export would create a Microsoft-specific *.pvk file, a format which is unsuitable for use with a LANCOM.

⑧ Finally, select the hash algorithm 'SHA-1' and send your certificate request with a click on **Submit**.



You can check on the status of your certificate request at any time via the Windows CA start page. Certificate requests can only be viewed from the same computer used to submit the request.

⑨ The certificate can be installed on your computer once the CA administrator has checked the request and created the certificate.

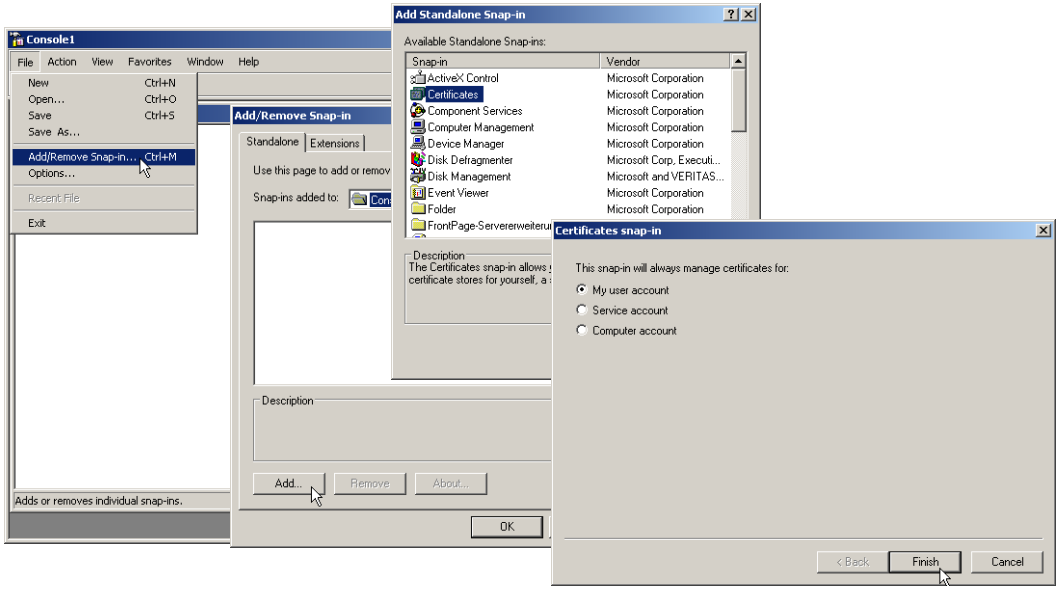
Certificates can only be installed on the same computer that was used for the request.

10.6.9 Export the certificate to a PKCS#12 file

The installation stores the certificate in your operating system but it is not yet available as a separate file. You will need this for installation to the LANCOM, though. For access to a certificate in file form, it has to be exported first.

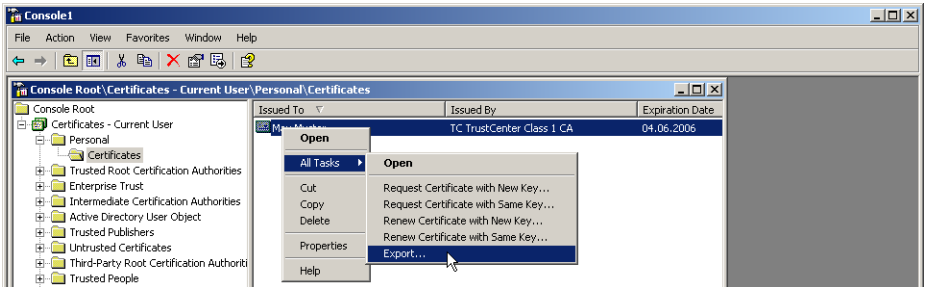
Export via the Windows console root

① Open the Management console with the command `mmc` at the command line and select the menu item **File** ▶ **Add/Remove Snap-In**.

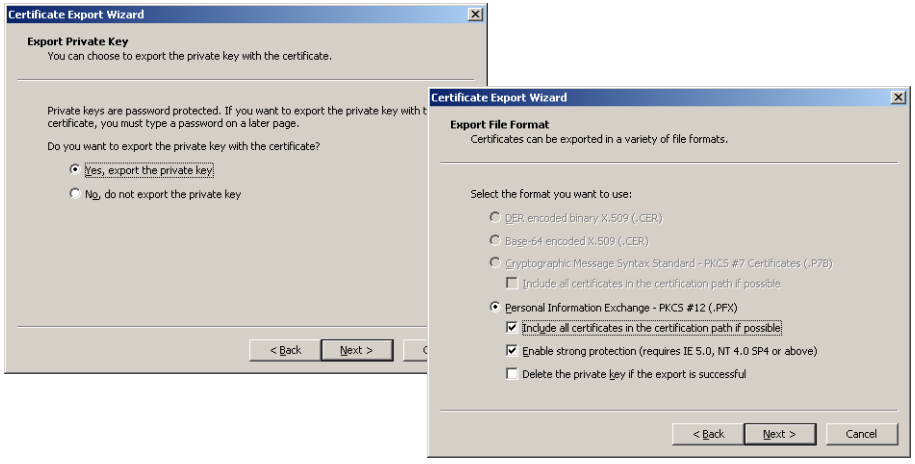


② Click on **Add...** and select 'Certificates'. Confirm with **Add**, then mark 'My user account' and click on **Finish**.

③ To export the desired certificate to a file, go to the Management console and click in the group **Certificates - current user** ▶ **My certificates**▶ **Certificates** with the right mouse key and, from the context menu, select **All tasks** ▶**Export**.



④ In the Certificate Export Wizard, activate the option to export the private key. You can optionally delete the private key from the system after exporting.



The option 'Include all certificates in the certification path' must be activated so that the root certificate is also exported to the PKCS#12 file.

⑤ You will be requested to enter a password to protect the private key. Ensure that you choose a secure password of sufficient length (passphrase). You will need this password later to install the certificated in the LANCOM.

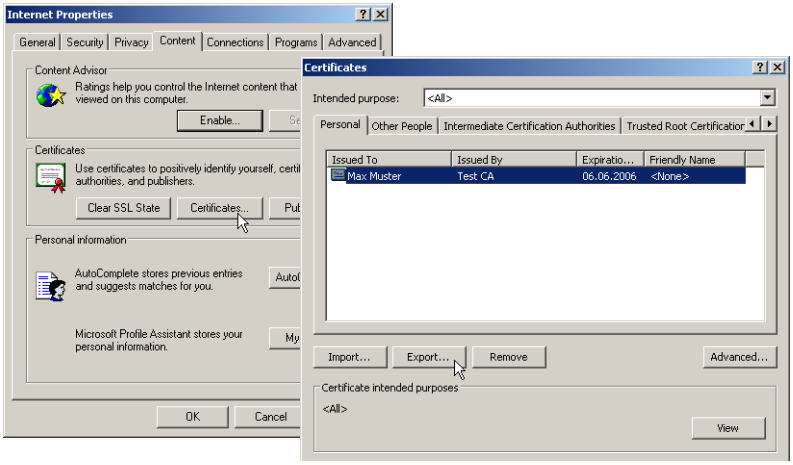
The term password is synonymous with other terms used in the different environments, e.g. "PIN".

Export via the Control Panel

As an alternative, you can open certificates on your system via the Control Panel.

① To do this, click on **Start** ▶ **Control Panel** ▶ **Internet Options**, the 'Contents' tab and the button **Certificates**.

② Choose the required certificate and click on **Export**.



The actions required in the Certificate Export Wizard that follows are identical to those described under 'Export via the Windows console root' → page 288.

10.6.10 Create certificates with OpenSSL

OpenSSL is a further possibility for creating proprietary certificates and to test certified connections. OpenSSL is an OpenSource project available for Linux and Windows at no cost; as a command-line tool, however, it does not offer the user-friendliness of other CA variants.

The configuration file openssl.cnf must be adapted to your specific needs. Further information is available in the OpenSSL documentation.

Installing OpenSSL

① Download the current version of OpenSSL from http://www.slproweb.com/products/Win32OpenSSL.html.

② Install the package and, in the directory `./bin/PEM/demoCA` create the following subdirectories:

- `/certs`
- `/newcerts`
- `/crl.`

③ In the file openssl.cnf, change the path in the `[CA_default]` group to: `dir= ./PEM/demoCA`

④ OpenSSL is started with a double-click on `openssl.exe` in the `./bin` directory.

Issue a certificate for Root CA

① Create a key for the CA with the command:

□ `genrsa -des3 -out ca.key 2048`

Remember the password that you enter after the request for the CA key as you will need it again later!

This command creates the file 'ca.key' in the current directory.

② Create a certificate request for the CA with the command:

□ `req -key ca.key -new -subj /CN="Test_CA" -out ca.req`

You will be requested to enter the password for the CA key here.

This command creates the file 'ca.req' in the current directory.

③ Create a certificate from the certificate request with the command:

□ `x509 -req -in ca.req -signkey ca.key -days 365 -out ca.crt`

Here, too, you will be requested to enter the password for the CA key.

This command signs the certificate request 'ca.req' with the key 'ca.key' and then issues the certificate 'ca.crt'.

Issue certificates for users or devices

① Create a key for the device or user with the command:

□ `genrsa -out device.key 2048`

This command creates the file 'device.key' in the current directory.

② Create a certificate request for the device or user with the command:

□ req -key device.key -new -subj /CN=DEVICE -out device.req

This command creates the file 'device.req' in the current directory.

③ Create a certificate from the certificate request with the command:

□ x509 -extfile openssl.cnf -req -in device.req -CAkey ca.key -CA ca.crt -CAcreateserial -days 90 -out device.crt

This command signs the certificate request 'device.req' with the key 'ca.key' and then issues the certificate 'device.cert'. The configuration file openssl.cnf is also involved in the procedure.

④ Export the certificate for the device or user with the command:

□ `pkcs12 -export -inkey device.key -in device.crt -certfile ca.crt -out device.p12`

This command combines and saves the key 'device.key', the certificate 'device.crt' and the root certificate 'ca.crt' in the file 'device.p12'. This PKCS#12 file can be uploaded directly to the required device ('Upload certificates to the LANCOM' → page 292).

10.6.11Upload certificates to the LANCOM

The following components must be available in a LANCOM for the establishment of VPN connections that are secured by certificate.

- The Root CA's certificate with the CA's public key
- A certificate for its own device with its own public key and the confirmation of identity. The hash value for this certificate is signed with the CA's private key.
- Its own private key

If you have followed the instructions for issuing certificates with a Windows CA and their export, then this information will now be available in the form of a combined PKCS#12 file. Alternatively you have used a different method and the individual components are available as separate files.

The certificate file can at this time only be uploaded to the devices with WEBconfig. Make sure that you use an HTTPS connection as the passphrase for the PKCS#12 file is transmitted unencrypted

① Use WEBconfig to log on to the required device; you will need administrator rights.

② Select the entry for **Upload file**.

③ Select the components that you wish to upload to the device:

□ Root certificate

□ Device certificate

□ Private key for the device

□ PKC#12 file with a combination of root certificate, device certificate and private key

The relevant password must be entered depending on the type of file to be uploaded.

The uploaded files can then be viewed in a list under **Expert configuration** ▶ **Status** ▶ **File system** ▶ **Content** .

A combined PKCS#12 file is divided up into the necessary components upon upload.

10.6.12Set up VPN connections to support certificates

Several areas of the configuration have to be changed to set up VPN connections to support certificates.

- IKE proposals
- IKE proposal lists
- IKE key
- VPN parameters
- Connection parameters

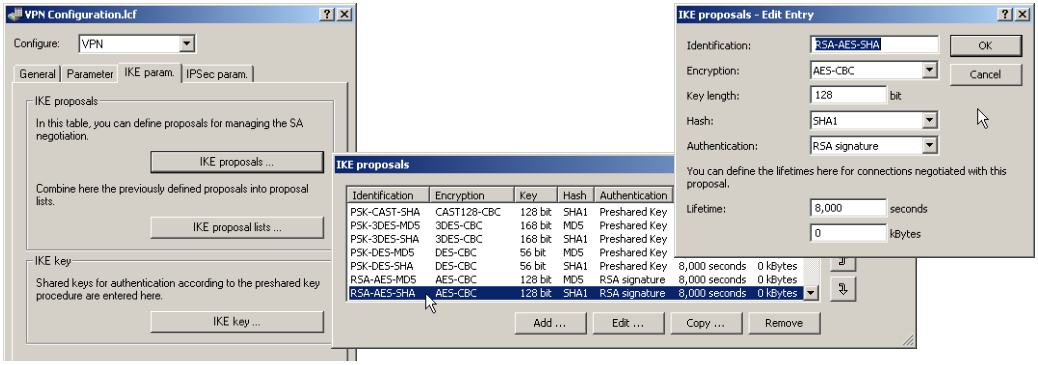
Some of the values may already be available in your device depending on its firmware version. In this case you just have to check that the values are set correctly.

If you are reconfiguring a remote device for certificate support with the method described below, and that device can only be reached via a VPN tunnel, then it is imperative that you reconfigure the remote device first before adjusting the connection in the local device. Changing the local configuration first would make the remote device unattainable!

① The proposals lists are to be supplemented with two new proposals with the exact description of 'RSA-AES-MD5' and 'RSA-AES-SHA', both of which use 'AES-CBC' for encryption and 'RSA signature' as the authentication mode, and which differ only in their hash method (MD5 and SHA1).

Configuration with LANconfig

IKE proposals are to be found in LANconfig under the configuration area 'VPN' on the 'IKE param.' tab by clicking on the **IKE proposals** button:



Configuration with WEBconfig or Telnet

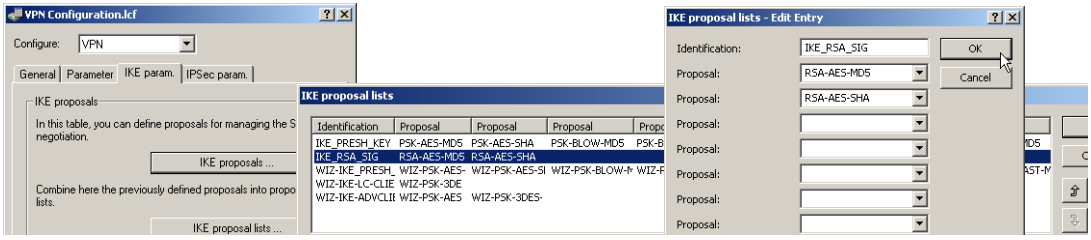
Under WEBconfig or Telnet you will find the IKE proposals at the following locations:

Configuration tool	Call
WEBconfig	Expert configuration ▶ Setup ▶ VPN ▶ Proposals ▶ IKE
Terminal/Telnet	`/Setup/VPN/Proposals/IKE`

② A new list will be required in the proposals lists with the exact name 'IKE_RSA_SIG' which contains the two new proposals 'RSA-AES-MD5' and 'RSA-AES-SHA'.

Configuration with LANconfig

The VPN proposal lists are to be found in LANconfig under the configuration area 'VPN' on the 'IKE param.' tab by clicking on the **IKE proposal lists** button:



Configuration with WEBconfig or Telnet

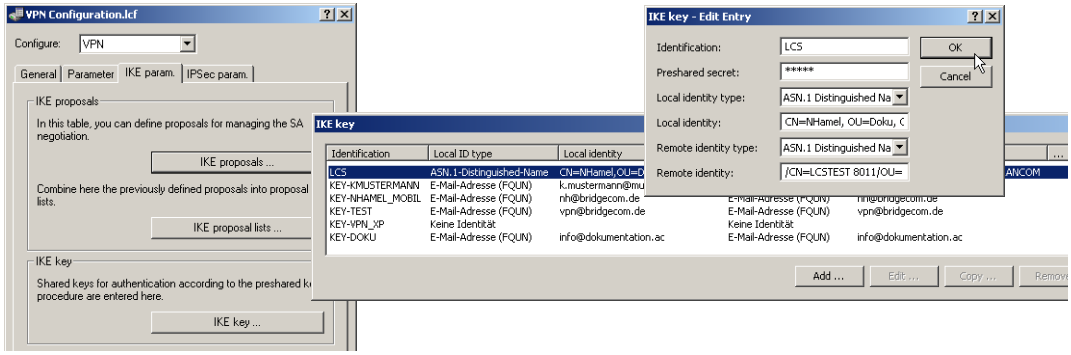
Under WEBconfig or Telnet you will find the IKE proposal lists at the following locations:

Configuration tool	Call
WEBconfig	Expert configuration ▶ Setup ▶ VPN ▶ Proposals ▶ IKE proposal lists
Terminal/Telnet	`/Setup/VPN/Proposals/IKE-proposal-lists`

③ In the list of IKE keys, all certificate connections must be set up with the corresponding identities.

Configuration with LANconfig

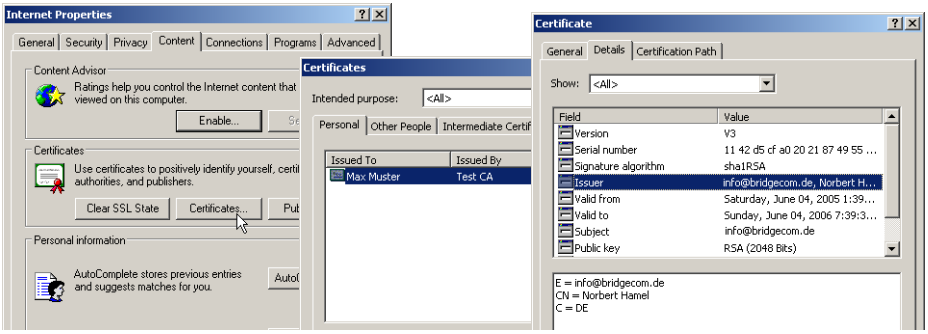
IKE keys are to be found in LANconfig under the configuration area 'VPN' on the 'IKE param.' tab by clicking on the **IKE key** button:



- Once it is no longer required, the preshared key can be deleted.
- The type of the identities is reset to ASN.1 Distinguished Names (local and remote).
- The identities are entered exactly as they stand in the certificates. The individual values such as 'CN', 'O' or 'OU' can be separated by commas or slashes.

  All of the values entered in the certificates must be listed in the same order. If necessary, check the certificate contents by using the Control Panel. To do this, click on **Start** ▶ **Control Panel** ▶ **Internet Options**, the 'Contents' tab and the button **Certificates**.

  Open the certificate and use the 'Details' tab to select the corresponding value. For the applicant you will find, for example, the necessary ASN.1 Distinguished Names and their abbreviations here. The values listed from top to bottom in the certificates must be entered into the IKE key from left to right. Observe the use of upper and lower case!



Special characters in the ASN.1 Distinguished Names can be entered by typing in the hexadecimal ASCII codes after a leading backslash. For example, "\61" corresponds to a small "a".

The display of certificates under Microsoft Windows shows for some values older short forms, for instance 'S' instead of 'ST' for 'stateOrPrivinceName' or 'G' instead of 'GN' for 'givenName'. Only use the new short forms 'ST' and 'GN'.

Configuration with WEBconfig or Telnet

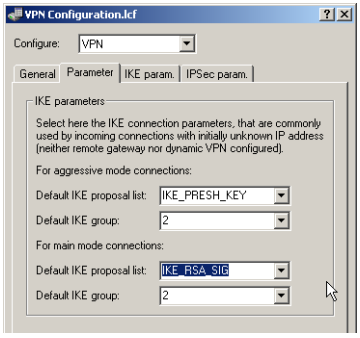
Under WEBconfig or Telnet you will find the IKE keys at the following locations:

Configuration tool	Call
WEBconfig	Expert configuration ▶ Setup ▶ VPN ▶ Certificates and keys ▶ IKE keys
Terminal/Telnet	`/Setup/VPN/Certificates-and-keys/IKE-keys`

④ In the IKE connection parameters, the default IKE proposal lists for incoming aggressive-mode and main-mode connections must be set to the proposal list 'IKE_RSA_SIG'. Also observe the settings in the default IKE group which are adjusted in the following step as necessary.

Configuration with LANconfig

The default IKE proposal lists and default IKE groups are located in LANconfig in the configuration area 'VPN' on the 'Parameters' tab.



Configuration with WEBconfig or Telnet

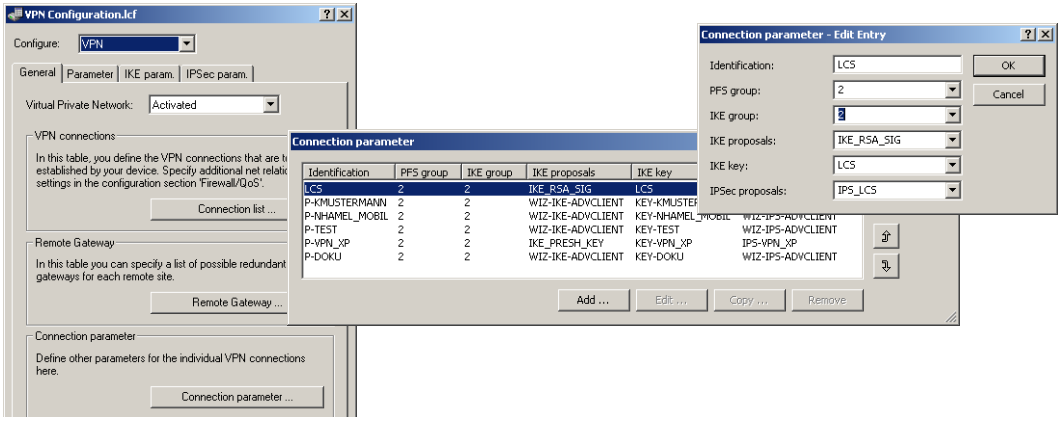
Under WEBconfig or Telnet you will find the default IKE proposal lists and the default IKE groups at the following locations:

Configuration tool	Call
WEBconfig	Expert-Configuration ▶ Setup ▶ VPN
Terminal/Telnet	`/Setup/VPN`

⑤ Finally, the VPN connection parameters must be set up to use the correct IKE proposals ('IKE_RSA_SIG'). The values for 'PFS group' and 'IKE group' must agree with the values set in the IKE connection parameters.

Configuration with LANconfig

The VPN connection parameters are to be found in LANconfig under the configuration area 'VPN' on the 'General' tab by clicking on the **Connection parameters** button:



Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you will find the VPN connection parameters at the following locations:

Configuration tool	Call
WEBconfig	Expert Configuration ▶ Setup ▶ VPN ▶ VPN layers
Terminal/Telnet	`/Setup/VPN/VPN-layers`

10.6.13Set up certificate-based VPN connections with the Setup Wizard

LANconfig is equipped with Setup Wizards with which you can set up certificate-based LAN coupling or RAS access via VPN.

VPN connections that support certificates can only be set up if the LANCOM is programmed with the correct time and if the corresponding certificates are loaded into the device. ('Upload certificates to the LANCOM' → page 292).

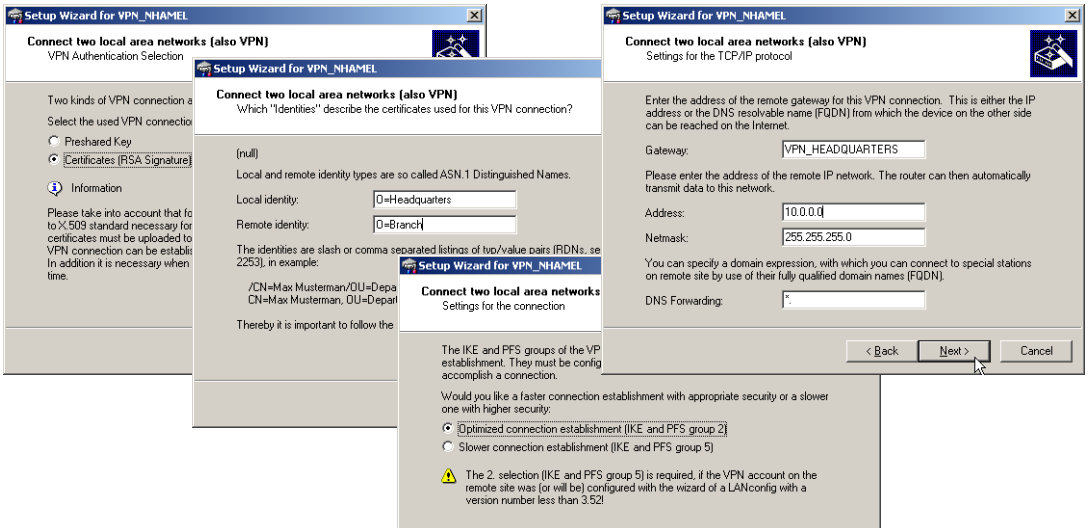
LAN coupling

① Choose the Wizard that connects two local area networks over VPN. In the appropriate dialog, select VPN connection authentication with certificates (RSA signature).

② Enter the identities contained in the certificates for the local and remote devices. Be sure to use the information from each certificate in full and in the right order: The ASN.1-Distinguished Names listed in Windows from top to bottom in the certificates must be entered into LANconfig from left to right.

Microsoft Windows displays some values in the certificates with outdated abbreviations, such as 'S' instead of 'ST' for 'stateOrProvinceName', or 'G' instead of 'GN' for 'givenName'. In these cases make sure that you use the current abbreviations 'ST' and 'GN'.

The Telnet command `show vpn cert` displays the content of the device certificate in a LANCOM, including the entered Distinguished Names (DN) under "Subject". The Distinguished Names are displayed in reverse order here until LCOS 6.00 and in the usual order as of LCOS 6.10!



③ If available choose the optimized connection establishment with IKE and PFS group 2. Only choose group 5 for IKE and PFS if this is required by the remote device. This will be the case if, for example, the VPN remote device is configured with LANconfig 3.52 or earlier.

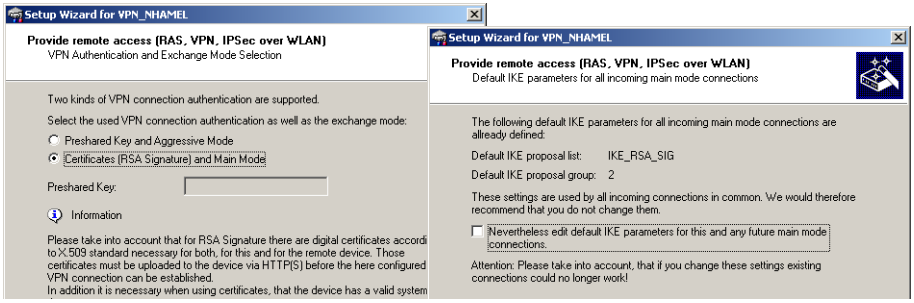
④ Enter the names of the VPN remote site, the IP address, the netmask for the remote network and, if applicable, the domain for the DNS forwarding. If required, activate the "Extranet" function and the "NetBIOS routing".

RAS connections

RAS connections that support certificates can be set up for the LANCOM Advanced VPN Client or for any other VPN client with user-defined parameters. The LANCOM Standard VPN Client does not support certificates.

Various parameters are requested depending on the choice of client or the options. This description shows all of the possible Wizard dialogs, some of which may not necessarily be relevant for your application.

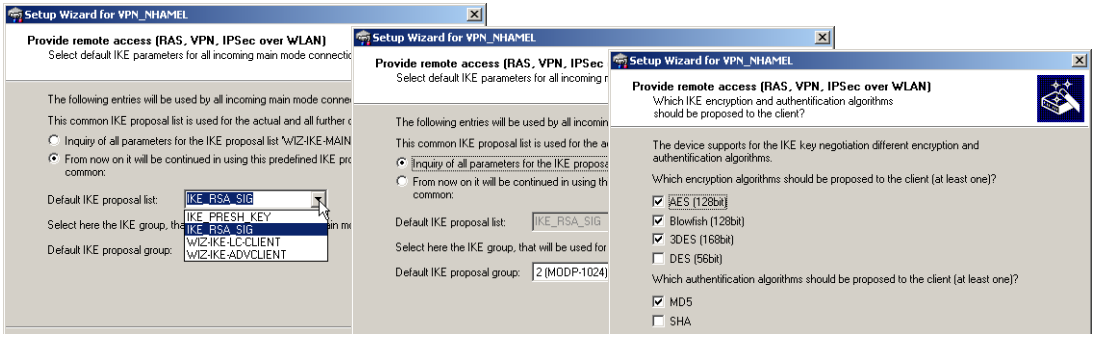
① Choose the Wizard that provides remote access over VPN. In the appropriate dialog, select VPN connection authentication with certificates (RSA signature). The default "Exchange Mode" is the Main Mode.



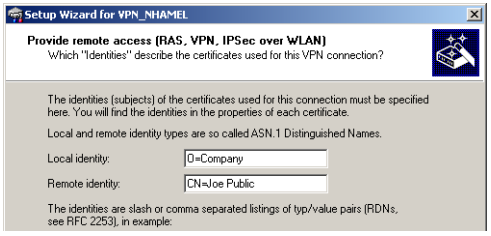
Only in the case of a user-defined VPN client

② The configuration normally presents standard IKE parameters for incoming main mode connections in the standard IKE proposal list 'IKE_RSA_SIG'. If possible use the list of prepared IKE parameters.

③ If you wish to use different parameters for incoming main mode connections, you can adapt the standard IKE parameters to fit your requirements. You can either create a new list 'WIZ-IKE-MAIN-MODE' or you can select one of the existing IKE proposal lists as the new "Standard IKE proposal list". The list defined here will be used for all incoming main mode connections in the future. For a new IKE proposal list, you can select the encryption and authentication methods that are to be used by the client during the IKE negotiation.



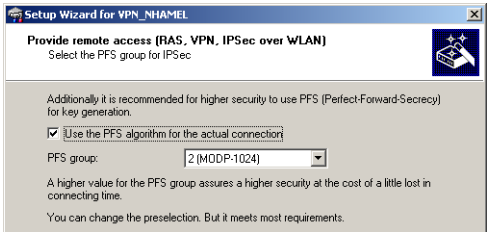
④ Enter the identities contained in the certificates for the local and remote devices. Be sure to use the information from each certificate in full and in the right order: The ASN.1-Distinguished Names listed in Windows from top to bottom in the certificates must be entered into LANconfig from left to right.



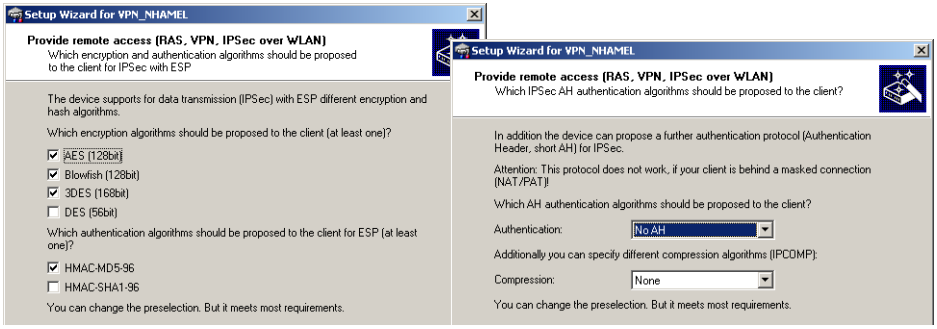
Microsoft Windows displays some values in the certificates with outdated abbreviations, such as 'S' instead of 'ST' for 'stateOrProvinceName', or 'G' instead of 'GN' for 'givenName'. In these cases make sure that you use the current abbreviations 'ST' and 'GN'.

The Telnet command `show vpn cert` displays the content of the device certificate in a LANCOM, including the entered Distinguished Names (DN) under "Subject". The Distinguished Names are displayed in reverse order here until LCOS 6.00 and in the usual order as of LCOS 6.10!

⑤ If available choose the optimized connection establishment with IKE and PFS group 2. Only choose group 5 as the PFS group if this is required by the client.



⑥ The following dialogs define the encryption and authentication methods, the authentication header and the data compression that the client will use for the transfer of the payload data with IPSec. Use the preset values as much as possible as long as the client does not demand different settings.

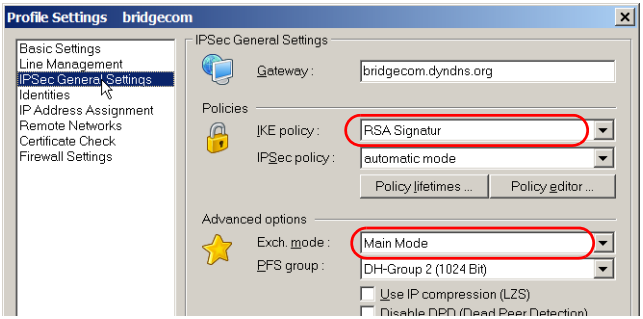


⑦ Enter the IP address of the client and for the address range that is to be accessible in the local network. If required, activate "NetBIOS routing".

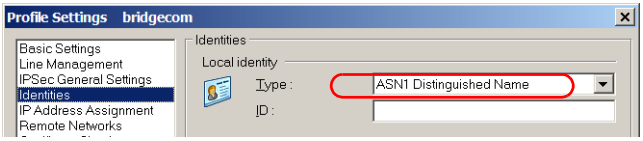
10.6.14Set up LANCOM Advanced VPN Client for certificate connections

To use the LANCOM Advanced VPN Client to dial-in to a LANCOM router, the appropriate profile settings must be adjusted to allow for the use of certificates.

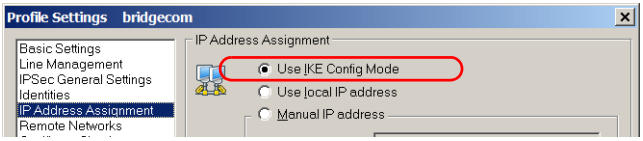
① In the IPSec General Settings for the profile, set the IKE policy to 'RSA signature'.



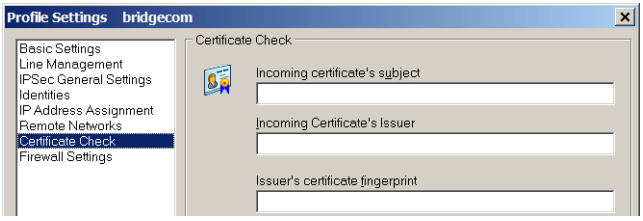
② Switch the identity to 'ASN1 Distinguished Names'. The 'identity' can remain blank since this information is taken from the certificate.



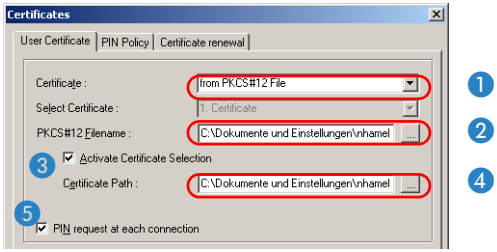
③ For the IP address assignment use the 'IKE Config Mode'.



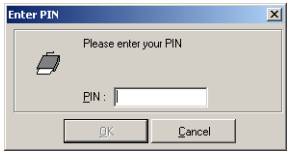
④ For the Certificate Check you can optionally place a limitation on the certificates accepted by the LANCOM Advanced VPN Client. To do this, you define the user and/or the issuer of the incoming certificate and, if applicable, the associated "fingerprint".



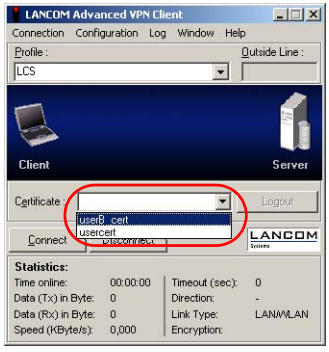
⑤ After storing the adapted connection profile, click on the menu item **Configuration** ▶ **Certificates** to open the settings for the User Certificate.



- □ Select the certificate type 'from PKCS#12 file' (1) and set the required certificate file (2).
- □ To work with various certificates, activate the option 'Certificate Selection' (3) and enter the path for the folder where the certificate files are stored (4).
- □ Define whether or not the PIN (password) has to be entered before connection establishment (5). Alternatively, you can save the PIN in the LANCOM Advanced VPN Client under the menu item **Connection ▶ Enter PIN** .



- □ If Certificate Selection is activated, the certificate corresponding to the connection can be chosen from a list displayed in the main window of the LANCOM Advanced VPN Client, as befits the selected profile.



10.6.15Diagnosis of VPN certificate connections

If the VPN connection establishment does not work as desired, then entering the following commands at the LANCOM console can provide useful information.

- `trace + vpn-status`

  Displays a trace of the current VPN connections.

- `show vpn long`
  Displays the contents of the VPN configuration, including the entered Distinguished Names (DN).
- `show vpn ca`
  Displays the content of the root certificate.
- `show vpn cert`
  Displays the content of the device certificate.

The Distinguished Names are displayed in reverse order here until LCOS 6.00 and in the usual order as of LCOS 6.10!

10.6.16Certificate revocation list - CRL

Certificates for VPN connections have a validity period by a start date and an end date. During this period, the certificate can be used to establish a VPN connection. Should an employee leave the company, then it should be possible for certificates, for example that were used for mobile VPN access, to be declared as invalid. This prevents continued access to the company network and does not require any changes to the VPN router configuration.

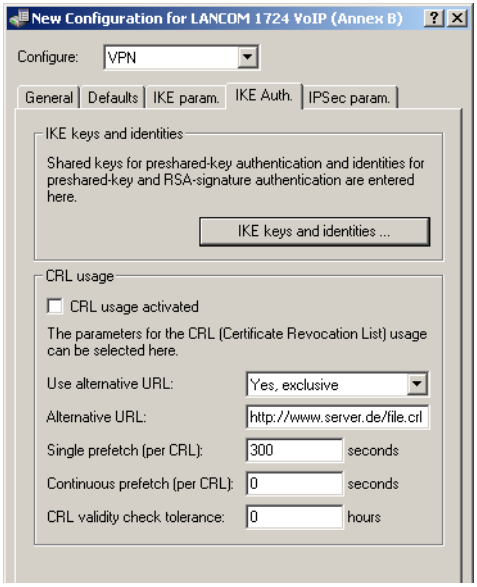
The certificate is physically located with the ex-employee and cannot be changed, which is why a certificate revocation list is of use. In einer solchen Zertifikatsperrliste (Certificate Revocation List – CRL), wie sie z.B. von der Microsoft CA oder von OpenSSL unterstützt werden, sind die ungültigen Zertifikate eingetragen. The CRL is available from a suitable server. The URL to be used by a router to download the CRL into its own memory is entered into the root certificate of the VPN router and/or into the configuration of the device itself.

The CRL is renewed by the CA on a regular basis, enabling changes in the CRL, such as withdrawn certificates, to be recognized by the VPN routers in good time. During the setup at the CA, a schedule is defined for the regular updating of the CRL. After an update to the CRL and its storage to the server (manual or automatic), the VPN router then has to update its infomation, too. To do this, the router reads out the validity period of the CRL and, briefly before expiry, attempts to load a current version. Alternativ kann auch ein regelmäßiges Update – unabhängig von der Gültigkeitsdauer der CRL – in einem LANCOM definiert werden.

When a connection is being established, the VPN router checks if the remote station's certificate is in the current CRL. Connections to remote stations without a valid certificate are rejected.

Configuring the CRL function

Configuration of the CRL function involves the definition of the path to the CRL and additional parameters such as the update interval.



Configuration tool	Call
LANconfig	VPN ▶ IKE Auth.
WEBconfig, Telnet	Expert Configuration > Setup > VPN > Certificates-and-Keys > CRLs

- **CRL-Funktionalität [Default: Aus]**
  - Enabled: During the certificate check, the CRL (if available) will be considered as well.

If this option is activated but no valid CRL is available (e.g. if the server can't be reached), then all connections will be rejected and existing connections will be interrupted.

- **Alternative URL benutzen [Default: No]**
  - No: Only the URL defined in the root certificate is to be used.
  - Yes, always: The alternative URL will always be used even if a URL is entered into the root certificate.
  - Yes, alternative: The alternative URL will only be used if there is no URL entered into the root certificate.
- **Alternative URL**
  - This is an alternative URL which can be used to retrieve a CRL.

- **Abruf vor Ablauf [Default: 300 Sekunden]**
  - The point in time prior to expiry of the CRL when the new CRL can be loaded. This value is increased by a random value to prevent server overload from multiple simultaneous queries. Once within this time frame, any coinciding regular planned updates will be stopped.

If the first attempt to load the CRL fails, new attempts are made at regular short intervals.

- **Abruf regelmäßig [Default: 0 Sekunden]**
  - The time period after which periodic attempts are made to retreive a new CRL. Useful for the early retreival of CRLs published at irregular intervals. The entry '0' disables regular retreival.

If with regular updates the CRL cannot be retreived, no further attempts will be started until the next regular attempt.

- **Validity tolerance**
  - Even after expiry of the CRL, certificate-based connections will continue to be accepted for the period defined here. This tolerance period can prevent the unintentional rejection or interruption of connections if the CRL server should be temporarily unavailable.

Within the time period defined here, even certificates in the CRL which have expired can still be used to maintain or establish a connection.

CRL status display in LANmonitor

Information about the validity period and the publisher of the current CRL in the LANCOM can be inspected in LANmonitor.

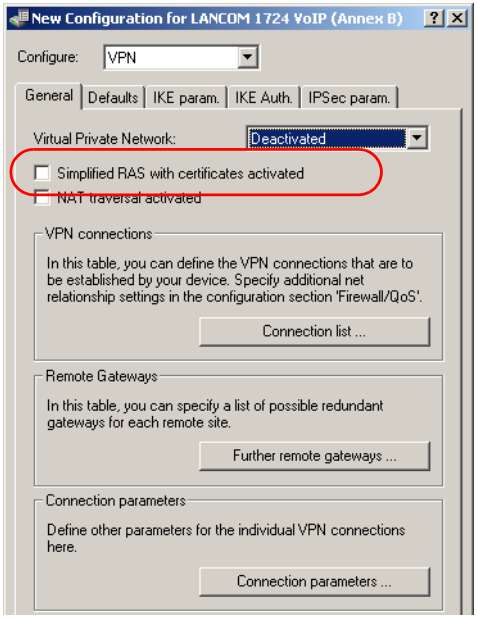
10.6.17Simplified RAS with certificates

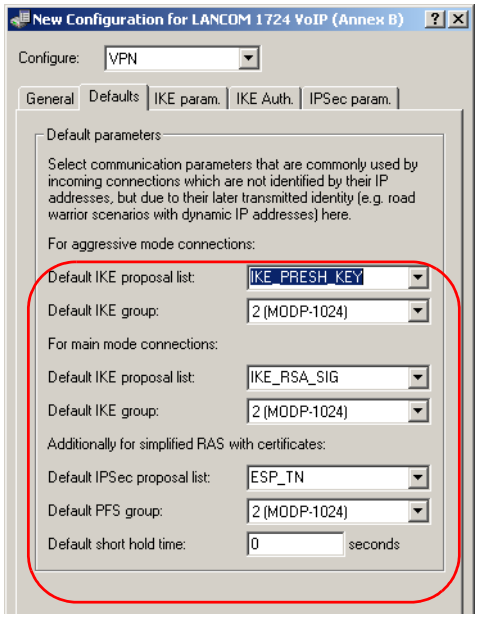
When dialling in, the identity of computers that use varying IP addresses is unknown at the initial stages of the IKE negotiation (Phase 1), so communication is facilitated by using default values for IKE proposal lists and IKE proposal groups. During negotiation, the identity is communicated and this is used to determine the parameters for phase 2 (IPSec proposal list and PFS group). For this to occur, every single user must be entered individually into the VPN router configuration.

With certificate-based RAS, the identity is communicated via the certificate. To avoid having to make individual user entries in the router configuration, common parameters for phase 2 can be defined for all users who are identified by certificate. All the user requires for simplified RAS is a valid certificate with a signature from the publisher of the root certificate in the device. Furthermore, the parameters used by the client during dial-in must agree with the default values in the VPN router.

Information about configuring the VPN client is available in the relevant documentation from the software manufacturer.

This function has to be activated to configure the simplified dial-in. The default parameters can be altered according to requirements.





Configuration tool	Call
LANconfig	VPN ▶ General and VPN ▶ General ▶ Defaults
WEBconfig, Telnet	Expert Configuration > Setup > VPN

By activating the simplified RAS with certificates, **all** clients that have a valid certificate signed by the publisher of the device's root certificate can dial in to the corresponding network. No further configuration of the router is necessary! Unwanted dial-ins are then prevented exclusively by using a CRL and blocking the certificates there.

10.7 NAT Traversal (NAT-T)

The insufficient number of publicly valid IP addresses has lead to the development of procedures such as IP masquerading or NAT (Network Address Translation), where a whole local network is masked by a single, publicly valid IP address. In this way, all clients in a LAN use the same IP address to exchange data with public networks such as the Internet. The assignment of the incoming and outgoing data packets to the different participants in the network is ensured by connecting the internal IP addresses to corresponding port numbers.

This process has proven its worth in the last few years and has since become the standard in almost all Internet routers. However, new difficulties arise when the hidden data packets are processed using VPN. As data connections over VPN are highly secured, mechanisms such as authentication and encryption are of great importance here.

Converting internal IP addresses to the gateway's central, publicly valid IP address and converting source and target ports can lead to problems in many applications, for example where the UDP port 500 that is usually used during the IKE negotiation has been changed and the IKE can no longer be successfully completed as a result. The address change using NAT is therefore assessed by a VPN gateway as a security-critical data packet change, the VPN negotiation fails and no connection is made. In fact these problems occur, for example, when you dial in using some UMTS mobile telephone networks where the network operator's servers do not support the address conversion in combination with IPSec-based VPNs.

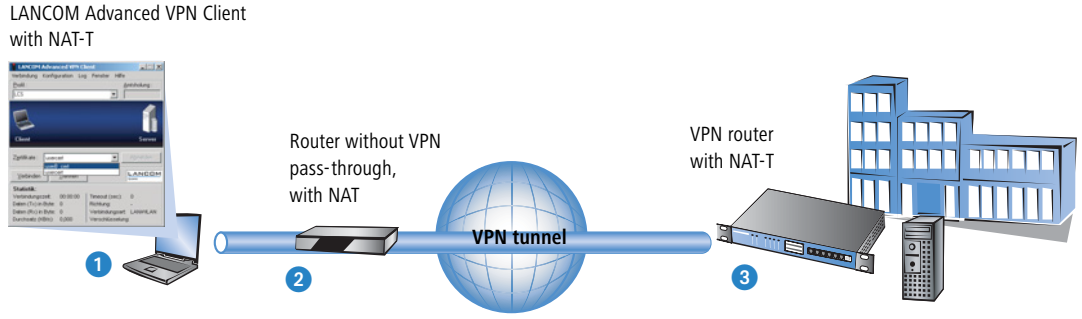
So you can successfully create a VPN connection even in such cases, NAT-T (NAT Traversal) provides a process that can overcome the problems described when handling data packets with changed addresses.

NAT-T can only be used with VPN connections that use ESP (Encapsulating Security Payload) for authentication. Unlike AH (Authentication Header), ESP does not consider the IP header of the data packets when determining the hash value for authentication. The hash value calculated by the receiver is therefore also equivalent to the hash value entered in the packets.

If the VPN uses AH for authentication, then in principle no connection can be established over sections with Network Access Translation, as the AH hash values similarly change when the IP addresses change, and the recipient would classify the data packets as untrustworthy.

The NAT Traversal process eliminates the problems that occur when establishing a VPN connection at the end points of the VPN tunnel. The following scenarios can be distinguished from one another:

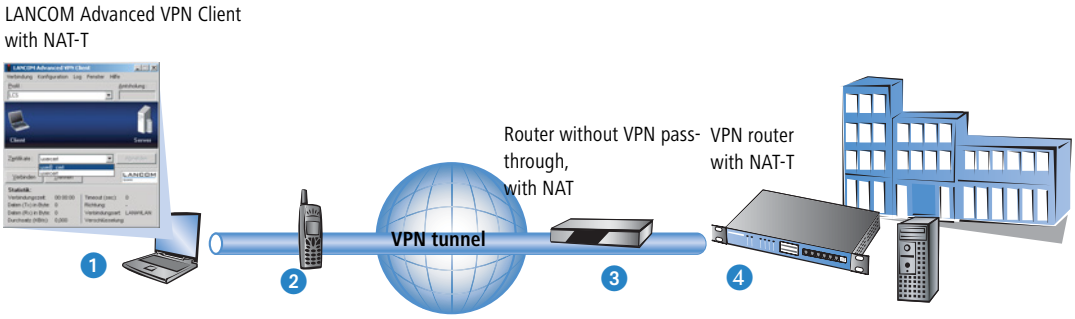
- A member of the field staff uses a LANCOM Advanced VPN Client to dial into the company VPN router **without** "VPN pass-through" support (i.e. IPSec masking) but **with** Network Address Translation.



□ Both tunnel end points LANCOM Advanced VPN Client 1 and VPN router 3 support NAT-T and can therefore also establish a VPN connection through the intermediary router.

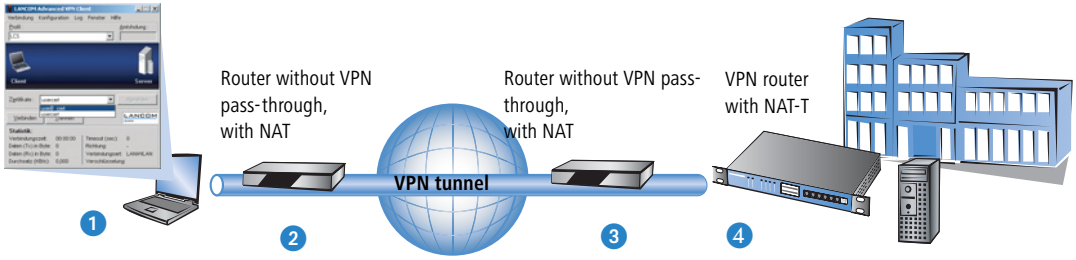
- □ Router 2 as a NAT device between the VPN end points performs straight forward NAT address conversion. This router does not require NAT but firewall ports 500 and 4500 must be open in order to enable NAT communication between both tunnel end points.

■ In the second example application, the travelling field worker dials in to the network at the headquarters with his notebook 1 and a mobile telephone or modem 2.



- □ At the headquarters, the VPN router 4 is located behind a terminating router 3, which only provides Internet access with the address conversion.
- □ Both tunnel end points LANCOM Advanced VPN Client 1 and VPN router 4 support NAT-T and can therefore establish a VPN connection, as in the first example.
- □ In the terminating router 2, the firewall ports 500 and 4500 have to be activated, as does port forwarding.

■ In both of these cases, the two ends of the connection are the straight-forward NAT routers 2 and 3. Teh VPN connection is established between the LANCOM Advanced VPN Client 1 and VPN router 4.



The two routers 2 and 3 have to permit the NAT-T connection between the two tunnel endpoints in that the firewall ports 500 and 4500 are activated, and port forwarding has to be activated in the terminating router at the headquarters, as well.

To enable this process, both ends of the VPN connection have to work with NAT-T. The process of establishing the VPN connection (reduced to the NAT-T-relevant operations) appears as follows:

① At an early stage of the IKE negotiation, there is a check to see if both ends of the VPN connection are NAT-T-compatible.

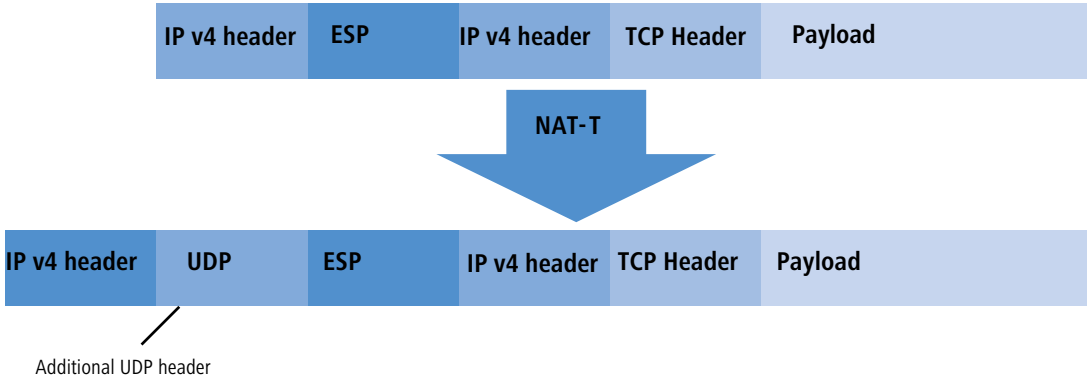
② In the second step, there is a check to see if the address is converted to NAT on the section between the two tunnel end points, and at what point in the connection the NAT devices are located.

③ To deal with problems with ports that may have changed, all negotiation and data packets are subsequently sent only via UDP port 4500 when a NAT device has been detected.

If the LANCOM functions as a NAT router between the VPN end points, ensure that UDP ports 500 and 4500 are activated in the firewall when you use NAT-T! This port is activated automatically if you use the firewall assistant in LANconfig.

If the VPN connections are first created on devices with LCOS version 5.20 or above using the VPN assistant and later with the firewall assistant from LANconfig, then no additional firewall settings are required for the NAT router.

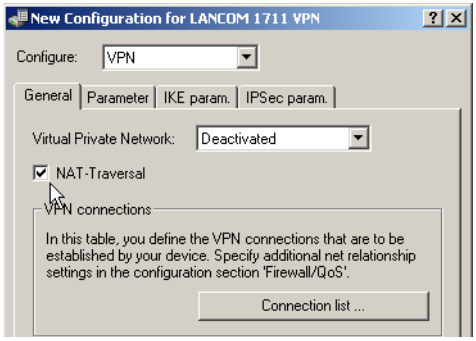
④ In the diagram below, the data packets are packed again into UDP packets (UDP encapsulation) and are also sent using port 4500. As a result of this additional encapsulation, changing the IP addresses for the VPN negotiation is no longer relevant and the VPN tunnel can be established without any problems. At the other end of the connection, the IP data is released again by the additional UDP header and can be processed by the router without further action.



In order to use this process, both ends of the VPN connection (such as the WLANmonitor and a LANCOM router) have to use NAT-T.

Configuration with LANconfig

You will find the button for activating NAT-T in LANconfig in the 'VPN' configuration area on the 'General' tab page.



Configuration with WEBconfig, Telnet or SSH

Under WEBconfig, Telnet or SSH client you will find the settings for activating NAT-T under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert Configuration ▶ Setup ▶ VPN ▶ NAT-T Operating
Terminal/Telnet	`Setup/VPN/NAT-T-Operating`

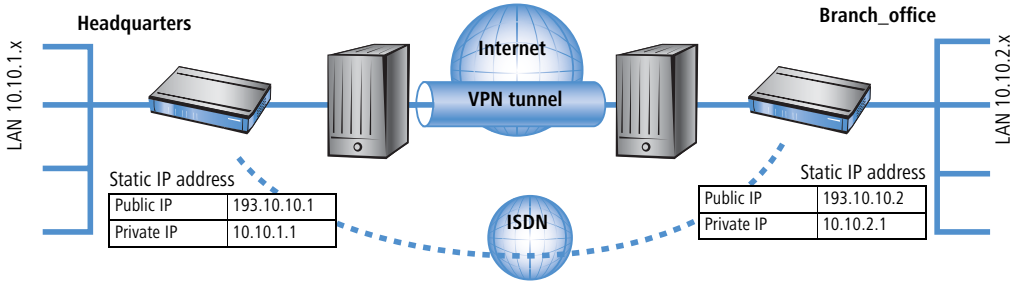
10.8 Specific examples of connections

This section covers the 4 possible types of VPN connections with concrete examples. These 4 different connection types are categorized by the type of IP address of the two VPN gateways:

- static/dynamic
- dynamic/static (the dynamic peer initiates the connection)
- static/dynamic (the static peer initiates the connection)
- dynamic/dynamic

There is a section for each of these types, together with a description of all required configuration information in the familiar table form.

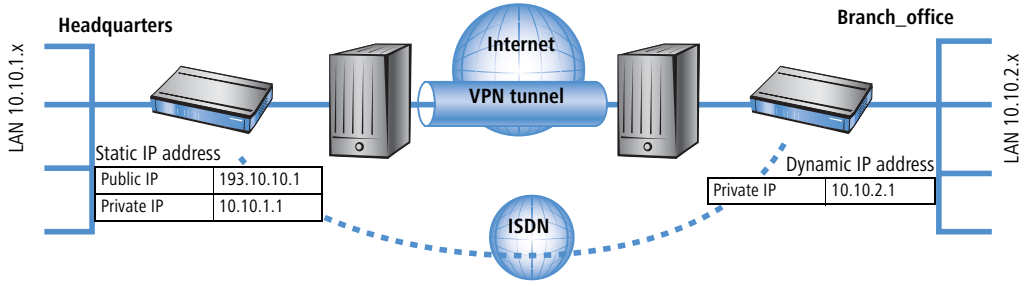
10.8.1 Static/static



A VPN tunnel via the Internet serves as the connection between the LANCOM **Headquarters** and **branch office**. Both gateways have static IP addresses. Thus, both can initiate the connection.

Entry	Headquarters		Branch_office
Type of local IP address	static		static
Type of remote IP address	static		static
Name of the local device	Headquarters		Branch_office
Name of the remote device	Branch_office		Headquarters
Shared Secret for encryption	secret	◄►	secret
IP address of the remote device	193.10.10.2		193.10.10.1
IP-network address of the remote network	10.10.2.0		10.10.1.0
Netmask of the remote network	255.255.255.0		255.255.255.0

10.8.2 Dynamic/static



The VPN gateway **Branch office** initiates a VPN connection to the gateway **Headquarters**. **Branch office** has a dynamic IP address that was chosen and assigned by the Internet service provider upon dialling in, whereas **Headquarters** has a fixed, static address. When the connection is set up, **Branch office** transmits its actual IP address to **Headquarters**. This is accomplished by a special ICMP packet (alternatively UDP, port 87).

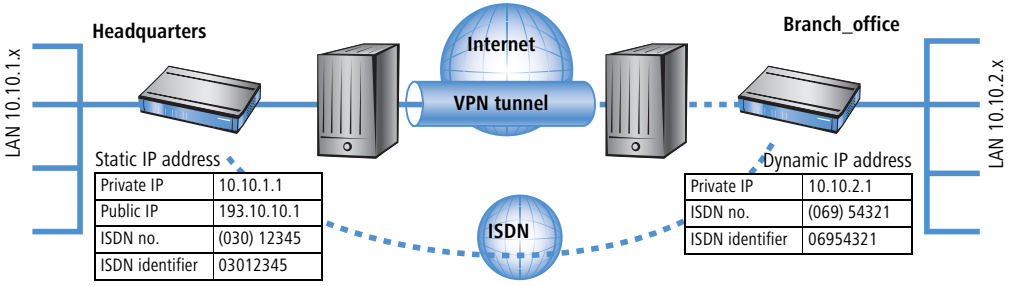
Entry	Headquarters		Branch_office
Type of local IP address	static		dynamic
Type of remote IP address	dynamic		static
Name of the local device	Headquarters		Branch_office
Name of the remote device	Branch_office		Headquarters
Password for the secure transmission of the IP address	confidential	◄►	confidential

Entry	Headquarters		Branch_office
Shared Secret for encryption	secret	◄►	secret
IP address of the remote device	–		193.10.10.1
IP-network address of the remote network	10.10.2.0		10.10.1.0
Netmask of the remote network	255.255.255.0		255.255.255.0

An ISDN line is not necessary for establishing this type of connection. The dynamic end communicates its IP address encrypted via the Internet protocol ICMP (or alternatively via UDP).

10.8.3 Static/dynamic (with LANCOM Dynamic VPN)

In this case (other than the example above), the peer with the static IP address initiates the VPN connection.



The VPN gateway **Headquarters** initiates a VPN connection to **Branch office**. **Headquarters** has a static IP address, **Branch office** a dynamic one.

The entries for the ISDN connection are needed for the transmission of the actual dynamic IP address solely. The Internet access wizard configures the connection to the Internet.

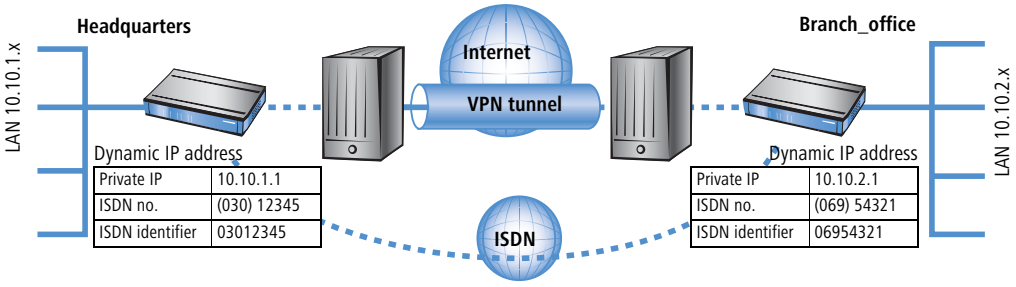
Alternatively, this application can be solved with the help of dynamic DNS. In this constellation, the headquarters with its static IP address connects to the branch office with the help of a dynamic DNS name which

is assigned to the current dynamic IP address. More information is available under 'Dynamic IP addresses and DynDNS' → page 257.

Entry	Headquarters		Branch_office
Type of local IP address	static	⇄	dynamic
Type of remote IP address	dynamic	⇄	static
Name of the local device	Headquarters	⇄	Branch_office
Name of the remote device	Branch_office	⇄	Headquarters
ISDN-calling number of the remote device	06954321		03012345
ISDN-caller ID of the remote device	06954321		03012345
Password for the secure transmission of the IP address	confidential	⟷	confidential
Shared Secret for encryption	secret	⟷	secret
IP address of the remote device			193.10.10.1
IP-network address of the remote network	10.10.2.0		10.10.1.0
Netmask of the remote network	255.255.255.0		255.255.255.0

The described connection set up requires an ISDN connection for both VPN gateways.

10.8.4 Dynamic/dynamic (with LANCOM Dynamic VPN)



A VPN tunnel via the Internet serves as the connection between the LANCOM **Headquarters** and **branch office**. Both sites have dynamic IP addresses. Thus, both can initiate the connection.

The entries for the ISDN connection are needed for the transmission of the actual dynamic IP address solely. The Internet access wizard configures the connection to the Internet.

Alternatively, this application can be solved with the help of dynamic DNS. Instead of a static IP address, a dynamic DNS name helps to find the dynamic IP address that is currently in use. More information is available under 'Dynamic IP addresses and DynDNS' → page 257.

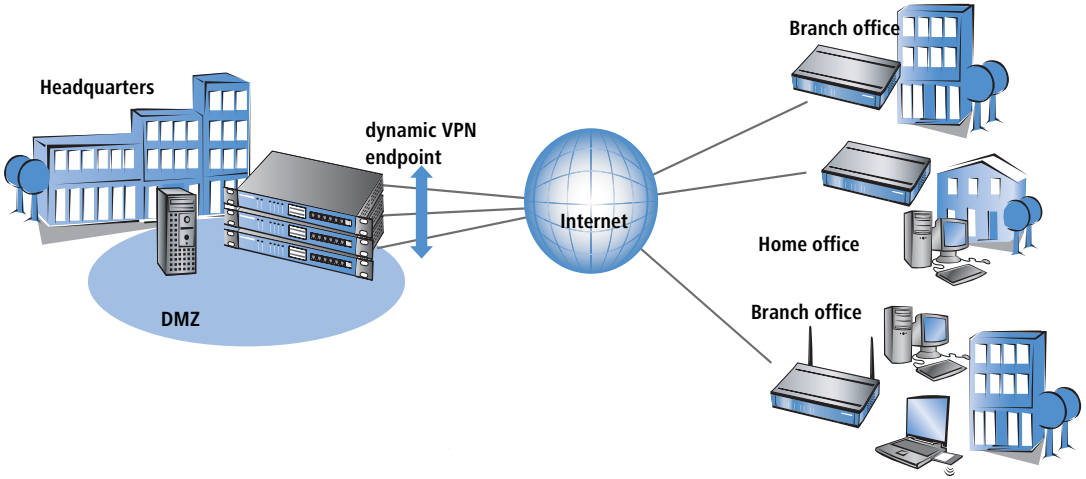
Entry	Headquarters		Branch_office
Type of local IP address	dynamic		dynamic
Type of remote IP address	dynamic		dynamic
Name of the local device	Headquarters		Branch_office
Name of the remote device	Branch_office		Headquarters
ISDN-calling number of the remote device	06954321		03012345
ISDN-caller ID of the remote device	06954321		03012345
Password for the secure transmission of the IP address	confidential		confidential
Shared Secret for encryption	secret		secret
IP-network address of the remote network	10.10.2.0		10.10.1.0
Netmask of the remote network	255.255.255.0		255.255.255.0

Dynamic VPN works only between LANCOM that each feature at least one ISDN port that can be used for the ISDN connection

10.9 VPN connections: High availability with VPN load balancing

10.9.1 Multiple VPN gateway addresses

In decentralized company structures that rely on VPN for networking the various locations, the availability of the central VPN gateway is of particular significance. The company-wide communications only remain reliable as long as these central dial-in nodes are working properly.



With the option of configuring several "remote gateway" addresses as "dynamic VPN endpoints" for a VPN connection, LANCOM VPN gateways offer a high level of availability by using redundant devices. This involves multiple gateways at the headquarters being set up with identical VPN configurations. On location at the satellite sites, all of these available gateways are entered as possible remote stations for the VPN connection. If one of the gateways is unavailable, the remote router automatically redirects the request to one of the other routers.

To ensure that the computers in the LAN at the headquarters know which VPN gateway it to be used to reach a particular satellite station, the outband router currently connected to the remote site is propagated via RIPv2 to the network at the headquarters.

A powerful mechanism for high availability with constant load balancing between the VPN gateways at the headquarters is attained with the configuration of the satellite stations to select the remote site for VPN connection on a random basis.

10.9.2 Configuration

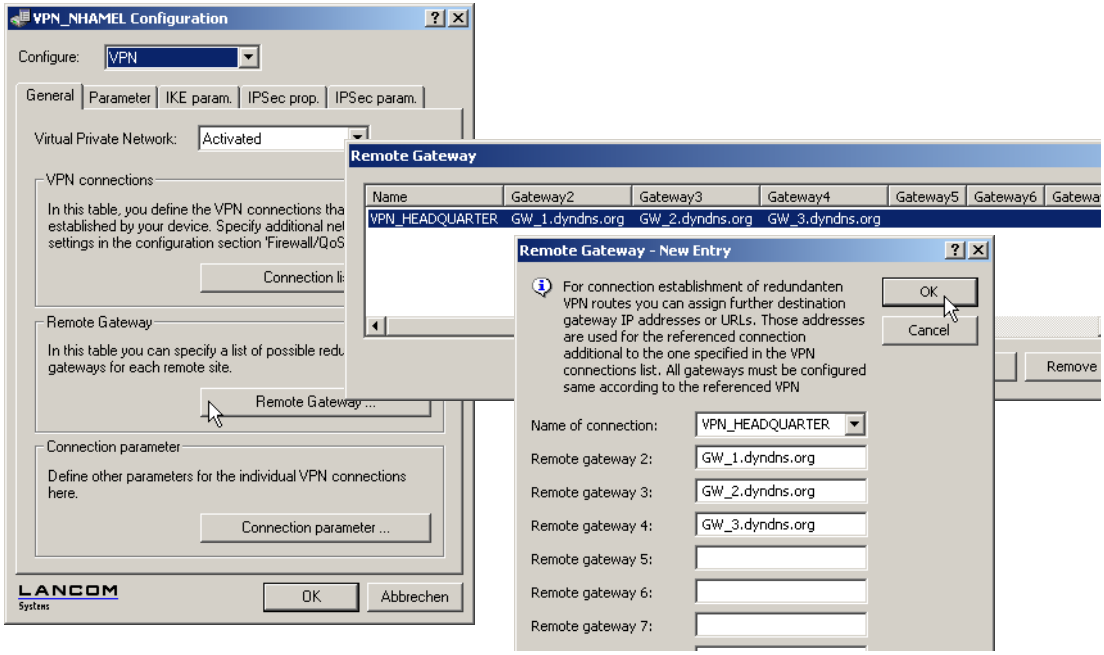
During configuration, additional destinations for a VPN connection should be entered in the list of "Remote gateways". The list consists of the following entries:

- Name: Name of the remote site from the VPN connection list, the "target" of the VPN connection.
- Gateway 2 to Gateway 9: Address of the alternative gateways, as an IP address or DNS-translatable address.
- Begin with: In which order should the entries are to be tried. You can select from:
  - Last used: Selects the entry for the VPN connection which was successfully used most recently.
  - First: Selects the first of the configured remote stations.
  - Random: Selects one of the configured remote stations at random. This setting provides an effective measure for load balancing between the gateways at the headquarters.

The entry for the gateway in the VPN connection list can be left blank if all of the possible gateways are entered into the list of "Remote gateways".

LANconfig

When using LANconfig for the configuration, you will find the list of gateway addresses in the configuration area VPN' on the 'General' tab under the button **Remote gateway**.



WEBconfig, Telnet or terminal program

Under WEBconfig, Telnet or terminal program, you will find the settings for the remote gateway addresses under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ Config ▶ Remote-gateway-list
Terminal/Telnet	`Setup/VPN/Remote-gateways`

The following options are available for defining the strategy for the utilization of the configured remote-gateway addresses:

- `last used`
- `first`
- `random`

Example:

The following command sets three gateways as target at the headquarters, one of which is to be selected at random:

```
set VPN_HEADQUARTERS 213.217.69.75 213.217.69.76 213.217.69.77 * * * * * random
```

10.10How does VPN work?

In practice, a VPN must fulfill a number of requirements:

- Unauthorized third parties must not be able to read the data (encryption)
- It should not be possible to manipulate the data (data integrity)
- Unambiguous identification of the sender of data (authentication)
- Simple key management
- Compatibility to VPN devices from a variety of manufacturers

LANCOM VPN achieves these five major goals by applying the widely used IPSec standard.

10.10.1IPSec—The basis for LANCOM VPN

The original IP protocol does not contain any provisions for security. Security problems are compounded by the fact that IP packets do not go directly to a specific recipient, but are sent scattershot to all computers on a given network segment. Anyone can help themselves and read the packets. This leaves the door open to the misuse of data.

IP has been developed further for this reason. A secure version is now available: IPSec. LANCOM VPN is based on IPSec.

IPSec stands for "**IP Sec**urity Protocol" and was originally the name used by a working group of the IETF, the **I**nternet **E**ngineering **T**ask **F**orce. Over the years, this group has developed a framework for a secure IP protocol that is generally referred to as IPSec today.

It is important to note that IPSec itself is not a protocol, but merely the standard for a protocol framework. IPSec actually consists of a variety of protocols and algorithms for encryption, authentication and key management. These standards will be introduced in the following sections.

Security in an IP environment

IPSec has been implemented almost completely within level 3 of the OSI model, i.e. in the network layer. The transfer of data packets using the IP protocol is realized on level 3 of IP networks.

IPSec thus replaces the IP protocol. Under IPSec, the packets have a different internal structure than IP packets. Their external structure remains fully compatible to IP, however. IPSec packets can therefore be transported without problems by existing IP networks. The devices in the network responsible for the transport of the packets cannot distinguish IPSec packets from IP packets on the basis of their exterior structure.

The exceptions in this case are certain firewalls and proxy servers that access the contents of the packets. Problems can arise from the (often function dependent) incompatibilities of these devices to the existing IP standard. These devices must therefore be adapted to IPSec.

IPSec will be firmly implemented in the next generation of the IP standard (IPv6). For this reason, we can assume that IPSec will remain the most important standard for virtual private networks in the future.

10.10.2Alternatives to IPSec

IPSec is an open standard. It is not dependent on individual manufacturers and is being developed by the IETF with input from the interested public. The IETF is a nonprofit organization that is open to everyone. The broad acceptance of IPSec is the result of this open structure which unites a variety of technical approaches.

Nevertheless, there are other approaches for the realization of VPNs. We will only mention the two most important of these here. They are not realized at the network level like IPSec, but at the connection and application levels.

Security at the connection level – PPTP, L2F, L2TP

Tunnels can already be set up at the connection level (level 2 of the OSI model). Microsoft and Ascend developed the **P**oint-to-**P**oint **T**unneling **P**rotocol (PPTP) early on. Cisco presented a similar protocol with **L**ayer **2** **F**orwarding (L2F). Both manufacturers agreed on a joint effort and the IETF produced the **L**ayer **2** **T**unnel **P**rotocol (L2TP).

Their main advantage over IPSec is that any network protocol can be used with such a network connection, especially NetBEUI and IPX.

A major disadvantage of the described protocols is the lack of security at the packet level. What's more, these protocols were designed specifically for dial-up connections.

Security at higher levels – SSL, S/MIME, PGP

Communications can also be secured with encryption at higher levels of the OSI model. Well known examples of this type of protocol are SSL (**S**ecure **S**ocket **L**ayer) mainly used for web browser connections, S/MIME (**S**ecure **M**ultipurpose **I**nternet **M**ail **E**xtensions) for e-mails and PGP (**P**retty **G**ood **P**rivacy) for e-mails and files.

In all of the above protocols, an application handles the encryption of the data, for example the Web browser on one end and the HTTP server on the other.

A disadvantage of these protocols in the limitation to specific applications. In addition, a variety of keys is generally required for the different applications. The configuration must be managed on the individual computers and can not be administered conveniently on the gateways only, as is the case with IPSec. Security protocols at the application level tend to be more intelligent as they know the significance of the data being transferred. They are usually much more complex, however.

All of these layer-2 protocols only support end-to-end connections; they are therefore not suitable for coupling entire networks.

On the other hand, these mechanisms do not require the slightest changes to the network devices or access software. And unlike protocols in lower network levels, they are still effective when the data content is already in the computer.

Combinations are possible

All of the alternatives listed above are compatible to IPSec and can therefore be used parallel to it. This permits a further increase of the security level. It would be possible, for example, to dial into the Internet using an L2TP con-

nection, set up an IPSec tunnel to a Web server and exchange HTTP data between the Web server and the browser in secure SSL mode.

Each additional encryption would reduce the data throughput, however. Users can decide on a case-by-case basis whether the security offered by IPSec alone is sufficient. Only in rare cases is a higher level of security really necessary. Particularly as the degree of security can be adjusted within IPSec.

10.11The standards behind IPSec

IPSec is based on a variety of protocols for the individual functions. These protocols are based on, and complement one another. The modularity achieved with this concept is an important advantage of IPSec over other standards. IPSec is not restricted to specific protocols but can be supplemented at any time by future developments. The protocols integrated to date also offer such a high degree of flexibility that IPSec can be perfectly adapted to virtually any requirements.

10.11.1IPSec modules and their tasks

IPSec has to perform a number of tasks. One or more protocols have been defined for each of these tasks.

- Authentication of packets
- Encryption of packets
- Transfer and management of keys

10.11.2Security Associations – numbered tunnels

A logical connection (tunnel) between two IPSec devices is known as an SA (**S**ecurity **A**ssociation). SAs are managed independently by the IPSec device. An SA consists of three values:

- **Security Parameter Index (SPI)**

  ID to distinguish multiple logical connections to the same target device with the same protocols
- **Target IP address**
- **Security protocol used**

  Designates the security protocol used for the connection: AH or ESP (further information will be provided on these protocols in the following sections).

An SA applies only to one communication direction of the connection (simplex). A complete send and receive connection requires two SAs. In addition, an SA only applies for one used protocol. Two separate SAs are also required if AH and ESP are used, i.e. two for each communication direction.

The SAs are managed in an internal database of the IPSec device that also contains the advanced connection parameters. These parameters include the algorithms and keys used, for example.

10.11.3Encryption of the packets – the ESP protocol

The ESP protocol (**E**ncapsulating **S**ecurity **P**ayload) encrypts the packets as protection against unauthorized access. This was once the only function of ESP, but in the course of the further development of the protocol it was expanded with options for the protection of integrity and verification of authenticity. In addition, ESP also features effective protection against replayed packets. ESP thus offers all of the functions of AH – in some cases, however, the use of AH parallel to ESP is advisable.

How ESP works

The structure of ESP is more complex than that of AH. ESP also inserts a header behind the IP header as well its own trailer and a block of ESP authentication data.

Transport and tunnel mode

Like AH, ESP can be used in two modes: transport and tunnel mode.

In transport mode, the IP header of the original packet is left unchanged and the ESP header, encrypted data and both trailers are inserted.

The IP header contains the unchanged IP address. Transport mode can therefore only be used between two end points, for the remote configuration of a router, for example. It cannot be used for the coupling of networks via the Internet – this would require a new IP header with the public IP address of the recipient. In such cases, ESP can be used in tunnel mode.

In tunnel mode, the entire packet including the original IP header is encrypted and authenticated and the ESP header and trailers are added at the entrance of the tunnel. A new IP header is added to this new packet, this time with the public IP address of the recipient at the end of the tunnel.

Encryption algorithms

As a higher-level protocol, IPSec does not require specific encryption algorithms. The manufacturers of IPSec products are thus free in their choice of the processes used. The following standards are common:

- **AES – Advanced Encryption Standard**
  AES is the official encryption standard for use by US authorities, and therefore one of the most important standards worldwide. Following a worldwide competition in the year 2000 to find the best of the numerous encryption algorithms, the **N**ational **I**nstitute of **S**tandards and **T**echnology (NIST) selected the Rijndael algorithm (pronounced: "Rinedoll") and declared it as the AES in 2001.

  AES is a symmetric key algorithm with variable block and encryption lengths. It has been developed by the Belgian scientists Joan Daemen and Vincent Rijmen, and features outstanding security, flexibility and efficiency.

- **DES – Data Encryption Standard**
  DES was developed by IBM for the NSA (National Security Agency) in the early 1970s and was the worldwide security standard for years. The key length of this symmetrical process is 56 bits. Today, it is considered to be insecure due to its short key length and in the year 2000 the NIST replaced it with the AES (Rijndael algorithm). It is no longer suitable for use.
- **Triple DES** (a.k.a. 3-DES)
  A further development of DES. The conventional DES algorithm is applied three times consecutively. Two or three different keys, each with a length of 56 bits are used. The key for the first run is reused for the third DES run. The result is a nominal key length of 168 bit, with an effective key length of 112 bits.

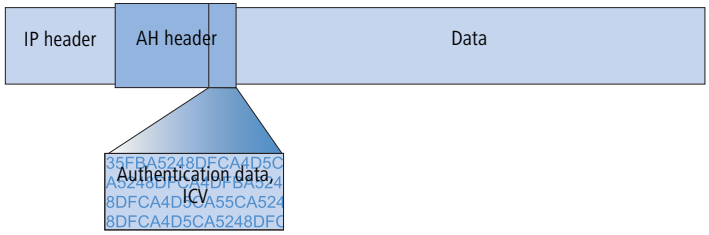
  Triple-DES combines the sophisticated DES technology with a sufficiently long key and is therefore considered to be highly secure. Triple-DES is slower than other processes, however.
- **Blowfish**
  This development by the renowned cryptographer Bruce Schneier is a symmetrical encryption process. Blowfish achieves outstanding data throughput on multifunction processors. The process is reputed to be extremely efficient and secure.
- **CAST** (from the authors **C**arlisle **A**dams and **S**tafford **T**avares)
  is a symmetrical process with a key length of 128 bits. CAST permits the modification of parts of the algorithm at runtime.

The encryption settings can be modified in the expert configuration within LANconfig. Modifications of this sort are generally only required when setting up VPN connections between devices from different manufacturers. LANCOM gateways offer the encryption as standard either after AES (128 bit), Blowfish (128 bit) or Triple-DES (168 bit).

10.11.4Authentication – the AH protocol

The AH protocol (**A**uthentification **H**eader) guarantees the integrity and authenticity of the data. Integrity is frequently regarded as a component of authenticity. In the following, we will consider integrity to be a separate problem that is resolved by AH. In addition to integrity and authenticity, AH also provides effective protection against the replay of received packets (Replay Protection).

AH adds its own header to IP packets immediately after the original IP header. The most important part of this AH header is a field containing authentication data, often referred to as the **I**ntegrity **C**heck **V**alue (ICV).



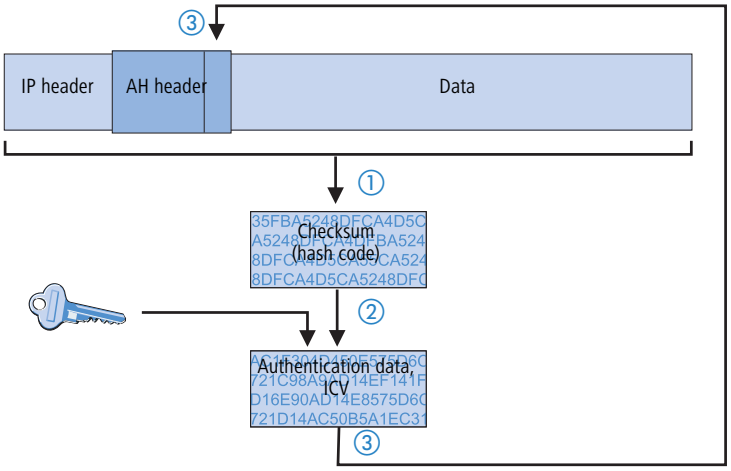
The AH process in the sender

In the sender, the authentication data is generated in 3 steps.

① A checksum is calculated for the complete package using a hash algorithm.

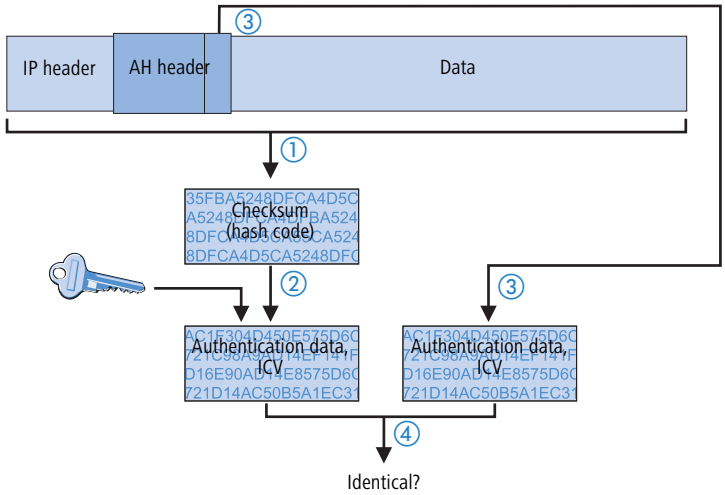
② This checksum is once again sent through a hash algorithm together with a key known to both the sender and the recipient.

③ This results in the required authentication data which is inserted in the AH header.



Checking of integrity and authenticity by the recipient

The AH protocol works in a very similar manner at the recipient's end. The recipient also uses his key to calculate the authentication data for the received packet. The comparison with the sent ICV of the packet determines the integrity and authenticity of the packet.



Determining the checksum for the integrity check

AH adds a checksum to each packet before it is sent to guarantee the integrity of the transferred packets. At the recipients end, AH checks whether the checksum and the contents of the package match. If this is not the case, the packet was either incorrectly transferred or deliberately manipulated. Such packets are discarded immediately and are not forwarded to higher protocol levels.

A variety of so-called hash algorithms are available to determine the checksum. Hash algorithms are distinguished by the fact that their results (the hash code) are a unique fingerprint of the original data. Conversely, the original data cannot be determined on the basis of the hash code. In addition, minimum changes of the input value entail a completely different hash code with a high-grade hash algorithm. Systematic analyses of several hash codes thus are made more difficult.

LANCOM VPN supports the two most common hash algorithms: MD5 and SHA-1. Both methods work without keys, i.e. on the basis of fixed algorithms. Keys do not play a role until a later step of AH: the final generation of the authentication data. The integrity checksum is only a necessary intermediate result on the way there.

Generation of the authentication data

In the second step, AH generates a new hash code using the checksum and a key, the final authentication data. A variety of standards are available under IPSec for this process as well. LANCOM VPN supports HMAC (**H**ash-based **M**essage **A**uthentication **C**ode). The hash functions MD5 and SHA-1 are available as hash algorithms. The HMAC versions are accordingly known as HMAC-MD5-96 and HMAC-SHA-1-96.

This clarifies why AH leaves the packet itself unencrypted. Only the checksum of the packet and the local key are added to the packet together with the ICV, the authentication data, in encrypted form as a verification criterion.

Replay protection – protection against replayed packets

In addition to the ICV, AH assigns a unique sequence number to each packet. The recipient can thus recognize which packets were intercepted by a third party and resent. Attacks of this type are known as "packet replay".

AH does not cater for the masking of IPSec tunnels unless additional measures, such as NAT-Traversal or an outer Layer-2-Tunneling (e.g. PPPT/L2TP), are used that offer "changeable" IP headers.

10.11.5Key management – IKE

The **I**nternet **K**ey **E**xchange Protocol (IKE) permits the integration of subprotocols for managing the SAs and for key administration.

Within IKE, two subprotocols are used in LANCOM VPN: Oakley for the authentication of partners and key administration, and ISAKMP for managing the SAs.

Setting up the SAs with ISAKMP/Oakley

Establishing an SA involves a sequence of steps (with dynamic Internet connections, these steps follow the exchange of the public IP addresses):

① The initiator sends a plain-text message to the remote station via ISAKMP with the request to set up an SA and with proposals for the security parameters of the SA.

② The remote station replies with the acceptance of a proposal.

③ Both devices now generate key pairs, each consisting of a public and private key, for Diffie-Hellman encryption.

④ In two further messages, the devices exchange their public keys for Diffie-Hellman. The further communication is encrypted with Diffie-Hellman.

⑤ Both ends use numbers that have been transferred (with the Diffie-Hellman method) and the Shared Secret to generate a common secret key that is used to encrypt the subsequent communication. Both sides additionally authenticate their Shared Secrets by using hash codes. Phase 1 of the SA setup is thus completed.

⑥ Phase 2 is based on the encrypted and authenticated connection established in Phase 1. In Phase 2, the session keys for the authentication and symmetrical encryption of the actual data transfer are generated at random and transferred.

Symmetrical processes are used for the encryption of the actual data transfer. Asymmetrical processes (also known as public-key encryption) are more secure as they do not require the exchange of secret keys. However, they require considerable processing resources and are thus significantly slower than symmetrical processes. In practice, public-key encryption is generally only used for the exchange of key material. The actual data encryption is then performed using the fast symmetrical process.

The regular exchange of new keys

ISAKMP ensures that new key material is regularly exchanged between the two devices during the SA. This takes place automatically and can be checked using the 'Lifetime' setting in the advanced configuration of LANconfig.

11 Virtual LANs (VLANs)

11.1 What is a Virtual LAN?

The increasing availability of inexpensive layer 2 switches enables the setup of LANs much larger than in the past. Until now, smaller parts of a network had been combined with hubs. These individual segments (collision domains) had been united via routers to larger sections. Since a router represents always a border between two LANs, several LANs with own IP address ranges arose by this structure.

By using switches, it is possible to combine much more stations to one large LAN. By the specific control of data on the individual ports, the available bandwidth can be utilized much better than by using hubs, and the configuration and maintenance of routers within the network can omitted.

But also a network structure based on switches has disadvantages:

- Broadcasts are sent like hubs over the entire LAN, even if the respective data packets are only important for a certain segment of the LAN. A sufficient number of network stations can thus lead to a clear reduction of the available bandwidth in the LAN.
- The entire data traffic on the physical LAN is "public". Even if single segments are using different IP address ranges, each station of the LAN is theoretically able to tap data traffic from all logical networks on the Ethernet segment. The protection of individual LAN segments with Firewalls or routers increases again the requirements to network administration.

One possibility to resolve these problems are virtual LANs (VLANs), as described in IEEE 802.1p/q. By this concept, several virtual LANs are defined on a physical LAN, which do not obstruct each other, and which also do not receive or tap data traffic of the respective other VLANs on the physical Ethernet segment.

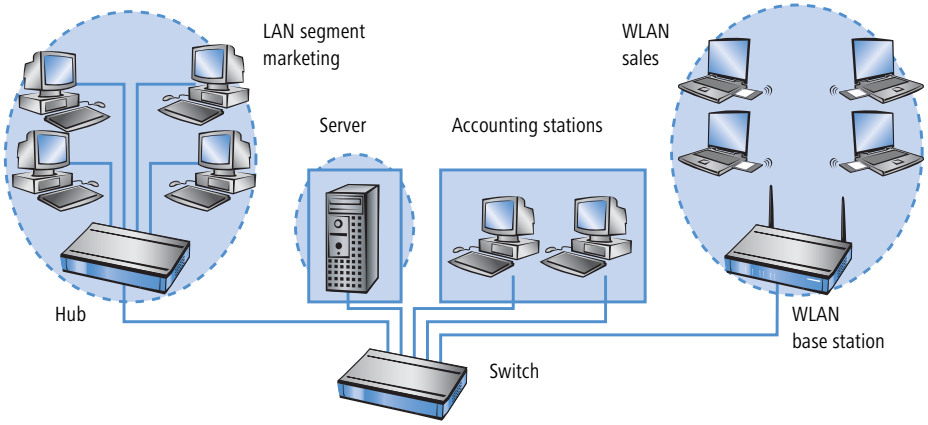
11.2 This is how a VLAN works

By defining VLANs on a LAN the following goals should be achieved:

- Data traffic of certain logical units should be shielded against other network users.
- Broadcast traffic should also be reduced to logical units, not bearing a burden on the entire LAN.
- Data traffic of certain logical units should be transmitted with a specific priority compared to other network users.

An example to clarify: A switch is connected to a hub within a LAN, which connects four stations from the marketing department to the network. One server and two stations of the accounting department are directly connected to the switch. The last section is the base station of a wireless network, where four WLAN clients reside from the sales department.

The stations from marketing and sales should be able to communicate with each other. Additionally, they should be able to access the server. The accounting department needs also access to the server, but should otherwise be shielded against the other stations.



11.2.1 Frame tagging

In order to shield or, if necessary, to priorities data traffic of a virtual LAN against the other network users, data packets must have an additional feature (a "tag"). That's why the respective process is also called "frame tagging".

Frame tagging must be realized such that the following requirements are fulfilled:

- Data packets with and without frame tagging must be able to exist in parallel on a physical LAN.
- Stations and switches in a LAN, which do not support VLAN technology, must ignore the data packets with frame tagging and/or treat them as "normal" data packets.

The tagging is realized by an additional field within the MAC frame. This field contains two important information for the virtual LAN:

- **VLAN ID**: A unique number describes the virtual LAN. This ID defines the belonging of data packets a logical (virtual) LAN. With this 12 bit value it is possible to define up to 4094 different VLANs (VLAN IDs "0" and "4095" are reserved resp. inadmissible).

VLAN ID "1" is used by many devices as the Default VLAN ID. Concerning unconfigured devices, all ports belong to this Default VLAN. However, this assignment can also be changed by configuration. ('The port table' → page 331).

- **Priority**: The priority of a VLAN-tagged data packet is indicated by a 3 bit value. "0" represents the lowest priority, "7" the highest one. Data packets without VLAN tag are treated with priority "0".

This additional field makes the MAC frames longer than actually allowed. These "overlong" packets can only be recognized and evaluated by VLAN-capable stations and switches. Frame tagging incidentally leads to the desired behavior for network users without VLAN support:

- Switches without VLAN support simply pass on these data packets and ignore the additional fields within the MAC frame.

- Stations without VLAN support are not able to recognize the protocol type due to the inserted VLAN tag and discard the packets silently.

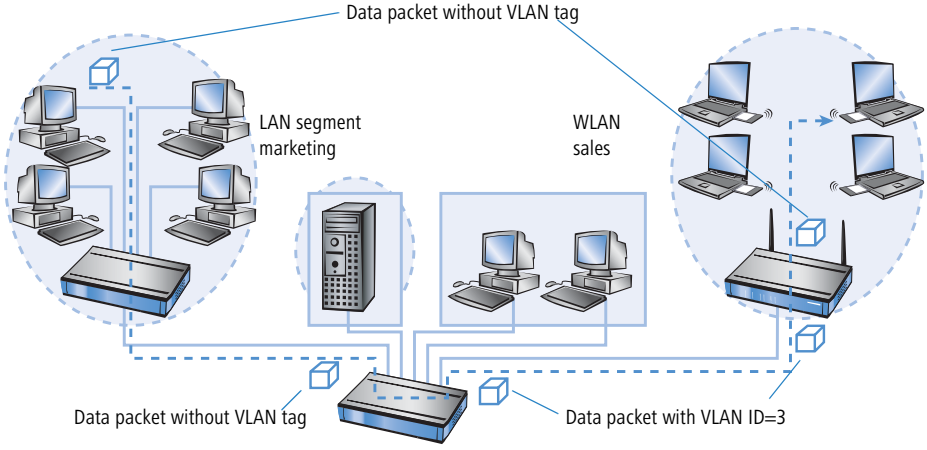
Older switches in the LAN are perhaps not able to pass on correctly the overlong frames between the individual ports and will reject the tagged packets.

11.2.2 Conversion within the LAN interconnection

Certain stations shall be grouped to logical units by virtual LANs. But the stations themselves are usually neither able to generate the required VLAN tags, nor able to handle them.

Data traffic between network users always runs over different interfaces of the distributors in the LAN. These distributors (switches, base stations) have got the task to insert VLAN tags according to the desired application into the data packets, to evaluate them and, if necessary, to remove them again. Because logical units are each connected to different interfaces of the distributors, the rules for generating and processing of the VLAN tags are assigned to the single interfaces.

Coming back again to the first example:



A workstation from the marketing sends a data packet to a workstation of the sales department. The marketing hub passes the packet simply on to the switch. The switch receives the packet at its port no. 1, and recognizes that this port belongs to a VLAN with the VLAN ID "3". It inserts an additional field into the MAC frame with the appropriate VLAN tag, and issues the packet only on ports (2 and 5), which also belong to VLAN 3. The base station of the sales department will receive the packet on its LAN interface. By its settings, the base station can recognize that the WLAN interface belongs also to VLAN 3. It will remove the VLAN tag from the MAC frame, and issues the packet again on the wireless interface. The WLAN client can handle the packet then, which has a "usual" length again, like each other data packet without VLAN tagging.

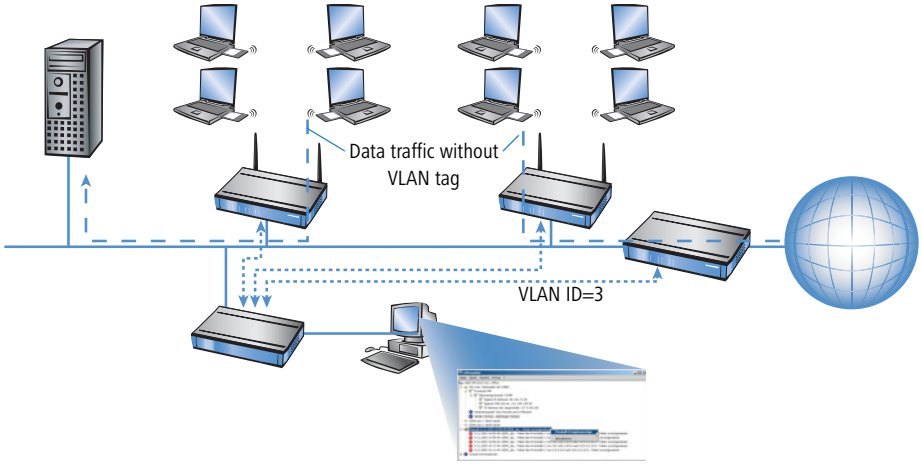
11.2.3 Application examples

Main application of virtual LANs is to install different logical networks on a physical Ethernet segment, whose data traffic is protected against the other logical networks.

The following sections present examples for the operation of virtual LANs on behalf of this background.

Management and user traffic on a LAN

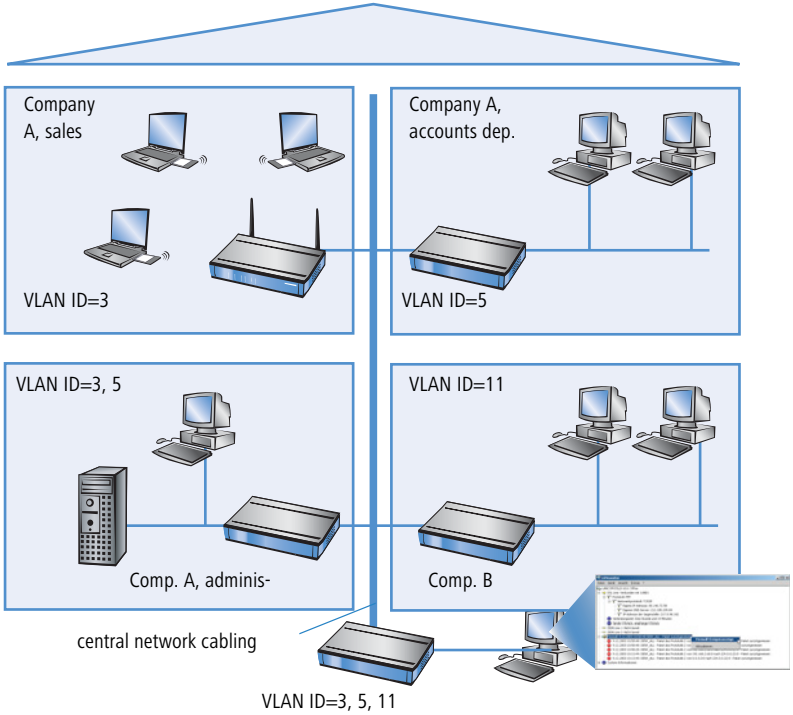
Several hot spots are installed on an university campus, so that students equipped with notebooks and WLAN cards have access to the Internet and to the server of the library. The hot spots are connected to the university LAN. Via this LAN the administrators also access the base stations to carry out several management tasks via SNMP.



By setting up a virtual LAN between the base stations and the administrator's switch, management data is shielded against all "public" traffic on the LAN.

Different organizations on one LAN

The flexibility of the modern world of work raises new challenges for administrators concerning planning and maintenance of network structures. The occupation of the rooms by leaseholders changes permanently in public office buildings, and also inside of a company, teams are often newly assembled. In both cases, the individual units must have an independent, protected LAN. But this task is very burdensome to realize by hardware changes, or even not at all, because e.g. only one single central cabling exists in the office building.



Virtual LANs enable to perform this task in a very smart way. Also when departments or companies change at a later time inside of the building, the network structure can be easily adjusted.

All network users in this example use the central Ethernet, which is, like the connected devices, supervised by a service provider. Company A has three departments on two floors. The sales department can communicate with the administration department via VLAN ID 3, the accounts department with the administration via VLAN ID 5. The networks of accounts department and sales do not see each other. Company B is also shielded by VLAN ID 11 against all other networks, only the service provider can access all devices for maintenance purposes.

11.3 Configuration of VLANs

VLAN technology functions are presently only supported by LANCOM Wireless devices.

The configuration of LANCOM Wireless devices within the VLAN realm has to perform two important tasks:

- Defining virtual LANs and assigning them a name, a VLAN ID and the affected interfaces.
- Defining for the interfaces how to proceed with data packets with or without VLAN tags.

11.3.1 The network table

In the network table are those virtual LANs defined, in which the LANCOM should participate. The table contains 32 entries at maximum with the following information:

- **Name**: The VLAN name serves only as a description during configuration. This name is used at no other place.
- **VLAN ID**: This number marks the VLAN unambiguously. Possible values range from 1 to 4094.
- **Port list**: All LANCOM interfaces belonging to the VLAN are entered into this list. As ports can be entered:
  - "LAN-n" for all Ethernet ports of the device.
  - "WLAN-n" for point-to-station WLAN ports.
  - "P2P-n" for point-to-point WLAN ports.

  Given a device with a LAN interface and a WLAN port, e.g. ports "LAN-1" and "WLAN-1" can be entered. In case of port ranges, the individual ports must be separated by a tilde: "P2P-1~P2P-4".

The available ports can be found in the port table (→ Seite 331).

Example for a network table:

Name	VLAN ID	Port list
Default	1	LAN-1, WLAN-1, WLAN-2
Sales	2	LAN-1, WLAN-1
Marketing	3	LAN-1, WLAN-2

11.3.2 The port table

The port table configures the individual ports of the device for use by the VLAN. The table has got an entry for each port of the device with the following values:

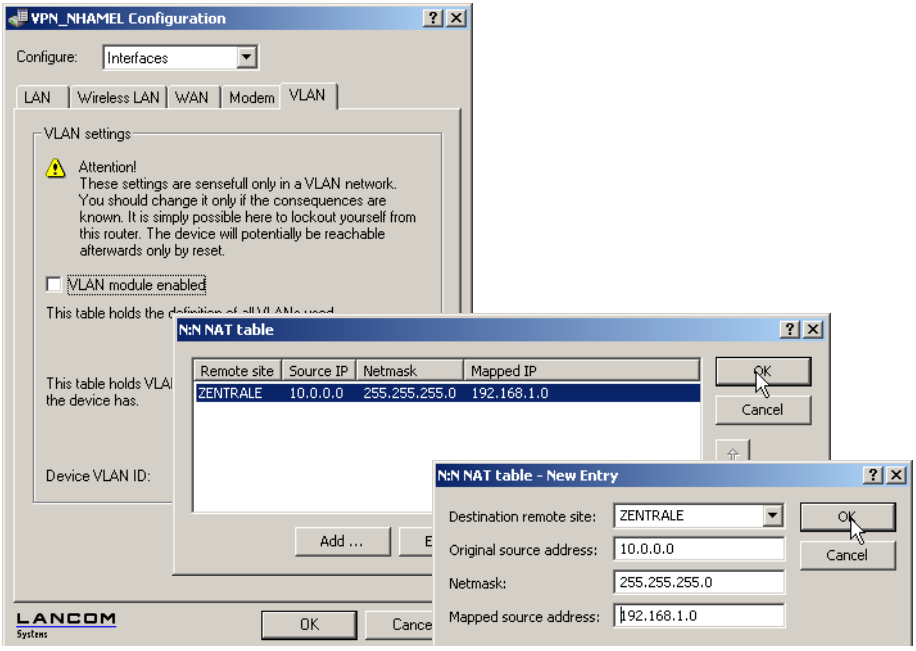
- **Port**: Name of the port, not editable.
- **Use tagging**: This option indicates, whether data packets should be tagged on this port. The tagging refers only to data packets **sent** over this port.
- **Allow untagged frames**: This option indicates, whether untagged data packets are passed on, which have been **received** on this port.
- **Allow all VLANs**: This option indicates, if tagged data packets with any VLAN IDs should be accepted even if the port itself is not belonging to the same VLAN ID.
- **Default ID**: This VLAN ID has two functions:
  - Untagged packets received on this port are provided with this VLAN ID.
  - If tagging for sent packets is switched on, this VLAN ID will **not** be assigned to the packets. If a packet with this VLAN ID is received, it will be passed on **without** this ID, although tagging has been switched on.

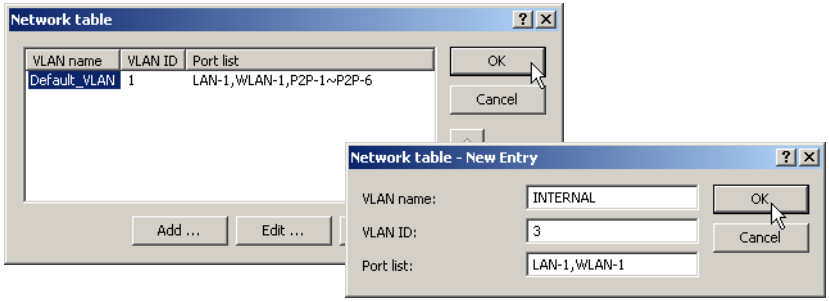
Example for a port table:

Port	Use tagging	Allow untagged frames	Allow all VLANs	Default ID
LAN-1	On	On	On	1
WLAN-1	Off	On	Off	1
WLAN-2	Off	On	Off	1
P2P-1	Off	On	Off	1
P2P-2	Off	On	Off	1
P2P-3	Off	On	Off	1
P2P-4	Off	On	Off	1
P2P-5	Off	On	Off	1
P2P-6	Off	On	Off	1

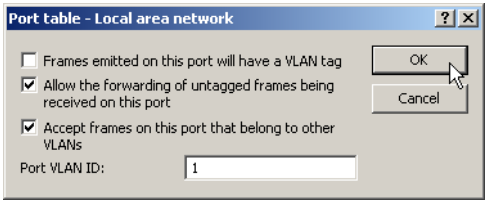
11.3.3 Configuration with LANconfig

Parameters for virtual networks can be set with LANconfig under 'Interfaces' on the register card 'VLAN'. The definition of the used virtual networks can be accessed via the button **VLAN table**:





The button **Port table** opens a drop down list where a VLAN port can be selected for editing:



11.3.4 Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet the tables for configuring the VLANs can be found via the following paths:

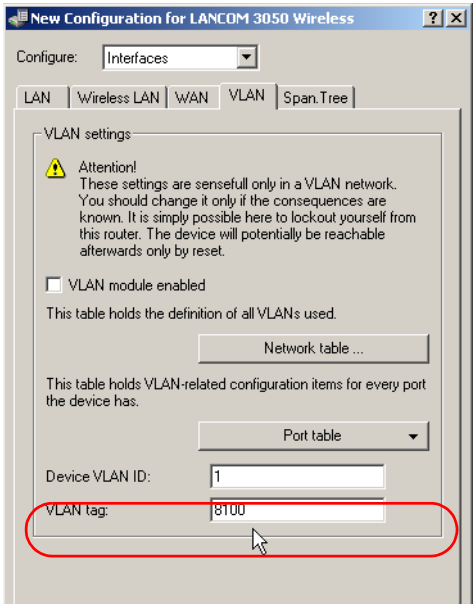
Configuration tool	Menu/table
WEBconfig	Expert Configuration ▶ Setup ▶ LAN Management ▶ VLAN Configuration
Terminal/Telnet	`cd /Setup/LAN Management/VLAN Configuration`

The VLAN configuration shows up under WEBconfig as follows

:

11.4 Configurable VLAN Protocol ID

When transmitting VLAN tagged networks via provider networks that use VLAN themselves, providers sometimes use special VLAN tagging IDs. In order to set VLAN transmission on the LANCOM to accommodate this, the Ethernet2 type of the VLAN tag can be set as a 16-bit hexadecimal value as 'tag value' under `Setup/LAN Bridge/VLAN` or in LANconfig in the configuration area under 'Interfaces' using the 'VLAN' tab in the field 'VLAN tag'. The default is '8100' (802.1p/q VLAN tagging) other typical values for VLAN tagging could be '9100' or '9901'.



11.5 Configurable VLAN IDs

11.5.1 Different VLAN IDs per WLAN client

VLANs are usually connected to a LAN interface on the LANCOM. Therefore, all packets that pass through this interface receive the same VLAN ID when the VLAN module is enabled. However, in some cases, administrators will want to assign different WLAN users to different VLANs.

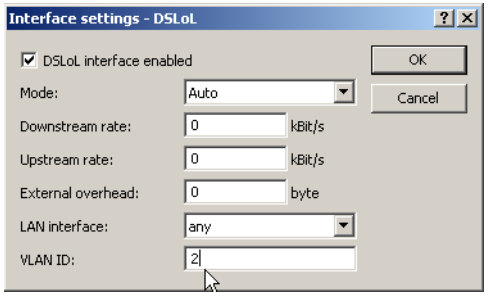
This can be accomplished by assigning a special VLAN ID to each MAC address under `Setup/WLAN/Access List`. The client-specific VLAN ID can take on values from 0 to 4094. The default value of '0' stands for an unspecified VLAN ID. In such a case, the client will be assigned to the VLAN port of the logical WLAN.

The following requirements must be met in order to ensure successful client-specific VLAN assignment:

- VLAN operation must be enabled.
- The VLAN IDs that are to be assigned to the individual clients must be included in the VLAN network table.
- The LAN interfaces and all WLAN interfaces that are used by the clients must be assigned to the corresponding VLAN.

11.5.2 Special VLAN ID for DSLoL interfaces

In order to better separate the data traffic on a DLSoL interface from other traffic, 'VLAN ID' can be set up for the DSLoL interface under `Setup/Interfaces/DSLoL` or in LANconfig in the configuration area 'Interfaces' using the 'WAN' tab under the interface settings for the DSLoL interface.



11.6 VLAN tags on layer 2/3 in the Ethernet

VLAN tags enable a simple form of QoS control even when using switches that cannot evaluate IP headers. Der Standard IEEE 802.1p definiert ein Prioritäts-Tag im VLAN-Header mit einer Länge von drei Bit, das den ersten drei Bit des DSCP-Felder (Differentiated Services Code Point – DiffServ) bzw. der Precedence im TOS-Feld (Type of Service) entspricht. The processing of VLAN tagged packets requires that packets in the receive direction are regarded differently to packets in the send direction.

- Upon receipt of a tagged Ethernet packet, it may be processed in one of three ways:

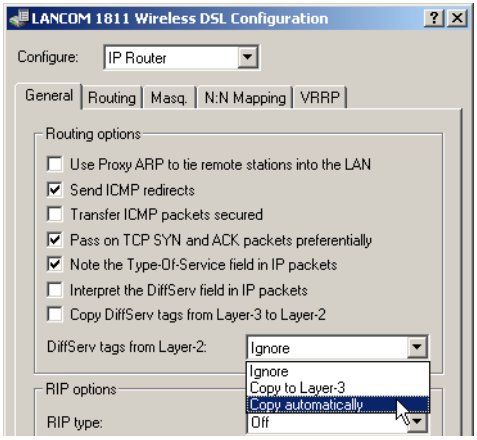
- □ The VLAN tag is ignored.
- □ The VLAN tag is always copied to the DiffServ or TOS field.
- □ The VLAN tag is copied to the DiffServ or TOS field if this is not marked already, i.e. the precedence is '000'.

■ When a packet is transmitted over Ethernet, the VLAN tag can be set depending on the precedence. This should only happen if the recipient of the tag can understand it, i.e. tagged packets can be received. Tags are thus only set for packets which are sent to addresses from which the LANCOM already received tagged packets.

When a tagged packet is received, the tag is saved to the associated entry in the connection list. If a packet is to be sent with a precedence setting, then the VLAN ID recorded earlier is entered into the packet together with the precedence to form a VLAN tag. Where a connection causes other connections to be opened, e.g. with FTP or H.323, then the tag is inherited to the new entries.

11.6.1 Configuring VLAN tagging on layer 2/3

Configuring VLAN tagging on layer 2/3 involves the definition of the general routing settings and the behavior upon receipt and transmission of tagged packets.



Configuration tool	Call
LANconfig	IP Router ▶ General
WEBconfig, Telnet	Expert Configuration > Setup > IP-Router > Routing-Method

■ **Routing method**

- □ Normal: TOS/DiffServ field is ignored.
- □ Type-Of-Service: The TOS/DiffServ field is regarded as a TOS field; the bits 'low delay' and 'high reliability' will be evaluated.

- DiffServ: The TOS/DiffServ field is regarded as a DiffServ field. After evaluating the precedence, packets with the code points 'AFxx' are saved and packets with the code points 'EF' receive preferential treatment. All other packets are transmitted as normal.

■ **Layer2-Layer3 tagging**

The setting for Layer2-Layer3 tagging regulates the behavior when a data packet is received.

- Off: VLAN tags are ignored.
- On: Priority bits in the VLAN tag are always copied to the precedence of the DSCP.
- Automatic: Priority bits in the VLAN tag are only copied to the DSCP precedence if this is '000'.

■ **Layer2-Layer3 tagging**

The setting for Layer3-Layer2 tagging regulates the behavior when a data packet is transmitted.

- Off: VLAN tags are not generated.
- On: VLAN tags with priority bits originating from the DSCP precedence will be generated if the recipient has sent at least one tagged packet.

11.7

12 Wireless LAN – WLAN

12.1 What is a Wireless LAN?

The following sections are a general description of the LCOS operating system functions in wireless networks. The precise functions supported by your device are described in its manual.

In this chapter we will show you briefly the technology of wireless networks. In addition, we give you an overview of the various applications, functions and abilities of your LANCOM Access Points and WLAN Router.

A Wireless LAN connects single terminals (e.g. PCs or notebooks) to a local network (also LAN – **L**ocal **A**rea **N**etwork). In contrast to a conventional LAN, communication takes place via radio links rather than via network cables. This is the reason why a Wireless LAN is also called a **W**ireless **L**ocal **A**rea **N**etwork (WLAN).

All functions of a cable-bound network are also available in a Wireless LAN: access to files, servers, printers etc. is as possible as the connection of individual stations to an internal mail system or to the Internet access.

The advantages of Wireless LANs are obvious: notebooks and PCs can be set up just where they are needed. Due to Wireless LANs, problems with missing connections or structural alterations belong to the past.

12.1.1 Standardized radio transmission by IEEE

IEEE 802.11

LANCOM network products comply with the IEEE 802.11 standards. These standard's family represents an extension to the already existing IEEE standards for LANs, of which IEEE 802.3 for Ethernet is the most popular one. Within the IEEE 802.11 family, different standards exist for the radio transmission in different frequency ranges and with different speeds. LANCOM base stations and AirLancer client adapters support according to their respective type different standards:

- IEEE 802.11a with up to 54 Mbps transfer rate in the 5 GHz band, up to 108 Mbps in turbo mode. (complement to standard)
- IEEE 802.11b with up to 11 Mbps transfer rate in the 2,4 GHz band
- IEEE 802.11g with up to 54 Mbps transfer rate in the 2,4 GHz band, up to 108 Mbps in turbo mode. (complement to standard)

IEEE 802.11a: 54 Mbps

IEEE 802.11a describes the operation of Wireless LANs in the 5 GHz frequency band (5,15 GHz to 5,75 GHz), with up to 54 Mbps maximum transfer rate. The real throughput depends however on the distance and/or on the quality of the connection. With increasing distance and diminishing connecting quality, the transmission rate lowers to 48 Mbps, afterwards to 36 Mbps etc., up to a minimum of 6 Mbps. The distance of transmission ranges from up to 125 m in open expanses, in buildings typically up to 25 m. The IEEE 802.11a standard uses OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) as modulation scheme.

OFDM

In the 5 GHz frequency band, the OFDM modulation scheme is used for IEEE 802.11a. OFDM is a modulation scheme, which utilizes multiple independent carrier frequencies for the signal transmission, and which modulates these mul-

tiple carriers each with a reduced data transfer rate. Thus the OFDM modulation scheme is very insensitive in particular to echoes and other impairments and enables high data transfer rates.

Turbo mode

In 'turbo mode', LANCOM Wireless base stations are able to use simultaneously two radio channels and can so increase the transfer rate up to maximum 108 Mbps. The turbo mode can be used in conjunction with the IEEE 802.11a standard between LANCOM base stations and AirLancer wireless network cards. The increase of the transfer rate must be switched on in the base station, but can also reduce the transmitting power and the range of the radio connection.

IEEE 802.11b: 11 Mbps

IIEEE 802.11b describes the operation of local Wireless LANs in the ISM frequency band (**I**ndustrial, **S**cientific, **M**edical: 2.4 up to 2.483 GHz). The maximum transfer rate is up to 11 Mbps. The real through-put depends however on the distance and/or on the quality of the connection. With increasing distance and diminishing connecting quality the transmission rate lowers to 5,5 Mbps, afterwards to 2 and finally to 1 Mbps. The range of the transmission distances is between up to 150 m in open expanses and in buildings typically up to 30 m. Due to different frequency bands in use, IEEE 802.11b is not compatible to IEEE 802.11a.

DSSS

For shielding against interferences by other transmitters, which have possibly the same frequency band, the DSSS procedure (**D**irect **S**equence **S**pread **S**pectrum) is used for IEEE 802.11b in the 2,4 GHz frequency band. A transmitter normally uses only a very narrow range of the available frequency band for transmission. If exactly this range is used by another transmitter, interferences in transmission would be the result. With the DSSS procedure the transmitter uses a broader spread of the possible frequencies and becomes more insensitive to narrow-band disturbances then. This procedure is also used in military range for increasing tap-proof security.

IEEE 802.11g: 54 Mbps

The IEEE 802.11g standard works likewise with up to 54 Mbps data transmission rate in the 2,4 GHz ISM-frequency band. Contrary to IEEE 802.11b, the OFDM modulation is used for IEEE 802.11g, like already introduced for IEEE 802.11a. IEEE 802.11g contains a special compatibility mode that ensures a downward compatibility to the popular IEEE 802.11b standard . However, in this compatibility mode you encounter reduced transmission speeds. Due to the different frequency bands, IEEE 802.11g can not be compatible to IEEE 802.11a. The transmission distances of IEEE 802.11g products are comparable with those of IEEE 802.11b products.

Turbo mode

With the 802.11g standard in 'turbo mode' the transfer rate can be increased to a maximum of 108 Mbps, by using two radio channels. But as a 2.4 GHz band uses less channels than the 5 GHz band, the turbo mode limits in this case the options of channels.

Transfer rates

The indicated transfer rates are always to be interpreted as gross data rates, i.e. the entire protocol overhead - as for example the complex protocols to secure the radio transmission - is included in the indicated transfer rates. The net data transfer rate can be thus lower than the indicated gross data rates, typically over up to the half for all IEEE 802.11 standards mentioned above.

Ranges

The actually obtained distances for radio transfers depend strongly on the individual environment. In particular influences of noise and obstacles have an effect on the range. Decisive is an optimal placement of the radio stations (both network adapters and base stations). For further increase of the transfer distance, we recommend the operation with additional antennas (e.g. AirLancer Extender).

IEEE standards

In order to guarantee a maximum of compatibility, LANCOM Systems Systems fully complies with the industry standards of the IEEE[1] described in the preceding paragraph. For this reason, your LANCOM base station operates without problems and with reliably also with devices of other manufacturers.

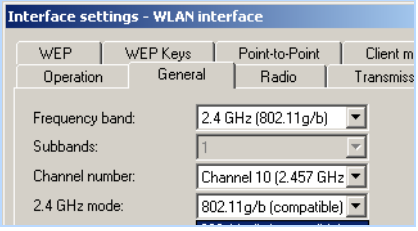
Your LANCOM base station supports - according to the model type - the standards IEEE 802.11g (downward-compatible to IEEE 802.11b), and/or IEEE 802.11a.

The operation of the integrated wireless card of your base station is only possible in one single frequency band, that is, either 2,4 GHz or 5 GHz. Thus a simultaneous operation of IEEE 802.11g and IEEE 802.11a is not possible. Since IEEE 802.11g is downward-compatible to IEEE 802.11b, an simultaneous operating of these two standards is possible, but with certain speed constraints.

Transfer rates in compatibility mode

Please notice that the reached data transfer rates depend on the used 2,4 GHz mode. You will achieve the highest transfer rates with a base station operating in the 802.11g mode. The transfer rate will go down when starting the compatibility mode, even, if only inactivated 802.11b stations are near to your base station. When these 802.11b stations start to be activated in a wireless network with operating compatibility mode, the actual transfer rate will fall again.

That's why you should only activate the compatibility mode, when you have really operating 802.11b and 802.11g stations in your wireless network.



Please notice that not all frequencies are permitted in each country! You will find a table with the allotted frequencies and the permission regulations in the appendix.

12.1.2 Operation modes of Wireless LANs and base stations

Wireless LAN technology and base stations in Wireless LANs are used in the following operation modes:

- Simple direct connections between terminals without base station (ad-hoc mode, only with 2.4 GHz)
- Larger Wireless LANs, connection to LANs with one or more base stations (infrastructure network)
- Connecting two LANs via a direct radio link (point-to-point mode, point-to-multipoint)

1. **I**nstitute of **E**lectrical and **E**lectronic **E**ngineers – International association, which established i.a. numerous technology standards.

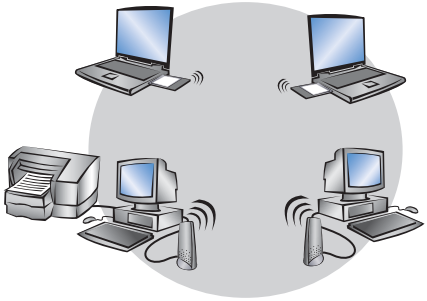
- Connecting of devices with Ethernet interface via base stations (client mode)
- Extending an existing Ethernet network with WLAN (bridge mode)
- Multiple radio cells with one access point (Multi-SSID)

The ad-hoc mode

When two terminals are equipped with compatible wireless interfaces, they both can communicate directly via radio. This simplest use is the so-called ad-hoc mode.

Only in IEEE 802.11b or IEEE 802.11g standard

In ad-hoc networks you connect two or more PCs with own wireless interfaces directly together for building a Wireless LAN.



This operation mode is generally called peer-to-peer network (spontaneous network). PCs can immediately get in touch and exchange data.

The infrastructure network

By use of one or more base stations (also called access point), a Wireless LAN becomes more comfortable and more efficient. A Wireless LAN with one or more base stations is referred to as an infrastructure network in Wireless LAN terminology.

In some devices the access point is built in, so called WLAN router.

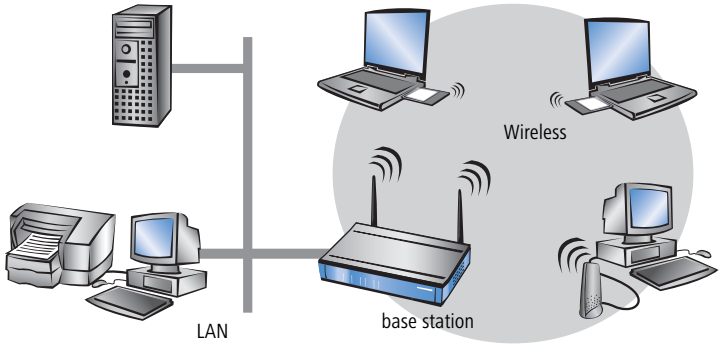
Interesting applications arise for the Wireless LAN from the LAN connection of base stations:

- Connecting the Wireless LAN to an existing LAN
- Extending the coverage of a Wireless LAN

Additionally, the use of a base station enables a central administration of the Wireless LAN.

Connection to an existing LAN

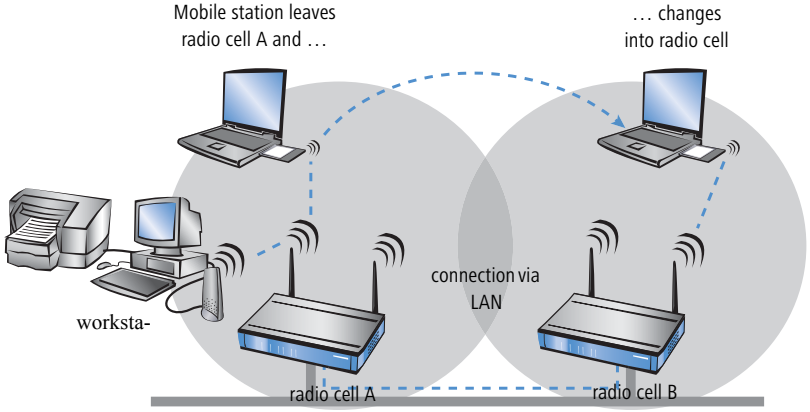
An infrastructure network is ideally suitable as an extension to existing wired LANs. For extension of a LAN in areas, where a wiring is not possible or uneconomical, the infrastructure network represents an ideal alternative.



Larger extension by roaming function

The area, in which mobile stations can get in touch with a base station, is called radio cell.

If the range of a radio cell is not sufficient any longer to serve all mobile stations of a wireless network, several base stations can be brought in action. It is possible to change from a radio cell into another one without interruption of the network connection. The transmission of roaming information and data between the base stations is enabled by the wired LAN connection.



In the example above, the roaming function of the mobile station enables the access to the workstation in radio cell A also after changing into radio cell B. After the radio cell change, the base station in radio cell B passes on the data of the mobile station via LAN to the base station in radio cell A. From there, they arrive via radio at the workstation in radio cell A. In this way, the connection between both devices remains existing at any time.

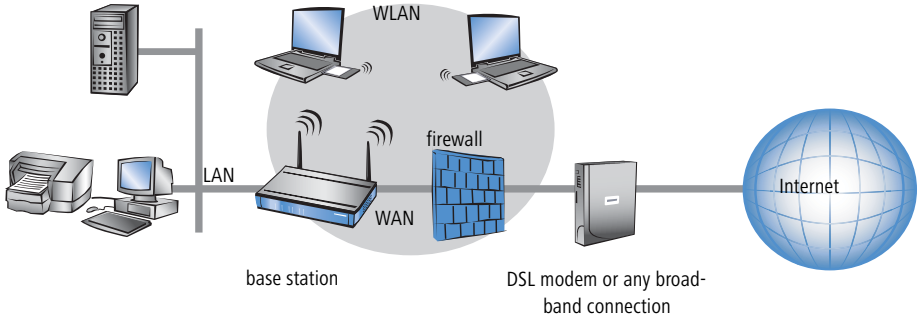
A Wireless LAN can consist of as many as desired radio cells. Thus the extension of a Wireless LAN is unlimited.

Base station as router

The LANCOM Wireless base station possesses a WAN connector for all current broadband modems with cable-bound Ethernet connection (DSL or cable modem). In this operation mode, the base station offers all functions of a complete

IP and IPX router as well. The base station serves in this connection variant as gateway to the Internet. The router checks for all received data packets whether they need to be transferred to another network or workstation. The router itself establishes the connections as required.

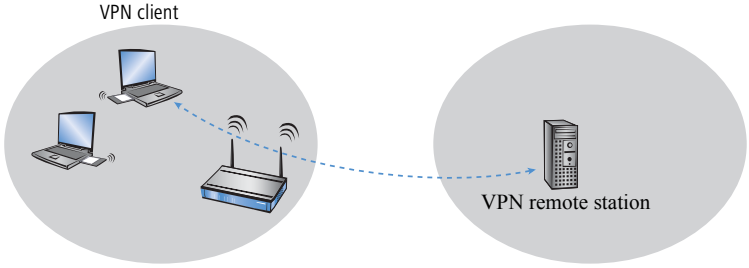
The integrated Stateful Inspection Firewall prevents effectively the penetration of undesired data traffic into the own network by permitting incoming data only as reaction to outgoing data traffic. For accessing the Internet, the IP masquerading function of the router hides all workstations of the LAN behind a single public IP address. The real identities (IP addresses) of the individual workstations remain concealed. Firewall filters of the router permit specific IP addresses, protocols and ports to be blocked. With MAC address filters it is also possible to specifically control the access of workstations in the LAN to the IP routing function of the device.



VPN pass-through

VPN technology (VPN=Virtual Private Network) is more and more frequently in use to protect sensitive data. The LANCOM Wireless base station is able to route and mask simultaneously the encrypted data between a VPN client of the WLAN and another workstation of the cable-bound LAN. This "passing-through" of VPN encrypted data is called in technical jargon "VPN pass-through". Following are provided:

- PPTP pass through
- IPsec pass through

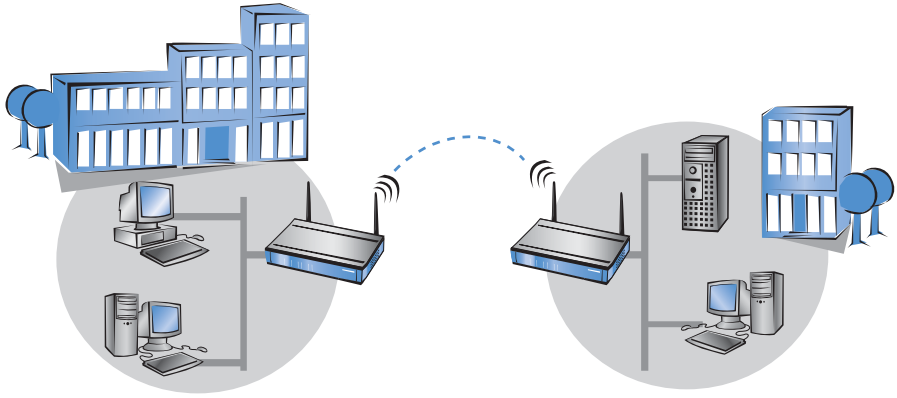


The LANCOM Wireless base stations support VPN pass-through function for multiple stations within a wireless network.

Wireless bridge between two Ethernet segments

With two base stations, two LANs can be connected via a radio link (point-to-point mode). In this so-called bridge mode, all data is transferred automatically to the remote network.

By the use of narrow beam antennas (e.g. AirLancer Extender), also larger distances can be bridged securely. An additional increase of reach can be achieved by use of further base stations, which operate in relay mode between two LAN segments.

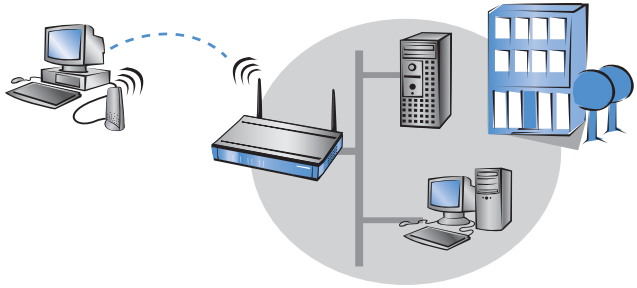


Point-to-multipoint operation

It is possible to couple up to seven remote network segments to an united network by wireless bridges in the so-called P2MP operation (point-to-multipoint) mode.

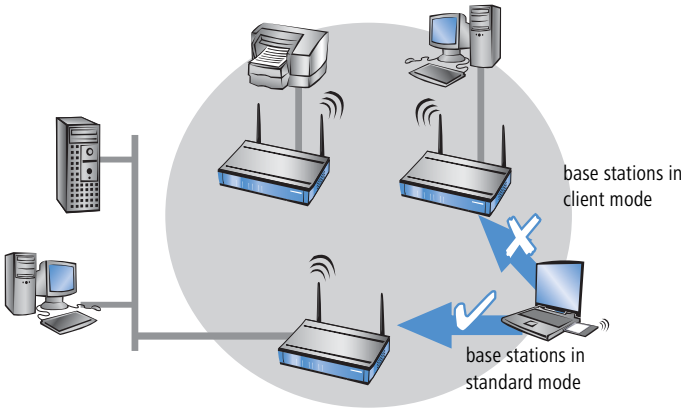
Point-to-station operation

The so-called P2Station operation (point-to-station) connects a single station is to a remote LAN.



Base station in client mode

For binding single devices with Ethernet interfaces to a Wireless LAN, LANCOM Wireless base stations can be put into the so-called client mode, in which they behave like a conventional Wireless LAN adapter and not like a base station. Due to the client mode, it is also possible to integrate devices like PCs or printers having only one Ethernet interface into a Wireless LAN.

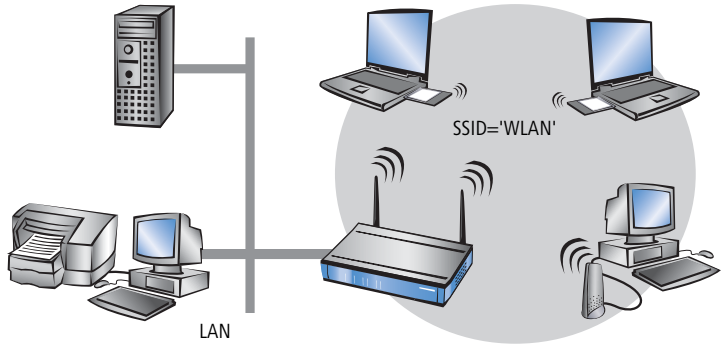


An Access Point in normal mode further clients can log on, but not in client mode.

Multiple radio cells with Multi-SSID

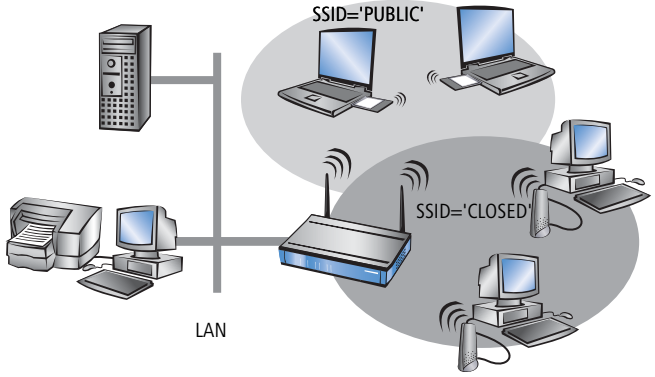
Conventionally, a wireless network card supports exactly one radio cell.

These radio cells are given a network name, known as the 'SSID' (**S**ervice **S**et **Id**entifier), that is entered into the access points and network cards during configuration. Certain settings that apply to the radio cell can be defined under the SSID during the configuration of the access point. The settings include, for example, the data transfer speed and the first WEP key, which is also used as passphrase for encryption with 802.11i and WPA. Those clients that are programmed with the SSID can make use of the radio cell and work with the parameters as defined. The access point treats all clients on an equal basis



In some applications, however, it may be desirable to divide the clients the radio cell into different groups, each of which is treated in a certain way by the access point. It may be necessary, for example, to operate a public wireless network without any encryption simultaneous to a protected, 802.11i-, WPA- or WEP-encrypted wireless network that excludes unauthorized parties.

The Multi-SSID function of the LANCOM access points is ideally suited to scenarios like this. This function enables a physical WLAN interface of an access point to be assigned with more than one SSID. Up to eight different logical radio cells—each with its own SSID—can be supported by a single WLAN interface.



12.2 Development of WLAN security

The WLAN standards WPA and 802.11i are currently redeeming the reputation of WLAN security, an issue which has recently been under attack. The processes incorporated into the original standard proved insufficient in practice. This lack led on the one hand to a series of proprietary extensions of the standard, like "CKIP" from Cisco, or "KeyGuard" from Symbol Technologies, and on the other hand to solutions which offered the required security on higher protocol layers with tools like PPTP or IPSec. All these processes are quite functional, but they introduce limitations, for instance those relative to interoperability or data transmission rates.

In the standard 802.11i released in Summer, 2004, the IEEE Committee has redefined the topic "WLAN and security" from the ground up. The result is a set of standardized methods that enable the construction of secure and manufacturer-independent WLANs in line with current standards.

On the way from the original WEP of the 802.11 standard to 802.11i, a whole series of concepts have arisen that have tended to increase confusion and insecurity among the users. This chapter should help to explain the concepts and the processes used, in chronological order of their development.

12.2.1 Some basic concepts

Even though one constantly hears the blanket term 'Security' when talking about computer networks, it is still important for the coming exposition to differentiate a little more closely between the requirements it actually entails.

Authentication

The first point in security is access security:

- Here, a protective mechanism is involved which allows access to the network only to authorized users.
- On the other hand, however, it must also be ensured that the client is connected to the precise desired access point, and not with some other access point with the same name which has been smuggled in by some nefarious third party. Such an authentication can be provided, for example, using certificates or passwords.

Authenticity

Authenticity: Proof of the authorship of the data and the originality of the data content; the process of establishing this proof is known as authentication.

Integrity

Once access is provided, one would like to ensure that data packets reach the receiver without any falsification, that is, that no-one can change the packets or insert other data into the communication path. The manipulation of data packets themselves cannot be prevented, but changed packets can indeed be identified using suitable checksum processes, and then discarded.

Confidentiality

Quite separate from access security is confidentiality, that is, unauthorized third parties must not be able to read the data traffic. To this end, the data are encrypted. This sort of encryption process is exemplified by DES, AES, RC4, or Blowfish. Along with encryption, of course, there must also be a corresponding decryption on the receiving end, generally with the same key (a so-called symmetric encryption process). The problem naturally then arises, how the sender can give the key to the receiver for the first time—a simple transmission could very easily be read by a third party, who could then easily decrypt the data traffic.

In the simplest case, this problem is left to the user, that is, one simply assumes that the user can make the key known at both ends of the connection. In this case, one speaks of pre-shared keys, or 'PSK'.

More sophisticated processes come into play when the use of pre-shared keys is impractical, for instance in an HTTP connection built over SSL—in this case, the user can't retrieve a key from a remote web server quite so easily. In this case, so-called asymmetric encryption methods such as RSA can be used, that is, to **de**crypt the data, a different key is used than the one used to **en**crypt it, meaning that key pairs are used. Such methods are, however, much slower than symmetric encryption methods, which leads to a two-phase solution:

- The sender possesses an asymmetric key pair. It transmits the public part of the key pair, i.e. the key for **en**cryption, to the receiver as a certificate, for example. Since this part of the key pair cannot be used for **de**cryption, there are no misgivings with regard to security.
- The receiver selects any symmetrical key. This symmetrical key that is used both for **en**cryption and for **de**cryption, must now be securely transmitted to the sender. It is encrypted with the sender's public key and returned to the sender. The only way that the symmetrical key can be decrypted again is with the sender's private key. Potential eavesdroppers observing the key exchange cannot decrypt this information, and consequently the transmission of the symmetrical key is secure.

This method can be used for the safe transmission of symmetrical keys via the Internet. In the following sections, we will see these methods again, sometimes in modified form.

12.2.2 WEP

WEP is an abbreviation for **W**ired **E**quivalent **P**rivacy. The primary goal of WEP is the confidentiality of data. In contrast to signals which are transmitted over cables, radio waves spread out in all directions—even into the street in front of the house and other places where they really aren't desired. The problem of undesired interception is particularly obvious in wireless data transmission, even though it can also arise in larger installations with wired networks—however, access to cables is far more easily restricted than is the case with radio waves.

During the development of the WLAN security standard, the IEEE Committee did not intend to develop a "perfect" encryption method. Such high-security encryption methods are, for instance, required and also used in electronic banking—in this case, however, the applications themselves use high-quality encryption methods, and it would be unnecessary to repeat this effort at the radio transmission level. With the new security standards, only those applications which normally work without encryption in wired LANs should be provided with sufficient security against eavesdropping by unauthorized third parties.

WEP is a symmetrical method of encryption and uses RC4 algorithm as its basic encryption technology, a process already well-known in other areas and considered highly secure. RC4 uses a key between 8 and 2048 bits in length, which is used to generate a pseudo-random series of bytes using a predetermined process. The data packet for encryption is then XOR'd byte by byte with this byte stream. The receiver simply repeats this procedure with the same key and in the same order to produce the original data packet again.

However, RC4 has one serious disadvantage: one may only use a particular RC4 key once for a single packet, as two different packets that have been coded with the same RC4 key potentially provide the basis to reproduce the original data. As it would be impracticable for the user to enter a new code key for every data packet, WEP combines this key with an additional internal key, the initial vector (IV). This is automatically changed from packet to packet.

The IEEE standard originally foresaw a relatively short key length of 40 bits, which was probably oriented towards the then-existing US export restrictions on strong cryptography; this variant in combination with the 24 bits of the IV is usually referred to as WEP64. Most WLAN cards today support a variant in which the user can configure a 104-bit key, which results in a 128 bit long RC4 key—correspondingly, this is often called WEP128. More seldom are key lengths of 128 bits (WEP152) or 232 bits (WEP 256). In principle RC4 can work with key lengths of up to 2048 bits (WEP keys of up to 2024 bits), although in practice key lengths reach a simple limit at which the user can manage to enter the columns of digits without making a mistake.

The IEEE standard specifies that up to four different WEP keys can exist in one WLAN. The sender encodes the number of the WEP key used in the encrypted packet along with the initial vector, so that the receiver can use the appropriate key. The idea behind this was that old keys in a WLAN could gradually be exchanged for new keys, in that stations which had not yet received the new key could still use an old key during a transition period.

One of the chief weakness of WEP is the length of the initial vector, which is far too short. As mentioned previously, the repetition of a key with RC4 presents a significant security loophole which, with a length of just 24 bits, can occur within just a few hours depending on the data rate. Since particular portions of the encrypted data packets can quickly offer conclusive information about the key, an eavesdropper only needs to process a small amount of the data traffic with specialized sniffer tools in order to crack the key. These weaknesses unfortunately degraded WEP to an encryption scheme which at best could be used to protect a home network against 'accidental eavesdroppers.'

12.2.3 WEPplus

As explained in the previous section, the use of 'weak' IV values was the problem which weakened the WEP process most. A first 'quick shot' to secure WLANs against this kind of program was the simple notion that the weak IV values are known, and that they could simply be skipped during encryption—since the IV used is after all transmitted in the packet, this procedure would be completely compatible with WLAN cards which didn't understand this extension, dubbed WEPplus. A true improvement in security would naturally only result once all partners in the WLAN were using this method.

In a network equipped with WEPplus, a potential attacker again has the chore of listening to the entire data traffic, waiting for IV repetitions—simply waiting for the few packets with weak IVs is no longer an option. This raises the bar for an attacker once again. Objectively speaking, WEPplus is a slight improvement--it is suitable for home use, provided that the key of reconfigured often enough. For use in a professional environment, however, this is not sufficient.

12.2.4 EAP and 802.1x

Obviously, an 'add-on' like WEPplus can't eliminate the basic problem of too-short IVs, without changing the format of packets on the WLAN, thus rendering all existing WLAN cards incompatible. There is, however, a possibility of solving several of our problems with one central change: no longer use the formerly fixed WEP key, but to negotiate them dynamically instead. As the process to be used for this purpose, the Extensible Authentication Protocol has emerged. As the name suggests, the original purpose of EAP is authentication, that is, the regulated access to a WLAN—the possibility of installing a valid WEP key for the next session is more or less a byproduct. Figure 2 shows the basic process of a session secured by EAP.

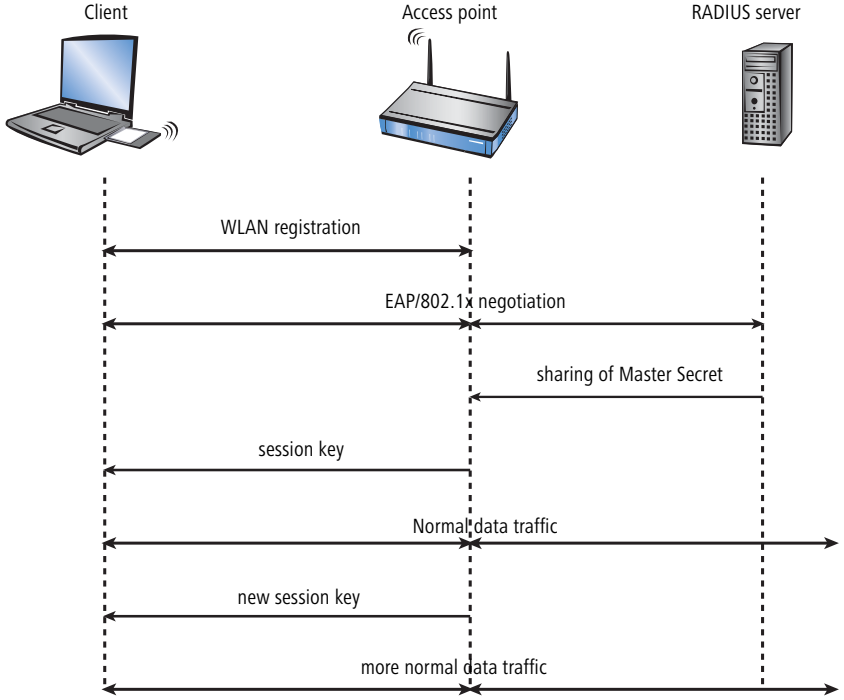


Figure 2: Schematic process of a WLAN session with EAP/802.1x

In the first phase, the client registers with the access point as usual, and enters the state in which it can now send and receive over the access point in normal WEP or WEPplus—but not with EAP, because in this state the client still doesn't have a key to secure its data traffic from eavesdropping. Instead, the client is in an 'intermediate state' from the point of view of the access point, in which only particular packets from the client are forwarded, and these are only directed to an authentication server. These packets are the EAÜ/802.1x mentioned previously. The access point packs these packets in RADIUS queries and sends them on to the authentication server. The access point converts the replies coming from the RADIUS server back into EAP packets, and sends them back to the client.

The access point is thus a sort of middle man between client and server. it doesn't have to check the contents of these packets, it just has to check that no other data traffic to or from the client can occur. Over this "tunnel" through the access point, the client and server authenticate one another, that is, the server checks the client's access privilege to the network, and the client checks that it is talking to the right network. "Wild" access points set up by hackers can be recognized in this way.

A whole series of authentication processes exist which can be used in this tunnel. A current process (and one supported by Windows XP) is for instance TLS, in which server and client exchange certificates; another is TTLS, in which only the server supplies a certificate—the client is authenticated using only a username and password.

After the authentication phase, a secure tunnel even without WEP encryption has been set up, in which the access point is connected in the next step. For this, the RADIUS server sends the so-called 'Master Secret', a session key calculated during the negotiation, to the access point. The LAN behind the access point is considered secure in this scenario, so that this transmission can be performed in clear text.

With this session key, the access point now takes over the tunnel and can use it to provide the actual WEP key to the client. Depending on the capabilities of the access point hardware, this can be a true session key (that is, a WEP key which will only be used for data packets between the access point and precisely this client), or a so-called group key, which the access point will use for communication with multiple clients. Classical WEP hardware can usually handle only group keys, these being the four mentioned in the chapter on WEP.

The particular advantage of this procedure is that the access point can regularly change the WEP key over the EAP tunnel, that is, it can perform a so-called rekeying. In this way, WEP keys can be replaced by new ones long before they run the risk of being cracked due to IV collisions. A common 'use time' for such WEP keys might be 5 minutes.

The disadvantage of the procedure is its complexity. The maintenance of the central RADIUS server and the certificates stored there is generally only possible in large installations with a separate IT department—it is less suitable for use in the home or in smaller companies. These practical hurdles have thus limited EAP/802.1x to professional use so far—the home user must simply make do with WEPplus, or address security problems on the applications level.

12.2.5 TKIP and WPA

As clarified in the last section, the WEP algorithm is flawed and insecure in principle; the measures taken so far were largely either 'quick fixes' with limited improvement, or so complicated that they were basically impractical for home use or smaller installations.

After the problems with WEP became public knowledge, the IEEE began with the development of the standard IEEE 802.11i. As an interim solution, the WiFi Alliance defined the Wifi Protected Access (WPA) 'standard'. WPA uses the following changes:

- TKIP and Michael as replacement for WEP
- A standardized handshake procedure between client and access point for determination/transmission of the session key.
- A simplified procedure for deriving the Master Secret mentioned in the last section, which can be performed without a RADIUS server.
- Negotiation of encryption procedure between access point and client.

TKIP

TKIP stands for **T**emporal **K**ey **I**ntegrity **P**rotocol. As the name suggests, it involves an intermediate solution for temporary use until a truly strong encryption procedure is introduced, but which deals with the problems of WEP, never the less. A requirement of this method was compatibility with existing WEP/RC4 hardware.

Encryption makes use of components familiar from WEP but benefits from decisive improvements with the "Michael hash" from improved encryption and the TKIP method for calculation of the RC4 key. Furthermore, the internally

incremented IV transmitted in clear text in the packet is 48 bits long instead of 24--thus the problem with the repeating IV value is practically excluded.

As a further detail, TKIP also mixes the MAC address of the sender into the calculation of the key. This ensures that the use of identical IVs by different senders cannot lead to identical RC4 keys and thus again to attack possibilities.

The Michael hash does not, however, represent a particularly tough cryptographic hurdle: if the attacker can break the TKIP key or get encrypted packets past the CRC check via modifications similar to those for WEP, then not many barriers remain. For this reason, WPA defines countermeasures if a WLAN card detects more than two Michael errors per minute: both the client and the access point break data transfer off for one minute, afterwards renegotiating TKIP and Michael keys.

The key handshake

In the discussion of 802.1x it was already noted that EAP/802.1x provides a possibility to inform the client at the outset of a session of the key valid for it. WPA now places that on a standardized basis, and considers the session-key option offered by modern access points that, in addition to the four 'global' keys, assigns each registered client with a session key that is used exclusively with data packets to or from that client. The key handshake under WPA involves first of all the exchange of the pairwise keys and then the group keys.

After a successful group key handshake, the access point can release the client for normal data transfer. The access point is free to perform a rekeying again during the session using the same type of packets. In principle, the client may also request rekeying from the access point.

WPA also takes the case of older WLAN hardware into account, in which the access point does not support pairwise keys, but only group keys. The first phase of the handshake in this case proceeds exactly as before, but doesn't result in the installation of a pairwise key—the group key handshake simply proceeds in clear text, but an encryption in the EAP packets themselves prevents an attacker from simply reading the keys.

WPA with passphrase

The handshake described in the previous section runs strictly under WPA, i.e. the user will never have to define any TKIP or Michael keys. In environments in which no RADIUS server is available to provide master secrets (for instance in smaller companies or home networks), WPA therefore provides the PSK method besides authentication using a RADIUS server; here, the user must enter a passphrase of 8 to 32 characters on the access point and on all stations, from which the master secret is calculated along with the SSID used using a hash procedure. The master secret is therefore constant in such a PSK network, although different TKIP keys still result.

In a PSK network—similar to classical WEP—both access security and confidentiality depend on the passphrase not being divulged to unauthorized people. As long as this is the case, WPA-PSK provides significantly improved security against break-ins and eavesdropping over any WEP variant. For larger installations in which such a passphrase would have to be made known to too large a user community for it to be kept secret, EAP/802.11i is used in combination with the key handshake described here.

Negotiating the encryption method

Since the original WEP definition specified a fixed key length of 40 bits, the registration of a client at an access point only had to communicate whether encryption should be used or not. Key lengths exceeding 40 bits require that the key length is announced. WPA provides a mechanism with which client and access point can agree on the encryption and authentication procedures to be used. The following information is made available:

- The encryption method to be used for broadcasts in this network (also the type of group key). Each client wanting to register in a WPA-WLAN must support this procedure. Here, besides TKIP, WEP is also still allowed, in order to support mixed WEP/WPA networks—in a pure WPA network, TKIP will be selected.
- A list of encryption methods which the access point provides for the pairwise key—here, WEP is explicitly disallowed.
- A list of authentication methods a client may use to show itself to the WLAN as authorized for access—possible methods are currently EAP/802.1x or PSK.

As mentioned, the original WPA standard specifies only TKIP/Michael as an improved encryption method. With the further development of the 802.11i standard, the AES/CCM method described below was added. In a WPA network it is now possible for some clients to communicate with the access point using TKIP, while other clients use AES.

12.2.6 AES and 802.11i

In mid-2004 the IEEE approved the long-awaited 802.11i standard that places the entire security concept of WLAN on a new basis. As mentioned in the last section, WPA has already implemented a whole series of concepts from 802.11i—so in this section we will only describe the components which are new compared to WPA.

AES

The most obvious extension is the introduction of a new encryption process, namely AES-CCM. As the name already hints, this encryption scheme is based on DES's successor AES, in contrast to WEP and TKIP, which are both based on RC4. Since only the newest generation of WLAN chips contain AES hardware, 802.11i continues to define TKIP, but with the opposite prerequisites: any 802.11i-compliant hardware must support AES, while TKIP is optional—in WPA that was exactly the other way around.

The suffix CCM denotes the way in which AES is used in WLAN packets. The process is actually quite complicated, for which reason CCM is only sensibly implemented in hardware—software-based implementations are possible, but would result in significant speed penalties due to the processors commonly used in access points.

In contrast to TKIP, AES only requires a 128-bit key, with which both the encryption and protection against undetected changes to packets is achieved. Furthermore, CCM is fully symmetric, i.e. the same key is used in both communications directions—a standards compliant TKIP implementation, on the other hand, requires the use of different Michael keys in the send and receive directions, so that CCM is significantly simpler in use than TKIP.

Similar to TKIP, CCM uses a 48-bit Initial Vector in each packet—an IV repetition is impossible in practice. As in TKIP, the receiver notes the last IV used and discards packets with an IV which is equal to or less than the comparison value.

Pre-authentication and PMK caching

802.11i is intended to help with the use of WLAN for speech connections (VoIP) in enterprise networks. Especially in connection with WLAN-based wireless telephony, quick roaming (switching from one access point to another without lengthy interruptions) is of special significance. In telephone conversations, interruptions of 100 milliseconds are irritating, but the full authentication process over 802.1x, including the subsequent key negotiation with the access point, can take significantly longer.

For this reason, the so-called PMK caching was introduced as a first measure. The PMK serves as the basis for key negotiation in an 802.1x authentication between client and access point. In VoIP environments it is possible that a user moves back and forth among a relatively small number of access points. Thus it may happen that a client switches back to an access point in which it was already registered earlier. In this case it wouldn't be sensible to repeat the entire 802.1x authentication again. For this reason, the access point can provide the PMK with a code, the so-called PMKID, which it transmits to the client. Upon a new registration, the client uses the PMKID to ask whether this PMK is still stored. If yes, the 802.1x phase can be skipped and the connection is quickly restored. This optimization is unnecessary if the PMK in a WLAN is calculated from a passphrase as this applies everywhere and is known.

A second measure allows for some acceleration even in the case of first-time registration, but it requires a little care on the part of the client. The client must already detect a degrading connection to the access point during operation and select a new access point while it is still in communication with the old access point. In this case it has the opportunity to perform the 802,1x negotiation with the new access point over the old one, which again reduces the "dead time" by the time required for the 802.1x negotiation.

12.2.7 Summary

After the security loopholes in WEP encryption became public knowledge, the presentation of short-term solutions such as WEPplus and the intermediate steps like WPA, the IEEE committee has now presented the new WLAN security standard 802.11i. The TKIP procedure used by WPA is based on the older RC4 algorithm, the foundation of WEP. AES is the first important and conclusive step towards a truly secure encryption system. 802.11i/AES have confined the practical and theoretical security loopholes in previous methods to history.

The AES procedure provides security on a level that satisfies the Federal Information Standards (FIPS) 140-2 specifications that are required by many public authorities.

LANCOM Systems equips its 54Mbps products with the Atheros chip set featuring a hardware AES accelerator. This guarantees the highest possible level of encryption without performance loss.

The user-friendly pre-shared key procedure (entry of a passphrase of 8-63 characters in length) makes 802.11i quick and easy for anybody to set up. Professional infrastructures with a larger number of users can make use of 802.1x and RADIUS servers.

In combination with further options such as Multi-SSID and VLAN tagging, it is possible to provide highly secure networks for multiple user groups and with different levels of security.

- VLAN tagging is available as of LCOS version 3.32.
- Multi-SSID is available as of LCOS 3.42.

- LANCOM Systems provides the PSK procedure as of the LCOS version 3.50.
- 802.1x will be supported as of LCOS version 3.52.

12.3 Protecting the wireless network

A wireless LAN does not, like conventional LAN, use cable as the transmitting medium for data transfer, but the air instead. As this medium is openly available to any eavesdropper, the screening of the data in a WLAN is an important topic.

Depending on how critical WLAN security is for your data, you can take the following steps to protect your wireless network:

① Activate the "Closed network function". This excludes all WLAN clients using "Any" as the SSID, and those that do not know your network SSID. (’Network settings’ → page 377)

② Do not use your access point's default SSID. Only take a name for your SSID that cannot be guessed easily. The name of your company, for example, is not a particularly secure SSID. (’Network settings’ → page 377)

③ If you know exactly which wireless network cards are permitted to access your WLAN, you can enter the MAC addresses of these cards into the access control list, thus excluding all other cards from communications with the access point. This reduces access to the WLAN only to those clients with listed MAC addresses. (’Access Control List’ → page 359)

④ Use encryption on the data transferred in the WLAN. Activate the strongest possible encryption available to you ((802.11i with AES, WPA or WEP) and enter the appropriate keys or passphrases into the access point and the WLAN clients (’Encryption settings’ → page 362 and ’WEP group keys’ → page 365).

⑤ Regularly change the WEP key. Also change the standard key (’Encryption settings’ → page 362) in the configuration. Alternatively, you can use a cron job to automatically change the key every day, for example (’Regular Execution of Commands’ → page 550). The passphrases for 802.11i or WPA do not have to be changed 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 that the now aged WEP method.

⑥ If the data is of a high security nature, you can further improve the WEP encryption by additionally authenticating the client with the 802.1x method (’IEEE 802.1x/EAP’ → page 380) or activate an additional encryption of the WLAN connection as used for VPN tunnels (’IPSec over WLAN’ → page 381). In special cases, a combination of these two mechanisms is possible.

Further information is available from our web site www.lancom-systems.com under **Support ▶ FAQ**.

12.3.1 LEPS—LANCOM Enhanced Passphrase Security

LEPS remedies the security issues presented by global passphrases.

The modern encryption methods WPA and IEEE 802.11i provide data traffic in the WLAN with far improved security from eavesdroppers than the older WEP can. It is very easy to handle a passphrase as a central key; a RADIUS server such as that for 802.1x installations is not required.

However, the use of WPA and IEEE 802.11i still has some weak spots:

- A passphrase applies **globally** for **all** WLAN clients
- The passphrase may fall into unauthorized hands if treated carelessly
- The "leaked" passphrase then offers any attacker free access to the wireless network

This means in practice that: Should the passphrase "go missing" or an employee with knowledge of the passphrase leaves the company, then the passphrase in the access point really needs to be changed—in every WLAN client, too. As this is not always possible, an improvement would be to have an individual passphrase for each user in the WLAN instead of a global passphrase for all WLAN clients. In the case mentioned above, the situation of an employee leaving the company requires merely his "personal" passphrase to be deleted; all others remain valid and confidential.

With LEPS (**L**ANCOM **E**nhanced **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 security loopholes that come with global passphrases.

LEPS uses an additional column in the ACL (access control list) to assign an **individual** passphrase consisting of any 8 to 63 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.

This combination makes the spoofing of the MAC addresses futile—and LEPS thus shuts out a potential attack on the ACL. If WPA or IEEE 802.11i is used for encryption, the MAC address can indeed be intercepted—but this method never transmits the passphrase over wireless. This greatly increases the difficulty of attacking the WLAN as the combination of MAC address and passphrase requires both to be known before an encryption can be negotiated.

LEPS can be used both locally in the device and centrally managed with a RADIUS server. LEPS works with all WLAN client adapters available on the market without any 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 secure, particularly when the ACL is stored on a RADIUS server.

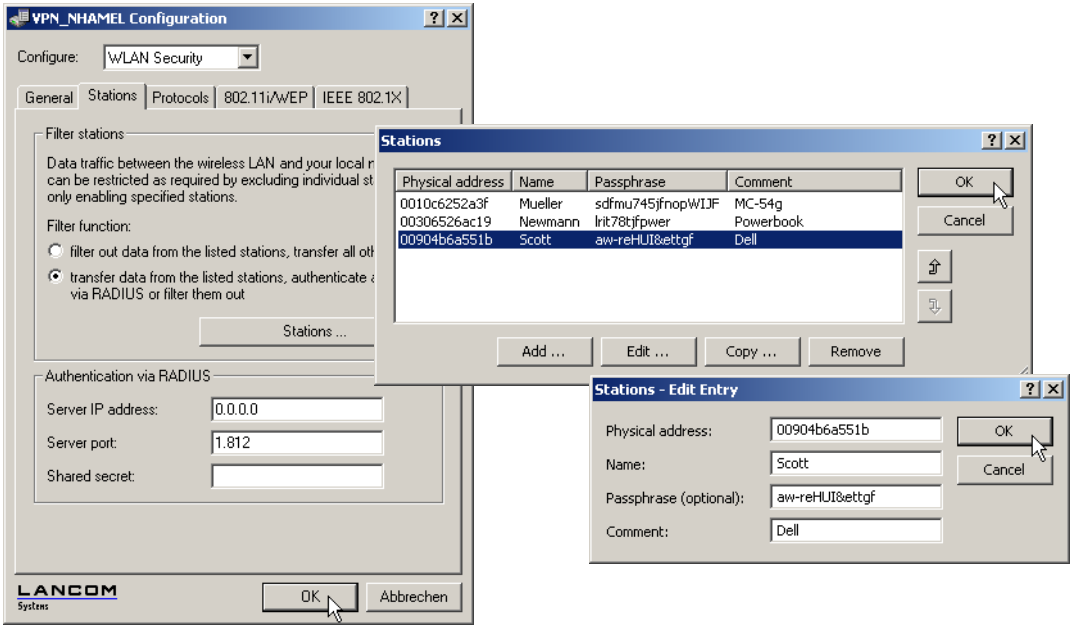
Configuration

The configuration of LEPS merely involves the assignment of an individual passphrase to the MAC address of each client that is approved for the WLAN. To this end, the MAC filter is set to positive, i.e. the data from clients entered here will be transmitted.

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

LANconfig

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



WEBconfig, Telnet or terminal program

Under WEBconfig, Telnet or a terminal program, you will find the access list for the wireless network under the following paths:

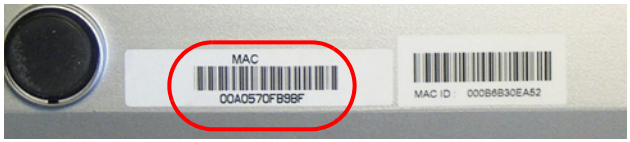
Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ WLAN ▶ Access-list
Terminal/Telnet	`Setup/WLAN/Access-list`

12.3.2 Standard WEP encryption

As of LCOS version 4.00, WEP128 encryption is activated for every unconfigured device as standard.

If your device has one or more WLAN interfaces, you can also carry out the "wireless" configuration from a computer with a WLAN card. To use a WLAN client to connect to a new LANCOM access point for wireless configuration, the WLAN client must be programmed with the 13-character standard WEP key.

The standard WEP key 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 character string labelled as "MAC address" that starts with "00A057". The other addresses that may be found are not the LAN MAC address.



A device with the LAN MAC address "00A0570FB9BF" thus has a standard WEP key of "L00A0570FB9BF". This key is entered into the 'Private WEP settings' of the device for each logical WLAN network as 'Key 1'.

To use a WLAN client to connect to a new (unconfigured) LANCOM access point, the WEP128 encryption must be activated in the WLAN client and the 13-character standard WEP key must be programmed in as described above.

12.4 Configuration of WLAN parameters

Changes to the wireless network settings can be made at various points in the configuration:

- Some parameters concern the physical WLAN interface. Some LANCOM models have one WLAN interface, others have the option of using a second WLAN card as well. The settings for the physical WLAN interface apply to all of the logical wireless networks supported by this card. These parameters include, for example, the transmitting power of the antenna and the operating mode of the WLAN card (access point or client).
- Other parameters are related solely to the logical wireless network that is supported by a physical interface. These include, for example, the SSID or the activation of encryption, either 802.11i with AES or WPA with TKIP or WEP.
- A third group of parameters affect the wireless network operation, but are not significant **only** to WLANs. These include, for example, the protocol filter in the LAN bridge.

12.4.1 WLAN security

In this part of the configuration, you can place limitations on the communications available to the users in the wireless network. This is done by limiting the data transfer between user groups according to individual stations or the protocol being used. Further, the key for the WLAN encryption is set here.

General settings

Communications between the WLAN clients

Depending on the application, it may be required that the WLAN clients connected to an access point can—or expressly cannot—communicate with other clients. You can centrally define the permissible communication for all physical and logical networks, and consider the three following cases in doing so:

- Allow data traffic: This setting allows all WLAN clients to communicate with other stations in their own and in other available wireless networks.

- Do not allow data traffic between stations that are logged on to this access point: In this case, WLAN clients can only communicate with mobile stations located in other available wireless networks, but not with the stations in their own WLAN.
- Do not allow data traffic: This last variant prevents all communications between the WLAN clients.

Roaming

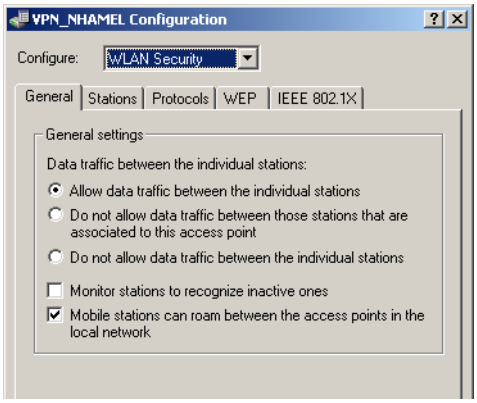
In addition to controlling the communication between the clients, you can define whether the mobile stations in the wireless network can change to a neighboring access point (roaming).

Monitor stations

In particular for public WLAN access points (public spots), the charging of usage fees requires the recognition of stations that are no longer active. Monitoring involves the access point regularly sending packets to logged-in stations. If the stations do not answer these packets, then the charging systems recognizes the station as no longer active.

Configuration with LANconfig

For configuration with LANconfig you will find the general WLAN access settings under the configuration area 'WLAN Security' on the 'General' tab.



Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you will find the general WLAN access settings under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ WLAN ▶ Inter-stations traffic, monitor stations or IAAP protocol (for roaming)
Terminal/Telnet	`cd /Setup/WLAN/Inter-station traffic`, `Monitor stations` or `IAAP protocol` (for roaming)

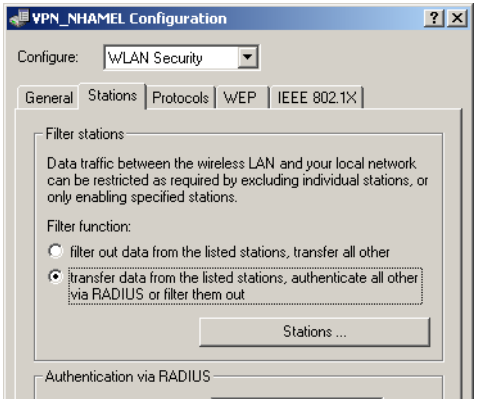
Access Control List

With the **A**ccess **C**ontrol **L**ist (ACL) you can permit or prevent the access to your wireless LAN by individual clients. The decision is based on the MAC address that is permanently programmed into wireless LAN adapters.

Configuration with LANconfig

For configuration with LANconfig you will find the general WLAN access settings under the configuration area 'WLAN Security' on the 'Stations' tab.

Check that the setting 'filter out data from the listed stations, transfer all other' is activated. New stations that are to participate in your wireless network are added with the button 'Stations'.



Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you will find the Access Control List under the following paths:

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

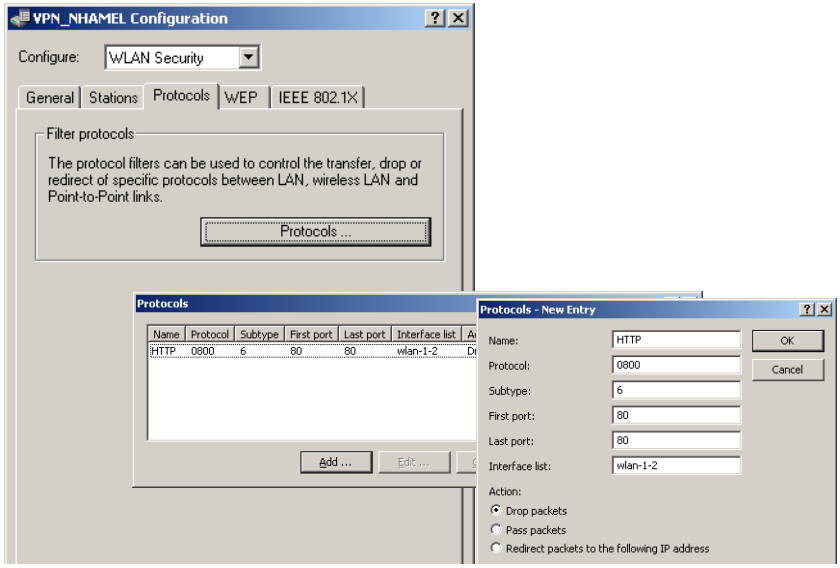
Protocol filter

With the protocol filter you can influence the handling of certain protocols during transfer from the WLAN to the LAN.

Packets from the WLAN for certain protocols/ports can be redirected to special IP addresses in the LAN by the protocol filter. This function known as "Redirect" is described in detail in the section 'Redirect function' → page 379.

Configuration with LANconfig

For configuration with LANconfig you will find the protocol filter under the configuration area 'WLAN Security' on the 'Protocols' tab.



Make an entry in the protocol list for each protocol that requires special handling. Enter the following values:

- A name of your choice for the filter entry
- Protocol number, e.g. '0800' for IP. If no protocol is entered, the filter will be applied to **all** packets.
- Subprotocol, e.g. '6' for TCP. If no subprotocol is entered, the filter will be applied to **all** packets of the entered protocol.
- Port start and port end, e.g. each '80' for HTTP. If no ports are entered, then this filter will be applied to all ports of the appropriate protocol/subprotocol.

Lists of the official protocol and port numbers are available in the Internet under www.iana.org.

- Action for the data packets:
  - Let through
  - Reject
  - Redirect (and state the target address)
- List of interfaces that the filters apply to
- Redirect address when the 'Redirect' action is selected

Example:

Name	Protocol	Sub-type	Start port	End port	Interface list	Action	Redirect IP address
ARP	0806	0	0	0	WLAN-1-2	Let through	0.0.0.0
DHCP	0800	17	67	68	WLAN-1-2	Let through	0.0.0.0
TELNET	0800	6	23	23	WLAN-1-2	Redirect	192.168.11.5
ICMP	0800	1	0	0	WLAN-1-2	Let through	0.0.0.0
HTTP	0800	6	80	80	WLAN-1-2	Redirect	192.168.11.5

ARP, DHCP, ICMP will be let through, Telnet and HTTP will be redirected to 192.168.11.5, all other packets will be rejected.

As soon as an entry is made in the protocol filter, all packets not matching the filter will be automatically rejected!

Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you will find the protocol filter under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ LAN-Bridge ▶ Protocol table
Terminal/Telnet	`cd /Setup/LAN-Bridge/Protocol-Table`

Encryption settings

Access points of the LANCOM range support the most up-to-date methods of encryption and security for data that is transferred via WLAN.

- The IEEE standard 802.11i/WPA stands for the highest degree of security that is currently available for WLAN connections. This standards uses a new encryption procedure (AES-CCM) which, in combination with other methods, achieves levels of security equalled only by VPN connections until now. When using AES-capable hardware (such as the 54-Mbit AirLancer clients and the 54-Mbit LANCOM access points) the transmissions are much faster than with comparable VPN security.
- WEP is also supported to ensure compatibility with older hardware. WEP (**W**ired **E**quivalent **P**rivacy) is the encryption method originally incorporated in the 802.11 standard for the encryption of data in wireless transmission. This method uses keys of 40 (WEP64), 104 (WEP128) or 128 bits (WEP152) in length. A number of security loopholes in WEP have come to light over time, and so the latest 802.11i/WPA methods should be used wherever possible.

Further information about the 802.11i and WPA standards are available under 'Development of WLAN security' → page 346.

The tab '802.11i/WEP' in the configuration area 'WLAN Security' is used for setting the encryption parameters for each logical WLAN. Open the list with the button for **WPA or Private WEP settings**.

Type of encryption

First of all, select the type of encryption for the individual logical WLAN interfaces:

- Yes—Access only for stations with encryption (recommended): In this mode, only the WLAN clients with activated WEP and the correct key can register with the access point.
- Yes—Access also for stations without encryption allowed: In this mode, WLAN clients with activated WEP and AirLancer MC 11 clients (without WEP) can register with this access point.
- No—No encryption

Method/ Key 1 length

Set the encryption method to be used here.

- 802.11i (WPA)-PSK – Encryption according to the 802.11i standard offers the highest security. The 128-bit AES encryption used here offers security equivalent to that of a VPN connection.
- WEP 152, WEP 128, WEP 64 – encryption according to the WEP standard with key lengths of 128, 104 or 40 bits respectively. This setting is only to be recommended when the hardware used by the WLAN client does not support the modern method.
- WEP 152-802.1x, WEP 128-802.1x, WEP 64-802.1x – encryption according to the WEP standard with key lengths of 128, 104 or 40 bits respectively, and with additional authentication via 802.1x/EAP. This setting is also only to be recommended when the hardware used by the WLAN client does not support the 802.11i standard. The 802.1x/EAP authentication offers a higher level of security than WEP encryption alone, although the necessity for a RADIUS server makes very high demands of the IT infrastructure.

Key 1/passphrase

In line with the encryption method activated, you can enter a special WEP key for the respective logical WLAN interface or a passphrase when using WPA-PSK:

- The passphrase, or the 'password' for the WPA-PSK method, is entered as a string of at least 8 and up to 63 ASCII characters.

Please be aware that the security of this encryption method depends on the confidential treatment of this passphrase. Passphrases should not be made public to larger circles of users.

- The WEP key 1, that applies only to its respective logical WLAN interface, can be entered in different ways depending on the key length. Rules of the entry of the keys can be found in the description of the WEP group key 'Rules for entering WEP keys' → page 366.

WPA session key type

If '802.11i (WPA)-PSK' has been entered as the encryption method, the procedure for generating a session or group key can be selected here:

- AES – the AES method will be used.
- TKIP – the TKIP method will be used.
- AES/TKIP – the AES method will be used. If the client hardware does not support the AES method, TKIP will be used.

Authentication

If the encryption method was set as WEP encryption, two different methods for the authentication of the WLAN client are available:

- The 'Open system' method does not use any authentication. The data packets must be properly encrypted from the start to be accepted by the access point.
- With the 'Shared key' method, the first data packet is transmitted unencrypted and must be sent back by the client correctly encrypted. This method presents potential attackers with at least one data packet that is unencrypted.

Default key

If WEP encryption is selected, the access point can select from four different WEP keys for each logical WLAN interface:

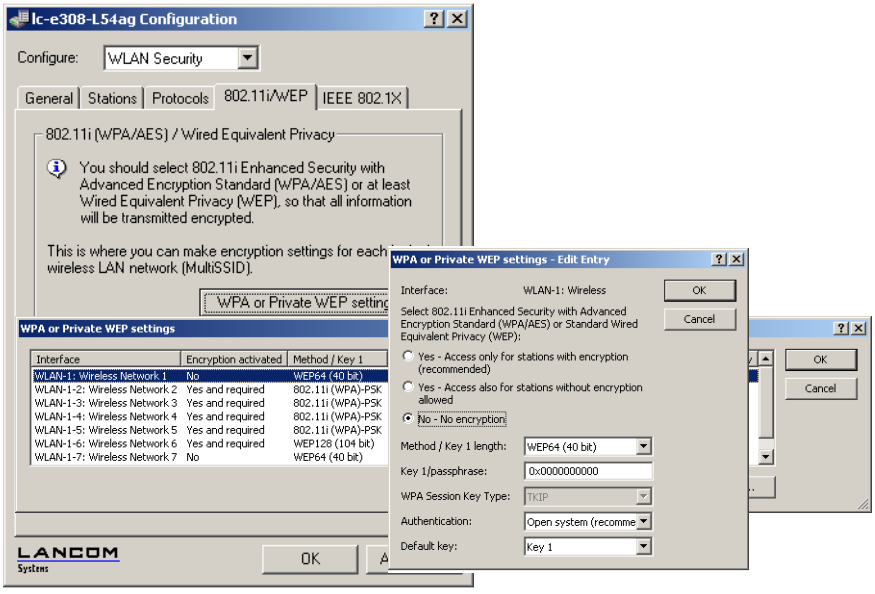
- Three WEP keys for the physical interface
- An additional WEP key particular to each logical WLAN interface

The private WEP settings are used to set the additional key for each logical WLAN interface (see 'Key 1/passphrase'). You should also select which of the four keys is currently to be used for the encryption of the data (default key). This setting can be used to change the key frequently, so increasing security.

Rules of the entry of the keys can be found in the description of the WEP group key 'Rules for entering WEP keys' → page 366.

Configuration with LANconfig

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



Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you will find the individual key settings for logical WLAN networks under the following paths:

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

WEP group keys

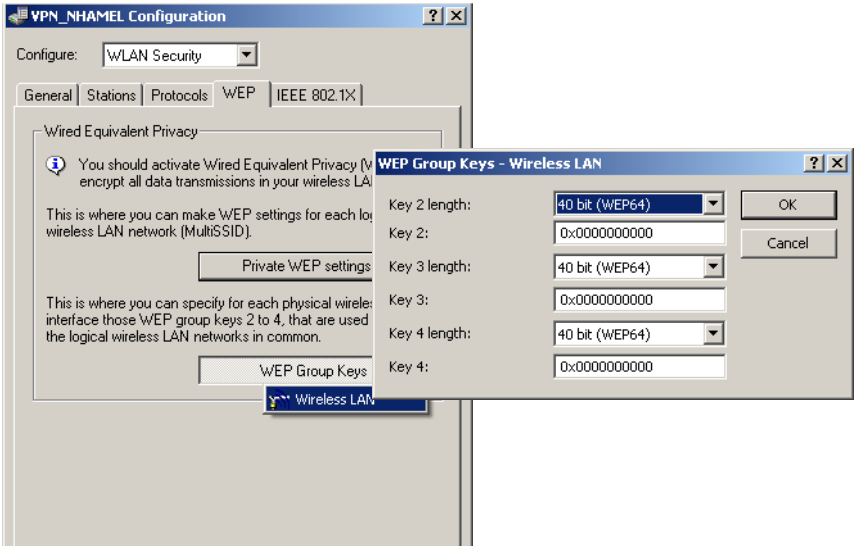
Wired **E**quivalent **P**rivacy (WEP) is an effective method for the encryption of data for wireless transmission. The WEP method uses keys of 40 (WEP64), 104 (WEP128) or 128 bits (WEP152) in length. Each WLAN interface has four WEP keys: a special key for each logical WLAN interface and three common group WEP keys for each physical WLAN interface.

If 802.1x/EAP is in use and the 'dynamic key generation and transmission' is activated, the group keys from 802.1x/EAP will be used and are consequently no longer available for WEP encryption.

Rules of the entry of the keys can be found in the description of the WEP group key 'Rules for entering WEP keys' → page 366.

Configuration with LANconfig

The tab '802.11i/WEP' in the configuration area 'WLAN Security' is used for setting the three WEP keys 2 to 4. Open the list with the button for **WEP Group Keys**. These WEP keys apply to the physical WLAN interface and thus globally to all of the associated logical WLAN interfaces.



Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you will find the group keys for the physical WLAN interface under the following paths:

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

Rules for entering WEP keys

WEP keys can be entered as ASCII characters or in hexadecimal form. The hexadecimal form begins with the characters '0x'. The keys have a length depending on the WEP method:

Method	ASCII	HEX
WEP 64	5 characters Example: 'aR45Z'	10 characters Example: '0x0A5C1B6D8E'
WEP 128	13 characters	26 characters
WEP 152	16 characters	32 characters

The ASCII character set includes the characters '0' to'9', 'a' to 'z', 'A' to 'Z' and the following special characters:
! " # $ % & ´ () * + , - ./ : ; < = > ? @ [\ ] ^ _ ' { | } ~

The HEX form uses the numbers '0' to '9' and the letters 'A' to 'F' to display each character as a character pair, which is why twice the number of characters is required to display a HEX key.

Select the length and the format (ASCII or HEX) of the key depending on the best option available in the wireless network cards that register with your WLAN. If the encryption in an access point is set to WEP 152, some clients may not be able to log into the WLAN as their hardware does not support the key length.

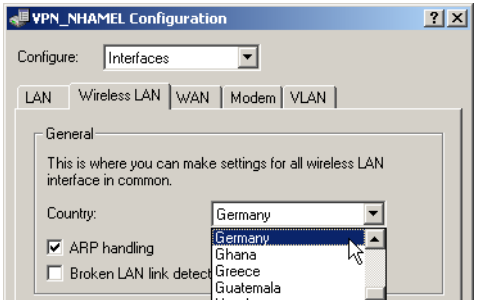
12.4.2 General WLAN settings

Country setting

Regulations for the operation of WLAN cards differ from country to country. The use of some radio channels is prohibited in certain countries. To limit the operation of the LANCOM access points to the parameters that are allowed in various countries, all physical WLAN interfaces can be set up for the country where they are operated.

Configuration with LANconfig

For the configuration with LANconfig, the country settings can be found in the configuration area 'Interfaces' on the tab 'Wireless LAN' in the group 'General':



This group includes two other parameters in addition to the country setting:

ARP handling

- Mobile stations in the wireless network that are on standby do not answer the ARP requests from other network stations reliably. If 'ARP handling' is activated, the access point takes over this task and answers the ARP requests on behalf of stations that are on standby.

Broken link detection

- The 'Broken link detection' deactivates the WLAN card if the access point loses contact to the LAN.

Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you will find the general WLAN parameters under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert-Configuration ▶ Setup ▶ WLAN
Terminal/Telnet	`cd /Setup/WLAN`

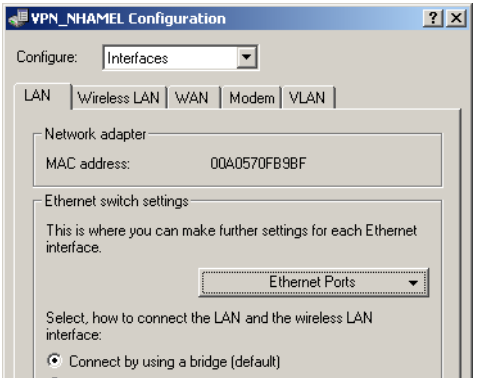
12.4.3 WLAN routing (isolated mode)

When set by default the data between LAN and WLAN is transmitted transparently. Thereby the data transmission between cabled and radio network does not pass over the IP Router. This means, that the features firewall and Quality of Service integrated in the IP router are not provided for transferring data between WLAN and LAN. To use these options nevertheless, the WLAN interface can be set to “isolated mode”, so the data is transferred deliberately over the IP router.

So the IP router can transfer data between LAN and WLAN correctly, both areas must have different IP address sections and the local routing must be activated in the IP router settings.

Configuration with LANconfig

When configuring with LANconfig you can find the WLAN routing in the configuration area 'Interfaces' on the tab 'LAN' in the section 'Ethernet switch settings':



Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you can find the WLAN routing as follows:

Configuration tool	Menu/Table
WEBconfig	Expert Configuration ▶ Setup ▶ LAN ▶ Isolated Mode
Terminal/Telnet	`cd /Setup/LAN/`Isolated Mode

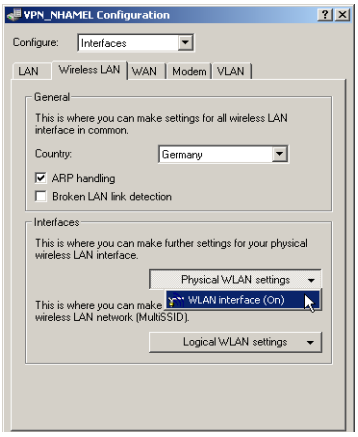
12.4.4 The physical WLAN interfaces

Setting up the WLAN card

Apart from the parameters common to all WLAN cards, there is a series of settings to be made that are particular to each WLAN card of the access point.

Configuration with LANconfig

For configuration with LANconfig you will find the settings for the WLAN card under the configuration area 'Interfaces' on the 'Wireless LAN' tab. Open the list of physical WLAN interfaces by clicking on the button **Physical WLAN settings**.



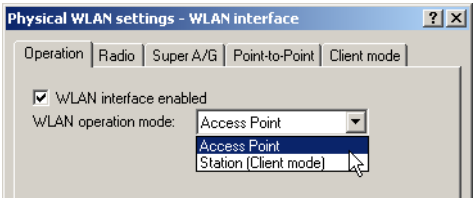
WLAN card operation

Operation mode

LANCOM Wireless devices can be operated in two basic operation modes:

- As an access point, it forms the link between the WLAN clients and the cabled LAN.
- In Client mode the device seeks another access point and attempts to register with a wireless network. In this case the device serves to link a cabled network device to another access point over a wireless connection.

Select the operation mode from the tab 'Operation'. If the WLAN interface is not required, it can be completely deactivated.



Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you can set the operation mode for the physical WLAN interface under the following paths:

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

Radio settings

Frequency band, Subband

When selecting the frequency band on the 'Radio' tab under the physical interface settings, you decide whether the WLAN card operates in the 2.4 GHz or in the 5 GHz band (also see 'Standardized radio transmission by IEEE' → page 338), and thus the available radio channels.

In the 5 GHz band, a subband can also be selected which is linked to certain radio channels and maximum transmission powers.

In some countries, the use of the DFS method for automatic channel selection is a legal requirement. Selecting the subband also defines the radio channels that can be used for the automatic channel selection.

Channel number

- Automatic selection of 5 Ghz WLAN channels over DFS with a "blacklist" and "whitelist".

  To avoid for instance disturbances through radar units and to achieve an even distribution of the WLAN devices on the frequency band the DFS method (dynamic frequency selection) selects a channel automatically. After switching-on or booting your LANCOM the device perchancely selects one channel out of a number of available channels (e.g. due to the country settings) and checks if a radar signals or a different wireless LANs are already working on this channel. This scanning procedure is repeated until a channel without radar signals and as less networks as possible is found. To assure that there are no radar signal, the selected channel is watched for about 60 seconds. The data transfer can therefore possibly be disconnected for about 60 seconds while the device is scanning or searching for a new free channel.

  To prevent the data transfer being interrupted whenever a new channel is being selected, a LANCOM (LCOS version 5.00 and higher) executes the scanning procedure **before** selecting a certain channel. Following information about the scanned channels is saved in an internal data base:

  - Has a radar signal been found on the channel?
  - How many other networks have been found on the channel?

  With the help of this data base a WLAN device can select a radar free channel with the least number of networks. As soon as a channel has been selected the data transfer can begin with no further waiting time.

  - The "blacklist" in the data base saves the channels which are blocked due to found radar signals. To keep the blacklist up to date every entry is deleted automatically after 30 minutes.
  - The "whitelist" contains the channels where no radar signals were found. As long as no radar signals occur on a channel an entry remains valid for the next 24 hours. If a radar signal is found, then the entry is directly deleted out of the list and saved in the blacklist.

  The 60 second scanning procedure is only necessary under following circumstances:

  - The device is switched on or a coldstart is done. In this case the data base is empty, the device cannot select a channel out of the whitelist.
  - If the device has been operating for 24 hours, the whitelist entries are deleted. In this case the data base has to be refilled.

To prevent the 60 second scanning procedure initiating to an unsuitable time, the time when the database is deleted can be adjusted with Telnet under the menu `/setup/WLAN` with the command `set DFS-Rescan-Hours [hour]`. The cron commands can be used for defining the time, e.g. '1,6,13' for a DFS scan at 1 a.m., 6 a.m. and 1 p.m, or '0-23/4' for a DFS scan every four hours from 0 a.m. to 11 p.m.. Precondition is the correct program time of the device.

The radio channel selects a portion of the conceivable frequency band for data transfer.

In the 2.4-GHz band, two separate wireless networks must be at least three channels apart to avoid interference.

Compatibility mode

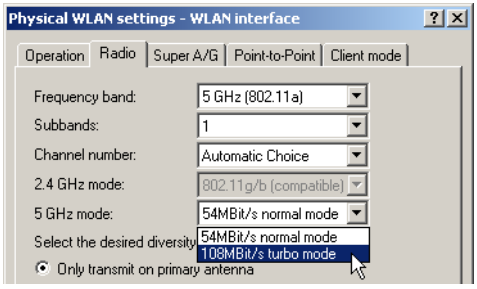
Two different wireless standards are based on the 2.4-GHz band: the IEEE 802.11b standard with a transfer rate of up to 11 Mbps and the IEEE 802.11g standard with up to 54 Mbps. When 2.4 GHz is selected as the frequency band, the data transfer speed can be set as well.

Please observe that clients supporting only the slower standards may not be able to register with the WLAN if the speeds set here are higher.

The 802.11g/b compatibility mode offers the highest possible speeds and yet also offers the 802.11b standard so that slower clients are not excluded. In this mode, the WLAN card in the access point principally works with the faster standard and falls back on the slower mode should a client of this type log into the WLAN. In the '2Mbit compatible' mode, the access point supports older 802.11b cards with a maximum transmission speed of 2 Mbps.

Turbo mode

Using two neighboring, vacant channels for wireless transmissions can increase the transfer speeds up to 108 Mbps. Set this option for the 2.4-GHz band by selecting the drop down list '2.4 GHz mode', for the 5-GHz band in the appropriate list '5 GHz mode' below.

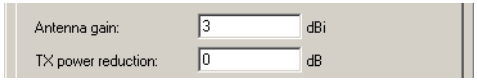


Antenna gain
Transmission power reduction

Where the transmission power of an antennae exceeds the levels permitted in the country of operation, the power must be attenuated accordingly.

- The field 'Antenna gain' is for the gain of the antenna minus the actual cable loss. For an AirLancer Extender O-18a antenna with a gain of 18dBi and a 4m cable with a loss of 1dB/m, the 'Antenna gain' would be entered as 18 - 4 = 14. This value for true antenna gain is dynamically used to calculate and emit the maximum permissible power with regards to other parameters such as country, data rate and frequency band.

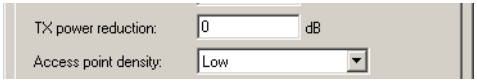
■ In contrast to this, the entry in the field 'Tx power reduction' causes a static reduction in the power by the value entered, and ignores the other parameters. Also see 'Establishing outdoor wireless networks' → page 390.



The transmission power reduction simply reduces the emitted power. The reception sensitivity (reception antenna gain) remains unaffected. This option is useful, for example, where large distances have to be bridged by radio when using shorter cables. The reception antenna gain can be increased without exceeding the legal limits on transmission power. This leads to an improvement in the maximum possible range and, in particular, the highest possible data transfer rates.

Access point density

The more access points there are in a given area, the more the reception areas of the antennae intersect. The setting 'Access point density' can be used to reduce the reception sensitivity of the antenna.



Maximum distance

Large distances between transmitter and receiver give rise to increasing delays for the data packets. If a certain limit is exceeded, the responses to transmitted packets no longer arrive within an acceptable time limit. The entry for maximum distance increases the wait time for the responses. This distance is converted into a delay which is acceptable for wireless communications.

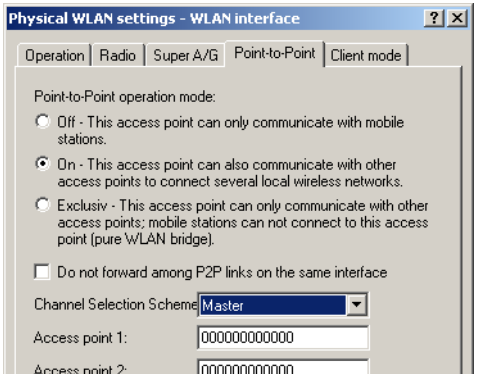
Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you will find the radio parameters under the following paths:

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

Point-to-point connections

Access points are not limited to communications with mobile clients; they can also transfer data from one access point to another. On the 'Point-to-Point' tab for the physical interface settings, you can allow the additional exchange of data with other access points. You can select from:



- Point-to-point 'Off': The access point only communicates with mobile clients
- Point-to-point 'On': The access point can communicate with other access points and with mobile clients
- Point-to-point 'Exclusive': The access point only communicates with other access points

The input fields are for the MAC addresses of the WLAN cards for the point-to-point connections (up to 7).

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.

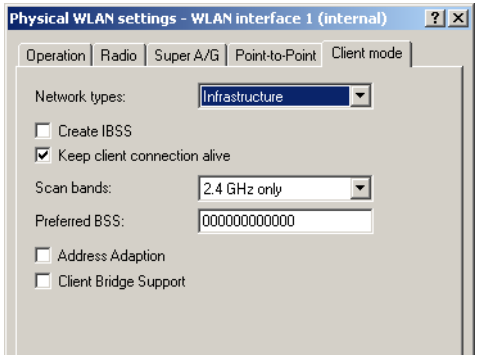
Configuration with WEBconfig or Telnet

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`

Client mode

If the LANCOM Wireless device is operating as a client, the tab 'Client mode' can be used for further settings that affect the behavior as a client.



Network types
'Network types' controls whether the station can register only with infrastructure networks, or also with adhoc networks. Further information about these network types can be found under 'The ad-hoc mode' → page 341 and 'The infrastructure network' → page 341.

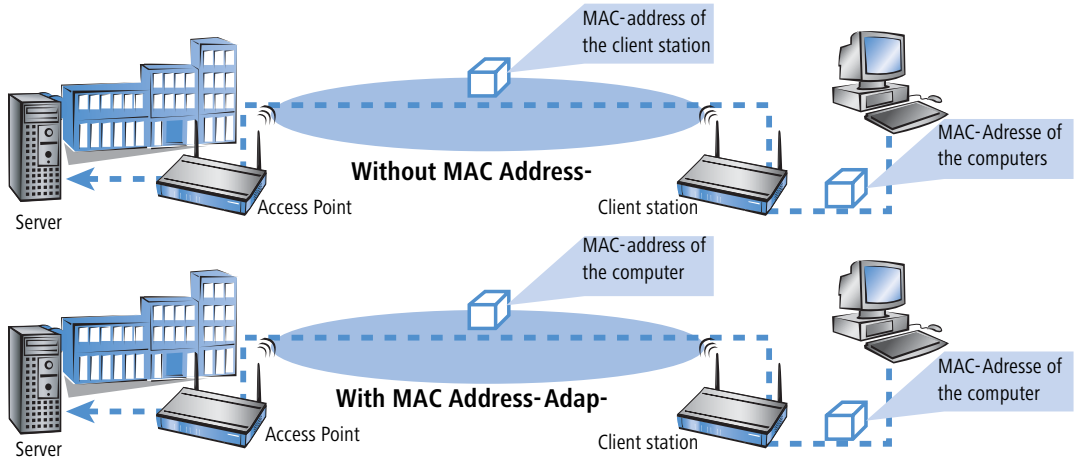
Create IBBS
If the station can establish an IBBS (Independent Basic Service Set), meaning an adhoc network, then the station can connect to other WLAN clients. For the connection of devices with a client station, this is mostly unwanted or not required.

Keep client connection alive
This option ensures that the client station keeps the connection to the access point alive even when the connected devices do not send any data packets. If this option is switched off, the client station will automatically log off from the wireless network if no packets are transferred over the WLAN connection within a given time.

Scan bands
This defines whether the client station scans just the 2.4 GHz, just the 5 GHz, or all of the available bands for access points.

Preferred BSS-ID
If the client station is only supposed to log in on a certain access point, you can enter the MAC address of the WLAN card from the access point.

Address Adaption
In client mode the client station usually replaces the MAC addresses contained in the data packets of the connected devices with the own MAC address. The access point on the other side of the connection therefore only "sees" the MAC address of the client station, but not the MAC address of the connected computer or computers.

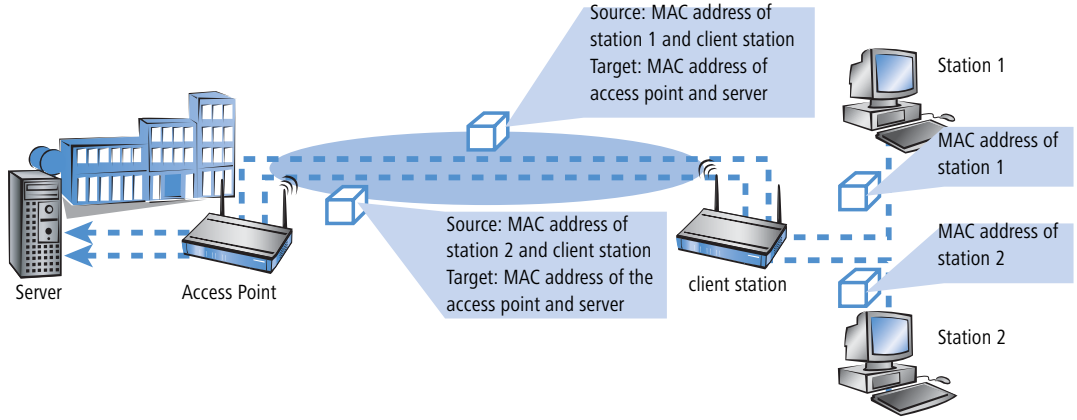


In some installations it is required, that the MAC address of the computer and not of the client station is transmitted. With the option Address-Adaption the replacement of the MAC address by the client stations is prevented and the data packets are transmitted with the original MAC address.

The address-adaption only works if only one computer is connected to the client station.

Client Bridge Support

With address-adaption ('Address Adaption' → page 374) the MAC address of only one connected device is visible to the access point. With a Client-Bridge Support all MAC addresses of the stations in the LAN behind the client stations are transmitted transparently to the access point.



In this operating mode not the usual MAC addresses for instance in client mode are used (in this example for server, access points and client stations), but in conformity to point-to-point connections four addresses (the MAC address of the station in LAN of the client station is additional). The fully transparent connection of a LAN to the client station

allows transmitting data packets in the WLAN and therefore works like TFTP downloads, which are triggered over a broadcast.

The Client-Bridge mode has following advantages compared to other methods:

- Compared to the "normal" client mode the address encryption (masquerading) is not required.
- Compared to a point-to-point connection the entry of the MAC addresses is not required. Additionally in the Client - Bridge mode more than six connections (with P2P limited) can be established.

The Client-Bridge mode can only be used between two LANCOM devices. Applying the Client-Bridge mode must also be activated in the settings for the logical network of the access point.

Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you will find the settings for the client mode under the following paths:

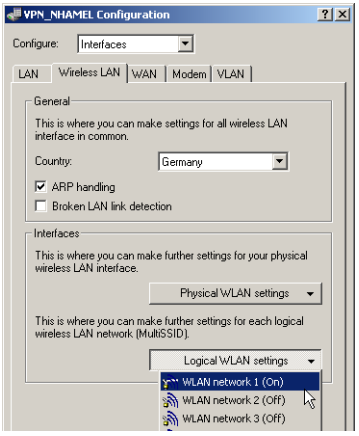
Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ Interfaces ▶ WLAN-Interfaces▶ Client-Settings
Terminal/Telnet	`cd /Setup/Interfaces/WLAN-Interfaces/ Client-Settings`

12.4.5 The logical WLAN interfaces

Every physical WLAN interface can support up to eight different logical wireless networks (Multi-SSID). Parameters can be defined specifically for each of these networks, without the need of additional access points.

Configuration with LANconfig

For configuration with LANconfig you will find the settings for the logical WLAN interface under the configuration area 'Interfaces' on the 'Wireless LAN' tab. Open the list of logical WLAN interfaces by clicking on the button **Logical WLAN settings** and select the required logical interface.



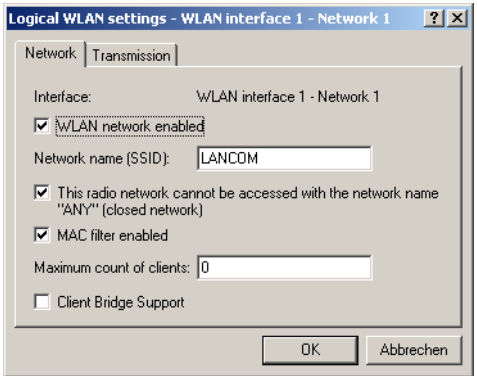
Network settings

Enablingf

The switch 'WLAN network enabled' enables the logical WLAN to be switched on or off separately.

Set the SSID

Define an unambiguous SSID (network name) for each of the logical wireless networks on the 'Network' tab for the logical interfaces. Only network cards that have the same SSID can register with this wireless network.



Closed network mode

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

Activate the closed network mode if you wish to prevent WLAN clients using the SSID 'ANY' from registering with your network.

Enable MAC filter

In the MAC filter list (**WLAN Security ▶ Stations ▶ Stations**) the MAC addresses of the Clients are entered, which may connect to the access point. With the switch 'MAC filter enabled' the MAC filter list for single logical networks can be switched off.

The MAC filter list is always required in logical networks, in which clients log in with an individual passphrase over LEPS. The Passphrase used with LEPS must also be enterd in the MAC filter list. For the log in with an individual Passphrase the MAC filter list is always considered, even if the option is deactivated at this place.

Maximum count of clients

Here you can specify the number of clients, that can connect to the access point. Further clients are rejected.

Client-Bridge-Support

Enable this option for an access point, if you have enabled the client-bridge support in the WLAN client mode for a client station.

The client-bridge mode can only be used between two LANCOM devices.

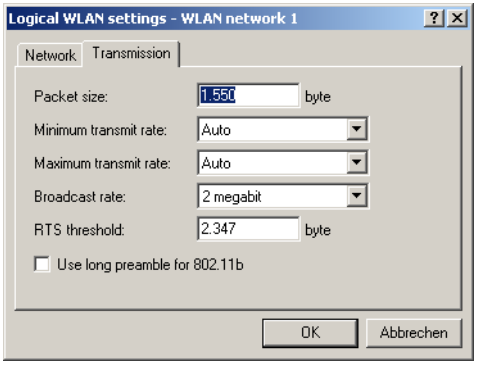
Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you can set the network settings for the logical WLAN interface under the following paths:

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

Transmission settings

Details for the data transfer over the logical interface are set on the 'Transmission' tab.



Packet size

Smaller data packets cause fewer transmission errors than larger packets, although the proportion of header information in the traffic increases, leading to a drop in the effective network load. Increase the factory value only if your wireless network is largely free from interference and very few transmission errors occur. Reduce the value to reduce the occurrence of transmission errors.

Minimum and maximum transmit rate

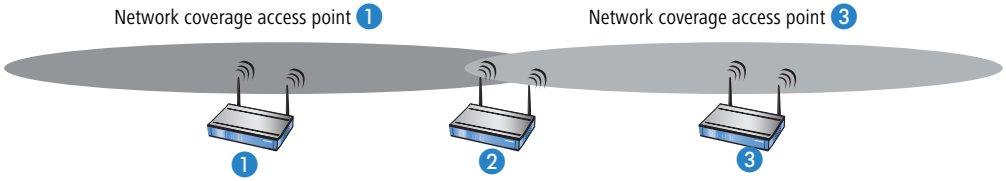
The access point normally negotiates the data transmission speeds with the connected WLAN clients continuously and dynamically. In doing this, the access point adjusts the transmission speeds to the reception conditions. As an alternative, you can set fixed values for the minimum and maximum transmission speeds if you wish to prevent the dynamic speed adjustment.

Broadcast rate

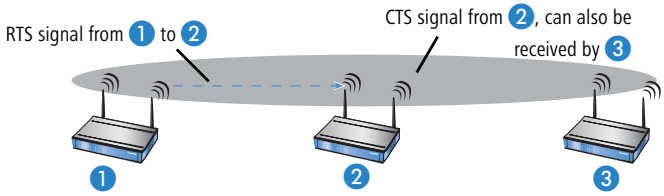
The defined broadcast rate should allow the slowest clients to connect to the WLAN even under poor reception conditions. A higher value should only be set here if all clients are able to connect "faster".

RTS threshold

The RTS threshold prevents the occurrence of the "hidden station" phenomenon.



Here, the three access points 1, 2, and 3 are positioned such that no direct wireless connection between the two outer devices is possible. If 1 sends a packet to 2, 3 is not aware of this as it is outside of 1's coverage area. 3 may also try, during the transmission from 1, to send a packet to 2 as well, because 3 has no knowledge of the medium (in this case the wireless connection) being blocked. A collision results and neither of the transmissions from 1 nor 3 to 2 will be successful. The RTS/CTS protocol is used to prevent collisions.



To this end, 1 precedes the actual transmission by sending an RTS packet to 2, that 2 answers with a CTS. The CTS sent by 2 is now within "listening distance" of 3, so that 3 can wait with its packet for 2. The RTS and CTS signals each contain information about the time required for the transmission that follows.

A collision between the very short RTS packets is improbable, although the use of RTS/CTS leads to an increase in overhead. The use of this procedure is only worthwhile where long data packets are being used and the risk of collision is higher. The RTS threshold is used to define the minimum packet length for the use of RTS/CTS. The best value can be found using trial and error tests on location.

Long preamble for 802.11b

Normally, the clients in 802.11b mode negotiate the length of the preamble with the access point. "Long preamble" should only be set when the clients require this setting to be fixed.

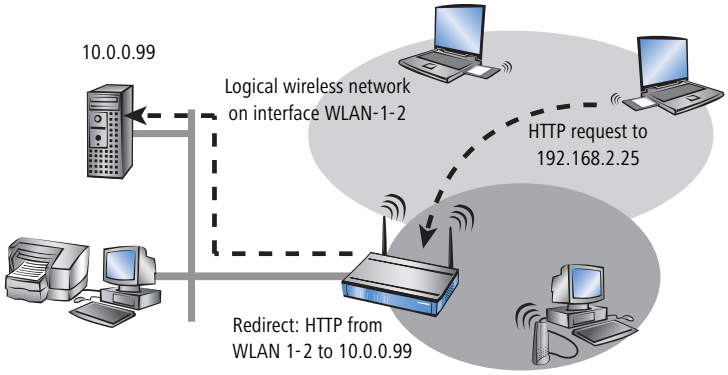
12.4.6 Additional WLAN functions

Apart from the different encryption methods 802.11i/AES, WPA/TKIP or WEP and the closed network, a variety of other functions exist for securing the operation of a wireless network. The Redirect function provides the convenient control over the connection of WLAN clients in changing environments. As this function has significance to other modules of the LANCOM LCOS, the configuration parameters are to be found outside of the WLAN settings.

Redirect function

Clients within wireless networks often have one main aspect in common: a high degree of mobility. The clients are thus not always connected to the same access point, but frequently change between access points and the related LANs.

The redirect function assist the applications being used by the WLAN clients to find the correct target computer in the LAN automatically. If a WLAN client's HTTP request from a certain logical wireless network should always be directed to a certain server in the LAN, then a filter setting for the appropriate protocol with the action "redirect" will be set up for the desired logical WLAN interface.



All requests with this protocol from this logical wireless network will automatically be redirected to the target server in the LAN. The returning data packets are sent to the senders' addresses and ports according to the entries in the connection statistics, which ensures the trouble-free operation in both directions. Further information to the configuration of the protocol filter can be found 'Protocol filter' → page 360

IEEE 802.1x/EAP

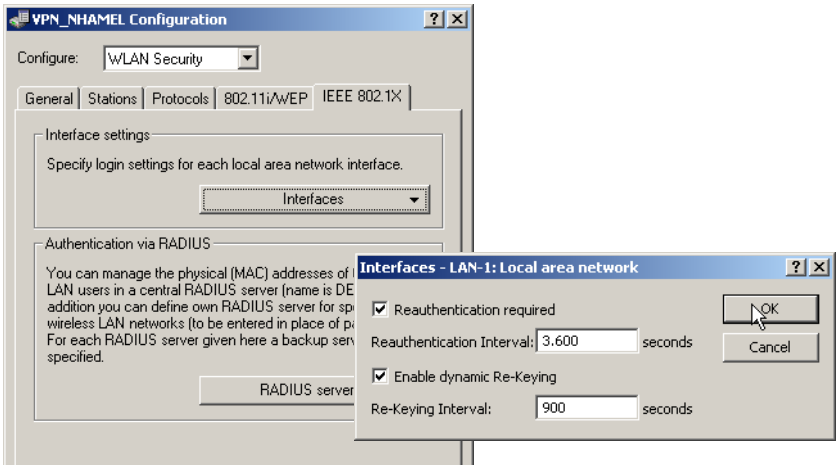
The international industry standard IEEE 802.1x and the **E**xtensible **A**uthentication **P**rotocol (EAP) enable access points to carry out reliable and secure access checks. The access data can be managed centrally on a RADIUS server and can be called up by the access point on demand.

This technology also enables the secure transmission and the regular automatic changing of WEP keys. In this way, IEEE 802.1x improves the security of WEP.

The IEEE-802.1x technology is already fully integrated in Windows XP. Client software exists for other operating systems.

Configuration with LANconfig

For the configuration with LANconfig you will find the IEEE-802.1x settings in the configuration area 'WLAN Security'. This is where you decide if you want to activate IEEE-802.1x. If IEEE-802.1x is activated, a RADIUS server must be defined for the IEEE-802.1x authentication.



Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you will find the settings for IEEE-802.1x under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ IEEE802.1x ▶ Ports
Terminal/Telnet	`cd /Setup/IEEE802.1x/Ports`

IPSec over WLAN

Only with the LANCOM VPN Option. Not available with all LANCOM devices.

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. To this end, the LANCOM Wireless access point is upgraded to a VPN gateway with the LANCOM VPN Option. In addition to the encryption per 802.11i, WPA or WEP, the LANCOM Wireless now offers the possibility of encrypting wireless connections with an IPSec-based VPN.

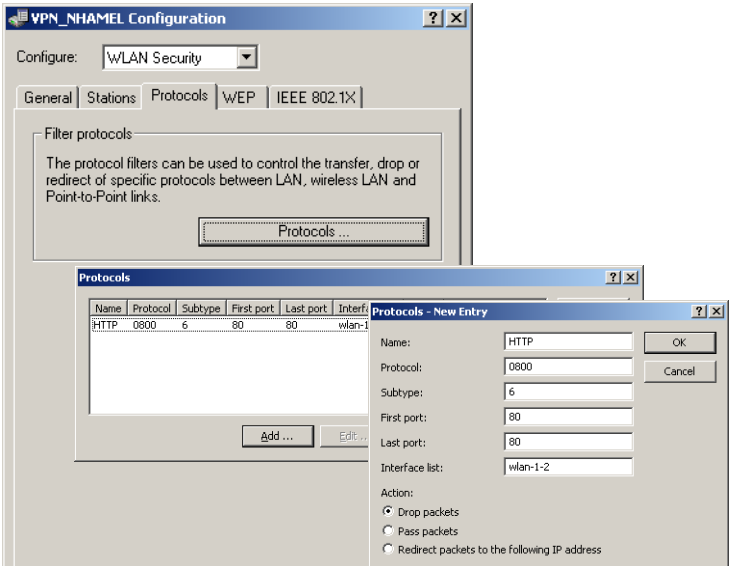
12.5 Extended WLAN protocol filters

With the protocol filter you can influence the handling of certain protocols during transfer from the WLAN to the LAN. The use of appropriate rules allows the definition of which data packets should be inspected, interfaces for which the filter applies and which action should be performed on the data packets.

Configuration

Follow the paths below for protocol filter configuration parameters:

Configuration tool	Menu/Table
LANconfig	WLAN security ▶ Protocols
WEBconfig	Expert configuration ▶ Setup ▶ LAN Bridge ▶ Protocol table
Terminal/Telnet	`cd /Setup/LAN Bridge/Protocol table`



12.5.1 Protocol filter parameters

The protocol table can accommodate up to 128 entries. Create an entry in the protocol list for each protocol that requires special handling. Enter the following values:

- **Name**: freely selectable name for the filter entry [maximum 16 characters]
- **DHCP source MAC**: Enabling of DHCP address tracking.
  - **Yes**: The rule applies if the source MAC address of the packet is listed in the table under `Status > LAN Bridge Statistics > DHCP Table` as an address which obtained an IP address using DHCP.
  - **No**: The rule applies if this is not the case.
  - **Irrelevant**: The source MAC address is not considered.

If DHCP address tracking is enabled, any IP addresses usually entered are disregarded. Please refer to 'DHCP address tracking' → page 386 for further information.

- **Destination MAC address**: The MAC address of the client to which the packet is to be sent.
  If no destination MAC address is entered, the filter is applied to **all** packets.
- **Protocol**: e.g. '0800' for IP.
  If '0' is entered as the protocol, the filter applies to **all** packets.
- **IP network** and **IP netmask**: The IP address of the network mask to which this filter applies. Only those IP packets whose source and destination IP addresses lie within this network are captured by the rule.
  If no network is entered, the filter applies to **all** packets.
- **Sub-protocol**: e.g. '6' for TCP.
  If '0' is entered as the sub-protocol, the filter applies to **all** packets of the protocol entered.
- **Start port** and **end port**: e.g. both '80' for HTTP.
  If '0' is entered as the start port, this filter will be applied to all ports of the corresponding protocol/sub-protocol. If '0' is entered as the end port, the start port becomes an end port.

Lists of the official protocol and port numbers are available in the Internet under www.iana.org.

- **Action**: Action performed for the data packets captured using this rule:
  - **Pass**: The packet is forwarded on without change.
  - **Drop**: The complete packet is dropped.
  - **Redirect**: The packet is forwarded on, albeit with changed destination IP address and target MAC address.
- **Interface list**: List of the interfaces to which the filter applies.
  All of the LAN interfaces, DMZ interfaces, logical WLAN networks and point-to-point connections in the WLAN may be entered as interfaces.

  The following examples illustrate how interfaces are specified: 'LAN-1' for the first LAN interface, 'WLAN-2-3' for the third logical WLAN network on the second physical WLAN interface, 'P2P-1-2' for the second point-to-point connection on the first physical WLAN interface.

  Groups of interfaces may be specified in the form 'WLAN-1-1~WLAN-1-6' (logical WLANs 1 to 6 on the first physical WLAN interface) or with a wildcard as 'P2P-1-*' (all P2P connections on the first physical interface).

Only filter rules with valid entries in the interface list are active. A rule with no specification of the interfaces does not apply to all of them - it is ignored instead.

- **Redirect IP address**: Destination IP address for the "Redirect" action
  On redirection, the destination IP address of the packets is replaced by the Redirect IP address entered here. Furthermore, the destination MAC address is replaced by the MAC address determined using ARP for the Redirect IP address.

If ARP was unable to determine the destination MAC address, the packet is dropped rather than redirected.

Example:

Name	DHCP source MAC:	Destination MAC address.	Prot.	IP address	IP net-work:	Sub-type	Start port	End port	Interface list	Action	Redirect IP address
ARP	irrelevant	000000000000	0806	0.0.0.0	0.0.0.0	0	0	0	WLAN-1-2	Pass	0.0.0.0
DHCP	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	17	67	68	WLAN-1-2	Pass	0.0.0.0
TELNET	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	6	23	23	WLAN-1-2	Redirect	192.168.11.5
ICMP	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	1	0	0	WLAN-1-2	Pass	0.0.0.0
HTTP	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	6	80	80	WLAN-1-2	Redirect	192.168.11.5

ARP, DHCP, ICMP are allowed to pass, Telnet and HTTP are redirected to 192.168.11.5 and all other packets are rejected.

12.5.2 Procedure for filter test

If no filter rules are defined for an interface, all packets from and destined to it are transmitted without alteration. As soon as a filter rule has been defined for an interface, all packets to be transferred via this interface are checked prior to being processed.

① As a first step, the information required for checking is read out of the packets:

- DHCP source MAC:
- Destination MAC address of the packet:
- Protocol, e.g. IPv4, IPX, ARP
- Sub-protocol, e.g. TCP, UDP or ICMP for IPv4 packets, ARP Request or ARP Response for ARP packets
- IP address and network mask (source and destination) for IPv4 packets
- Source and destination port for IPv4 TCP or IPv4 UDP packets

② As a second step, this information is checked against the information from the filter rules. All those rules in which the source **or** destination interface is included in the interface list are considered. Checking of the rules for the individual values is as follows:

- For DHCP source MAC, protocol and sub-protocol, the values read out of the packets are checked for consistency with the values defined in the rule.
- With IP addresses, the source **and** destination address of the packet are checked to see whether they lie within the range formed by the IP address and the network mask of the rule.
- Source and destination ports are checked to see whether they lie in the range between start port and end port.

If none of the rule values specified (not filled by wildcards) agree with the values read out of the packet, the rule is not considered applicable and is disregarded. If several rules apply, the most accurate rule action is carried out. Parameters are more accurate the further down the list of parameters they are or the further right they appear in the protocol table.

If rules are defined for an interface, but there is no match with one of the rules for a packet from/for this interface, the default rule for this interface is used for the packet. The default rule is pre-configured for each interface with the 'drop' action but this is not visible in the protocol table. To modify a default rule for an interface, a rule with the name 'default-drop' is defined. Besides the interface naming, this rule can only contain wildcats and the required action.

Checking of MAC addresses in packets sent over the respective interface takes on a different form to that with in-coming packets.

- With out-going packets, the source MAC address read out of the packet is checked against the destination MAC address entered in the rule.
- The destination MAC addresses read out of the packet are then checked to see whether they are listed as currently active DHCP clients.
- Rules with the 'Redirect' action are ignored if they apply for an interface over which the packet is to be sent. Please refer to section 'Redirect function' → page 379 for further information.

③ In the third step, the action associated with the applicable rule is carried out.

12.5.3 Redirect function

The Redirect function

With the Redirect action, IPv4 packets can not only be transferred and dropped, they can also be communicated specifically to a particular destination. As a general rule, the destination IP address of the packet is replaced by the Redirect IP address entered. The destination MAC address of the packet is replaced by the MAC address determined by ARP and associated with the Redirect IP address.

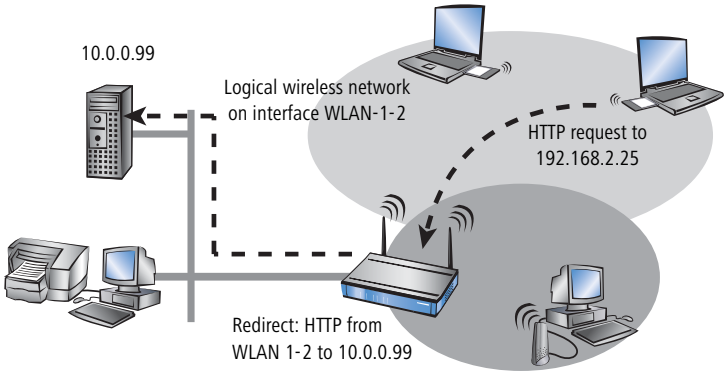
In order for the redirected packets to find the correct sender on their "return trip", a dynamic table is compiled with automatic filter rules that apply to packets leaving via this interface. This table can be viewed under `Status > LAN Bridge > Connection table`. Rules in this table have a higher priority than other matching rules with the 'Transfer' or 'Drop' actions.

Example application

Clients within wireless networks often have one aspect in common: a high degree of mobility. Consequently, clients are not necessarily always connected to the same access point, but frequently change between access points and the related LANs.

The redirect function assists WLAN client applications to automatically find the correct target computer in the LAN. If a WLAN client's HTTP request from a particular logical wireless network is to be always directed to a particular

server in the LAN, a filter setting with the "Redirect" action is set up for the appropriate protocol for the desired logical WLAN interface.



All requests with this protocol from this logical wireless network are automatically redirected to the target server in the LAN. The returning data packets are sent to the senders' addresses and ports according to the entries in the connection statistics, ensuring trouble-free operation in both directions.

12.5.4 DHCP address tracking

DHCP address tracking keeps a record of which clients have received their IP addresses using DHCP. The relevant information for an interface is automatically maintained in a table under `Status > LAN Bridge Statistics > DHCP Table`. DHCP tracking is enabled on an interface if, for this interface, a minimum of one rule is defined where 'DHCP Source MAC' is set to 'Yes'.

The number of clients which may be connected to an interface via DHCP can be configured in the Port table under `Setup > LAN Bridge > Port Data`. Setting the entry to '0' means that any number of clients can register at this interface via DHCP. If the maximum number of DHCP clients is exceeded by a further attempt to register, the oldest entry in the list is deleted.

When checking data packets, IP addresses and the IP network mask defined in the rule are not used. Consequently no check is made as to whether the destination IP address of the packet lies within the range specified. Instead, a check is made as to whether the source IP address of the packet matches the IP address assigned to the client via DHCP. The connection of the two IP addresses is made based on the source MAC address.

This check can be used to block clients which have received an IP address via DHCP, but which actually use a different IP address (either intentionally or inadvertently). A rule in which the DHCP Source MAC parameter is set to 'Yes' would not apply since the two addresses do not match. The packet would instead be processed either by other rules or the default rule.

In order for DHCP tracking to work, at least two more rules must be set up for this interface, rules which are not dependent on DHCP tracking. This is necessary since the required DHCP information is not exchanged until the end

of DHCP handshake. This is why packets due to be sent beforehand must be allowed by rules which do not use DHCP tracking. These usually included TCP/UDP packets on port 67 and 68 and ARP packets.

If DHCP tracking is enabled on an interface, packets received on this interface from HDCP servers are automatically dropped.

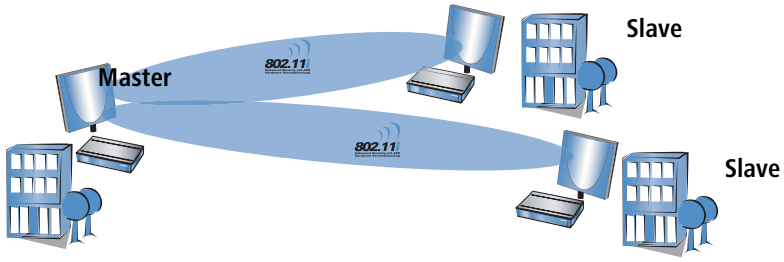
12.6 IEEE 802.11i for point-to-point connections in the WLAN

12.6.1 More security in P2P mode

IEEE 802.11i can be used to attain a significant increase in the security of point-to-point connections in the WLAN. 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).

12.6.2 Configuration

To make use of the advantages of 802.11i encryption on P2P connections, the point-to-point mode must first of all be activated in the participating devices. Further, each connection requires one device to be configured as 'master' and one device as 'slave'. Finally, the MAC address of the opposite WLAN client must be entered at both ends of the connection.



Finding MAC addresses with WEBconfig, Telnet or a terminal program

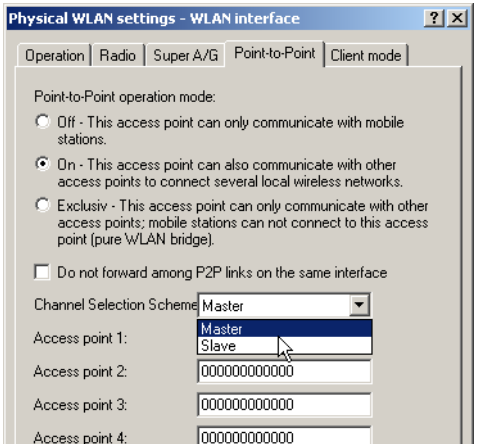
Under WEBconfig, Telnet or a terminal program, you will find the MAC addresses for the WLAN cards in the devices under the following paths:

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

As an alternative, you will find the WLAN MAC address on a sticker on the base of the device. 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.

LANconfig

For configuration with LANconfig you will find the settings for P2P connections under the configuration area 'Management' on the 'Wireless LAN' tab. Click on the button **Physical WLAN settings** to open the corresponding WLAN interface and select the tab for 'Point-to-Point'. Activate the point-to-point mode here and set the 'Channel selection scheme' to either 'Master' or 'Slave'. Enter the appropriate MAC address for the WLAN card at the remote station.

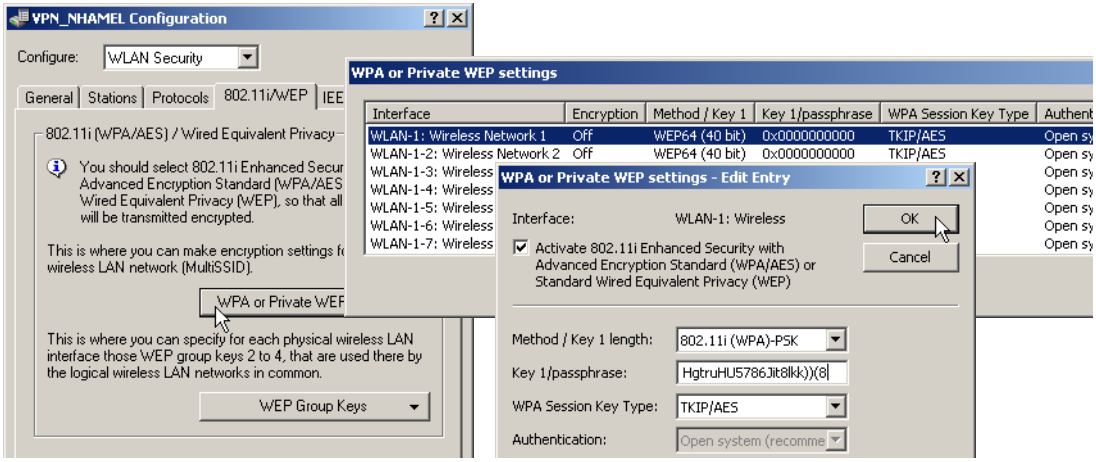


To activate the 802.11i encryption for the P2P connection, adjust the settings for the first logical WLAN network in the WLAN interface that is used (i.e. WLAN-1 if you are using the first WLAN card for the P2P connection, WLAN-2 if you are using the second card, e.g. as with a LANCOM 3550 Wireless).

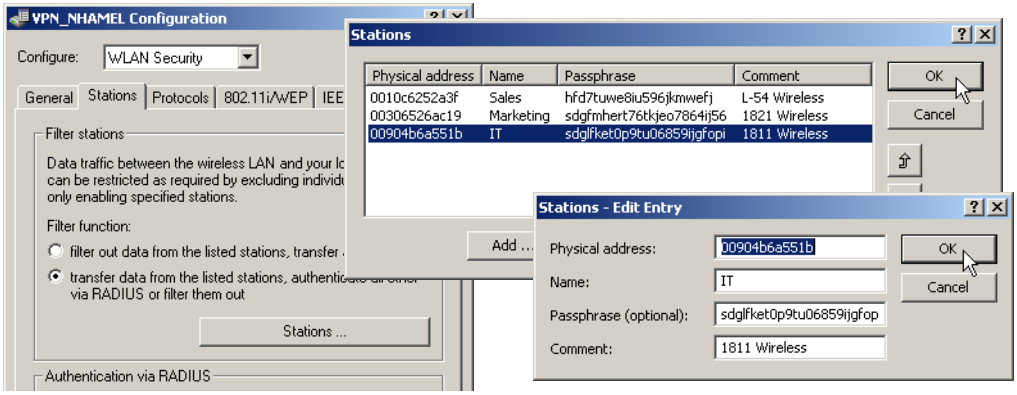
- Activate the 802.11i encryption.
- Select the method '802.11i (WPA)-PSK).
- Enter the passphrase to be used.

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

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



An even higher degree of security can be attained by using LEPS in addition, which involves the matching of MAC address and passphrase. When using LANconfig for the configuration, you enter the passphrases of the stations approved for the WLAN in the configuration area 'WLAN Security' on the 'Stations' tab under the button **Stations**.



Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you can set the settings for the point-to-point operation of the physical WLAN interfaces under the following paths:

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

The encryption settings for the individual logical WLAN networks can be found under:

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

The access list for the matching of MAC addresses to the passphrases (LEPS) can be found under:

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

12.7 Establishing outdoor wireless networks

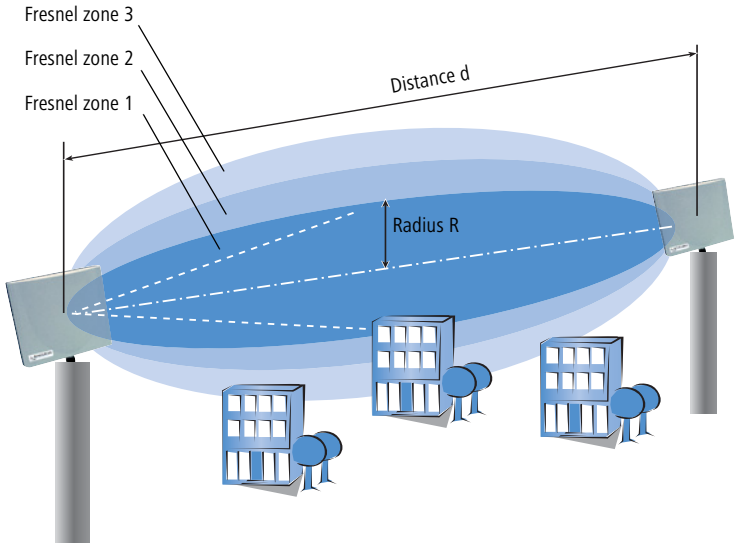
LANCOM access points in combination with appropriate external antennae are ideally suited to establishing point-to-point wireless connections to other access points.

There are two main questions to be answered when setting up the wireless connection:

- How should the antennae be positioned to ensure a problem-free connection?
- What performance characteristics do the antennae need to ensure sufficient data rates within legal limitations?

12.7.1 Geometrical layout of the transmission path

Antennae do not emit their signals linearly, but within an angle that depends on the model in question. The spherical expansion of the signal waves is characterized by constructive and destructive interference between these waves at certain distances perpendicular to the line of sight between transmitter and receiver. The areas where the waves amplify or cancel themselves out are known as Fresnel zones.



To ensure an optimal signal reception between transmitter and receiver, the Fresnel zone 1 should remain free from any obstruction. Any disturbances from elements protruding into this zone will significantly reduce 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 the signal reception.

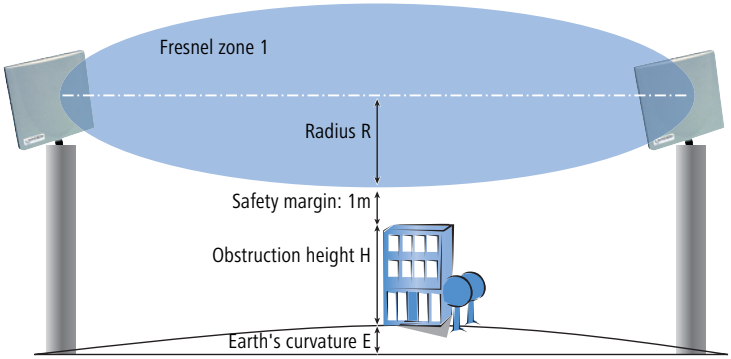
The radius (R) of Fresnel zone 1 is calculated with the following formula assuming that the signal wavelength (λ) and the distance between transmitter and receiver (d) are known.

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

The wavelength in the 2.4-GHz band is approx. 0.125m, 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 antennae must exceed that of the highest obstruction by this radius. The full height of the antenna mast (M) should be as depicted:



M = R + 1m + H + E (Earth's curvature)

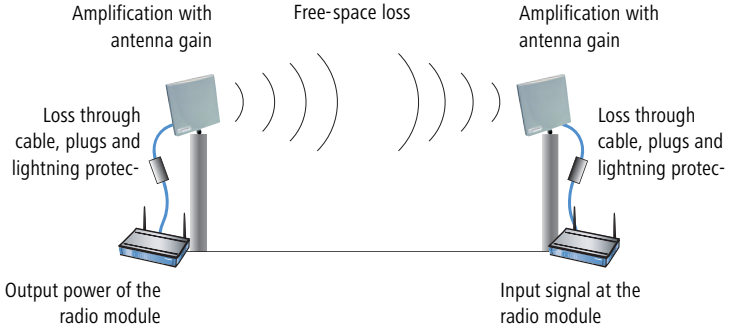
The height of the Earth's curvature (E) is calculated from the distance (d) $E = d^2 * 0{,}0147$ – even at a distance of 8 km that results in almost 1m!

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**.

12.7.2 Antenna power

The power of the antenna must be high enough to ensure acceptable data transfer rates. On the other hand, the country's legal limitations on 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, and even the air, and amplifying elements such as the external antennae.



① The calculation of the power over the path begins at the transmitters's radio module. The radio module in the LANCOM access points in 802.11a mode emits the following power levels depending on the channel used and the data transmission rate:

Mbps	5.150 - 5.250 GHz	5.250 - 5.350 GHz	5.470 - 5.725 GHz	5.725 - 5.850 GHz
6	17	17	17	17
9	17	17	17	17
12	17	17	17	17
18	17	17	17	17
24	17	17	17	17
36	14	14	14	14
48	13	13	13	13
54	12	12	12	12
72 (Turbo)	14	14	14	14
96 (Turbo)	13	13	13	13
108 (Turbo)	12	12	12	12

To achieve a data transmission rate of 24 Mbps the radio module emits a power of 17 dBm.

The data transmission rate is set according to the reception power. A WLAN module has an input sensitivity equivalent to a power level of, for example, -80dBm. If the received power falls below this level, then a lower data rate can be switched in that corresponds with an improved sensitivity with a lower level of power.

② Outdoor wireless connections are usually realised with external antennae and extension cables together with lightning protection for safety. The power loss from the cable is approx. 1 dB per metre. A cable 4 m long thus reduces power by 4 dB, the lightning protection and the various plug connections also lead to the loss of a further 1 dB. Thus the power of the external antenna is:
17 dBm - 4 dB - 1 db = 12 dBm.

③ The power received by the antenna is then amplified. An AirLancer Extender O-18a (with an emitting angle of 18°) supplies an antenna gain of 18 dBm. The total power output from the antenna is thus:

12 dBm + 18 dBm = 30 dBm.

This power emission must be within the legal limits of the country where the antenna is in operation!

④ Radio transmission through air is subject to power attenuation from the so-called "free-space loss" x, which is logarhythmically related to the distance d (in km) between transmitter and receiver.

x = 100 + 20 * log (d) [dB] in the 2.4-GHz band

x = 105 + 20 * log (d) [dB] in the 5-GHz band

A 802.11a transmission over a distance of 4 km results in a free-space loss x of:

x = 105 dB + 20 * log (4) dB = 105 dB + 12 dB = 117 dB.

⑤ A 10 dB safety margin is added to this attenuation so that the total loss for this example can be taken as 127 dB.

⑥ This loss between the transmitting and receiving antenna is subtracted from the output power of the transmitting antenna:

30 dBm - 127 dBm = - 97 dBm.

This determines the reception power at the receiving antenna.

⑦ The receiving end also has amplifying and attenuating elements. If the same antenna is used as at the transmitter, the antenna gain is 18 dB and the loss from cable (again 4m), lightning protection and plug connectors is 5 dB. The radio signal thus arrives at the receiver's radio module with the following power:

- 97 dBm + 18 dBi - 5 dB = -84 dBm.

⑧ From the table for reception sensitivity of the radio module, the attainable data rate can be read off, in this case 24 Mbps:

	Reception sensitivity 802.11a [dBm]	
Mbps	**5.150 - 5.725 GHz**	**5.725 - 5.850 GHz**
6	-90	-85
9	-89	-84
12	-88	-83
18	-87	-82
24	-85	-80
36	-81	-76
48	-76	-71
54	-73	-68
72 (Turbo)	-78	-73
96 (Turbo)	-73	-68
108 (Turbo)	-70	-65

This values are the result of a calculation that includes a 'safety margin' of 10dB. As every radio path is unique, these values can only serve as a rough guide.

12.7.3 Emitted power and maximum distance

For a simplified calculation of attainable distances and data rates for AirLancer Extender antennae, please refer to the following table. All tables include a 10 dB safety reserve and can be considered to be realistic.

For each antenna, the table has a column for point-to-point mode (P2P, connection between two access points) and for point-to-multipoint mode (P2mP, connection from an access point to the registered clients, e.g. notebooks).

The last column in the table shows the transmission power reduction to be set so that the upper limits of 30 dBm (802.11a) or 20 dBm (802.11b/g) cannot be exceeded.

The specifications for 802.11a apply only for Germany, the Netherlands, Luxembourg and Great Britain. In Belgium, Austria and Switzerland, only the 802.11b/g standard is approved for outdoor use.

AirLancer Extender O-18a (802.11a)

- Antenna gain: 18 dBi
- Assumed cable loss: 4 dB

	Maximum distance [km]	
Mbps	**P2P**	**P2mP**
6	7,94	1,78
9	7.08	1,58
12	6,31	1,41
18	5,62	1,26
24	4,47	1,00
36	2,00	0,45
48	1,00	0,22
54	0,63	0,14
72 (Turbo)	1,41	0,32
96 (Turbo)	0,71	0,16
108 (Turbo)	0,45	0,10

AirLancer Extender O-30 (802.11b/g)

- Antenna gain: 15 dBi

- Assumed cable loss: 9 dB

	Maximum distance [km]	
Mbps	**P2P**	**P2mP**
1,0	2,82	1,58
2,0	2,51	1,41
5,5	2,24	1,26
6,0	2,24	1,26
9,0	2,24	1,26
11,0	2,00	1,12
12,0	1,78	1,00
18,0	1,41	0,79
24,0	1,00	0,56
36,0	0,71	0,40
48,0	0,35	0,20
54,0	0,18	0,10

AirLancer Extender O-70 (802.11b/g)

- Antenna gain: 8.5 dBi
- Assumed cable loss: 6 dB

	Maximum distance [km]	
Mbps	**P2P**	**P2mP**
1,0	1,26	1,06
2,0	1,12	0,94
5,5	1,00	0,84
6,0	1,00	0,84
9,0	1,00	0,84
11,0	0,89	0,75
12,0	0,79	0,67
18,0	0,63	0,53
24,0	0,45	0,38

	Maximum distance [km]	
Mbps	P2P	P2mP
36,0	0,32	0,27
48,0	0,16	0,13
54,0	0,08	0,07

12.7.4 Transmission power reduction

Every country has regulations concerning the permissible output power from WLAN antennae, often with differences according to the WLAN standard or divided according to indoor or outdoor use. The output power from external antennae may not exceed these maximum power levels. The relevant power level is the result of adding the radio module power and the antenna gain, and subtracting the loss from cable, connectors and lightning protection.

Setting the transmission power reduction is described in the section 'Radio settings' → page 370.

12.8 Enhanced UMTS Card Support for the LANCOM 3550 Wireless

In combination with the LANCOM UMTS/VPN option, devices of type LANCOM 3550 Wireless can provide an additional WAN interface via UMTS and, with this, realize the following applications, among others:

- Backup via UMTS if DSL or other WAN connections break down, especially in connection with VRRP. The LANCOM 3550 Wireless is therefore suitable for securing any network using UMTS as long as the routers that are used in the network (Cisco or similar products) work with VRRP (see also 'Backup Solutions and Load Balancing with VRRP' → page 501).
- "Last Mile" via UMTS as broadband Internet access in regions without DSL
- Mobile conference room for flexible work groups

The LCOS version 5.20 offers LANCOM enhanced card support (status: December 2005):

Card	Network Operator	Services
Novatel U530, U630	T-Mobile Vodafone O2 e-plus	GPRS/UMTS GPRS/UMTS GPRS/UMTS GPRS/UMTS
Option GT 3G Fusion (from LCOS 5.20)	T-Mobile e-plus NL-KPN	GPRS/UMTS/WLAN GPRS/UMTS/WLAN GPRS/UMTS/WLAN
Option GT 3G Quad (from LCOS 5.20)	T-Mobile Vodafone	GPRS/UMTS GPRS/UMTS

Option UMTS cards are currently marketed, for example, by Vodafone as "Mobile Connect 3G/WLAN/GPRS Data Cards" and by T-Mobile as "Multimedia NetCard GPRS/UMTS/WLAN" and "Multimedia NetCard GPRS/UMTS".

The latest interoperability list can be found on the LANCOM Internet site.

For LANCOM 3550 Wireless models the Option UMTS cards are supported only as of hardware revision "MOD D1", "MOD D2" and later. Devices with a hardware revision prior to "MOD D1" resp. without any MOD labelling are not suitable for operation with Option cards due to the clock rates used. The hardware revision (MOD 0, MOD 1, MOD 2 etc.) can be found on a sticker at the bottom of the device.

12.9 Bandwidth limits in the WLAN

The bandwidths that are available can be limited so that they can be better distributed among several participants in the WLAN. This bandwidth limit is available for wireless ISPs, for example, who want to provide their customers with a defined bandwidth.

Unlike bandwidth management using QoS (Quality of Service), this procedure does not allow a minimum bandwidth, but an exactly defined maximum bandwidth instead. Even if more bandwidth were actually available due to low traffic from other network stations, only the bandwidth specified here is provided to the user.

The settings differentiate between operating a device as an access point or in client mode.

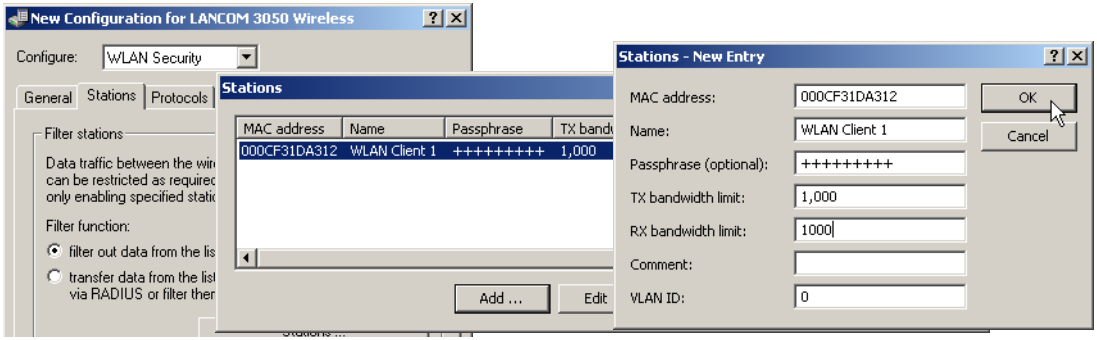
12.9.1 Operating as an access point

In the access point operating mode, the maximum permitted bandwidths can be specified in Tx and Rx direction for the WLAN clients that register with the access point. The values of the maximum Tx and Rx bandwidths are entered in kbps in the MAC access list. A value of '0' indicates that there is no intention to restrict the bandwidth in this transmission direction. The bandwidth that is actually provided is determined from the value that is entered here and the value that is transmitted by the client.

The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an access point, Rx stands for "Send data" and Tx stands for "Receive data".

Configuration with LANconfig

The maximum bandwidths for the connected clients are entered in LANconfig in the MAC access list in the 'WLAN Security' configuration area on the 'Stations' tab page.



Configuration with WEBconfig, Telnet or SSH

Under WEBconfig, Telnet or SSH client you will find the MAC access list under the following paths:

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

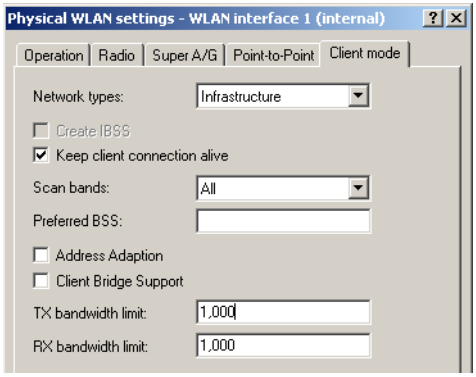
12.9.2 Operating as a Client

If the device is operated as a WLAN client, the device can transmit its maximum bandwidth when it registers with the access point. The access point then provides the actual maximum bandwidths with proprietary limits for this client where necessary.

The significance of the Rx and Tx values depends on the device's operating mode. In this case, as a client, Tx stands for "Send data" and Rx stands for "Receive data".

Configuration with LANconfig

The maximum bandwidths for a device in client mode are entered in LANconfig in the 'Interfaces' configuration area on the 'Wireless LAN' tab page for the 'Physical WLAN Settings' on the 'Client Mode' tab page.



Configuration with WEBconfig, Telnet or SSH

Under WEBconfig, Telnet or SSH client you will find the client settings under the following paths:

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

12.10WLAN according to 802.11h – ETSI 301 893

12.10.1Standards

IEEE standards

In November 2002, the 5 GHz band was released for private use in Germany, and opened up the path for significantly faster WLAN connections according to the IEEE 802.11a standard, which had already been available for a while. The wider use of 5 GHz WLANs was, however, restricted by its exclusive use in closed spaces and the relatively low transmission power.

With the 802.11h enhancement in September 2003, the private use of the 5 GHz band was finally possible even outside closed spaces. To protect military applications in the 5 GHz band, the DFS (Dynamic Frequency Selection) and TPC (Transmission Power Control) procedures were prescribed. Moreover, the use of DFS and TPC can achieve significantly higher transmission powers (maximum 1000 mW) than the other standards that were previously valid.

ETSI standards

ETSI adopted the first standard for controlling remote data transfers back in 1996 under the name of Hiperlan (High Performance Radio Local Area Networks). The first version (Hiperlan Type 1) was intended for use in the frequency range of 5.15 to 5.30 GHz with a transmission rate of 20 MBit/s. As no manufacturers took up this standard, Hiperlan initially had no practical significance.

With the new version, Hiperlan Type 2, in 2000, ETSI introduced a WLAN solution that operates in the 5 GHz band similarly to IEEE 802.11a, and also provides a gross data rate of 54 MBps. However, as the frequencies and the OFMD modulation method that was also used for 802.11a overlapped, it was necessary to adapt the standards between IEEE and ETSI to avoid disruptions to the systems.

European harmonization

To standardize the use of the 5 GHz band in Europe, the European Commission issued the ETSI 301 893 standard on July 11, 2005. The member states of the EU are obliged to implement this by October 31, 2005.

Instead of the three sub-bands described in the 802.11a/h standards (5150 - 5350 MHz, 5470 - 5725 MHz and 5725 - 5875 MHz for the UK), the ETSI 301 893 standard regulates the three following areas with different specifications:

- 5150 -5250 MHz
- 5250 -5350 MHz

- 5470 - 5725 MHz

The guidelines focus on preventive measures for avoiding disruptions to other systems that use the same frequency band. This includes radar equipment that counts as "primary applications". The "secondary applications" such as WLAN have to change the frequency as soon as a conflict is detected.

- Dynamic Frequency Selection – DFS

  Dynamic Frequency Selection (DFS) was stipulated to prioritize primary applications. DFS initially assumes that no channel is available in the corresponding frequency band. The WLAN device selects an arbitrary channel at the start and performs what is known as a Channel Availability Check (CAC). **Before** sending to a channel for 60 seconds (Channel Observation Time, COT), a check is run to see if a different device is already working on this channel and the channel is therefore occupied. If this is the case, then a different channel is checked by the CAC. If not, then the WLAN device can perform the transmission operation.

  Even during operation, a check is run to see if a primary application such as a radar device is using this channel. This exploits the fact that radars frequently work according to the rotation method, whereby a tightly bundled directional transmission signal is transmitted by a rotating antenna. A remote receiver perceives the radar signal as a short pulse (radar peak). If a device receives such a radar peak, then it initiates the transmission operation and monitors the channel for further pulses. If additional radar peaks occur during the COT, then a new channel is selected automatically.

  Such as check has to take place every 24 hours. This is why interrupting the data transmission for 60 seconds is unavoidable.

  DFS is stipulated for the frequency ranges of 5250 - 5350 MHz and from 5470 - 5725 MHz. It is optional for the frequency range of 5150 - 5250 MHz.

- Transmission Power Control – TPC

  Dynamically adjusting the transmission power is intended to reduce interference from radio technology.

  Dynamically adjusting the transmission power facilitates the shared use of the 5250-5350 MHz and 5470 - 5725 MHz frequency bands with satellite services. TPC should cause an average reduction in the transmission power by at least 3 dB compared with the maximum permitted transmission power. TPC determines the minimum transmission power necessary to maintain the connection with the partner (such as an access point). If TPC is not used within these frequency bands, then the highest permissible average EIRP and the corresponding maximum EIRP density are reduced by 3 dB. This restriction does not apply to the frequency range of 5150 - 5350 MHz.

  Without DFS and TPC, a maximum of only 30 mW EIRP is permitted. When DFS and TPC are used, a maximum 1000 mW EIRP is permitted as the transmission power (compared with 100 mW with 802.11 b/g, 2.4 GHz, DFS and TPC are not possible here). The higher maximum transmission power not only compensates for the higher attenuation of 5 GHz radio waves in air, it also makes noticeably longer ranges possible than in the 2.4 GHz range.

Differences from USA and Asia

The USA and Asia use different frequency bands and different maximum signal strengths to the European standard.

In the USA, three sub-bands, each 100 MHz wide, are used for wireless networks in the 5 GHz band. The "lower band" ranges from 5150 - 5250 MHz, the "middle band" ranges from 5250 - 5350 MHz and the "upper band" ranges from 5725 - 5825 MHz. In the lower band, a maximum average EIRP of 50 mW is permitted; in the middle band this is 250 mW and 1 W in the upper band.

In Japan, the use of the 5 GHz band is possible to a limited extent: only the lower band of 5150 - 5250 MHz is released for private use.

12.10.2Radio channels in the 5 GHz band:

In the usable frequency space of 5.13 to 5.805 GHz, up to 19 channels are available in Europe, divided into frequency ranges to which different conditions of use can apply:

- 5150 -5250 MHz (channels 36, 40, 44 and 48)
- 5250 - 5350 MHz (channels 52, 56, 60 and 64)
- 5470 - 5725 MHz (channels 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 and 140)
- 5725 - 5875 MHz (channels 147, 151, 155 and 167)

Note that the frequency ranges and radio channels in the 5725 to 5875 MHz range can only be used in Great Britain.

The following overview shows which channels may be used in the different regions.

Chan-nel	Frequency	ETSI (EU)	FCC (US)	Japan
36	5.180 GHz	yes	yes	yes
40	5.200 GHz	yes	yes	yes
44	5.220 GHz	yes	yes	yes
48	5.240 GHz	yes	yes	yes
52	5.260 GHz	yes	yes	no
56	5.280 GHz	yes	yes	no
60	5.300 GHz	yes	yes	no
64	5.320 GHz	yes	yes	no
100	5.500 GHz	yes	no	no
104	5.520 GHz	yes	no	no
108	5.540 GHz	yes	no	no
112	5.560 GHz	yes	no	no
116	5.580 GHz	yes	no	no
120	5.600 GHz	yes	no	no

Chan-nel	Frequency	ETSI (EU)	FCC (US)	Japan
124	5.620 GHz	yes	no	no
128	5.640 GHz	yes	no	no
132	5.660 GHz	yes	no	no
136	5.680 GHz	yes	no	no
140	5.700 GHz	yes	no	no
147	5.735 GHz	no	yes	no
151	5.755 GHz	no	yes	no
155	5.775 GHz	no	yes	no
167	5.835 GHz	no	yes	no

12.10.3Frequency ranges for indoor and outdoor use

The use of the methods described in ETSI 301 893 for reducing mutual interference in the 5 GHz band (TPC and DFS) is not stipulated for all fields of application. The following table gives information about the permitted use and corresponding transmission powers within the EU:

Frequency (GHz)	Transmission-power (mW/dBm)	Use	DFS	TPC
5,15-5,25	30/13	Indoor		
5,15-5,25	60/14	Indoor		✔
5,15-5,25	200/23	Indoor	✔	✔
5,25-5,35	200/23	Indoor	✔	✔
5,470-5,725	1000/30	Indoor/Outdoor	✔	✔

Other regulations may apply to use in other countries. Please refer to the current wireless network regulations for the country in which you want to operate a wireless LAN device, and make sure you configure the country in which you are operating the device in the WLAN settings.

□ WLAN according to 802.11h – ETSI 301 893

13 Voice over IP (VoIP)

13.1 Introduction

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 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.

Different terminology is used for telephony over a network (LAN or Internet) The terms "Voice over IP" or "IP telephony" are used as synonyms, although in actual fact they have different meanings.

- Strictly speaking, "Voice over IP" is merely a term for the technology of transmitting calls across data networks in real-time using the IP protocol (Internet protocol). The term is also used when the technology is implemented only in the provider's core networks, in what is known as the backbone
- The term "IP telephony" is used when the VoIP technology is also used in the terminal equipment, so that the call subscriber uses the IP network for telephony.
- "Internet telephony" is also used to describe telephony using VoIP over the Internet in general.

In the following, "Voice over IP" is usually used even to refer to IP telephony in accordance with general custom.

There are four basic types of terminal equipment that can be used for VoIP telephony:

- With software running on the PC, known as a "softphone".
- With an IP or VoIP telephone that is connected directly to the local network.
- With a conventional telephone that is connected to the local network by an adapter (analog telephone adapter, ATA).
- Via a VoIP gateway that converts telephone calls from telephones (analog and ISDN) to VoIP and can then communicate between the two "telephone worlds" like a PBX.

There is a basic difference between a VoIP connection being established between two pieces of terminal equipment that are connected directly to the data network (PC or IP telephone) and the situation where a subscriber in the land-line or mobile telephone network requires the conversion of the signaling, numbers and voice data. To differentiate the various connection variants, a device in the LAN has become known as a "PC", and a device in the land-line network has become known as a "phone".

PC-to-PC communication

With this application, the terminal equipment has to be integrated directly into the user's LAN. Examples are a PC, an IP telephone or a telephone that is connected to the LAN using an ATA.

Different software solutions are available for the PC, known as "softphones". Note that some of these programs can only communicate with users of the same software and not with softphones from other manufacturers. Communication is usually free of charge within the Internet. A current example is Skype, which uses its own protocol.

PC-to-phone and phone-to-PC communication

In this case, the call data has to be transmitted from the Internet to the landline network, usually using what are known as VoIP gateways. In general, these gateways are provided by providers and are subject to a fee.

VoIP routers offer another option that can switch VoIP calls to an ISDN line. Examples are different LANCOM VoIP Router types with an SIP gateway and ISDN interfaces. When the calls are transferred to the landline network, the usual telephone operator fees are charged.

So that the subscriber can even be called on a PC, he or she needs a VoIP telephone number that is usually provided by a provider.

VoIP providers usually only provide individual numbers and not complete number ranges with a root number and extension numbers. This is why the numbers that are provided by public providers are not attractive to many business customers. When the LANCOM VoIP Router is used with a SIP gateway, previously-used numbers can be maintained; the functions of VoIP telephony can also be used.

13.2 VoIP implementation in the LANCOM VoIP Router

The main task of the VoIP implementation in the LANCOM VoIP Router is to connect telephone calls from different local interfaces (LAN, WLAN, ISDN) to the WAN connections that can be accessed by the router. This enables switching between the local interfaces (local call) as well as between WAN interfaces.

The basis for the implementation and switching is the SIP protocol. The calls over all interfaces are converted into SIP by the interface converter (this mainly concerns the ISDN interfaces). The ISDN-ISDN bridge function is a special case that is activated when ISDN protocols cannot be mapped in SIP, which is why a bit-transparent connection is created between an ISDN-TE (external ISDN connection) and an ISDN-NT (internal ISDN connection).

Furthermore, the bit-transparent connection is usually used for calls between multiple local ISDN interfaces to achieve the highest possible compatibility and quality.

13.2.1 Example Applications

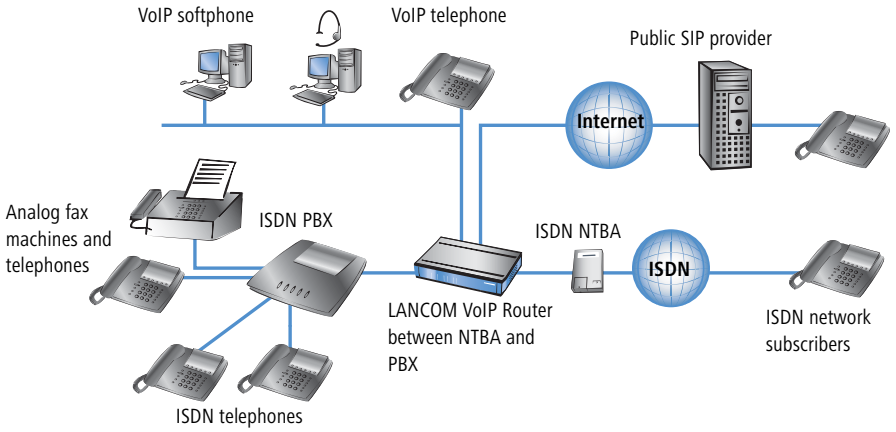
Voice over IP solutions offers advantages across a broad spectrum of applications, starting with small companies and extending to large corporations with extensive networks of subsidiaries. In the following section, we will demonstrate a number of examples.

Detailed information about configuration is available in the chapter 'Configuration of VoIP functions'.

Supplementing existing ISDN 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 ISDN connection (e.g. ISDN NTBA) and the ISDN PBX.

Telephone calls over the PBX and its ISDN telephones 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 telephones, VoIP telephones or VoIP softphones can be included in the telephone infrastructure. VoIP subscribers in the internal LAN are also able to call external ISDN subscribers.
- The ISDN telephones continue to function, and additionally they can call all of the internal VoIP 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, any other SIP subscriber worldwide can be called, irrespective of the provider network. As an alternative to a direct ISDN connection, ISDN 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.

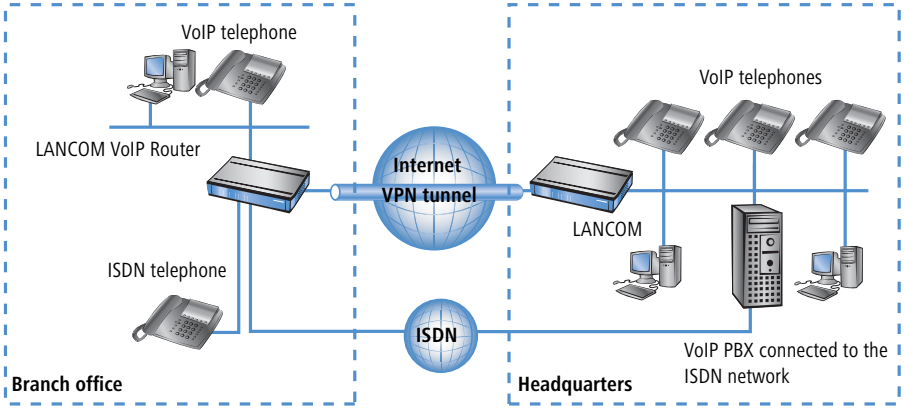
Connecting subsidiaries or home offices to the headquarters

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. Mit dem Einsatz von VoIP können die firmeninternen Gespräche über die ohnehin vorhandene VPN-Verbindung kostenlos und – dank der VPN-Verschlüsselung – abhörsicher geführt werden.

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

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 telecomms provider.

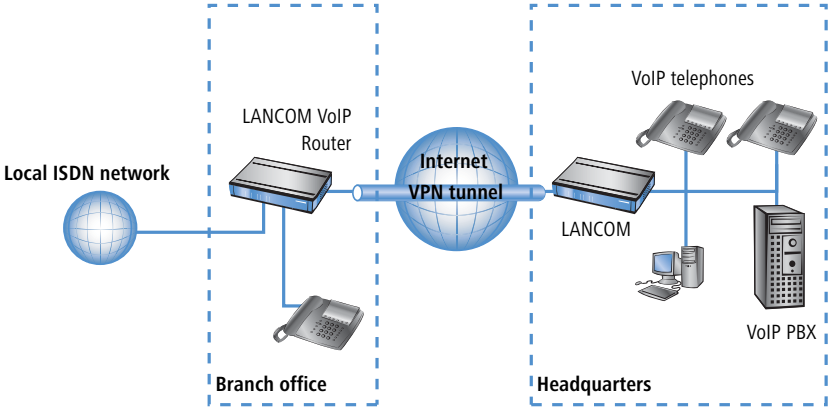
Connecting local ISDN lines with a remote SIP gateway

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 and ISDN telephones at a branch office to the SIP-PBX at headquarters; it can also integrate local ISDN networks into corporate communications with help of the "SIP Gateway" function.

The SIP 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 gateway located at their sales office in Italy. Customers can then reach support

or service numbers via a standard national telephone number. Calls from the local ISDN network 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.

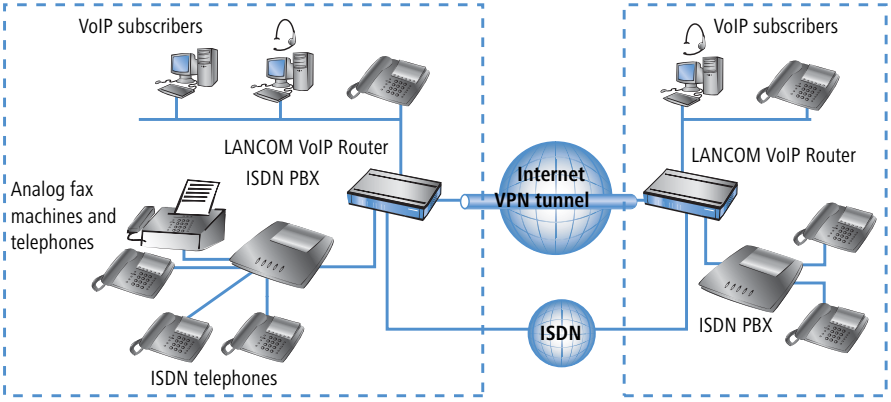


Advantages of the SIP gateway:

- The local ISDN 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 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 automatically directed to the optimal line for cost optimization.
- Incoming calls can be switched directly to the appropriate employee at a different location.

13.2.2 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 ISDN infrastructure with ISDN PBX and ISDN 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 ISDN world via ISDN NTBA or upstream ISDN 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.

- 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.

- 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.
- 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.

13.3 Call switching: Call routing

Alle Gespräche zwischen den internen Teilnehmern und den über die externen Leitungen erreichbaren Teilnehmern werden im LANCOM wie SIP-Gespräche behandelt – auch wenn die Verbindung zwischen zwei ISDN-Teilnehmern aufgebaut wird.

The call router in the LANCOM VoIP Router switches the call. The switching relies mainly on the information in two tables:

- For telephone numbers arriving at the call router, rules in the call-routing table are able to alter these numbers if needed and can decide which line to use for a call.

- The table for the locally registered user provides information about which terminal device is available at which internal telephone number.

The bandwidth reservation, QoS settings and firewall settings that are necessary for reliable transmission of voice data are carried out automatically by the LANCOM.

- When establishing a connection, the LANCOM checks (under consideration of the permitted codecs) which **maximum** bandwidth will potentially be required.
  - This bandwidth is then automatically reserved by the QoS module upon initiation of the connection.
  - If negotiation shows that the maximum bandwidth is not available, the connection will not be made.
  - If negotiations between the terminal devices can agree upon a codec with lower bandwidth requirements, then the reserved bandwidth will be lowered accordingly.
- All packets from ISDN users are given a DiffServ marking by the LANCOM (with SIP users, the QoS marking is usually handled by the telephones or softphones).
  - SIP packets for signaling are marked as CS1.
  - RTP packets are marked as EF.
- The ports required for the transmissions are activated automatically.

13.3.1 SIP proxy and SIP gateway

The tasks involved in switching calls between the different lines of SIP and ISDN subscribers are handled by two functions in the LANCOM VoIP Router.

- SIP proxy

  A SIP proxy handles the switching between callers.

- SIP gateway

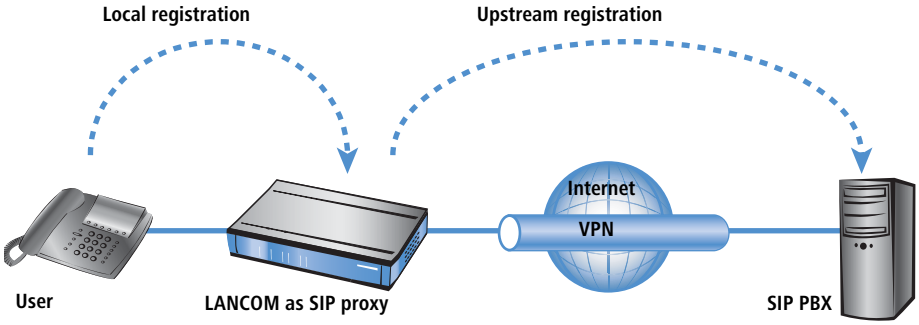
  The SIP gateway handles the conversion between IP-based telephony that uses the SIP protocol and other (telephone) networks, for example the ISDN network.

13.3.2 User registration at the SIP proxy

A LANCOM VoIP Router represents the central exchange for SIP calls between different subscribers who wish to communicate over different types of line. The task of switching in the LANCOM are handled by the SIP proxy. A telephone signals the SIP proxy that it needs to establish a connection, and the SIP proxy uses certain rules to decide which line is to be used for the connection. Conversely, incoming calls are assigned to a certain terminal device by the SIP proxy according to its rules.

For terminal devices to be able to take part in this switching, they must be registered with the SIP proxy. Where the registration is limited to call switching by the LANCOM, we refer to "local registration".

Werden weitere Vermittlungsstellen – wie z.B. eine SIP-TK-Anlage an einem anderen Standort – in die Vermittlung der Gespräche mit einbezogen, spricht man von einer übergeordneten Anmeldung. In this case, the LANCOM accepts the request for registration and forwards it upstream. In this instance, the LANCOM is described as "transparent proxy".



The great advantage with this two-stage registration comes to bear in the backup event: If the connection to an upstream SIP PBX is not available, the SIP proxy can handle the user who is registered upstream as a local user and can then direct the calls over alternative lines.

Registration at the LANCOM VoIP Router (local registration)

For local registration at the LANCOM, it is initially sufficient for the user to send a valid VoIP domain to the SIP proxy. The internal VoIP domains of the LANCOM VoIP Router are valid, as are all domains entered in a SIP line.

- For SIP terminal devices in the LAN (SIP telephone or SIP softphone), the domain is entered in the configuration. There is no need for an entry as a SIP user in the configuration of the LANCOM. This variant is known as "automatic registration".
- The domain cannot be entered into ISDN terminal equipment; instead, ISDN users have to be registered in the LANCOM configuration with a corresponding entry as an ISDN user (→ Dynamic ISDN users at point-to-point connections).
- To prevent unknown subscribers from registering, authentication at the SIP proxy can be set as a prerequisite to local registration (local authentication). In this case, an entry as a SIP or ISDN user in the LANCOM configuration is essential.

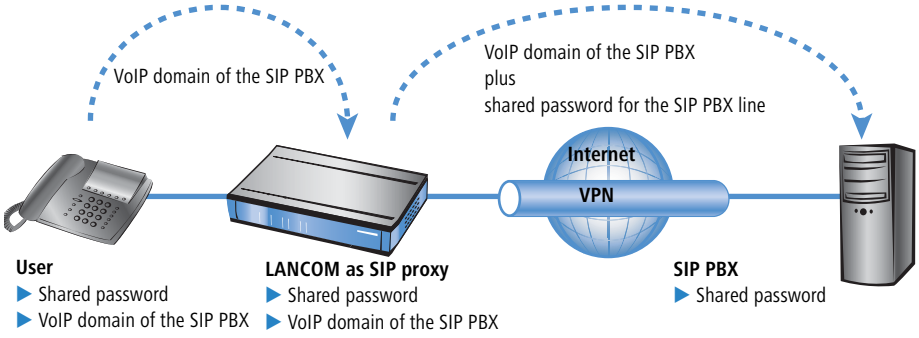
Automatic registration without entering a password is restricted to the SIP users in the LAN. SIP users in the WAN require an appropriate user entry and authentication by password.

Registration at an upstream SIP PBX (upstream registration)

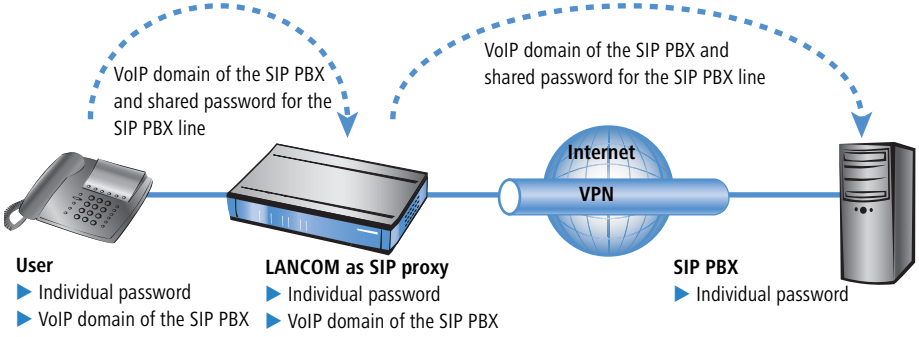
Generally, authentication by user and password is always required for registration at a SIP PBX. There are two possible ways of transmitting the authentication data to the SIP PBX:

- All SIP and ISDN users at the LANCOM VoIP Router end use the same shared access information. In this case, only the VoIP domain for the SIP PBX and the appropriate user ID are entered into the SIP terminal device. For

ISDN users, the VoIP domain of the SIP PBX is entered into the LANCOM as an ISDN user. The SIP proxy recognizes the request for registration at the upstream SIP PBX if the domain communicated from the client agrees with a domain entered into the SIP PBX line. The proxy then forwards the registration data together with the shared password to the SIP PBX.



- If SIP or ISDN users at the LANCOM VoIP Router are entered into the SIP PBX with different passwords, then the users have to enter their individual passwords upon registration. Consequently, each SIP or ISDN user has an entry into the LANCOM with the individual passwords, which are also entered into the SIP terminal devices. Users with shared and individual passwords can be managed in parallel.



Particular aspects for ISDN users

Integrating ISDN terminal equipment into the LANCOM VoIP environment and the necessary steps for configuration depend upon the application at hand and, if applicable, upon the options available with a PBX. The main questions to be answered by the user are as follows:

- Can ISDN terminal devices telephone internally with SIP users?
- Are ISDN terminal devices available externally over SIP lines?
- Can ISDN terminal devices telephone externally over SIP lines?

To answer these questions, we differentiate between the following constellations:

- If ISDN terminal equipment can be reached over an ISDN TE interface on the LANCOM, it is described as "upstream". From the perspective of the LANCOM, the ISDN terminal devices are on an external line. This ISDN terminal equipment is normally not classified as being for local users, and so no entries for ISDN users are necessary.

  ISDN terminal equipment at an upstream ISDN PBX...

  - can make internal calls to SIP users if the corresponding telephone numbers are configured as internal MSNs in the ISDN PBX.
  - can receive internal calls from SIP users if the internal MSNs of the ISDN equipment are output to the ISDN line by the call-routing table, for example over a standard route.
  - can only make calls over SIP lines if the PBX is able to output certain call numbers over its internal ISDN bus. Otherwise, all calls not matching with its internal MSNs would be forwarded by the ISDN PBX to the public telephone network.
  - can only receive calls from an upstream SIP PBX if entered into the LANCOM as an ISDN user and registered as such with the SIP PBX.
- If ISDN terminal equipment can be reached over an ISDN NT interface on the LANCOM, it is described as "downstream". For the LANCOM, this is then a local subscriber that can be reached via the list of registered users. As ISDN terminal equipment cannot send domain information to register at the LANCOM, it must be entered as an ISDN user so that it can be recognized by the VoIP system.

  ISDN terminal equipment at a downstream ISDN PBX...

  - can make internal calls to SIP users by entering the character for an outside line as required by the PBX and then dialing the SIP user's internal number. Die TK-Anlage gibt den Anruf dann mit der internen Rufnummer des SIP-Benutzers – ohne das Amtsholungszeichen – auf ihrem externen ISDN-Bus an das LANCOM weiter.
  - can receive internal calls from SIP users as long as the entry for the ISDN user contains the correct allocation of the internal number to the appropriate MSN. The LANCOM takes a call to the ISDN user's internal number, translates it to the MSN, and outputs it to the allocated ISDN bus. The PBX receives the MSN as if it were an external call and forwards it to the corresponding ISDN terminal equipment.
  - can conduct incoming and outgoing calls over SIP and ISDN just like SIP users. Again, the outside-line code may be necessary for outgoing calls.

Dynamic ISDN users at point-to-point connections

When connecting downstream PBXs to a point-to-point interface of the LANCOM VoIP Router, the number of possible ISDN terminal devices is only limited by the length of the extension number. With three-figure extension numbers, almost 1000 terminal devices can be connected, all of which can be managed as ISDN users in the LANCOM VoIP Router.

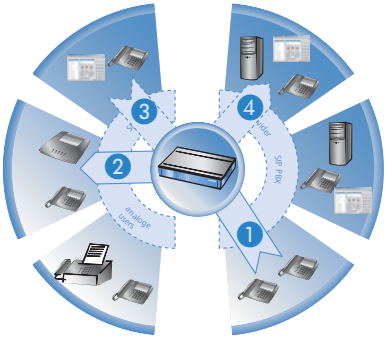
Through an ISDN user entry with a # character as a placeholder for the telephone numbers, all ISDN terminal devices with their respective extension numbers can be set up as dynamic ISDN users.

User entries that use # characters to map user groups cannot be used for registration at an upstream PBX. This registration always demands a specific entry for the individual ISDN user.

13.3.3 Number translation at network transitions

LANCOM VoIP Router switch calls between different telephone networks, e.g. the ISDN network, various SIP provider networks, and the internal telephone network. These networks generally have different ranges of numbers or even completely different conventions for addressing subscribers. Whereas the traditional land-line network uses numerical characters with country code and area access codes, the world of SIP allows alphanumerical names along with domain information.

The transition between these zones must guarantee the correct translation of "telephone numbers" so that the intended subscriber can be reached. For example, when a call from the land-line network arrives at a public MSN, the requested telephone number has to be translated to the ISDN user's internal number. This act of translation is known as "mapping". Mapping incorporates not only the **called** number, which represents the destination, but the **calling** number for the source as well.



Mapping the destination telephone number
1. external MSN from the ISDN network
2. internal telephone number of the ISDN user

Mapping the source telephone number
3. internal telephone number of the SIP user
4. external SIP telephone number in the SIP provider's network

Depending on the application at hand, both the called and the calling numbers have to be modified so that a return call can be made to the source number.

Call number translation at the transition to outside lines is primarily implemented by mapping entries in the ISDN and SIP lines and by rules in the call-routing table.

13.3.4 The Call Manager

The Call Manager has the central task of allocating the calls waiting to be switched to a certain line or to a certain user. The Call Manager makes this allocation by using the call-routing table and the list of registered users. The calls are switched in the following steps:

- Processing of called numbers (Calling Party ID)

  First of all there is a check to see whether a numeric or alphanumeric number is available. Typical dialing separators such as "()-/" and <blank> are removed. A leading "+" is left in place. In this case, the number is still

treated as a numeric number. If the check reveals any other alphanumerical character, the number is treated as alphanumeric and remains unchanged.

- Resolving the call in the call routing table

  After processing the Called Party ID, the call is passed over to the call-routing table. Entries in the call-routing table consist of sets of conditions and instructions. Die Einträge – mit Ausnahme der Default-Routen – werden der Reihe nach durchsucht, der erste Eintrag wird ausgeführt, bei dem **alle** angegebenen Bedingungen erfüllt sind.

- Resolution of the call with tables of local subscribers

  If no entry is found in the call-routing table, then the Call Manager searches through the list of local subscribers. Call routing considers all of the users known to the call router (registered SIP users, configured ISDN users). If an entry is found that agrees with the called number and that has the matching destination domain, then the call is delivered to the corresponding subscriber.

  If there is no local subscriber with matching number and destination domain, then the following cycle searches for an agreement between the number of the local subscriber and the called number; the destination domain is ignored.

- Resolution of the call with default entries in the call-routing table

  If the preceding cycles referring to the call-routing table and lists of local subscribers remain unsuccessful, then the waiting call is checked once again with the call-routing table. This pass only takes the default routes into account, however. The numbers and destination domains entered into the default routes are ignored. Only the source filters are processed, assuming that the default routes has these filters.

Specific examples of call-routing procedures can be found in the configuration examples described.

13.3.5 Making telephone calls with the LANCOM VoIP Router

Using the LANCOM VoIP Router opens up a variety of new possibilities for making telephone calls. Depending on the constellation of terminal equipment implemented (e.g. SIP or ISDN telephones, SIP or ISDN PBX systems) and, depending on the configuration for call routing in the LANCOM VoIP Router, certain information is critical for understanding the establishment of connections.

Automatic outside line access

Using the LANCOM VoIP Router and the enhancement with VoIP functionality within your telephone structure is designed to support the users' telephone behavior with the greatest possible convenience. One of the core aspects of this is the use of "spontaneous" or "automatic" outside line access, a feature that is familiar to users of standard PBX systems.

- Die meisten TK-Anlagen sind so eingestellt, dass die Telefonteilnehmer der gewünschten Rufnummer eine „0“ voranstellen müssen, um eine Amtsleitung zu bekommen – um also ein Gespräch über ein öffentliches Telefonnetz führen zu können.

Without the "0" prefix, the number dialed is considered to be an internal number from another extension line on the private PBX.

- If "automatic outside line access" is set up, all numbers dialed are directed over the public telephone network. In this case, internal telephone calls to other extensions are not possible or only possible when a special symbol is dialed before the number.

When the telephone structure is extended with a LANCOM VoIP Router, a variety of new possibilities become available for connecting telephone terminal equipment. This includes the existing analog or ISDN telephones (where necessary, connected to the respective PBX) or VoIP terminal equipment such as SIP telephones or PCs with VoIP software.

As a new and central building block in the telephone structure, the LANCOM VoIP Router assumes many of the PBX tasks for connected terminal equipment. As such, you can also set up the automatic outside line access for the terminal equipment connected to the LANCOM VoIP Router directly for the ISDN or SIP subscriber groups, thereby adapting it to existing telephone behavior.

- When automatic outside line access is turned off, subscribers must dial a "0" before the desired number in order to carry out a telephone conversation via a public telephone network.

  All calls without a "0" preceding the number will be treated as calls to internal extensions within the private telephone network.

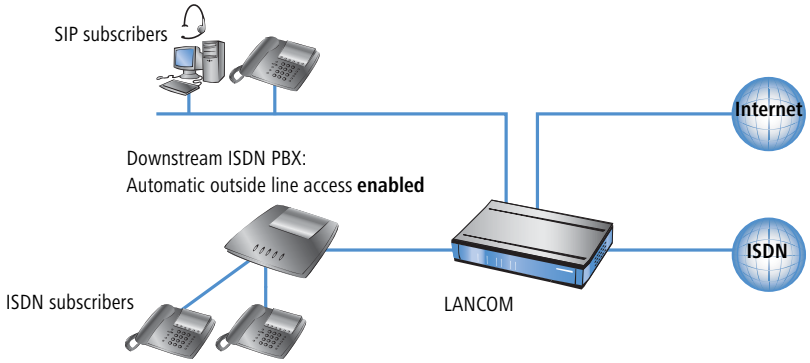
- If automatic outside line access is turned on, all numbers dialed will be directed over a public telephone network.

  For telephone calls to internal extensions, a special symbol or a specific number combination must be dialed before the number. With the standard settings, when automatic outside line access is enabled, a star * is activated as the identification symbol for an internal number. This setting can be adjusted to match the character that you are familiar with.

If you operate the LANCOM VoIP Router on the extension line of a PBX, it is recommended that outside line access for the router be configured in the same way as for the PBX so that the behavior remains the same from the user's perspective.

■ Example of a downstream PBX

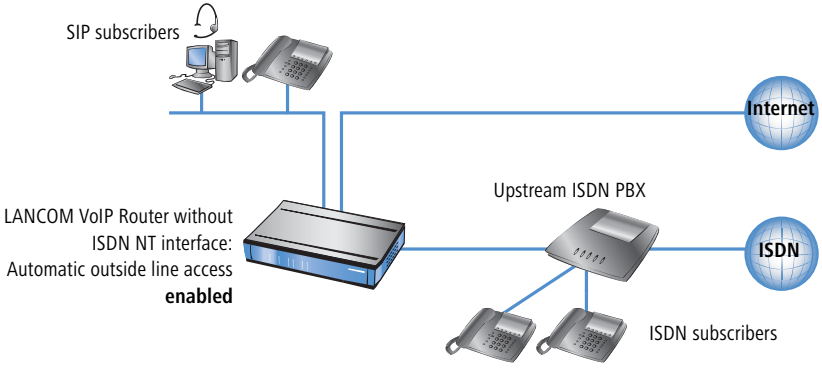
A LANCOM is switched between the ISDN outside line and the existing ISDN PBX. In the PBX, automatic outside line access is enabled, the call router settings for the LANCOM decide whether or not a "0" must be dialed for outside line access for the connected ISDN and SIP subscribers.



If the LANCOM VoIP Router in this constellation is not available, for example, due to a power outage, the ISDN connection for the downstream ISDN PBX is automatically "bridged" to the external ISDN connection (when life-line support is enabled). For a LANCOM VoIP Router **without** automatic outside line access, the ISDN subscribers should not dial a "0" before the number while the life-line support is active.

■ Example of an upstream PBX

A LANCOM VoIP Router is connected to an ISDN PBX extension line. In the LANCOM VoIP Router, automatic outside line access is enabled, the settings for the upstream PBX decide whether or not a "0" must be dialed for outside line access for the connected ISDN and SIP subscribers.



Dialing various numbering areas

When dialing other parties, the following numbering areas are available for use:

- **Internal numbers** are comparable to the extension line numbers for traditional PBX systems ("extension"). Subscribers can reach each other directly using these internal numbers without having to go through a public telephone network.

  The internal numbers must be unique for all subscribers within the private telephone network, this also includes any other PBX systems that may be connected!

  The internal subscribers can be reached by simply dialing the internal number without a "0" preceding it.

Depending on the settings for automatic outside line access ('Automatic outside line access' → page 418), a special preceding dialing signal may be required.

- Via **local telephone numbers** you can reach external parties who are in the same local telephone network as the LANCOM VoIP Router, i.e. users with the same area code as the public line for the LANCOM VoIP Router.

  In decentralized locations that extend beyond city or state boundaries, the physical location of the device is decisive, even if a central PBX is located at a different location. Therefore, for a LANCOM VoIP Router in London, all telephone subscribers in the local telephone network for London can be reached using local numbers, even if a SIP PBX connected via VPN can be reached in Manchester.

Depending on the settings for automatic outside line access ('Automatic outside line access' → page 418), a "0" prefix may be required.

- The **national and international numbers** behave in the same way as local numbers; here, the physical location of the devices is decisive for the assignment of corresponding access codes. Therefore, a LANCOM VoIP Router in Austria belongs to the national telephone network in Austria, even if there is a VPN connection to the SIP PBX at the headquarters in Germany.

Depending on the settings for automatic outside line access ('Automatic outside line access' → page 418), a "0" prefix may be required.

Special numbers

Certain special numbers (emergency numbers, toll-free or particularly expensive service numbers) can be subjected to special treatment by the call router.

- For example, this ensures that emergency numbers for the police or fire department are always secured, even if the subscribers do not dial the correct preceding dialing signal for outside line access.

  With the standard settings, the emergency numbers "110" and "112" are configured in such a way that they can be dialed correctly with or without the preceding "0".

- For toll-free numbers such as "0800", a direct connection via ISDN is usually selected in order to use the toll-free land-line to land-line connection.

Dialing using specific lines

With the LANCOM VoIP Router, other lines, in addition to the previously existing ISDN exchange lines, can be defined for voice communication, i.e. to a SIP PBX connected via VPN or to a public SIP provider via the Internet. Each time a connection is established, the call router decides which of the existing lines is to be used for the call based on predetermined rules.

As an alternative to the automatic selection by the call router, you can direct individual calls to a certain line, for example when you want to call a party purposely via ISDN and not via the SIP PBX at the headquarters. For this purpose, the call router assigns specific code numbers to existing lines, such as "98" for ISDN or "97" for a SIP provider. The targeted call via this line is then initiated with the corresponding identifier:

- The call with "020 123456" is assigned to a corresponding line by the call router, e.g. via the SIP PBX at the headquarters.
- However, the call with "98 020 123456" is made directly via the ISDN connection by the call router.

13.3.6 Supporting digital calls

LANCOM VoIP Routers support digital calls, e.g. when using Group 4 fax machines or when using ISDN terminal equipment for dialing in to particular networks. To direct these calls over an ISDN interface of the LANCOM VoIP Router, destination numers can be given special prefixes ('Dialing using specific lines' → page 422).

13.4 Configuration parameters for the Voice Call Manager

13.4.1 Basic settings

- **Voice Call Manager (VCM) activated, operating**
  Switches the Voice Call Manager between active / not active

Configuration tool	Call
LANconfig	Voice Call Manager ▶ General
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager

- **Domain**
  Name of the domain in which the connected telephones and the LANCOM VoIP Router are operated.
  - □ Terminal devices working in the same domain register as local subscribers at the LANCOM VoIP Router and make use of the SIP proxy.

□ Terminal devices working with the other domain of an active SIP PBX line register themselves as subscribers at an upstream PBX.

Configuration tool	Call
LANconfig	Voice Call Manager ▶ General
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > General

■ **Dial completion after, Overlap Timeout**

When dialing from an ISDN telephone, this time period is waited until the called number is considered as complete and sent to the call router.

Valid values: 1 to 99

Special values: With a dial delay of '0', a '#' has to be entered at the end of the called number. Entering the '#' character after the called number manually reduces the dial delay.

Configuration tool	Call
LANconfig	Voice Call Manager ▶ Users
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > General

■ **Generate dial tone, Internal-Dial-Tone**

The dial tone determines the noise an ISDN user hears after lifting up the receiver. The "internal dial tone" is the same as the tone that a user hears at a PBX without spontaneous outside-line access (three short tones followed by a pause). The "external dial tone" is thus the same as the tone that indicates an external line when the receiver is lifted (constant tone without any interruptions). If necessary, adapt the dial tone for ISDN users with spontaneous outside-line access to simulate the behavior of a standard ISDN connection.

Configuration tool	Call
LANconfig	Voice Call Manager ▶ Users
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > User > ISDN User

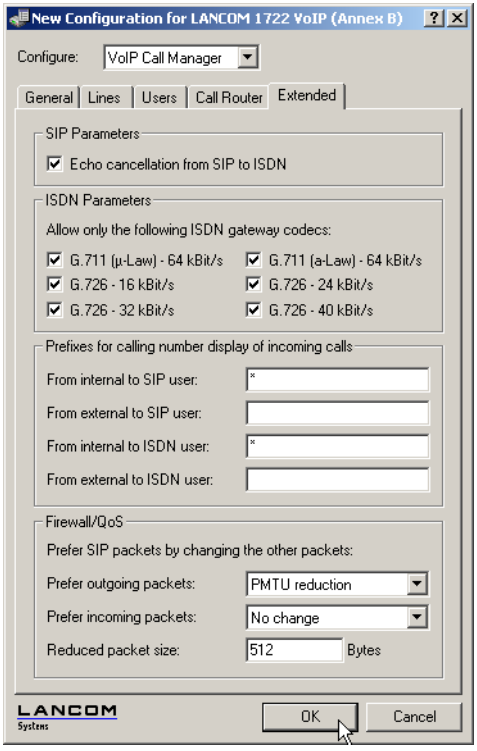
■ Force local authentication, Local-authentication

The SIP proxy usually accepts a registration from all SIP users who register themselves with a valid domain. If local authentication is forced, only those subscribers who are saved in one of the user tables with relevant access information can register with the SIP proxy.

Configuration tool	Call
LANconfig	Voice Call Manager ▶ Users
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > General

Automatic registration without entering a password is restricted to the SIP users in the LAN. SIP users from the WAN and ISDN users must always be authenticated by a user entry with password.

13.4.2 Extended settings



- **Echo canceling from SIP to ISDN, Echo-Canceler**

  Activates the echo canceling of remote echoes. With an echo that is too strong, subscribers can hear their own voices after a short delay. Activating this option reduces the ISDN echo at the SIP > ISDN gateway.

- **ISDN gateway codecs**

  During connection establishment, the ISDN terminal devices negotiate which codecs are to be used to compress the voice data. Use the codec filter to restrict the codecs that are permitted and to permit only certain codecs.

- **Prefer outgoing packets, Outgoing-packet-reduction**

  Depending on the audio codec that is used for SIP calls, sufficient bandwidth through the firewall is reserved (provided sufficient bandwidth is available). To control the firewall, you can configure how the remaining data packets that do not belong to the SIP data stream are handled.

  ▷ **PMTU reduction**

  The subscribers of the data connection are informed that they should only send data packets up to a certain length (Path Maximum Transmission Unit, PMTU).

▷ **Fragmenting**

The LANCOM VoIP Router reduces the data packets by fragmenting them to the required length.

▷ **No change**

The length of the data packets is not changed by the VoIP operation.

For more information, see the description of PMTU and fragmenting with regard to quality of service ('Reducing the packet length' → page 243).

■ **Prefer incoming packets, Incoming-packet-reduction**

Similar to the outgoing data packets, you configure how non-VoIP data packets are handled when bandwidth is reserved for SIP data.

▷ **PMTU reduction**

The subscribers of the data connection are informed that they should only send data packets up to a certain length (Path Maximum Transmission Unit, PMTU).

▷ **No change**

The length of the data packets is not changed by the VoIP operation.

■ **Reduced packet size, Reduced-packet-size**

This parameter specifies the packet size that should be used for PMTU adjustment or fragmentation while the SIP data have priority.

Configuration tool	Call
LANconfig	Voice Call Manager ▶ Extended
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > General

■ **Internal prefix for SIP users, Intern-Cln-Prefix**

This prefix is added to the calling party ID, if available, for an incoming, **internal** call if the call is directed to a SIP user.

A call is regarded as external if it comes from a "line". If this line is a SIP PBX line, then the call is only external if the incoming calling party ID is preceded by a "0". All other calls are regarded as internal.

For more information about handling the calling party ID, see 'Behandlung der Calling Party ID' → Seite 473.

Configuration tool	Call
LANconfig	Voice Call Manager ▶ Extended
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > SIP User

- **External prefix for SIP users, Extern-Cln-Prefix**

  This prefix is added to the calling party ID, if available, for an incoming, **external** call if the call is directed to a SIP user.

Configuration tool	Call
LANconfig	Voice Call Manager ▶ Extended
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > SIP User

- **Internal prefix for ISDN users, Intern-Cln-Prefix**

  This prefix is added to the calling party ID, if available, for an incoming, **internal** call if the call is directed to an ISDN user. If a line prefix is defined, this is placed in front of the whole of the called number.

Configuration tool	Call
LANconfig	Voice Call Manager ▶ Extended
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > ISDN User

- **External prefix for ISDN users, Extern-Cln-Prefix**

  This prefix is added to the calling party ID, if available, for an incoming, **external** call if the call is directed to an ISDN user. If a line prefix is defined, this is placed in front of the whole of the called number.

Configuration tool	Call
LANconfig	Voice Call Manager ▶ Extended
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > ISDN User

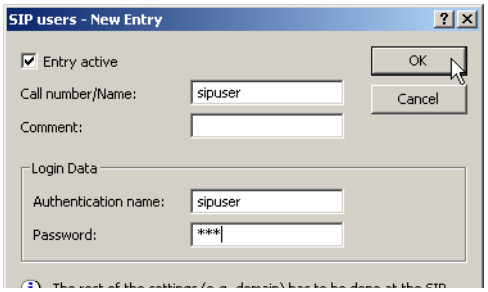
13.4.3 Configuration of users

Local users are the terminal equipment/telephones that are connected to the LANCOM VoIP Router. There is a difference between:

- SIP users: Users who are connected to the LAN by means of a SIP telephone. For the user configuration, it does not matter whether the LAN is connected directly to LANCOM, or whether it is connected via a VPN (over the Internet).
- ISDN users: Users who are connected by ISDN. They use the SIP gateway to telephone using the VoIP function.

SIP users

Depending on the model, different numbers of SIP users can be created. You cannot create more than the maximum number of users permitted; similarly, duplicate names or called numbers are not permitted.



The domain that is used by the SIP subscriber is usually configured in the terminal equipment itself.

The following parameters can be used to define a SIP user:

- **Telephone number/SIP name, Number/Name**

  Telephone number of the SIP telephone or name of the user (SIP URL).

- **Authentication name, Auth-Name**

  Name for the authentication during registration to the SIP proxy. If nothing is entered here, the authentication is attempted using the SIP name.

- **Password, Secret**

  User password.

- **Entry active, Active**

  User is active / not active.

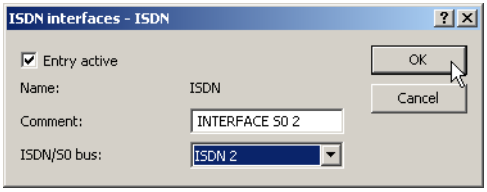
- **Comment**

  Comment on the user

Configuration tool	Call
LANconfig	Voice Call Manager ▶ User ▶ SIP User
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > User > SIP User

ISDN interface, Interfaces

For users who are connected by an ISDN line, the interface that is used is configured globally. An ISDN T interface (external) or even an ISDN TE interface (internal) can be configured. The latter is the case if users of an upstream PBX are to be managed as local users.



- **ISDN interface, Ifc**

  Interface to which the ISDN subscribers are connected.

- **Entry active, Active**

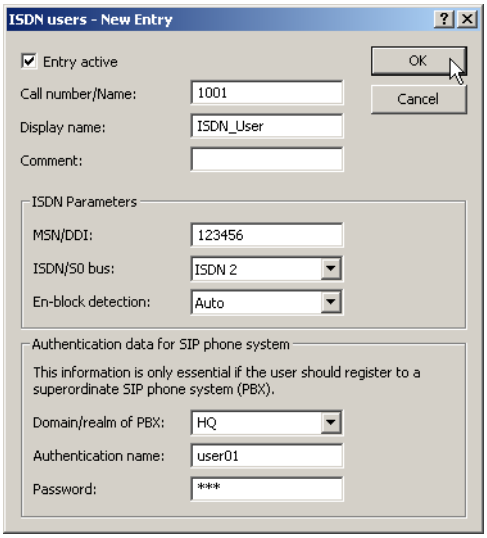
  Interface is active / not active.

- **Comment**

  Comment on the ISDN interface

Configuration tool	Call
LANconfig	Voice Call Manager ▶ User ▶ ISDN User
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > User > ISDN User > Interfaces

ISDN subscribers



- **Telephone number/SIP name, Number/Name**

  Internal number of the ISDN telephone or name of the user (SIP URL).

By using the # character as a placeholder, entire groups of numbers (e.g. when using extension numbers at a point-to-point connection) can be addressed via a single entry. With the number '#' and the DDI '#', for example, extension numbers can be converted into internal telephone numbers without making any changes. With the call number '3#' and the DDI '#', for example, an incoming call for extension '55' is forwarded to the internal number '355', and for outgoing calls from the internal number '377', the extension number '77' will be used.

User entries that use # characters to map user groups cannot be used for registration at an upstream PBX. This registration always demands a specific entry for the individual ISDN user.

- **Display name, Display-Name**

  Name for display on the telephone being called.

- **ISDN/S_0 bus, Ifc**

  ISDN interface that should be used to establish the connection.

- **MSN/DDI**

  Internal MSN that is used for this user on the internal ISDN bus.

  - MSN: Number of the telephone connection if it is a point-to-multipoint connection.
  - DDI (Direct Dialing in): Telephone extension number if the connection is configured as a point-to-point line.

By using the # character as a placeholder, entire groups of call numbers, e.g. when using extension numbers, can be addressed via a single entry ('Telephone number/SIP name, Number/Name' → page 430).

User entries that use # characters to map user groups cannot be used for registration at an upstream PBX. This registration always demands a specific entry for the individual ISDN user.

- **Block dial, Dial-Compl**

  Block dial detection:

  - automatic: Block dialing is detected automatically (for example, with speed dial or repeat dialing), so that the call is established more quickly. Suffix dialing is not possible.
  - off: No block dialing; the number can be marked as complete with '#' and the call can be initiated.

- **Domain/realm, Domain**

  Domain of the upstream SIP PBX.

  Only required when the user registers at an upstream SIP PBX.

- **Authentication name, Auth-Name**

  Name for the authentication during registration to the SIP proxy.

  Only required when the user registers at an upstream SIP PBX.

- **Password, Secret**

  User password.

  Only required when the user registers at an upstream SIP PBX.

- **Entry active, Active**

  User is active / not active

- **Comment**

  Comment on the user

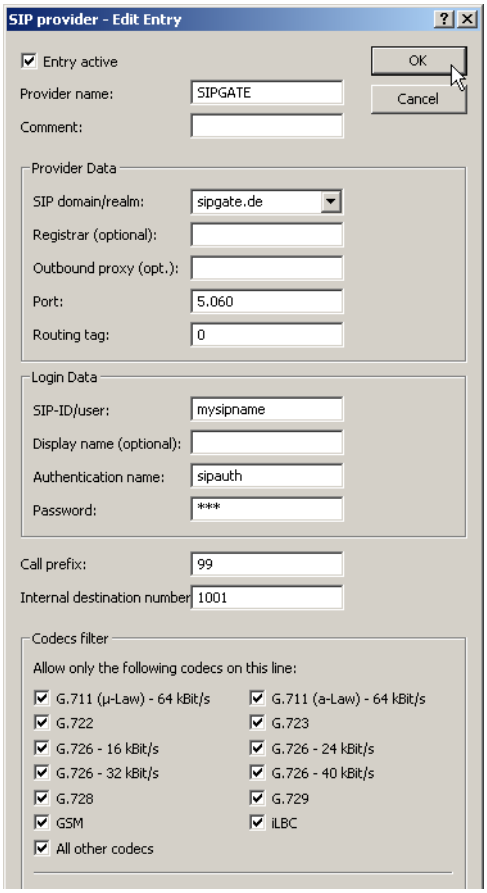
Configuration tool	Call
LANconfig	Voice Call Manager ▶ User ▶ ISDN User
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > User > ISDN User

13.4.4 Line configuration

Lines from/to SIP remote stations

The device uses these lines to register with other SIP remote stations (usually SIP providers or remote gateways at SIP PBXs). The connection is made either over the Internet or a VPN tunnel.

Up to 16 SIP lines can be entered.



■ **Mode**

SIP line operating mode:

- Single account: The line provides a connection to a SIP provider account that has a single telephone number. This line can only be used for one call at a time. Incoming calls will be forwarded to the internal number entered under 'Internal dest. number'.
- Trunk: The line provides a connection to a SIP provider account that has a root number and multiple extension numbers (DDI). This line can support multiple telephone calls at once. Incoming calls will, together with the registered DDI, be passed over to the call router. Calls with an unknown DDI will be forwarded to the internal number entered under 'Internal dest. number'.

- □ Gateway: The line provides a connection to an upstream SIP PBX as a transparent gateway. The numbers of incoming and outgoing calls are not modified. This line can support multiple telephone calls at once.

Please observe the notices about 'SIP mapping' → page 435.

- **Provider name, Name**

  Name of the line; may not be identical to another line that is configured in the device.

- **SIP domain/realm, Domain**

  Domain of the SIP remote station.

- **Outbound proxy, Ip**

  Further information about the SIP remote station for the proxy that is in use can optionally be entered here.

- **Port**

  TCP / UDP port that is used for the connection.

  Standard value '5060'.

  This port has to be activated in the firewall for the connection to work.

- **Routing tag**

  Routing tag for selecting a certain route in the routing table for connections to this SIP provider (also see 'Policy-based routing' → page 109).

- **SIP ID/user, Name**

  Telephone number of the SIP account or name of the user (SIP URL).

  For a SIP trunking account, the root number is entered here.

  - □ For incoming calls, any numerals after the root number are interpreted as extension numbers (DDI) and these are passed to the call router.
  - □ For outgoing calls, DDI numbers received from the call router are combined with the root number.

Please observe the notices about 'SIP mapping' → page 435.

- **Authentication name, Auth-Name**

  Name for the authentication during registration to the SIP proxy

- **Password, Secret**

  User password.

- **Call prefix, Cln-Prefix**

  With incoming calls using this line, this prefix is placed in front of the calling number so that the correct line is automatically selected for a return call.

■ **Internal destination number, Number/Name**

The function of the internal destination number depends on the SIP line mode.

- □ Single account: The SIP account works with just one number, so that for incoming calls it is not clear to which terminal equipment the call is to be directed. Incoming calls on this line are therefore transferred to the call router with this destination number. If no suitable entry for forwarding this number is found, the call is delivered directly to this telephone number as an internal number.
- □ Trunk: Any numerals after the root number are interpreted as extension numbers (DDI). If the SIP account sends the root number (global call), then the call is forwarded to the number defined here.
- □ Gateway: The internal destination number has no function in this operating mode.

■ **Codec filter, Codecs**

While the connection is being established, the terminal equipment concerned negotiate which codecs are to be used to compress the voice data. Use the codec filter to restrict the codecs that are permitted and to permit only certain codecs.

If no common the codecs can be agreed upon, no connection is made.

■ **Quality/bandwidth, Codec-Order**

This parameter influences the order in which the codecs are presented during connection establishment.

- □ No optimization

  Leaves the order of the codecs unchanged
- □ Best quality

  Changes the order of the codecs that are offered to achieve the best voice quality possible.
- □ Minimum bandwidth

  Changes the order of the codecs that are offered to achieve the lowest bandwidth possible.

■ **Entry active, Active**

SIP line is active / not active

■ **Comment**

Comment on the line

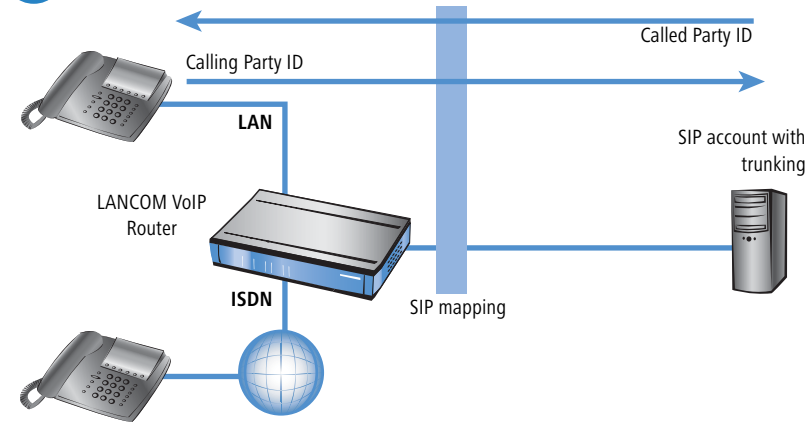
Configuration tool	Call
LANconfig	Voice Call Manager ▶ User ▶ Lines ▶ SIP Provider
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > Line > SIP Line

SIP mapping

The entries made under SIP mapping establish a series of rules for number translation to SIP lines in the trunk or gateway mode. Up to 40 mapping rules can be entered.

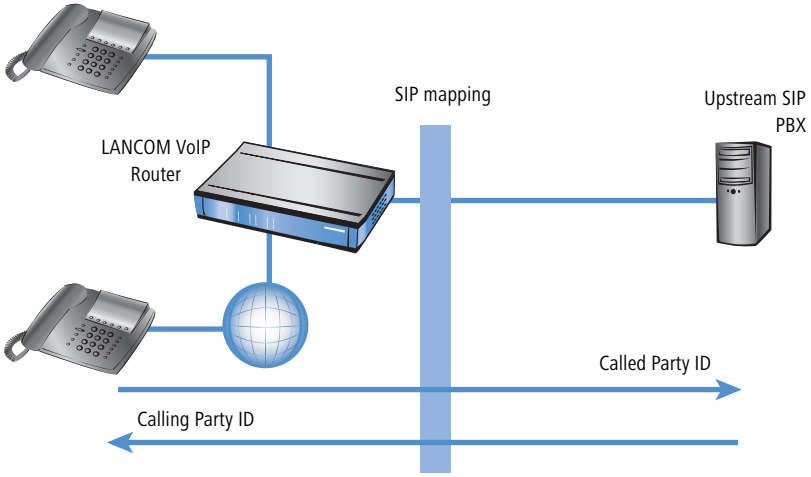
- A SIP line in trunk mode is used for mediating between internal numbers and the range of telephone numbers offered by a SIP account.
  - For incoming calls, the destination number (called party ID) is modified. The internal number is used if the called party ID matches with the external telephone number.
  - For outgoing calls, the calling party ID is modified. The external number is used if the calling party ID matches with the internal telephone number.

For SIP mapping on trunk lines, only the extension (DDI) is mapped. The extension is interpreted as those numerals which follow the root number (SIP ID or SIP line).



- For a SIP line in gateway mode, the telephone number plan of the upstream SIP PBX is adapted to the internal numbers in the call router.
  - For incoming calls (from the SIP line), the calling party ID is modified. The internal number is used if the calling party ID matches with the external telephone number.
  - For outgoing calls (to the upstream PBX), the destination number (called party ID) is modified. The external number is used if the called party ID matches with the internal telephone number.

For SIP mapping to gateway lines, the full telephone number is mapped.
Depending on the configuration, the call number arriving at the ISDN interface can be subjected to further mapping (ISDN mapping).



- **Trunk/gateway name**

  Name of the line which is the target of the call number mapping.

- **Comment**

  Comment about this rule.

- **External number / name**

  Call number within the range of those used by the SIP trunk account or upstream SIP PBX.

- **Rufnummern-Länge [Default: 0]**

  This value defines the number of numerals required for a called number to be regarded as complete. It only applies to SIP gateway lines with entries that end in a # symbol.

  For an outgoing call, the external called number generated from this entry is automatically regarded as complete according to the defined number of numerals, and then forwarded. This process speeds up the dialing process. Alternatively, the called number is regarded as complete when:

  - The user concludes the dialed number with a # symbol, or
  - a precisely matching entry was found in the SIP mapping table without a # symbol, or
  - the wait time expires.

Setting the length of called number to '0' deactivates premature dialing from the length of called number.

■ **Internal destination number**

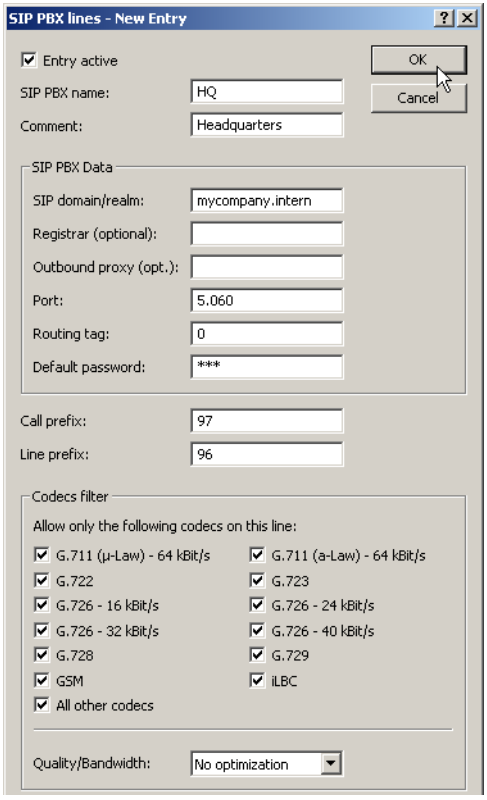
Called number inside the range of the LANCOM VoIP Router.

Using the # symbol as a placeholder allows blocks of numbers to be captured by one rule.

Line from/to upstream SIP PBXs

These lines are used to configure connections to upstream SIP PBXs, which are usually connected via VPN.

Up to 4 SIP PBXs can be entered.



■ **SIP PBX name, Name**

Name of the line; may not be identical to another line that is configured in the device.

■ **SIP domain/realm, Domain**

Domain of the SIP provider.

- **Proxy or registrar, Ip**

  You have the option of entering further information about the SIP provider or registrar for the proxy that is used.

- **Port**

  TCP / UDP port that is used for the connection.

  Standard value '5060'.

  This port has to be activated in the firewall for the connection to work.

- **Routing tag**

  Routing tag for selecting a certain route in the routing table for connections to this SIP provider.

- **Standard password, Secret**

  Password for registering at the SIP PBX. This password is only required if SIP subscribers want to register at the PBX, but are not created as SIP users with their own access information in the list of SIP users.

- **Call prefix, Cln-Prefix**

  With incoming calls using this line, this prefix is placed in front of the calling number so that the correct line is automatically selected for a return call.

- **Line prefix, Line-Prefix**

  With outgoing calls using this line, this prefix is placed in front of the calling number to create a complete telephone number that is valid for this line. With incoming calls this prefix is removed, if present.

- **Codec filter, Codecs**

  While the connection is being established, the terminal equipment concerned negotiate which codecs are to be used to compress the voice data. Use the codec filter to restrict the codecs that are permitted and to permit only certain codecs.

If no common the codecs can be agreed upon, no connection is made.

- **Quality/bandwidth, Codec-Order**

  This parameter influences the order in which the codecs are presented during connection establishment.

  - □ No optimization

    Leaves the order of the codecs unchanged

  - □ Best quality

    Changes the order of the codecs that are offered to achieve the best voice quality possible.

  - □ Minimum bandwidth

    Changes the order of the codecs that are offered to achieve the lowest bandwidth possible.

- **Entry active, Active**

  Line is active / not active.

■ **Comment**

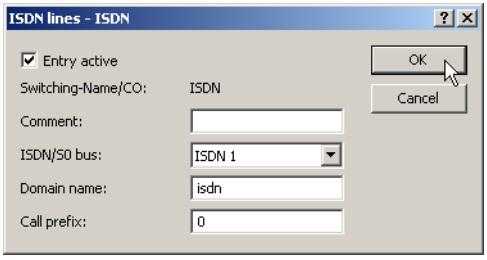
Comment on the line

Configuration tool	Call
LANconfig	Voice Call Manager ▶ User ▶ Lines ▶ SIP PBX Lines
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > Line > SIP PBX

13.4.5 ISDN network lines

The ISDN connections are configured over these lines. In addition to the physical ISDN line to be used, a telephone number translation is configured as well. This ensures the internal telephone number or SIP URL is converted to an external ISDN number.

ISDN lines



■ **Switching name/CO**

Name of the line; may not be identical to another line that is configured in the device.

■ **ISDN/S_0 bus, Ifc**

ISDN interface(s) with which the LANCOM VoIP Router is connected to the ISDN network. The line entered here are usually configured as ISDN-TE.

■ **Domain name, Domain**

Domain in which the calls from/to the ISDN line are managed in LANCOM's SIP world.

■ **Call prefix, Cln-Prefix**

With incoming calls using this line, this prefix is placed in front of the calling number so that the correct line is automatically selected for a return call.

■ **Entry active, Active**

Line is active / not active.

■ **Comment**

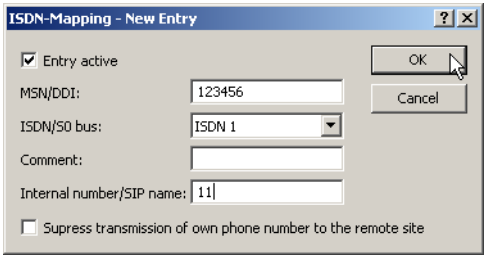
Comment on the line

Configuration tool	Call
LANconfig	Voice Call Manager ▶ User ▶ Lines ▶ ISDN Lines
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > Line > ISDN > Interfaces

ISDN mapping

ISDN mapping assigns external ISDN telephone numbers (MSN or DDI) to the telephone numbers that are used internally.

You can enter up to 64 telephone number assignments.



■ **MSN/DDI**

External telephone number of the connection in the ISDN network.

For incoming calls that are directed to this number, the corresponding internal telephone number is entered as the destination number. For outgoing calls, this number is transmitted as the caller's number, unless this has been suppressed.

- □ MSN: Number of the telephone connection
- □ DDI (Direct Dialing in): Telephone extension number if the connection is configured as a point-to-point line.

By using the # character as a placeholder, entire groups of call numbers, e.g. when using extension numbers, can be addressed via a single entry.

■ **ISDN/S_0 bus, Ifc**

ISDN interface(s) used for connecting terminal devices to the LANCOM VoIP Router. These line have to be configured as ISDN-NT.

■ **Telephone number/SIP name, Number/Name**

Internal telephone number of the ISDN telephone or name of the user (SIP URL).

For incoming calls, this is the SIP name or internal telephone number of the telephone to which the call from this interface is switched with the corresponding MSN/DDI. For outgoing calls, the SIP name is replaced by the MSN/DDI of the corresponding entry.

By using the # character as a placeholder, entire groups of call numbers, e.g. when using extension numbers, can be addressed via a single entry.

- **Hide your telephone number from the person called, CLIR**
  The display of your telephone number is suppressed so the person called cannot see it.
- **Entry active, Active**
  External telephone number is active / not active.
- **Comment**
  Comment on the external telephone number.

Configuration tool	Call
LANconfig	Voice Call Manager ▶ User ▶ Lines ▶ ISDN Mapping
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > Line > ISDN > Mapping

13.5 Processing Destination Domains

As the VoIP implementation in the LANCOM VoIP Router handles all calls as SIP calls, telephone numbers and SIP subscribers contain domain information. Furthermore, SIP numbers can also contain alphanumeric characters.

The SIP domains are used in LCOS as follows:

- When SIP subscribers register at upstream PBXs or at the LANCOM VoIP Router itself.
- When SIP subscribers establish a connection.

LCOS supports the following defined domains:

- ISDN for the ISDN interfaces
- All domains that are entered for the lines

13.5.1 Registration at upstream exchanges

Local SIP subscribers can only register using the domains that are known. The subscribers authenticate themselves at the local LANCOM VoIP Router with their user name and password. This excludes domains that correspond to an upstream SIP PBX. These registrations are authenticated in the upstream SIP PBX.

If a subscriber tries to register with an unknown domain, then this may be accepted as a local registration ('Force local authentication, Local-authentication' → page 424).

13.5.2 Switching internal calls

For internal connections, internal numbers are generally assigned unambiguously. However, SIP telephones, for example, can register with several "lines", such as '1011@provider.com' and '1011@isdn.com', so that a line can be assigned specifically to the required connection.

With internal switching, an attempt is made to find a subscriber whose number and domain match. Only if this was not successful is the call placed using the destination number only. The domain remains unchanged.

For example, calls that are incoming via ISDN (from <calling pty id>@isdn) are switched to subscriber 1011 (to 1011@isdn). The call to the SIP telephone is displayed on the ISDN line key. If there is no such subscriber with such a domain, then the call is delivered to the first known subscriber '1011'.

13.6 ISDN interface configuration

LANCOM VoIP Router routers feature several ISDN interfaces with which they can be connected to ISDN exchange lines, or with which ISDN terminal equipment can be connected to them.

- 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.
- 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, up to eight B channels as a backup or for dial-in.
- With multiple NT interfaces, for example, a downstream ISDN PBX can be provided with up to eight 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 connnection to be used (point-to-multipoint or point-to-point).

13.6.1 Point-to-multipoint and point-to-point connections

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-Nummer (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.

13.6.2 Bus termination, life-line support and power relay

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

- **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.

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!

Not for all LANCOM VoIP Router

- 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 device 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 at another ISDN bus. 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!

Further information about settings for life-line support and ISDN power relay can be found in the user manual for your LANCOM VoIP Router.

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.

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.

13.6.3 Protocol setting

Paramters 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 maintain the ISDN timing of the connected ISDN line, please refer to 'ISDN connection timing'
- **Off**

NT mode operation always has to be set manually.

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

13.6.4 ISDN connection timing

To ensure trouble-free transmission, all of the components in the ISDN system (LANCOM VoIP Router, upstream and downstream ISDN PBXs and ISDN terminal devices) 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.

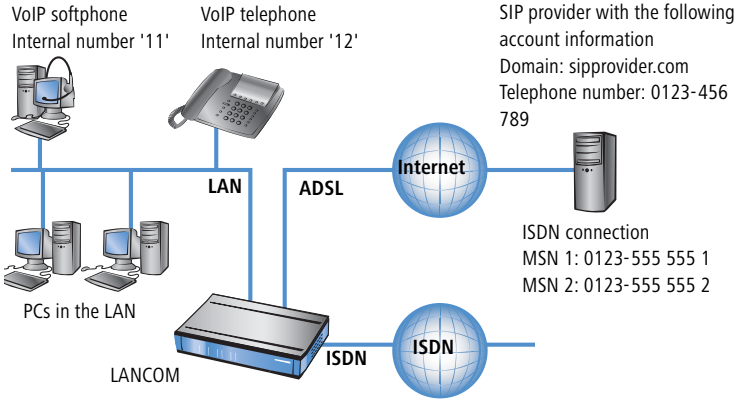
There are various ISDN interface settings to define the ISDN interface which is to supply the LANCOM VoIP Router with the ISDN timing to be passed on to the devices at the NT interfaces.

- **Automatic**: If no interface has been manually selected for the timing, the device automatically searches for a TE interface that is supplying a timing. To ensure that the timing is synchronous, the TE connectors constanty try to keep the connection activated. This ensures that the timing continues to be supplied even if one of multiple TE lines should be shut off. If none of the TE connectors supply a timing, then the timing system runs "freely" and uses the internal timing of the LANCOM VoIP Router.
- **DSS1 timing**: 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. Apart from passing on the ISDN timing, the interface is not active.
- **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.

13.7 Configuration examples

13.7.1 VoIP telephony for stand-alone use

This example shows how to configure a LANCOM which is used as a central device for Internet connectivity and VoIP telephony at a new site.



Target

- Internal telephony with SIP telephones and SIP softphones.
- Access to internal terminal equipment via the MSNs.
- External telephony via the SIP provider with backup over ISDN.
- Calls to emergency and special numbers via ISDN.

Requirements

- LANCOM connected to the LAN and WAN, an ISDN TE interface is linked to the ISDN NTBA. The Internet connection has been set up.
- A telephone number plan with a unique internal telephone number for all terminal equipment to be connected, here, for example, the number '11' for the VoIP softphone and the number '12' for the VoIP telephone.
- A SIP provider account.

Using the information during configuration

The following table provides a summary of the information required for configuration and where it can be entered. SIP terminal equipment parameters can be entered using the SIP telephone keypad, the corresponding configuration software, or the softphone configuration menu.

	LANCOM	SIP terminal equipment
Internal VoIP domain	4	4
Internal numbers	4	4
External SIP telephone number	4	
Access information for SIP account	4	
External ISDN telephone numbers (MSNs)	4	
Country and local area code	4	

Configuring the LANCOM

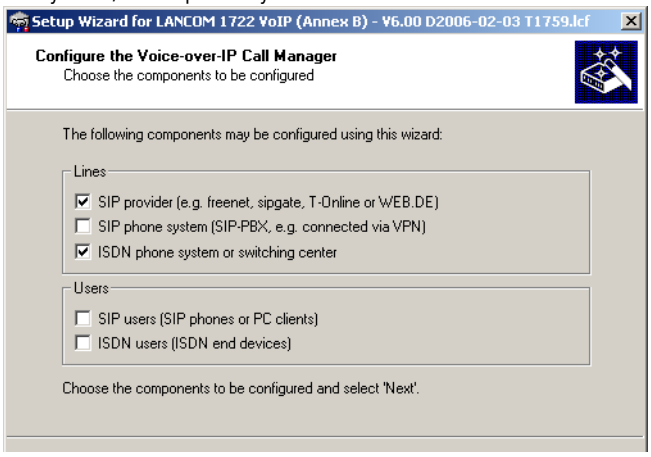
When configuring the LANCOM, the following steps must be carried out:

- Setting up the line to the SIP provider
- Enabling the ISDN interface and assigning MSNs to the internal numbers

In this example, it is not necessary to configure SIP users: The SIP users are registered at the LANCOM with the settings created in the terminal equipment (softphone and VoIP telephone).

Detailed instructions on configuring the LANCOM:

① Under LANconfig, start the setup wizard for configuring the VoIP Call Manager. Enable the options 'SIP phone system', 'ISDN phone system' and 'ISDN users'.



② Enter a unique domain for the local VoIP domain which describes the local VoIP range for the site (e.g. 'mycompany.internal'.)

③ Configure the line leading to the SIP provider, for example with the name 'SIPPROVIDER' with the following values:

- Internal standard number: All calls that come in through the SIP provider are forwarded to this internal number. Enter an internal number from your telephone number plan here, e.g. '11'.
- SIP domain/realm: You received this domain from your SIP provider; it is usually entered in the format 'sipdomain.tld' without the part that designates a specific server.
- Registrar (FQDN / IP) (optional):
- Outbound proxy (optional)

The server description is generally not required; the DNS query for the SIP domain returns this information. Enter a server designation here only if your provider has informed you of the corresponding addresses.

- SIP ID / user: Enter the SIP number with local area code here, providing that the SIP provider does not require any other information.
- Display name (optional): The display name is only required if the SIP provider verifies this during registration. If you enter a display name here, then this name will be displayed at the remote site. If the field remains empty, then the display name for the corresponding internal user is transmitted.
- Authentication name (optional): Special authentication names are not supported by all SIP providers. In many cases, the authentication name is the same as the SIP ID or the user name. Complete this field only if your SIP provider has issued you a special authentication name.
- Password: Enter the password for SIP access here.

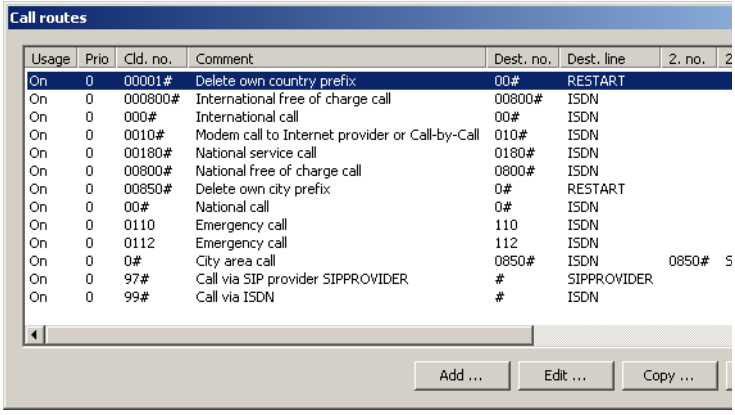
This description applies to a "user-defined configuration". If you select a special SIP provider from the list, then some of the parameters will be pre-configured automatically.

④ Configure an ISDN line for VoIP telephony use. For every MSN on your ISDN connection, make an assignment to an internal number within your telephone number plan during ISDN mapping.

- MSN 1 '555 555 1' ▶ internal number '11'
- MSN 2 '555 555 2' ▶ internal number '12'

⑤ Enter the local and national area code for the device's location. Using this information, the Voice Call Manager can decide whether or not outgoing calls are local calls, national or international long distance calls.

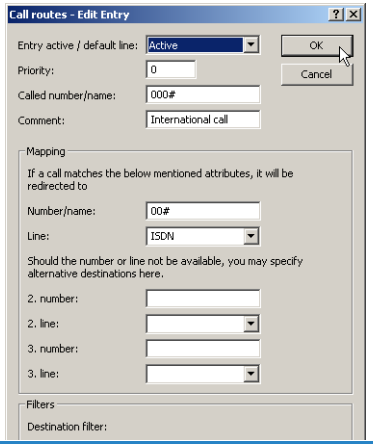
⑥ Based upon the entries made so far, the LANconfig creates a suggestion for the call routing table which you can adapt to fit your requirements as follows:



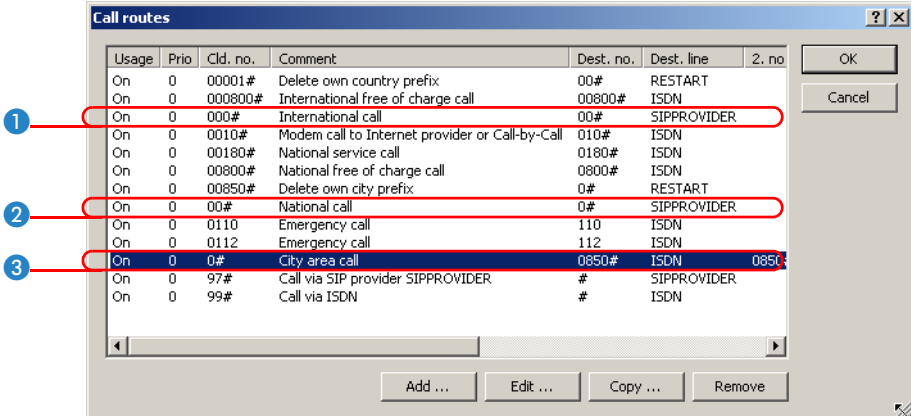
The # sign is a placeholder for any character string. The entry '0#' is therefore suitable for all numbers dialed that have at least one '0' preceding them.

This suggested call routing table would place all external calls over the ISDN line. The SIP line is set up as a backup for international and national long distance calls and local calls that are not in the list of special or emergency numbers.

In order to channel calls to special destinations, such as international and national long distance calls, over the SIP provider, double-click on the corresponding entry in the table and switch the line used from 'ISDN' to 'SIPPROVIDER'. Don't forget to switch the backup line from SIP to ISDN, if necessary!



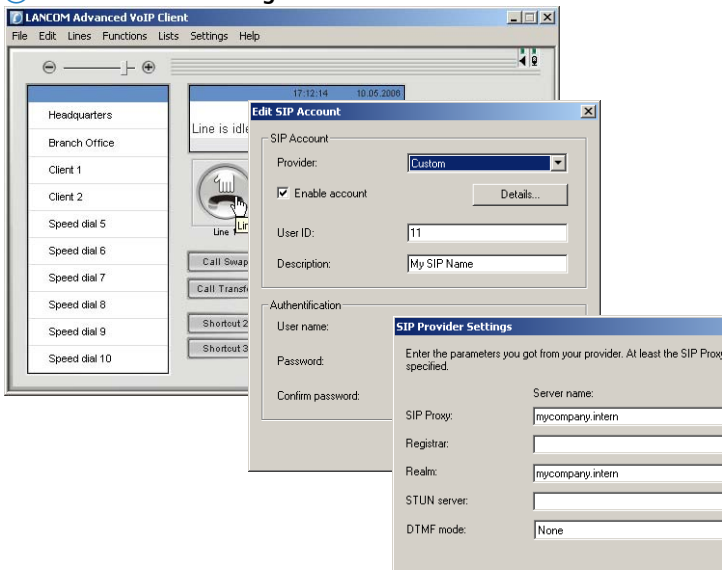
After being adapted for international (1) and national (2) long distance, the call routing table should appear as follows:



Configuring the VoIP terminal equipment

Enter the registration information for the first SIP user in the softphone (example for LANCOM Advanced VoIP Client).

① Select the menu **Settings ▶ SIP accounts / Audio** and create a new SIP account with **Add**.



② Enter the following values:

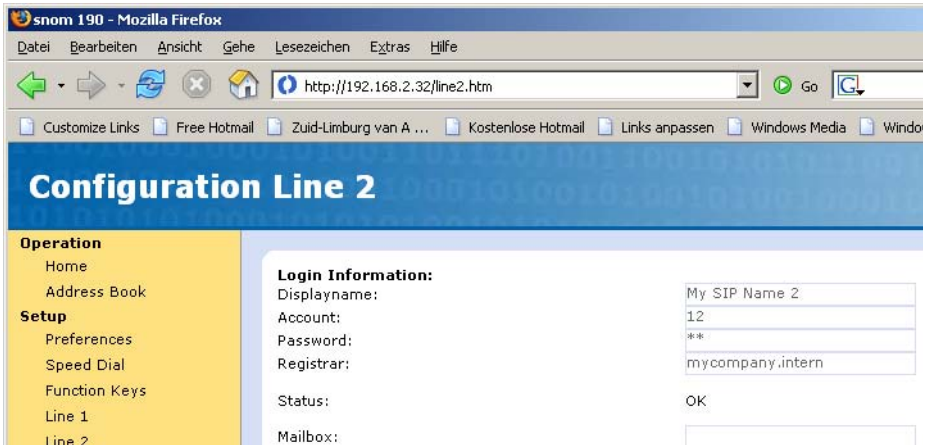
- □ User ID: Internal number for the user.
- □ Description: Name of the user as it is to be displayed at the remote site.

③ With the button **Details**, open the dialog for the advanced settings and enter the following values:

- □ SIP proxy: Internal VoIP domain for the LANCOM.
- □ Realm: Internal VoIP domain for the LANCOM.

Enter the registration data for the second SIP user in the VoIP telephone (example for Snom 190).

① From the **Setup** menu, select one of the possible lines, e.g. 'Line 2'.



② Enter the following values:

- Registrar: Internal VoIP domain for the LANCOM.
- Account: Internal number for the user.
- Displayname: Name of the user as it is to be displayed at the remote site.

If you use another softphone or VoIP telephone, please consult the documentation for this device for information on configuring the software.

Call routing procedure on outgoing calls

On outgoing calls, the Call Manager first searches the call routing table from top to bottom. If the Call Router cannot find a matching entry there, it uses the list of registered users:

	User	dials	correct call route	correct user	mapping, number in use	Destination line
①	VoIP telephone	11	none	VoIP softphone	11	Internal
②	VoIP telephone	0 555 555	③ 0#		0241#: 0241 555 555	ISDN
③	VoIP telephone	0 0123 666 666	② 00#		0#: 0123 666 666	SIP provider

① The Call Router cannot find a an entry that corresponds to '11' in the call routing table. Now it searches the list of registered users and finds the internal SIP user there.

For call routing, not just the users configured in the LANCOM, but all of the users that are actually registered on the Call Router are used. The SIP users can register themselves as long as they are not entered in the in the LANCOM. The entry for the internal VoIP domain on the LANCOM is sufficient for registration, assuming that local authentication is not required.

② The entry 3 in the call routing table depicted above matches the number dialed. The call router removes the '0' outside-line access prefix, completes the area code for the local telephone network and completes the call to '0241 555 555' using the ISDN line.

The area code for the local telephone network is added on because calls via SIP providers usually require the area code to be dialed.

③ The entry 2 in the call routing table is suitable here. The call router removes the '0' prefix for access to the outside line and completes the call to '0123 555 555' via the SIP line. If the SIP line is not available, then the call is made over the ISDN line.

Call routing procedure on incoming calls

For incoming calls, the telephone network exchange removes the prefix from the number dialed (destination number). Therefore, the LANCOM only receives the number itself, which may be treated differently depending on the source:

- Numbers from the ISDN network are translated with the ISDN mapping table to the internal number which is entered for the receiving MSN.
- Calls from a SIP network are converted to the internal destination number that is entered for the respective SIP line.

With the altered number, the Call Manager begins to search the call routing table from top to bottom. If the Call Router cannot find a matching entry there, the call is forwarded directly to the internal number:

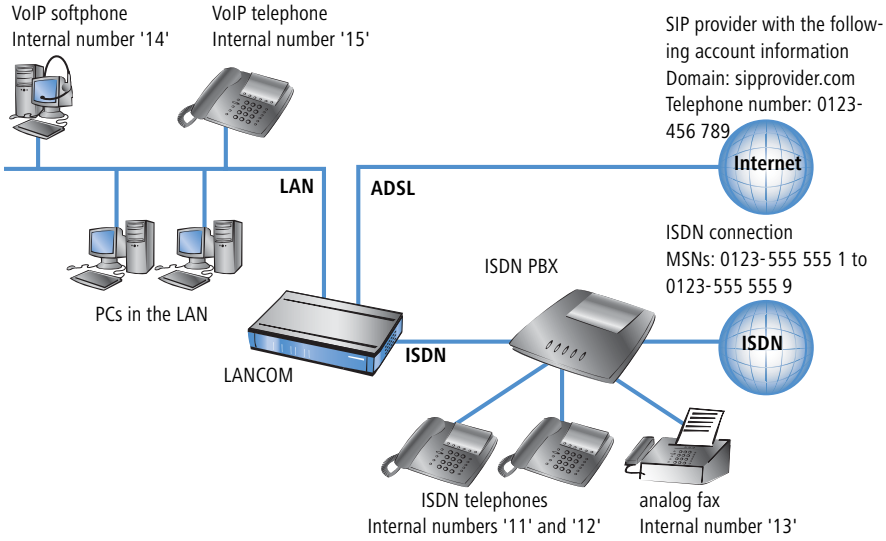
	Remote site dials	Call router receives	Assigned via	number in use	correct call route	Destination line
①	0 123 456 789	456 789	internal destination number for SIP line	11	none	Internal
②	0 123 555 555 1	555 555 1	ISDN mapping	11	none	Internal
③	0 123 555 555 2	555 555 2	ISDN mapping	12	none	Internal

13.7.2 Using VoIP telephony to extend the upstream ISDN PBX

This example shows how to configure a LANCOM when an upstream ISDN PBX is enhanced with VoIP telephony capability. Until now, the MSNs '11' to '13' for the ISDN connection have been used for two ISDN telephones and one analog fax.

The PBX is configured so that subscribers dial '0' to access an outside line.

The LANCOM is operated on an ISDN PBX extension line.



Target

- Internal telephony with ISDN and SIP telephones and SIP softphones.
- External telephony with VoIP terminal equipment via the SIP provider with backup over ISDN.
- External telephony with ISDN terminal equipment in the PBX. Depending on the functionality of the ISDN PBX, ISDN terminal equipment can also use the SIP lines in the LANCOM VoIP Router ('Configuring ISDN PBX' → page 458).
- Accessing internal terminal equipment (ISDN and SIP) via the MSNs.
- Calls to emergency and special numbers via ISDN.

Requirements

- LANCOM connected to the LAN and WAN, an ISDN TE interface is linked to the extension interface on the ISDN PBX. The Internet connection has been set up.

- A telephone number plan with a unique internal telephone number for all terminal equipment to be connected. In general, the numbers used are predetermined by the PBX, which often only allows certain number ranges.
- A SIP provider account.

Using the information during configuration

Telephone number plans with ISDN PBX systems.

When crossing from the ISDN network to the internal subscribers, the ISDN PBX converts the external MSNs to internal MSNs. When operating a LANCOM VoIP Router at the extension interface of the ISDN PBX, there is another conversion of the internal MSNs to the internal numbers of the VoIP range. For reasons of clarity, we recommend using congruent internal MSNs/numbers for terminal equipment for all connections.

The following table provides a summary of the information required for configuration and where it can be entered. SIP terminal equipment parameters can be entered using the SIP telephone keypad, the corresponding configuration software, or the softphone configuration menu.

	LANCOM	SIP terminal equipment	ISDN PBX	ISDN terminal equipment
Internal VoIP domain	4	4		
Internal numbers	4	4	4	4
External SIP telephone number	4			
Access information for SIP account	4			
External ISDN telephone numbers (MSNs)			4	
Country and local area code	4			

Configuring the LANCOM

When configuring the LANCOM, the following steps must be carried out:

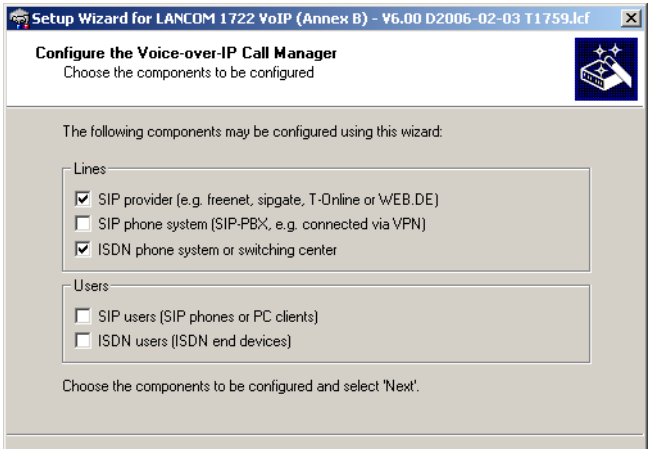
- Setting up the line to the SIP provider
- Enabling the ISDN interface and assigning internal MSNs in the PBX to the internal numbers of the LANCOM VoIP Router
- Adapting the call routing table

In this example, it is not necessary to configure SIP or ISDN users:

- The SIP users are registered at the LANCOM with the settings created in the terminal equipment (softphone and VoIP telephone).
- The ISDN devices can be reached via a corresponding entry in the call routing table.

Detailed instructions on configuring the LANCOM:

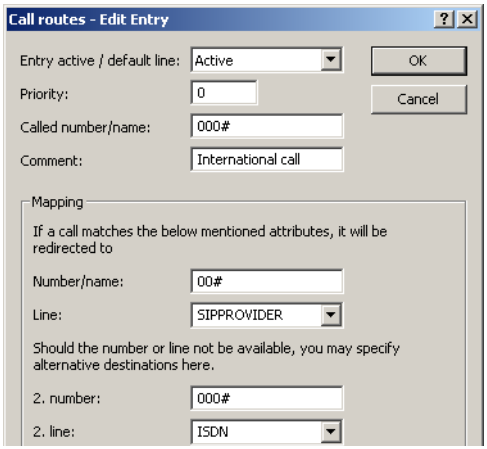
① Under LANconfig, start the setup wizard for configuring the VoIP Call Manager. Enable the options 'SIP phone system', 'ISDN phone system' and 'ISDN users'.



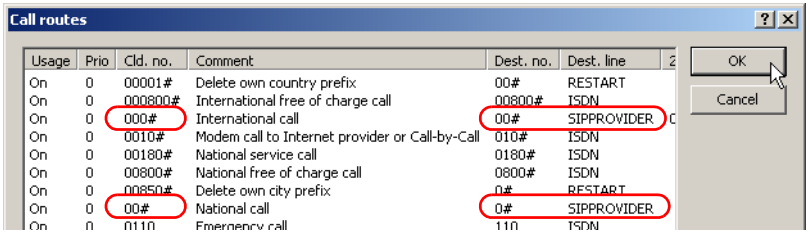
② Configure the device as described in the preceding examples:

- Unique local VoIP domains
- one line to a SIP provider
- ISDN line

③ Adapt the suggested call routing table in order to direct calls to special numbers automatically over the SIP provider's line. The following example shows the entry for international calls.



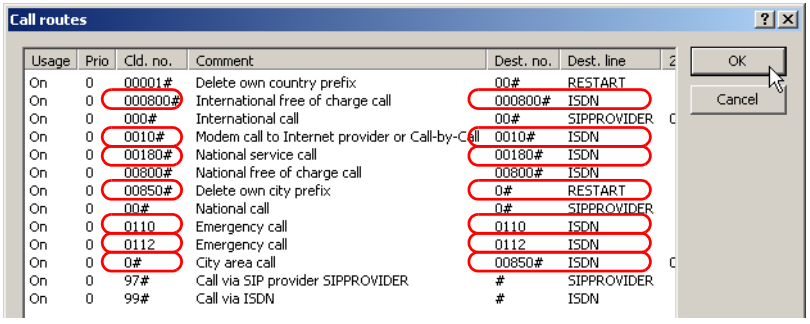
After being adapted, the call routing table should appear as follows:



Therefore, for every long distance call, the '0' preceding the number is removed, the call is made via the SIP provider.

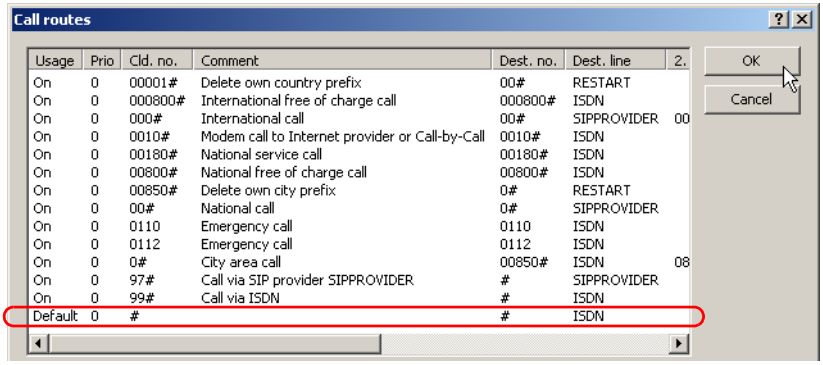
④ For all ISDN calls, however, the '0' may not be removed from the destination number because the upstream ISDN PBX requires the '0' to access an outside line! Therefore, adapt the destination number for all entries with the target line 'ISDN'.

After being adapted, the call routing table should appear as follows:



⑤ In order to allow the ISDN subscribers to be contacted internally by the VoIP users, a standard route is also set up which directs all calls that have not yet been resolved to the ISDN line without changing the numbers.

After being adapted, the call routing table should appear as follows:



This call routing table is only valid for PBX systems in which the subscribers have to dial '0' to access an outside line. If the PBX uses another mechanism for accessing an outside line, then the table must be adapted accordingly.

Configuring the VoIP terminal equipment

The VoIP terminal equipment is configured as described in the preceding examples with internal VoIP domains and internal numbers for the local site.

Configuring ISDN PBX

When configuring the PBX, external MSNs are assigned to internal MSNs. For every VoIP terminal device, a free internal MSN is linked to an external MSN.

External and internal calls from ISDN terminal devices into VoIP telephony

First, the ISDN terminal devices forward the desired destination number to the ISDN PBX when the call is being established. If the number is an internal number/MSN, then the PBX directs the call to the internal ISDN bus. The SIP terminal equipment connected to the LANCOM can therefore only be reached via an internal call when the PBX knows the internal number for the VoIP user.

If your PBX is able to direct external numbers to the internal ISDN bus, then the ISDN terminal devices can also use the lines configured in the LANCOM, such as the SIP provider line, for outgoing external calls.

Configuring the ISDN terminal equipment

Configuring the ISDN terminal equipment is generally limited to entering the internal MSN used in the PBX.

Call routing procedure on outgoing calls

	User	dials	correct call route	correct user	mapping, number in use	Destination line
①	VoIP tele-phone	14	none	VoIP softphone	14	internal
②	VoIP tele-phone	11	❸ # (Standard)		#: 11	ISDN
③	ISDN tele-phone	14	■ PBX	VoIP softphone	14	internal
④	VoIP tele-phone	0 555 555	❷ 0#		00241#: 0 555 555	ISDN
⑤	ISDN tele-phone	0 555 555	■ PBX		555 555	ISDN outside line
⑥	VoIP tele-phone	0 0123 666 666	❶ 00#		0#: 0123 666 666	SIP provider

① Internal call between two VoIP terminal devices.

② Internal call from VoIP to ISDN. In the first pass (without the standard routes), the number '11' does not match any of the routes. Similarly, no matching entry can be found in the list of registered users. In the second pass, the standard route meets '#' (entry ❸ in the call routing table depicted above) and directs the call to the ISDN line **unchanged**. The PBX receives the call on its internal ISDN bus, recognizes the called number as an internal MSN and again forwards the call to the internal ISDN bus to which the respective ISDN terminal device is connected.

③ Internal call from ISDN to VoIP. The ISDN PBX recognizes the destination number '14' as an internal MSN and directs the call to the corresponding internal ISDN bus. The Call Router receives the call to '14', does not find a matching entry in the call routing table but does find an entry in the list of registered users.

④ External call from the VoIP into the local telephone network. The entry ❷ in the call routing table depicted above matches the number dialed. The Call Router completes the area code for the local telephone network and sends the call out to the ISDN line. Only now does the SIP PBX removes the '0' outside-line access prefix and completes the call to '0241 555 555' via the ISDN outside line.

⑤ External call from ISDN into the local telephone network. The ISDN PBX recognizes the destination number as an external destination, removes the '0' outside-line access prefix and completes the call to '555 555' via the ISDN outside line.

⑥ External call from VoIP into the national telephone network. The entry ❶ fits in the call routing table here. The call router removes the '0' outside-line access prefix and completes the call to '0123 555 555' via the SIP line. If the SIP line is not available, then the call is made over the ISDN line. In this case, the '0' is not removed from the destination number in order to gain access to an outside line through the PBX.

Call routing procedure on incoming calls

	Remote site dials	Call Router receives	Assigned via	number in use	correct call route	Destination line
①	0 123 456 789	456 789	internal destination number for SIP line	11	none	ISDN
②	0 123 555 555 1		ISDN PBX	11		internal
③	0 123 555 555 4	14	■ ISDN PBX ■ List of local users	14	none	internal

① The incoming call for the SIP line number is directed to the Call Router along with the internal destination number that has been configured. The Call Router cannot find a matching entry in the call routing table, but it can find a registered user with the matching internal number. Since the user is an ISDN user, the Call Router directs the call to the ISDN line. The PBX receives the number '11' and can determine this call to be an internal call for the connected ISDN telephone.

② The incoming calls to the MSNs for the connected ISDN terminal equipment can be assigned directly by the PBX itself, the Call Router is not involved here.

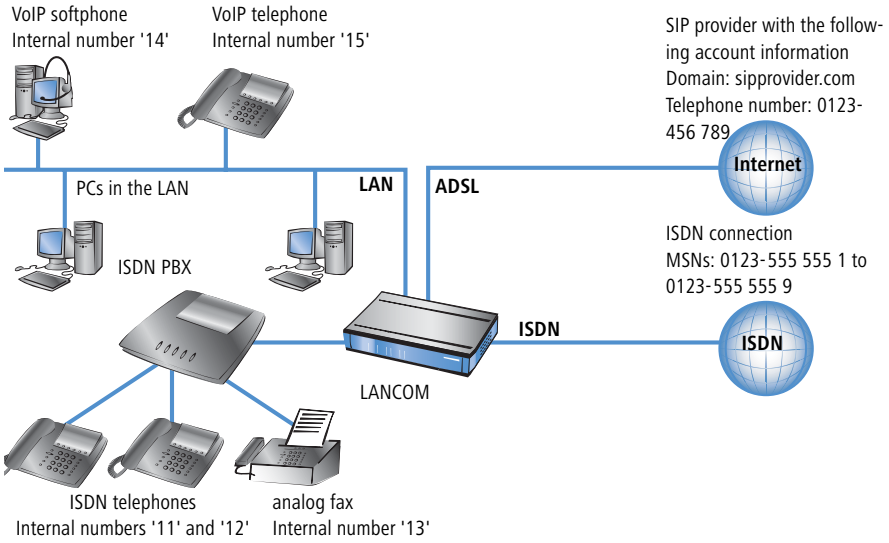
③ The PBX directs incoming calls to the MSNs for the connected VoIP terminal equipment to the internal ISDN bus with the internal MSN. The Call Router receives these calls as if they were internal calls and forwards them to the appropriate user since no corresponding entry can be found in the call routing table here either.

13.7.3 Using VoIP telephony to extend the downstream ISDN PBX

This example shows how to configure a LANCOM when a downstream ISDN PBX is enhanced with VoIP telephony capability. Until now, the MSNs '11' to '13' for the ISDN connection have been used for two ISDN telephones and one analog fax. The LANCOM will now be switched between the public ISDN connection and the ISDN PBX.

The PBX is configured to allow subscribers to receive immediate access to an outside line when they pick up the receiver.

This ISDN PBX is operated as a downstream PBX on the ISDN NT interface of the LANCOM.



Target

- Internal telephony with ISDN and SIP telephones and SIP softphones.
- External telephony with ISDN and SIP terminal equipment over ISDN.
- Accessing internal terminal equipment (ISDN and SIP) via the MSNs.

Requirements

- LANCOM connected to the LAN and WAN, an ISDN NT interface is linked to the outside line exchange on the ISDN PBX. The Internet connection has been set up.
- A telephone number plan with a unique internal telephone number for all terminal equipment to be connected. In general, the numbers used are predetermined by the PBX, which often only allows certain number ranges.
- A SIP provider account.

Using the information during configuration

Telephone number plans with ISDN PBX systems.

When crossing from the ISDN network to the internal subscribers, the ISDN PBX converts the external MSNs to internal MSNs. When operating a LANCOM VoIP Router at the extension interface of the ISDN PBX, there is another conversion of the internal MSNs to the internal numbers of the VoIP range. For reasons of clarity, we recommend using congruent internal MSNs/numbers for terminal equipment for all connections.

The following table provides a summary of the information required for configuration and where it can be entered. SIP terminal equipment parameters can be entered using the SIP telephone keypad, the corresponding configuration software, or the softphone configuration menu.

	LANCOM	SIP terminal equipment	ISDN PBX	ISDN terminal equipment
Internal VoIP domain	4	4		
Internal numbers	4	4	4	4
External SIP telephone number	4			
SIP account access information	4			
External ISDN telephone numbers (MSNs)	4			
Country and local area code	4			

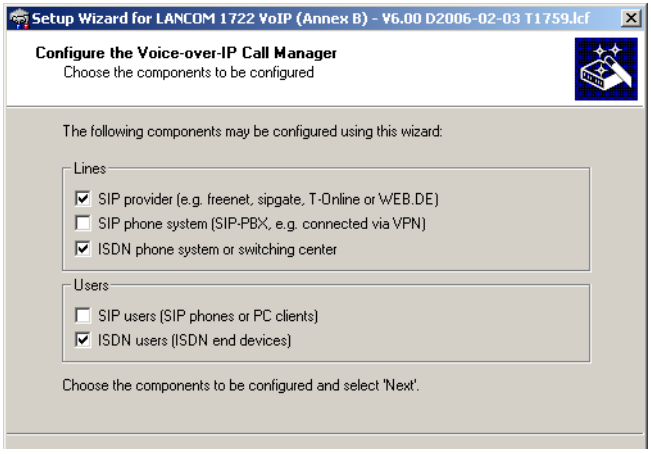
Configuring the LANCOM

When configuring the LANCOM, the following steps must be carried out:

- Setting up the line to the SIP provider
- Enabling the ISDN interface and assigning MSNs to the internal numbers in the LANCOM VoIP Router
- Creating ISDN users
- Adapting the call routing table

Detailed instructions on configuring the LANCOM:

① Under LANconfig, start the setup wizard for configuring the VoIP Call Manager. Enable the options 'SIP phone system', 'ISDN phone system' and 'ISDN users'.



② Configure the device as described in the preceding examples:

- Unique local VoIP domains
- one line to a SIP provider

③ Enable the external ISDN outside line and the internal ISDN bus in order to use the VoIP functionality. Enter all external MSNs for the ISDN outside line in the ISDN mapping table with their assignment to the internal numbers in the VoIP range.

④ Enter all connected ISDN terminal devices as ISDN users with the following values:

- Telephone number / SIP name: This number will be assigned to the ISDN terminal device as an "internal number". The telephone structure will remain clear if you use the same internal number for a terminal device here as it uses in its own ISDN environment.
- MSN/DDI: Enter the external MSNs for the ISDN outside line here; this will also be assigned to the terminal device by the ISDN PBX.

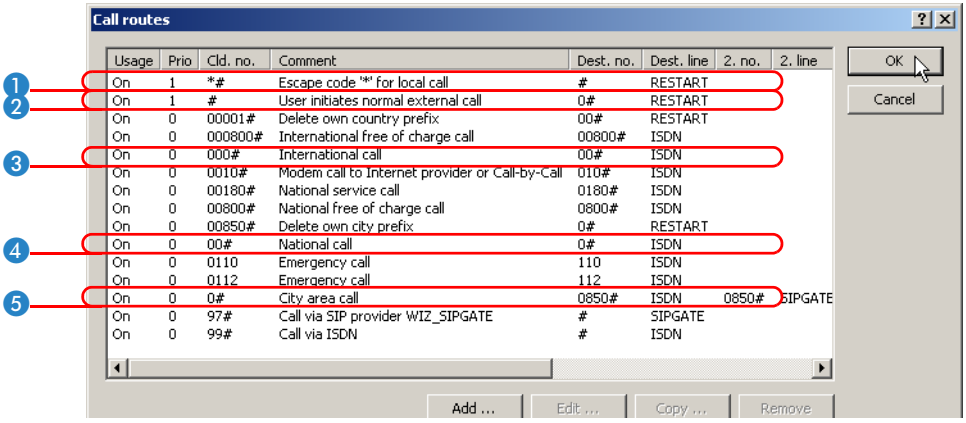
⑤ Enable spontaneous outside line access for ISDN and SIP users in order to keep the subscribers' telephone behavior as consistent as possible.

⑥ The call routing table suggested by the setup wizard automatically allows spontaneous outside line access for ISDN and SIP users ① and ②.

Routes for spontaneous outside line access

Entering the source line 'USER' is not visible in the screenshot. Using this filter, the route will only be in effect for calls that originate from a local user. The destination line 'RESTART' prompts a new pass through the call routing table, whereby the source line is deleted. Due to the missing source line, the route does not match this call during the second pass.

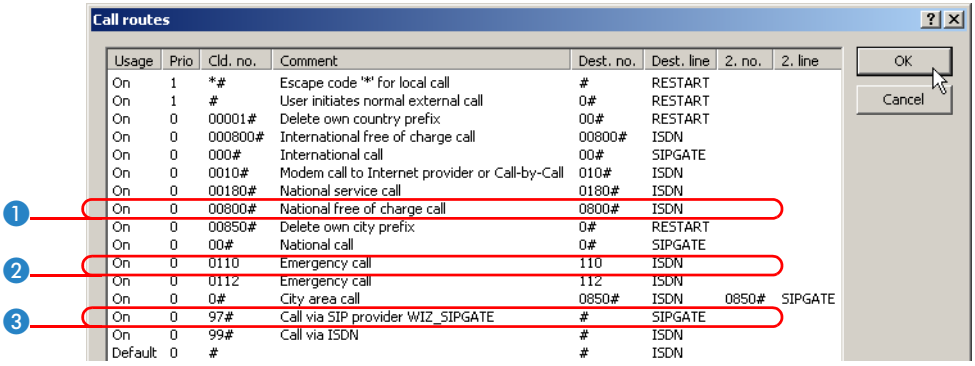
As a result of both of these routes, any stars '*' that might have preceded the numbers are removed before each call from a local user. For all other calls from local users, the number is preceded with a '0', as it is automatically assumed that the user is trying to establish an outside connection.



Usage	Prio	Cld. no.	Comment	Dest. no.	Dest. line	2. no.	2. line
On	1	*#	Escape code '*' for local call	#	RESTART		
On	1	#	User initiates normal external call	0#	RESTART		
On	0	00001#	Delete own country prefix	00#	RESTART		
On	0	000800#	International free of charge call	00800#	ISDN		
On	0	000#	International call	00#	ISDN		
On	0	0010#	Modem call to Internet provider or Call-by-Call	010#	ISDN		
On	0	00180#	National service call	0180#	ISDN		
On	0	00800#	National free of charge call	0800#	ISDN		
On	0	00850#	Delete own city prefix	0#	RESTART		
On	0	00#	National call	0#	ISDN		
On	0	0110	Emergency call	110	ISDN		
On	0	0112	Emergency call	112	ISDN		
On	0	0#	City area call	0850#	ISDN	0850#	SIPGATE
On	0	97#	Call via SIP provider WIZ_SIPGATE	#	SIPGATE		
On	0	99#	Call via ISDN	#	ISDN		

The other routes are used to carry out international 3 and national 4 long distance calls as well as local calls 5 as standard over the ISDN line. The Call Router removes the preceding zeros from the number again and sends the call out to the ISDN line.

In order to channel calls to special destinations, such as international and national long distance calls, over the SIP provider and not over ISDN, double-click on the corresponding entry in the table and switch the line used form 'ISDN' to 'SIPPROVIDER'. Don't forget to switch the backup line from SIP to ISDN, if necessary!



Usage	Prio	Cld. no.	Comment	Dest. no.	Dest. line	2. no.	2. line
On	1	*#	Escape code '*' for local call	#	RESTART		
On	1	#	User initiates normal external call	0#	RESTART		
On	0	00001#	Delete own country prefix	00#	RESTART		
On	0	000800#	International free of charge call	00800#	ISDN		
On	0	000#	International call	00#	SIPGATE		
On	0	0010#	Modem call to Internet provider or Call-by-Call	010#	ISDN		
On	0	00180#	National service call	0180#	ISDN		
On	0	00800#	National free of charge call	0800#	ISDN		
On	0	00850#	Delete own city prefix	0#	RESTART		
On	0	00#	National call	0#	SIPGATE		
On	0	0110	Emergency call	110	ISDN		
On	0	0112	Emergency call	112	ISDN		
On	0	0#	City area call	0850#	ISDN	0850#	SIPGATE
On	0	97#	Call via SIP provider WIZ_SIPGATE	#	SIPGATE		
On	0	99#	Call via ISDN	#	ISDN		
Default	0	#		#	ISDN		

This call routing table is only valid for PBX systems that forward the special character star '*' for internal calls on their external ISDN bus. If the PBX processes this character in a different manner, then the table must be adapted accordingly.

Configuring the VoIP terminal equipment

The VoIP terminal equipment is configured as described in the preceding examples with internal VoIP domains and internal numbers for the local site.

Configuring ISDN PBX

When configuring the PBX, external MSNs are assigned to internal MSNs. For every VoIP terminal device, a free internal MSN is linked to an external MSN. The internal number for the SIP user can be used as an external MSN for the VoIP terminal equipment in the PBX.

Configuring the ISDN terminal equipment

Configuring the ISDN terminal equipment is generally limited to entering the internal MSN used in the PBX.

Call routing procedure on outgoing calls

	User	dials	correct call route	correct user	mapping, number in use	Destination line
①	VoIP telephone	*14	1 *#	VoIP softphone	#: 14	internal
②	VoIP telephone	*11	1 *#	ISDN users	#: 11	ISDN

① Internal call between two VoIP terminal devices. On the first pass, only the star is removed from the number, the source line is deleted. During the second pass, no other route matches this call but the Call Router finds a matching entry for a SIP user in the list of registered users and can complete the call.

② Internal call from VoIP to ISDN. On the first pass, the star is removed from the number again, the source line is deleted. During the second pass, no other route matches this call but the Call Router finds a matching entry for an ISDN user in the list of registered users and establishes the call via the ISDN interface configured for this user. The destination number is replaced by the MSN entered for this user '555 555 1' . The PBX receives the call to '555 555 1' on its external ISDN bus and again determines that this is an external MSN and can channel the call to the corresponding ISDN telephone.

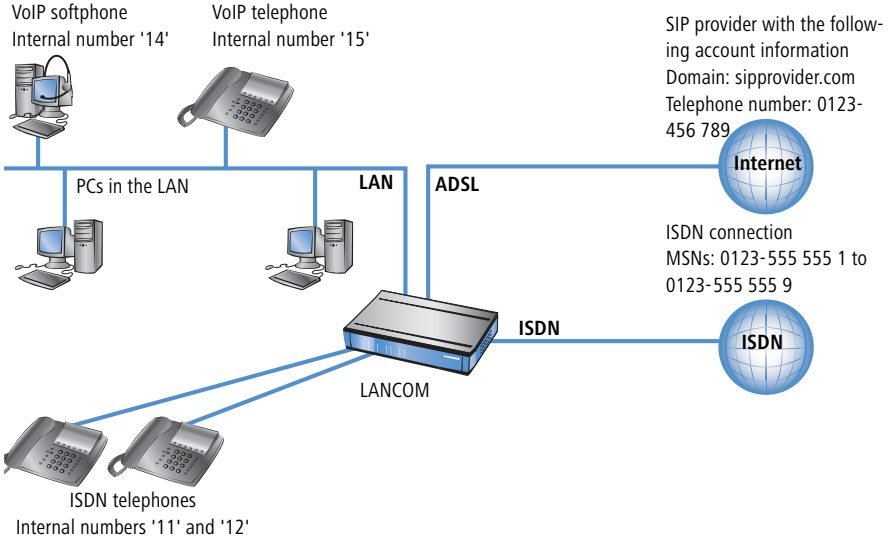
Call routing procedure on incoming calls

	Remote site dials	Call Router receives	Assigned via	number in use	correct call route	Destination line
①	0 123 555 555 1	555 555 1	■ ISDN mapping table ■ List of local ISDN users	11		ISDN NT

① The incoming call via the number to the MSNs for the connected ISDN terminal equipment is converted into an internal number by the ISDN mapping table and passed on to the Call Router. The Call Router cannot find a matching entry in the call routing table, but it can find a registered user with the matching internal number. Since the user is an ISDN user, the Call Router directs the call to the ISDN line with the MSN entered for this user, '555 555 1'. The PBX receives the call to '555 555 1' on its external ISDN bus and again determines that this is an external MSN and can channel the call to the corresponding ISDN telephone.

13.7.4 Using VoIP telephony to supplement existing ISDN telephones

This example shows how to configure a LANCOM when the ISDN telephones used unit now are to be enhanced with VoIP telephony. The external MSNs '555 555 1' and '555 555 2' on the ISDN bus at the NTBA were used for two ISDN telephones until now. The LANCOM will now be switched between the public ISDN connection and the internal ISDN bus connected to the ISDN telephones.



Target

- Internal telephony with ISDN and SIP telephones and SIP softphones.
- External telephony with ISDN and SIP terminal equipment over ISDN.
- Accessing internal terminal equipment (ISDN and SIP) via the MSNs.

Requirements

- LANCOM connected to LAN and WAN, an ISDN NT interface connected to the ISDN telephone, an ISDN TE interface connected to the ISDN outside line (NTBA). The Internet connection has been set up.
- A telephone number plan with a unique internal telephone number for each piece of terminal equipment to be connected.
- A SIP provider account.

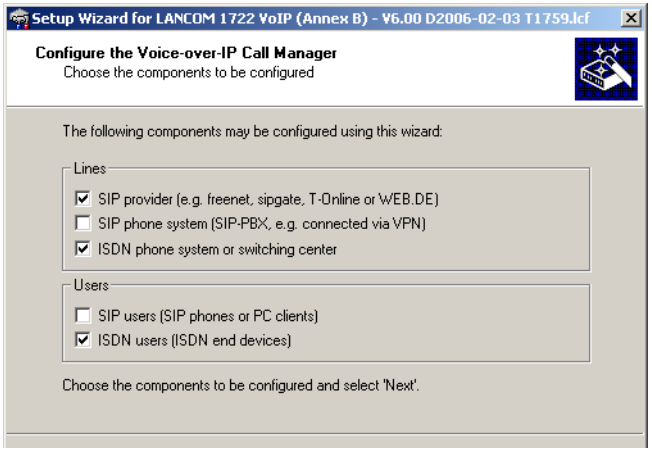
Configuring the LANCOM

When configuring the LANCOM, the following steps must be carried out:

- Setting up the line to the SIP provider
- Enabling the ISDN interface and assigning MSNs to the internal numbers in the LANCOM VoIP Router
- Creating ISDN users
- Adapting the call routing table

Detailed instructions on configuring the LANCOM:

① Under LANconfig, start the setup wizard for configuring the VoIP Call Manager. Enable the options 'SIP phone system', 'ISDN phone system' and 'ISDN users'.



② Configure the device as described in the preceding examples:

□ Unique local VoIP domains

- one line to a SIP provider

③ Enable the external ISDN outside line and the internal ISDN bus in order to use the VoIP functionality. Enter all external MSNs for the ISDN outside line in the ISDN mapping table with their assignment to the internal numbers in the VoIP range.

④ Enter all connected ISDN terminal devices as ISDN users with the following values:

- Telephone number / SIP name: This number will be assigned to the ISDN terminal device as an "internal number". The telephone structure will remain clear if you use the same internal number for a terminal device here as it uses in its own ISDN environment.
- MSN/DDI: Here, enter the external MSN of the ISDN outside line which was formerly entered into the ISDN telephone.

Assigning external MSNs to internal telephone numbers

In this example, the external MSNs and the internal telephones will be assigned "crossed over":

- In the ISDN mapping table, the external MSN '555 555 1' is assigned to the internal telephone number '11', for example. An external call to '555 555 1' will be switched by the LANCOM as a call to '11'.
- By assigning the MSN '555 555 1' to the internal telephone number of the ISDN user '11', the call will be directed over the internal ISDN bus of the LANCOM with the target telephone number '555 555 1'.

Because the ISDN telephone "listens" out for its own MSN, exactly as it used to before implementing the LANCOM VoIP Router, the call is placed to the correct telephone.

Should the LANCOM VoIP Router fail due to a power outage, the life-line support and power relay over the ISDN bus, if activated, enable the connected telephones to continue to function.

⑤ Enable spontaneous outside line access for ISDN and SIP users in order to keep the subscribers' telephone behavior as consistent as possible.

⑥ The continued configuration and changes to the call routing table are carried out just as in the example 'Using VoIP telephony to extend the downstream ISDN PBX'.

Configuring the VoIP terminal equipment

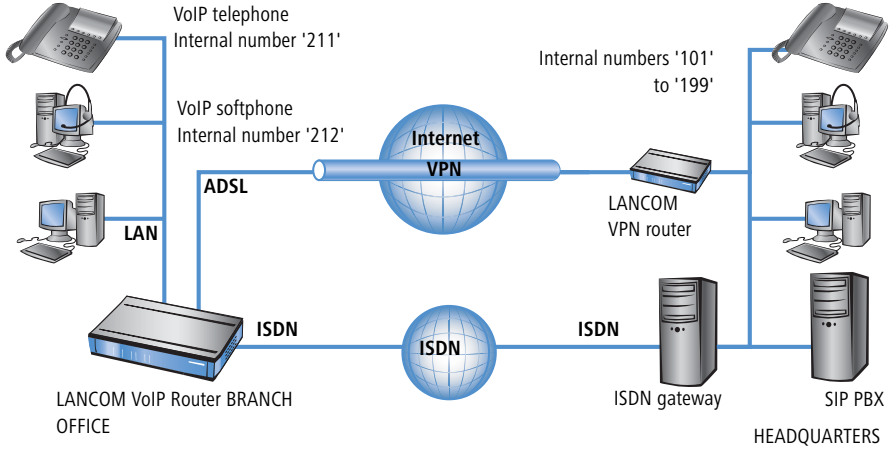
The VoIP terminal equipment is configured as described in the preceding examples with internal VoIP domains and internal numbers for the local site.

Configuring the ISDN telephones

Configuring the ISDN terminal equipment is generally limited to entering the external MSN. As a rule, the MSNs were already entered into the ISDN telephones before, and so no changes should be necessary.

13.7.5 Connecting to an upstream SIP PBX

In this example, a branch office network will be connected to the headquarters network over VPN. In addition to data transfer, the telephone structure in the branch office is also connected to the central SIP PBX. A LANCOM VoIP Router is used in the branch office network and a LANCOM VPN router, for example, could act as the VPN end point at the headquarters. The telephony subscribers at the headquarters receive internal extensions from the number range '101' to '199'; for each of the branch offices, a 10-digit block from the 200 range is reserved - in this example, '211' to '219'.



Target

- Internal telephony between all locations.
- External telephony from the branch office via the SIP PBX at the headquarters with backup over ISDN.
- Calls from the branch office into the local telephone network via ISDN.
- Calls to emergency and special numbers via ISDN.

Requirements

- LANCOM connected to the LAN and WAN, an ISDN TE interface is linked to the ISDN NTBA.
- The Internet connection has been set up, as has the network connection between both of the locations by means of a VPN tunnel. Any terminal equipment that is connected can be reached with the IP addresses used.
- A telephone number plan with a unique internal telephone number for all terminal equipment to be connected.
- A SIP provider account.

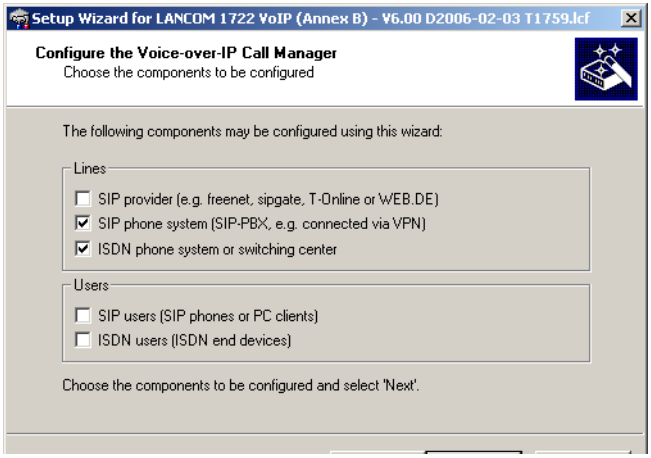
Configuring the LANCOM

The following table provides a summary of the information required for configuration and where it can be entered. Basically, all that is needed is a SIP PBX line for each location that is correspondingly setup at the remote location

	LANCOM Branch office	SIP terminal equipment Branch office	SIP PBX Headquarters
Internet VoIP domain	mycompany.BRANCH01	mycompany.HQ	mycompany.HQ
Internal SIP subscriber numbers at the branch office		4	4
External ISDN telephone numbers (MSNs)	4		
Country and local area code	4		
SIP PBX line	HQ		
SIP PBX domains	mycompany.HQ		
SIP PBX registration password	4		4
Call route	■ Number called '2#' ■ Destination line 'LOCATION_B' ■ Destination number '2#'		

Detailed instructions on configuring the LANCOM:

① Under LANconfig, start the setup wizard for configuring the VoIP Call Manager. Enable the options 'SIP phone system', 'ISDN phone system' and 'ISDN users'.



② Configure the device as described in the preceding examples:

- □ ISDN line with MSN mapping
- □ Area and country code for each location

③ Enter a unique domain for the local VoIP domain which describes the local VoIP range for the branch office, e.g. 'mycompany.BRANCH01' for the first branch.

④ Configure the line leading to the SIP PBX with the following values:

- □ SIP PBX line name: Unique name for the line leading to the SIP PBX, e.g. 'HQ' for "Headquarters".
- □ PBX SIP domain/realm: Internal VoIP domain or SIP PBX, e.g. 'mycompany.HQ'.
- □ Registrar (FQDN or IP) (optional): SIP PBX address in the headquarters network, in the event that the device cannot be identified via DNS resolution of the VoIP domain (PBX SIP domain/realm).

Use the SIP PBX IP address from the private IP address range at the headquarters that can be reached via VPN here.

- □ Outbound proxy (optional): It is generally not necessary to designate the outbound proxy. Only enter a server designation here should your SIP PBX require corresponding addresses.
- □ Shared PBX password: This password is used by all SIP users when registering at the SIP PBX.

Shared or user-dependent SIP PBX password

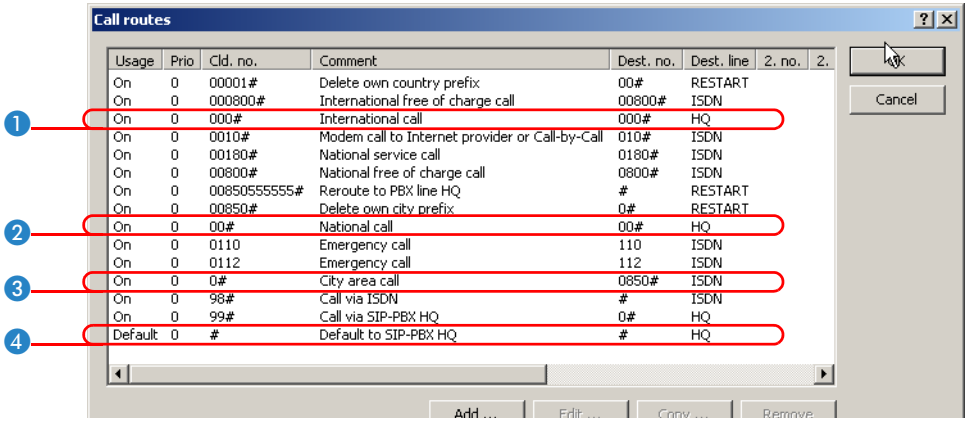
If registration with a shared password is not desired, then an individual password can be used for each SIP user. In this case, each SIP user is configured with its own password in the LANCOM.

- □ Public PBX number: Here, enter the number at which the SIP PBX is to be reached over the public telephone network from the location of the LANCOM. The number is entered with the **necessary** prefixes, but without an extension number. For example, if the SIP PBX is located in London and the LANCOM is in Birmingham, then the public PBX number is '020 12345'.

⑤ The call routing table suggested by the setup wizard automatically allows international 1 and national 2 long distance calls to be made via the SIP PBX at the headquarters.

In addition, a **standard route** 4 is used in order to conduct calls from the LANCOM VoIP range to internal SIP PBX numbers via the corresponding SIP PBX lines.

This special entry is only used during the second pass in the call routing table, after the first pass found no corresponding entry for "normal" routes and if no matching internal number was found in the list of local users.



Configuring the VoIP terminal equipment

The VoIP terminal equipment is configured as described in the preceding examples. However, here, the SIP PBX VoIP domain and the internal numbers configured in the SIP PBX are used.

Automatic SIP user registration with the LANCOM and the SIP PBX.

By using the SIP PBX domain with VoIP terminal equipment, the user is registered in two ways:

- Since registration takes place with a valid domain defined in the LANCOM, terminal devices are registered as "local users".

Since the domain that is used does not correspond to the LANCOM's own VoIP domain, a simultaneous attempt is made at registering with the upstream SIP PBX. If the password used corresponds to the password stored in the SIP PBX for this user, then the registration on the SIP PBX will be successful.

Configuring the SIP PBX

In the SIP PBX, all users from the branch office network are entered with their own internal number. For this purpose, either the shared password is entered or a separate password is assigned for each user ('Shared or user-dependent SIP PBX password' → page 471).

Call routing procedure on outgoing calls

	User	dials	correct call route	correct user	mapping, number in use	Destination line
①	Branch VoIP telephone	212	none	VoIP softphone	212	internal
②	Branch VoIP telephone	199	4 #	SIP subscribers at the head-quarters	#: 199	SIP PBX
③	Branch VoIP telephone	0 555 555	3 0#		0241#: 0241 555 555	ISDN
④	Branch VoIP telephone	0 0123 666 666	2 00#		00#: 0123 666 666	SIP provider

① Internal call between two VoIP terminal devices at the branch office. The number dialed, '212', does not match any of the routes listed in the call routing table. Therefore, the call router searches the local user list, finds the correct entry there and can forward the call internally.

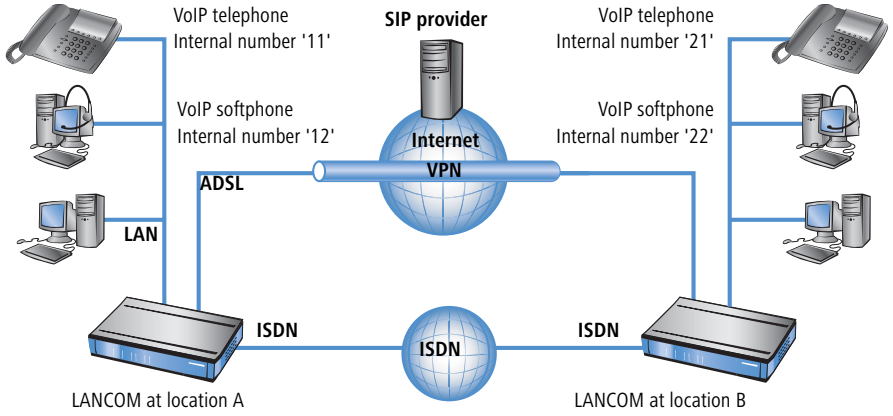
② Internal call between a VoIP terminal device at the branch office and the internal subscriber '199' at the head-quarters. The number dialed, '199', does not match any of the routes listed in the call routing table during the first pass. Similarly, no matching entry can be found in the local user list. In the second pass through the call routing table, the standard routes are considered too. The route with the number called '#' 4 corresponds to all calls which could not be assigned earlier. The call to '199' is therefore carried out over the SIP PBX line.

③ External call from the branch office into the local telephone network. The number dialed, '0 555,555', matches the route '0#' 3 in the call routing table. The call router removes the '0' outside-line access prefix, completes the area code for the local telephone network and completes the call to '0241 555 555' using the ISDN line.

④ External call from the branch office into a national telephone network. The number dialed, '0 0123 555 555', matches the route '00#' 2 in the call routing table. The call router sends the call out to the SIP PBX line **unchanged**. Only now does the SIP PBX removes the '0' outside-line access prefix and completes the call to '0123 555 555' via the ISDN outside line.

13.7.6 VoIP coupling for locations 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.



Target

- Internal telephony at and between both locations.
- External telephony via the SIP provider with backup over ISDN.
- Calls to emergency and special numbers via ISDN.

Requirements

- LANCOM connected to the LAN and WAN, an ISDN TE interface is linked to the ISDN NTBA.
- The Internet connection has been set up, as has the network connection between both of the locations by means of a VPN tunnel. Any terminal equipment that is connected can be reached with the IP addresses used.
- A telephone number plan with a unique internal telephone number for all terminal equipment to be connected. For each site, a separate number range is used; in this example, the internal numbers for location A begin with a '1' and the internal numbers for location B begin with a '2'.
- Each site has a SIP provider account.

Configuring the LANCOM

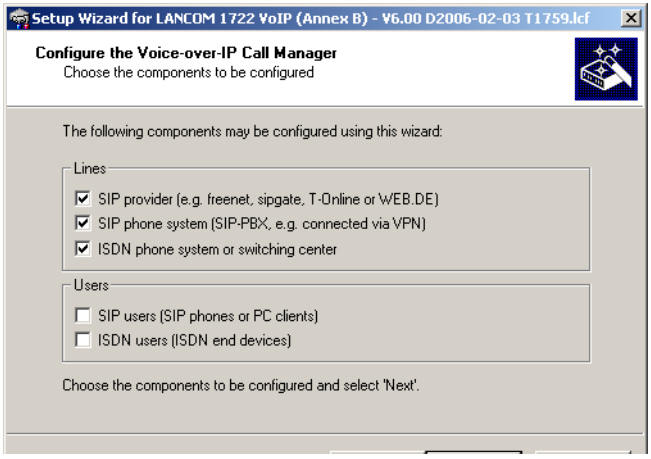
The following table provides a summary of the information required for configuration and where it can be entered. Basically, all that is needed is a SIP PBX line for each location that is correspondingly setup at the remote location

	LANCOM Location A	SIP terminal equipment location A	LANCOM Location B	SIP terminal equipment location B
Internal VoIP domain	location_A.internal	location_A.internal	location_B.internal	location_B.internal
Internal numbers		10 to 19		20 to 29
External SIP telephone number	4		4	
Access information for SIP account	4		4	
External ISDN telephone numbers (MSNs)	4		4	
Country and local area code	4		4	
SIP PBX line	LOCATION_B		LOCATION_A	
SIP PBX domains	location_B.internal		location_A.internal	
Call route	■ Number called '2#' ■ Destination line 'LOCATION_B' ■ Destination number '2#'		■ Called number '1#' ■ Destination line 'LOCATION_A' ■ Destination number ''1#'	

Although SIP PBX lines are the subject of the configuration presented here, you can still use this function even without a PBX.

Detailed instructions on configuring the LANCOM:

① Under LANconfig, start the setup wizard for configuring the VoIP Call Manager. Enable the options 'SIP phone system', 'ISDN phone system' and 'ISDN users'.



② Configure the device as described in the preceding examples:

- one line to a SIP provider
- ISDN line with MSN mapping
- Area and country code for each location

③ Enter a unique domain for the local VoIP domain which describes the local VoIP range for the site. Both sites use **different** VoIP domains, e.g. 'location_A.internal' or 'location_B.internal'.

④ Configure the line leading to the SIP PBX with the following values:

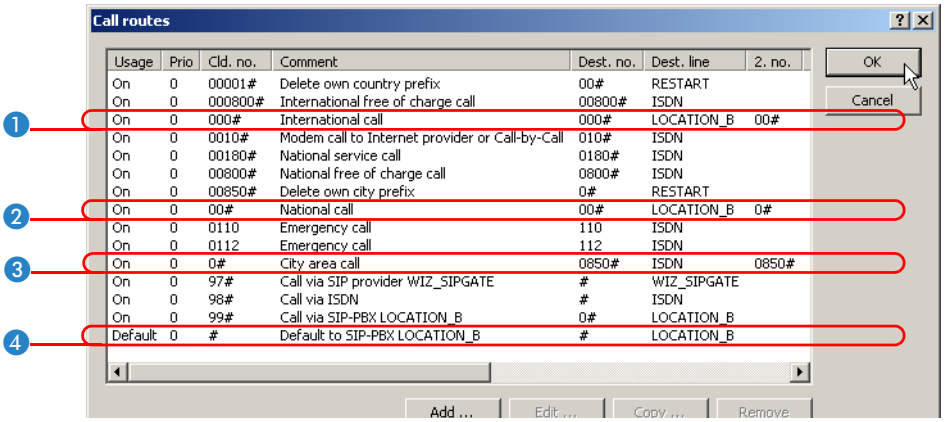
- SIP PBX line name: Unique name for the line leading to the remote site.
- PBX SIP domain/realm: Internal VoIP domain for the remote site.
- Registrar (FQDN or IP): Address for the LANCOM at the remote site, in the event that the device cannot be identified via DNS resolution of the VoIP domain (PBX SIP domain/realm).

Use the private IP address that can be reached via VPN for the LANCOM here, not the public IP.

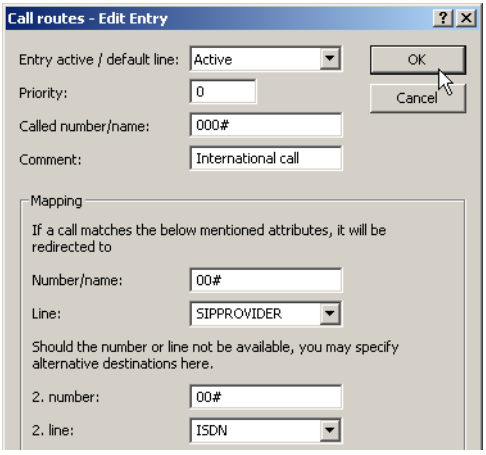
- Leave the field for the shared password empty when registering to the SIP PBX.
- Leave the field for the public PBX number empty.

⑤ The call routing table suggested by the setup wizard automatically allows international ① and national ② long distance calls to be made via remote site's line, local calls ③ are routed via ISDN.

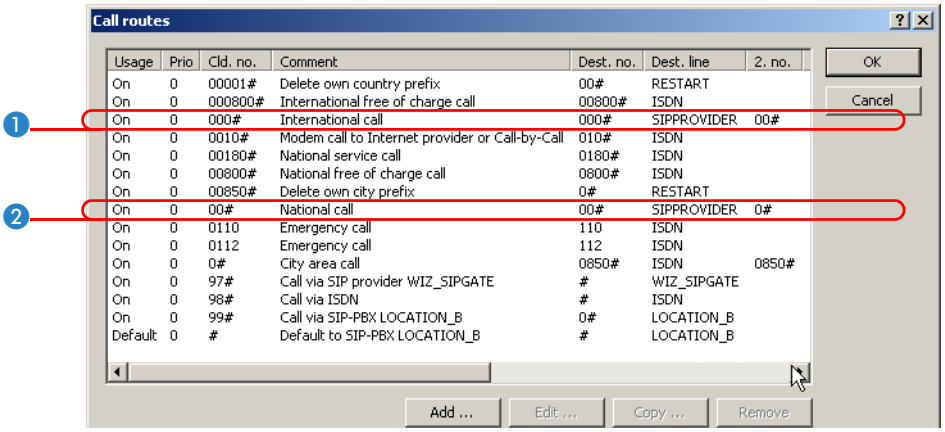
In addition, a **standard route** ④ directs all numbers which cannot be resolved to the remote location's line.



⑥ Adapt the suggested call routing table in order to make international and national long distance calls via the SIP provider line with backup over ISDN. When doing so, please observe that the '0' preceding the number must be removed.



After being adapted for international ① and national ② long distance, the call routing table should appear as follows:



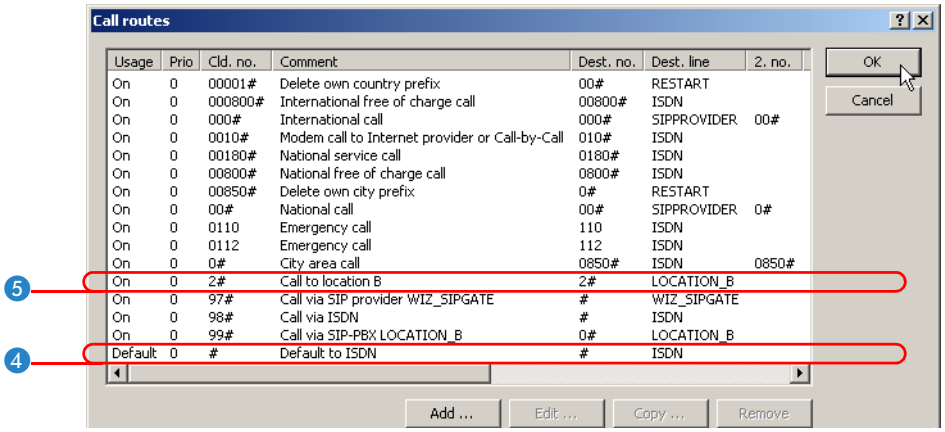
⑦ In this state, all calls that cannot be resolved by the call routing table and which do not have a corresponding entry in the local user list are automatically forwarded to the remote site.

If this is not desired, for example, where more than two sites are connected in this way, an additional entry can detect only the internal calls to a particular site. For this, make a new entry (for the number range '20' to '29' at location B) in the call routing table ⑤ with the following values:

- Called number / name: e.g. '2#' for all numbers that begin with a 2.
- Number / name: The number called is remains unchanged and is used as a destination number, i.e. here, also '2#'.
- Line: Enter the SIP PBX line for the remote location here, i.e. 'LOCATION_B'.

In doing so, the standard route ④ is adjusted so that all numbers which cannot be resolved are transmitted via ISDN.

After being adapted, the call routing table should appear as follows:



This entry for 'LOCATION_B' is placed well down toward the end of the call routing table so as not to affect the more general rules. However, for interaction with the other routes, verify that only the internal numbers for the remote site are directed to the respective line.

Configuring the VoIP terminal equipment

The VoIP terminal equipment is configured as described in the preceding examples with internal VoIP domains and internal numbers for the local site.

Call routing procedure on outgoing calls

For this application, most calls take place as described in the preceding examples. Internal calls between locations are resolved as follows:

	User	dials	correct call route	correct user	mapping, number in use	Destination line
①	VoIP telephone location A	21	2#	none	21	LOCATION_B

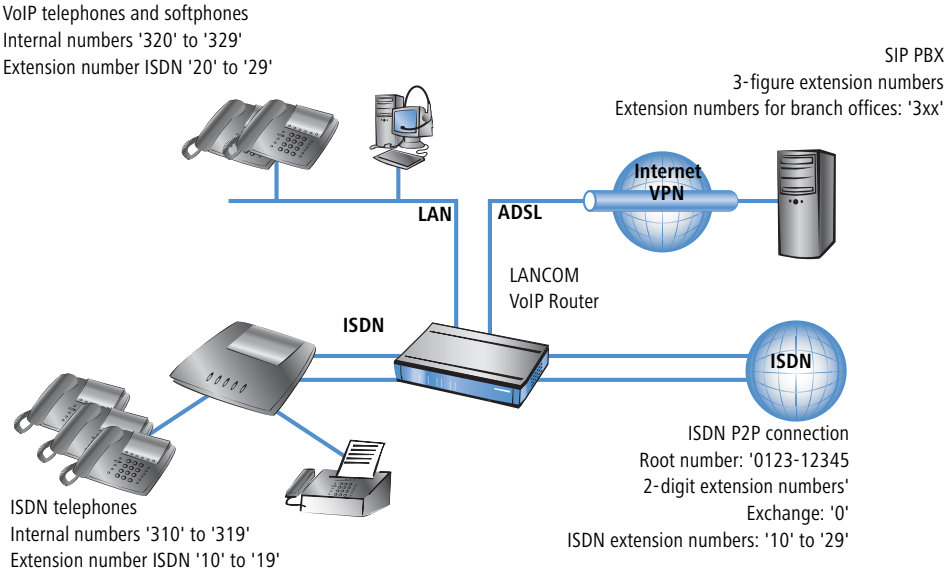
① Internal call between two VoIP terminal devices at locations A and B. The number dialed '21' matches the route 5 '2#' in the call routing table. The call router sends the call out over the line to the remote SIP PBX without changing the number.

13.7.7 The LANCOM VoIP Router at a P2P (point-to-point) connection

Many companies use a point-to-point ISDN connection instead of the more common point-to-multipoint connection. Point-to-point connections offer two significant advantages:

- Über die Durchwahlfähigkeit (DDI – Direct Dialing In) können alle Endgeräte über eine gemeinsame Stammnummer mit nachgestellter Durchwahl zur Auswahl der einzelnen Geräte erreicht werden.
- A larger number of B channels can be used with the same range of telephone numbers, whereas with a point-to-multipoint connection there are only two B channels, typically supporting up to 10 telephone numbers.

ISDN-P2P-Anschlüsse sind als Basisanschluss (Basic Rate Interface – BRI) mit jeweils zwei B-Kanälen oder als Primärmultiplexanschluss (Primary Rate Interface – PRI) mit üblicherweise 30 B-Kanälen verfügbar. LANCOM VoIP Router unterstützen ausschliesslich ISDN-Basisanschlüsse. To be able to use more than four B channels, a P2P connection can be switched to multiple basic rate interfaces with the same range of telephone numbers.



Objectives in implementing the LANCOM VoIP Router

- Connecting additional SIP devices at the branch office.
- Internal calls to users based at the headquarters and other branch offices via the SIP PBX located at the headquarters (using VPN connection).

Requirements

- LANCOM connected to LAN and WAN (via DSL/ADSL), ISDN-TE interface(s) are connected to the ISDN P2P connection, ISDN-NT interface(s) are connected to an ISDN PBX.
- The Internet connection has been set up by means of a VPN tunnel, as has the network connection between the two locations. All terminal devices can contact each other with the IP addresses used.
- A telephone number plan with a unique internal telephone number for each piece of terminal equipment to be connected.

Configuring the LANCOM

The configuration of the SIP client or connection to the SIP PBX as a SIP PBX line named 'HQ' has already been described in other example applications and, here, is assumed to be familiar to you. The SIP PBX at headquarters uses the SIP domain 'mycompany.HQ' and the branch office has the internal domain 'mycompany.BRANCH01'.

This is how the LANCOM is configured for operation at a point-to-point line:

① The ISDN mapping table translates the DDI (extension numbers) to the internal numbers for processing as SIP calls.

MSN/DDI	ISDN/S0 Bus	Internal number	Comment
0	ISDN1, ISDN2	300	Maps DDI '0' to internal number '300'
#	ISDN1, ISDN2	3#	Adds the prefix '3' to all other DDI '0' for the internal numbers

Both entries in this example apply to the ISDN interfaces 1 and 2, which are connected to the ISDN line. The activation of two ISDN interfaces makes four B channels available for use. If both B channels of an ISDN interface are engaged, there is an automatic attempt to redirect calls to another ISDN interface with free B channels.

② Based on the ISDN user entries, the internal numbers are translated back to the DDI numbers.

Internal number	MSN/DDI	ISDN/S0 Bus	Comment
300	0	ISDN3, ISDN4	Maps internal number '300' to DDI '0'. Useful if the exchange is on the ISDN PBX.
31#	1#	ISDN3, ISDN4	Removes the leading '3' from all internal numbers beginning with '3'.

With the second entry, all ISDN terminal devices with the ISDN extension numbers '10' to '19' are made known to be ISDN users in the VoIP system. A single entry here suffices for all subscribers. All ISDN users then use the same data to register at the SIP PBX.

ISDN users entered with the # symbol can only be reached from the SIP PBX if this does not require users to register. For ISDN users to register, separate entries in the ISDN user list are required.

Both entries in this example apply to the ISDN interfaces 3 and 4, which are connected to the ISDN PBX. Here, too, the four B channels of the two interfaces can be used "dynamically" for the connection between the ISDN PBX and the LANCOM VoIP Router.

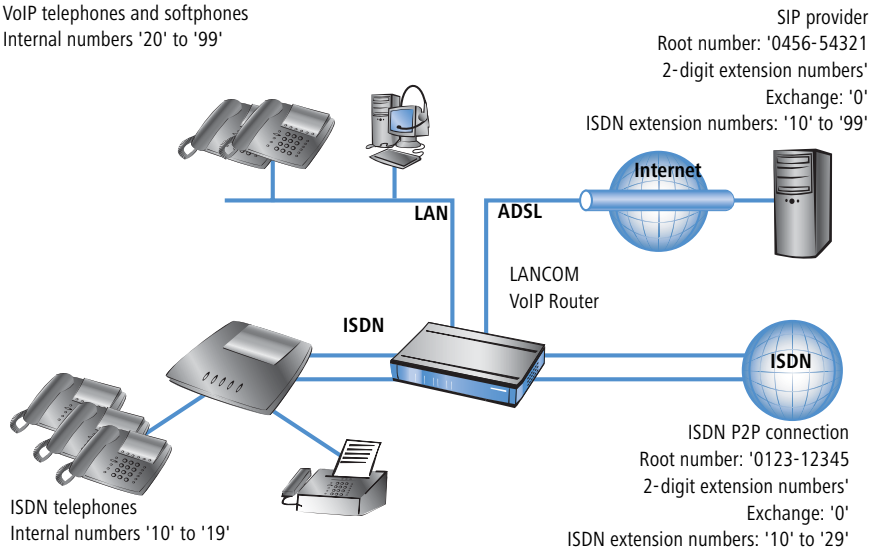
③ Routing of calls is governed by the call routing table. If you use the LANconfig Wizard, the call-routing table is preset so that all outgoing calls from ISDN and SIP devices are conducted via the SIP PBX with the exception of local calls and calls to service numbers, such as 0800 numbers.

13.7.8 SIP trunking

In telecommunications jargon, trunking is the process by which several lines or connections are combined into one shared line. In the world of VoIP, SIP providers are increasingly offering products which provide the ability to make several calls simultaneously using a single account. Together with the possibility of being able to contact SIP participants via a shared root number with individual extensions (DDIs), these types of accounts are also becoming attractive for business customers.

There are two possible options when using a SIP account with trunking:

- The customer retains his previous ISDN connection, along with any corresponding telephone numbers from the telephone company, and sets up an additional account having a separate number range with a SIP provider.
- The customer ports the numbers used thus far from the telephone company to the SIP provider and from then on uses the same numbers using SIP.



In this example we will take a look at a company planning to add a SIP trunking account, with up to 100 extension numbers, to its current ISDN point-to-point line having 20 extensions. The ISDN terminal devices with point-to-point line extensions used thus far can be retained. All new employees are to be issued with a SIP telephone with an extension via the SIP account.

Unique extensions are used since staff members have to be able to call each other internally. In order to migrate smoothly towards SIP, all ISDN terminal devices are to be contactable using **both** extension number and root number of the SIP account. So an ISDN telephone should react in the same way for calls to '0123-12345 12' as it does for calls to '0456-54321 12'.

With the exception of emergency calls and service numbers, such as "0800" numbers, out-going calls are generally made using the SIP account. The signaling of SIP telephone numbers to call parties is paving the way for the medium-term discontinuation of ISDN telephone numbers.

Objectives in implementing the LANCOM VoIP Router

- Connection of additional SIP terminal devices
- Internal calls between ISDN and SIP terminal devices.
- Continuation of availability using ISDN telephone numbers used thus far.
- Low-cost calls by using a shared SIP account.

Requirements

- LANCOM connected to LAN and WAN (via DSL/ADSL), ISDN-TE interface(s) are connected to the ISDN P2P connection, ISDN-NT interface(s) are connected to an ISDN PBX.
- The Internet connection has been set up. All terminal devices can contact each other with the IP addresses used.
- A telephone number plan with a unique internal telephone number for each piece of terminal equipment to be connected.

Configuring the LANCOM

This is how the LANCOM is configured for operation at a point-to-point line:

① The LANCOM is configured for operation at a point-to-point line by adding two simple entries in the ISDN mapping table and in the list of ISDN users.

ISDN mapping table

MSN/DDI	ISDN/S0 Bus	Internal number	Comment
#	ISDN1, ISDN2	#	Outputs the unchanged DDI as an internal telephone number.

ISDN user list

Internal number	MSN/DDI	ISDN/S0 Bus	Comment
#	#	ISDN3, ISDN4	Outputs the unchanged internal number as a DDI.

② When configuring SIP clients, just the internal VoIP domain of the LANCOM VoIP Router and the associated internal number are entered. The extension numbers previously used for the ISDN terminal devices remain unallocated.

③ A SIP provider line is created for the SIP account. The 'Trunk' option is selected as the mode for this line.

④ Routing of calls is governed by the call routing table. When using the Wizards available with LANconfig, the call routing table is pre-configured such that all out-going calls from ISDN and SIP devices are made using the SIP trunk account (with the exception of local calls and calls to service numbers such as the emergency services or "0800" numbers).

Process of call routing

In this example, call routing benefits from the unique internal telephone numbers.

- Bei ankommenden Rufen – egal ob über ISDN oder SIP – wird nur die DDI an den LANCOM VoIP Router übergeben. Since the DDI and internal numbers are the same in this example, an extension number can be used to put through calls to locally registered SIP users or to dynamic ISDN users.

If the reported DDIs can not, or should not, be used directly as internal numbers, corresponding telephone number translations are defined in the ISDN and SIP mapping tables, see 'ISDN mapping' → page 440 and 'SIP mapping' → page 435.

- With out-going calls, the decision as to whether calls are made using ISDN or SIP may be controlled from the call routing table. In the default setting after using the Wizards, SIP is taken to be the normal destination line (with the exception of local calls and special numbers). Local calls, for example, may be switched to SIP by changing an entry in the call routing table.

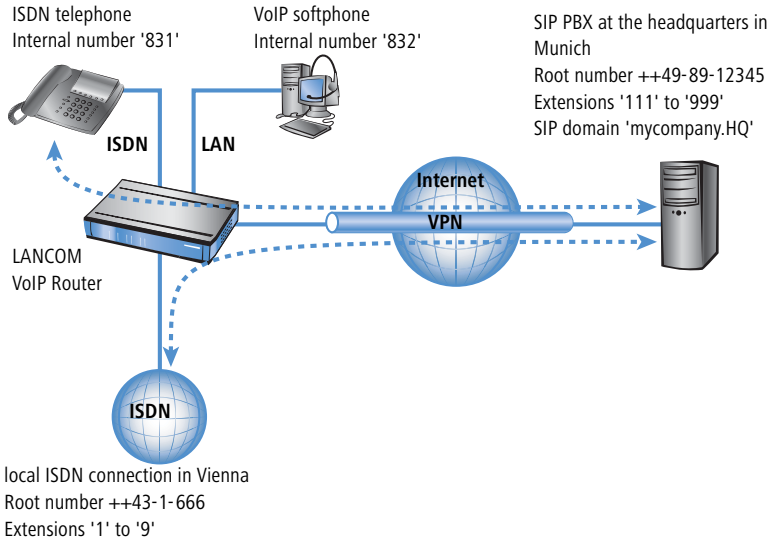
In this case, the SIP number is displayed at the subscribers on the other side of the connection, even if the call originates from an ISDN terminal device.

13.7.9 Remote gateway

Distributed company structures usually provide ISDN connections at branch offices to allow staff local access to the telephone network using appropriate ISDN terminal devices.

- A connection from the local ISDN terminal devices to a SIP PBX at the headquarters can easily be set up using a LANCOM VoIP Router.
- Furthermore, the "Remote Gateway" function can be used to connect both the terminal devices and the local ISDN connections to the central PBX. Benefits of the remote gateway:
  - The local ISDN connections are made available to all users in the company network. Calls to the local ISDN network can be made from anywhere as local calls (even from beyond state boundaries).

□ Alle Gespräche – auch von den lokalen Benutzern ins „eigene" Ortsnetz – können über die SIP-TK-Anlage geführt werden und ermöglichen so eine zentrale Administration und Protokollierung.



In this example we'll take a look at a company headquartered in Munich. The branch office in Vienna should be in a position to call the headquarters using the internal numbers. "83" numbers are taken from the headquarter's number range and are reserved for Vienna for this purpose. The sales and support departments at the company headquarters should also be contactable from Austria as a local, or national long-distance call from Vienna. The purchasing department would also like to be able to contact suppliers in Austria using national long-distance calls.

Objectives in implementing the LANCOM VoIP Router

- Internal calls to users based at the headquarters and other branch offices via the SIP PBX located at the headquarters (using VPN connection).
- Integration of the local ISDN interface into the telephone structure of the organization.

Requirements

- LANCOM Connected to LAN and WAN (via DSL/ADSL), ISDN-TE interface(s) are connected to the ISDN connection, ISDN-NT interface(s) are connected to an ISDN PBX or the ISDN terminal devices.
- The Internet connection has been set up by means of a VPN tunnel, as has the network connection between the two locations. All terminal devices can contact each other with the IP addresses used.
- A telephone number plan with a unique internal telephone number for each piece of terminal equipment to be connected.

Configuring the LANCOM

The following steps are involved when configuring the LANCOM VoIP Router:

- An entry is created for each ISDN user so that the terminal equipment can register with the upstream SIP PBX.
- For SIP clients, this registration information is entered in the VoIP telephone or the softphone.
- The connection to the SIP PBX, as a SIP-PBX line with the name 'HQ', has already been described in other application examples and familiarity with it is assumed from here on.
- In addition to this connection, a further connection "Gateway" needs to be made to the SIP PBX, which helps in making the local ISDN connection known to the upstream SIP PBX.
- The connection between the local ISDN connection and the remote SIP PBX is made using the entries in the call-routing table.

This is how the LANCOM is configured for operation as a remote gateway:

① In the ISDN mapping table, local DDIs (extension numbers) are converted to internal telephone numbers for processing as SIP calls.

MSN/DDI	ISDN/S0 Bus	Internal number	Comment
#	ISDN1, ISDN2	#	All DDIs pending at the ISDN interfaces are switched further without being changed.

② A new entry is created in the list of SIP provider connections with the following information:

- Name of the connection: 'GW.HQ'
- Mode: Gateway
- SIP domain: SIP domain of the headquarters 'mycompany.HQ'
- SIP ID: Account name for the SIP gateway in the SIP PBX located at the headquarters
- Authentication name and password: Registration data for the SIP gateway

③ Additional entries are created in the call-routing table to switch calls between the headquarters and the local ISDN connection:

Called number	Destination number	Source line	Destination line	Comment
#	83#	ISDN	GW.HQ	Forwards all in-going calls arriving at the LANCOM VoIP Router over ISDN to the headquarters via the gateway. The DDI is preceded by '83' so as to map correctly to the internal numbers.
9	555	ISDN	GW.HQ	Forwards all in-going calls arriving at the LANCOM VoIP Router over ISDN to the headquarters via the gateway. '555' is used as the number for support.
0043#	0#	GW.HQ	ISDN	Forwards all out-going calls from the headquarters to the Austrian national network to the local ISDN connection (without country code).
#	#			Forwards all other calls without change.

Call routing procedure on outgoing calls

	User	dials	Call router receives	Call router sends	Assigned via	Source line	Destination line
①	ISDN network D	089-12345-831	831	831	■ List of local ISDN users	GW.HQ	Internal
②	ISDN network A	666-1	1	831	■ Call routing table ■ List of local ISDN users	ISDN	GW.HQ
③	ISDN network A	666-9	9	555	■ Call routing table	ISDN	GW.HQ
④	SIP exchange	0043-662-33333	0043-662-33333	0662-33333	■ Call routing table	GW.HQ	ISDN

① Call from customer in Hamburg to staff in Vienna. The customer dials the number of the Munich headquarters using the correct extension '089-12345-831'. Because the ISDN user is registered with the internal telephone number, the PBX at the headquarters receives only the DDI '831' and passed it on via the SIP PBX line. The LANCOM VoIP Router receives '831', locates a matching entry in the list of locally registered users and is able to connect the call.

② Call from customer in Vienna to the branch office in Vienna. The customer dials the number of the branch office in Vienna using the correct extension '666-1'.

- □ The LANCOM VoIP Router receives the DDI '1' and is not able to locate a matching entry in the list of locally registered users. Using the call-routing table, the telephone number is changed to '831' and forwarded on to the PBX in Munich via the SIP gateway connection. The PBX recognizes the registered ISDN user with the internal telephone number '831' and passes the call back to the LANCOM VoIP Router via the SIP PBX line.
- □ The LANCOM VoIP Router then receives '831', locates a matching entry in the list of locally registered users and is able to connect the call.

③ Call from customer in Salzburg to the support number in Vienna. The customer dials the number of the branch office in Vienna using the correct extension '666-9'. The call is automatically put through to the internal support number '555' using the call routing table.

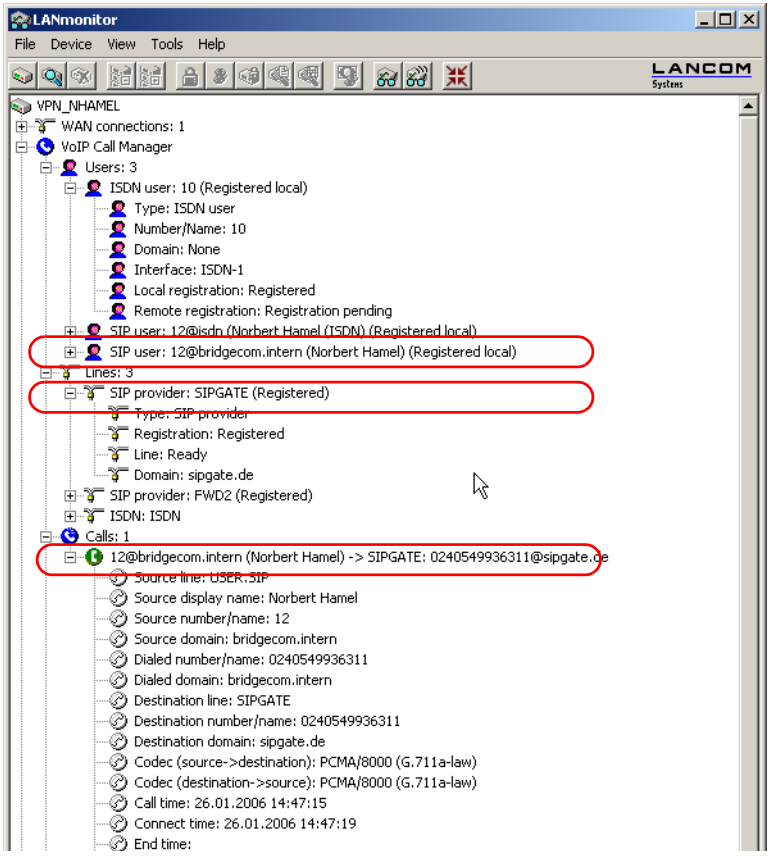
④ Call from employee in Munich to customer in Salzburg. The employee dials '0043-662-33333'. The PBX in Munich is configured such that all calls to Austria are forwarded via the SIP gateway connection to the LANCOM VoIP Router. The call router receives the complete number, drops the country code as per the routing table having source line 'GW.HQ' and forwards the remaining number to the ISDN line.

Here the call number from Munich is displayed at the remote site.

13.7.10Connection diagnosis with LANmonitor

LANmonitor displays a wealth of information about calls switched in the LANCOM:

- Information about the registered users.
- Information about the lines available.
- Information about current calls, including the translation of telephone numbers and domains by the Call Manager.


LANmonitor
File Device View Tools Help
LANCOM Systems
VPN_NHAMEL
WAN connections: 1
VoIP Call Manager
Users: 3
ISDN user: 10 (Registered local)
Type: ISDN user
Number/Name: 10
Domain: None
Interface: ISDN-1
Local registration: Registered
Remote registration: Registration pending
SIP user: 12@isdn (Norbert Hamel (ISDN) (Registered local)
SIP user: 12@bridgecom.intern (Norbert Hamel) (Registered local)
Lines: 3
SIP provider: SIPGATE (Registered)
Type: SIP provider
Registration: Registered
Line: Ready
Domain: sipgate.de
SIP provider: FWD2 (Registered)
ISDN: ISDN
Calls: 1
12@bridgecom.intern (Norbert Hamel) -> SIPGATE: 0240549936311@sipgate.de
Source line: USER.SIP
Source display name: Norbert Hamel
Source number/name: 12
Source domain: bridgecom.intern
Dialed number/name: 0240549936311
Dialed domain: bridgecom.intern
Destination line: SIPGATE
Destination number/name: 0240549936311
Destination domain: sipgate.de
Codec (source->destination): PCMA/8000 (G.711a-law)
Codec (destination->source): PCMA/8000 (G.711a-law)
Call time: 26.01.2006 14:47:15
Connect time: 26.01.2006 14:47:19
End time:

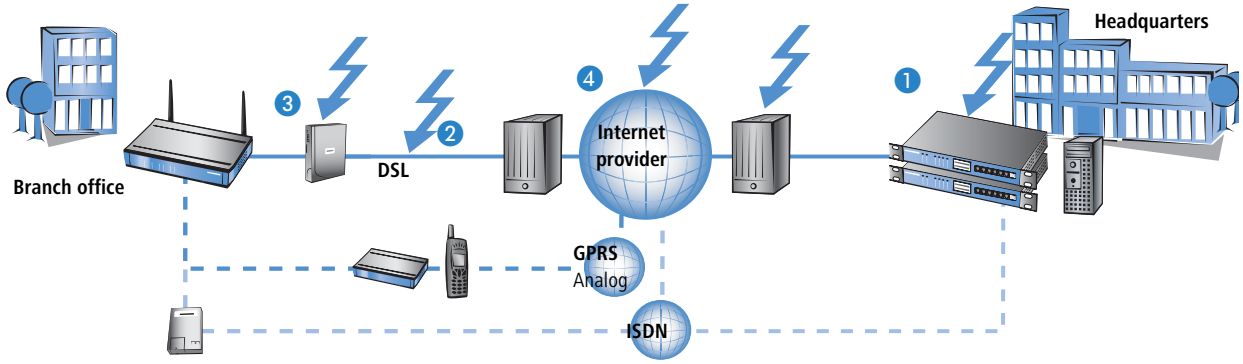
14 High availability – backup solutions

14.1 High availability for networks

Networked cooperation between several offices or even between continents has become an everyday part of modern business. The paths of communication between headquarters, subsidiaries and field workers increasingly rely upon public infrastructures. VPN has become established as the de facto standard for cost-effective and secure enterprise communications over the Internet.

However, many of important elements in these network structures remain susceptible to failure which could have severe consequences for business operations:

- The remote Internet gateway (1) itself can fail.
- The physical lines for the connection to the Internet or to a remote network can fail:
  - The Internet-access cable between the site and the provider (2) could fail; after damage from construction work, for example.
  - The DSL connection (3) may fail, while the ISDN connection remains functional.
- The provider's network (4) may be disturbed or even fail.



Internet routers and access points from LANCOM offer a range of security and backup functions that can be used for the protection of your network from disturbance.

14.1.1 How is a network-connection disturbance detected?

The first stage in protecting a network connection from the effects of a disturbance is to detect the disturbance itself. The following methods are available to check the connections:

- Check the PPP connection to the provider with PPP LCP echo monitoring.
- Check if remote stations can be contacted via name or IP address with ICMP polling (ping from end to end).
- Check the tunnel end points with "dead peer detection" (DPD).

PPP LCP echo monitoring

The method checks the PPP connection to a certain remote site with regular LCP requests. This method is typically used to check the connection to the Internet provider. LCP requests are directly sent to the access server.

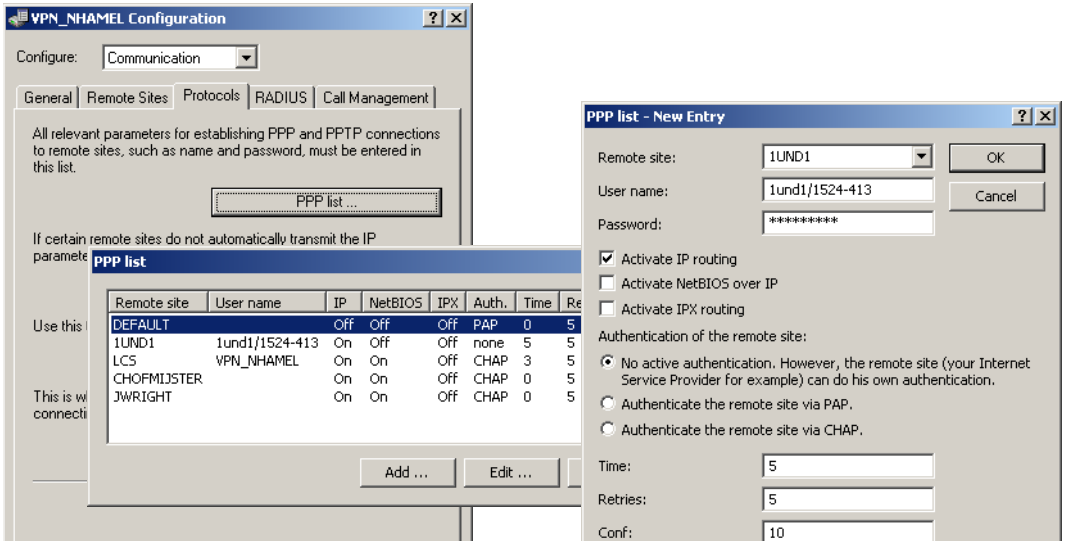
In the PPP list, a time interval for the transmission of LCP requests to the remote site is defined for this connection. Further, for the event that LCP replies are missed, the number of retries before the transmission of a new LCP request is defined. Should the transmitter not receive any reply to the retries, the line is considered to have failed.

- **Time:** The time entered into the PPP list must be multiplied by the factor 10 to arrive at the actual interval between two LCP requests. Entering the time as "5" means that an LCP request will be prompted every 50 seconds.
- **Retries:** If no reply to an LCP request is received then the remote site will be checked in shorter intervals. The device then tries to reach the remote site once a second. The number of retries defines how many times these attempts are repeated. Entering "5" under retries means that the LCP request will be repeated 5 times before the connection is considered to have failed.

PPP LCP monitoring only checks the PPP connection path as far as the Internet provider.

Configuration with LANconfig

The LCP monitoring is set up with LANconfig in the configuration area 'Communication' on the 'Protocols' tab in the 'PPP list'.



Configuration with WEBconfig, Telnet or SSH

Under WEBconfig, Telnet or SSH client you will find the settings for the LCP monitoring under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ WAN ▶ PPP list
Terminal/Telnet	`Setup/WAN/PPP-list`

ICMP polling

Similar to LCP monitoring, ICMP polling transmits regular requests to a remote site. Ping commands are transmitted and the answers to them are monitored. Unlike LCP monitoring, the target site for ICMP pings can be freely defined. Pinging a router in a remote network thus provides monitoring for the entire connection and not just the section to the Internet provider.

A ping interval is defined for the remote site in the polling table. Further, for the event that replies are missed, the number of retries before the transmission of a new LCP request is defined. Should the transmitter not receive any reply to the retries, the target for the ping requests is classified as unavailable.

Up to four different IP addresses can be entered for each remote site that will be checked in the remote network in parallel. Only if all of the IP addresses are unavailable is the connection considered to have failed.

With the ICMP polling, an entire connection can be monitored from end to end.

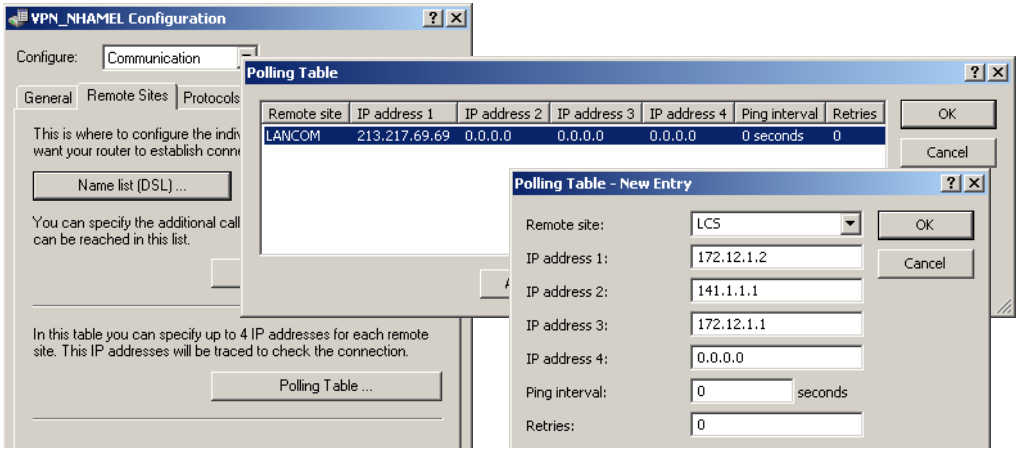
- **Name of the remote site**
- **IP address 1-4:** IP addresses for targeting with ICMP requests to check the remote site.

If no IP address is entered for a remote site that can be checked with a ping, then the IP address of the DNS server that was determined during the PPP negotiation will be checked instead.

- **Ping interval:** The time entered into the polling table defines the time interval between ping requests. If the value "0" is entered, then the standard value of 30 seconds applies.
- **Retries:** If no reply to a ping is received then the remote site will be checked in shorter intervals. The device then tried to reach the remote site once a second. The number of retries defines how many times these attempts are repeated. If the value "0" is entered, then the standard value of 5 retries applies.

Configuration with LANconfig

The ICMP polling is set up with LANconfig in the configuration area 'Communication' on the 'Remote sites' tab in the 'Polling table'.



Configuration with WEBconfig, Telnet or SSH

Under WEBconfig, Telnet or SSH client you will find the settings for the LCP monitoring under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ WAN ▶ Polling table
Terminal/Telnet	`Setup/WAN/Polling-table`

Dead peer detection (DPD)

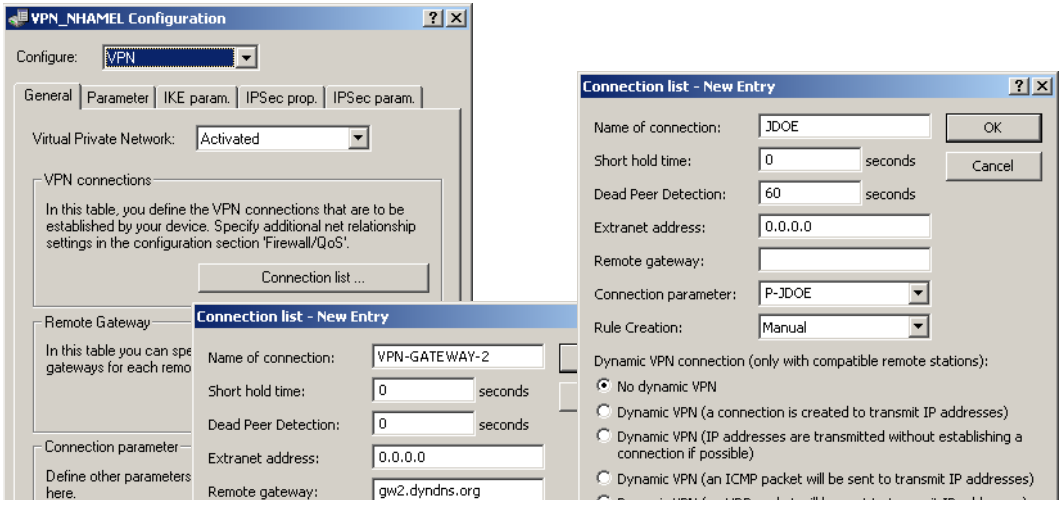
This method of connection monitoring is used when VPN clients dial-in to a VPN gateway. This is designed to ensure that a client is logged out if there is an interruption to the VPN connection, for example when the Internet connection is interrupted briefly. If the line were not to be monitored, then the VPN gateway would continue to list the client as logged-on. This would prevent the client from logging in again as, for example, the WLANmonitor prevents single serial numbers from multiple simultaneous log-ins.

For the same reason, without line monitoring a user with the same "identity" (user name) would be prevented from dialling in because the associated user would still be in the list for the logged-in client.

With dead peer detection, the gateway and client regularly exchange "keep alive" packets. If no replies are received, the gateway will log out the client so that this identity can be registered anew once the VPN connection has been re-established. The DPD time for VPN clients is typically set to 60 seconds.

Configuration with LANconfig

The dead peer detection is set up with LANconfig in the configuration area 'VPN' on the 'General' tab in the 'Connection list'.



Configuration with WEBconfig, Telnet or SSH

Under WEBconfig, Telnet or SSH client you will find the settings for the dead peer detection under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ VPN ▶ VPN-Peers
Terminal/Telnet	`Setup/VPN/VPN-Peers`

14.1.2 High-availability of lines – backup connections

If there is a disturbance to the connection with the Internet provider or to a remote network, a backup line can act as a temporary replacement for the normal data line. This requires the existence of a second physical connection which can be used to contact the remote site. Examples of backup lines are typically:

- An ISDN line as a backup for DSL Internet access
- An ISDN line as a backup for VPN network coupling
- A modem connection (GSM or analog) as a backup for DSL or ISDN lines and VPN connections

Configuration of the backup connection

The following steps are necessary to define a backup connection:

① The backup connection requires the appropriate WAN interface to be set up so that the remote site can be reached via this alternative route. If, for example, the ISDN line is to serve as the backup connection, then the remote site is set up as an ISDN remote site (along with the necessary entries in the communications layers and in the PPP list).

② If the connection to the remote site cannot be checked with LCP requests, the monitoring of the connection should be initiated with an entry in the polling table.

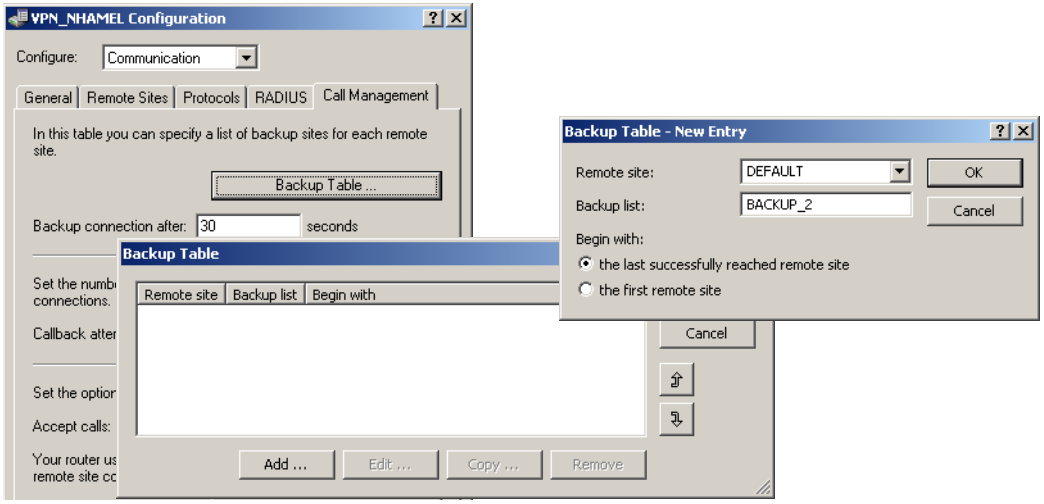
③ Assignment of the new backup connection to the remote site which is to be backed up. This entry is made in the backup table. Dedicated entries in the routing table are not required for a backup connection. The backup connection automatically takes over the source and target networks from the remote site that routes the data under normal operating conditions.

A remote site can be assigned with multiple backup lines in the backup table. In the case of backup, the system decides which backup line is to be used first:

- The last remote site that was reached successfully
- The first remote site in the list

Configuration with LANconfig

The backup table is set up with LANconfig in the configuration area 'Communication' on the 'Call management' tab in the 'Backup table'.



Configuration with WEBconfig, Telnet or SSH

Under WEBconfig, Telnet or SSH client you will find the settings for the backup table under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ WAN ▶ Backup table
Terminal/Telnet	`Setup/WAN/Backup-table`

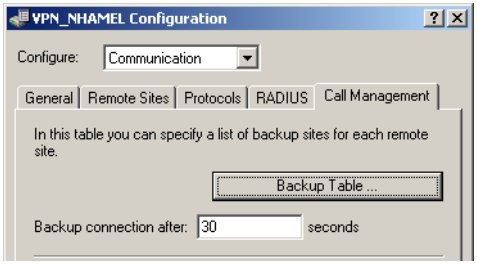
Triggering the backup connection

The backup is triggered when the monitoring mechanisms defined for the standard connection (LCP or ICMP polling) detect that contact to the remote site has been lost.

The backup connection will be established if:

- The backup delay time has expired and
- either
  - a data packet is to be transferred or
  - a hold time of 9999 seconds has been defined for the backup connection.

The backup delay time is set with LANconfig in the configuration area 'Communication' on the 'Call management' tab or alternatively with Telnet under `/Setup/WAN-Modul/Backup-delay-seconds`.



Return to the standard connection

The router constantly tries to establish the standard connection while the backup connection is active. As soon as the standard connection has been established, the backup connection is terminated and the line monitoring with LCP or ICMP polling is resumed.

Only keep-alive connections return automatically!

The standard connection will only be automatically re-established after a backup event if the hold time for the connection is configured properly:

- A hold time of "0" means that the connection will not be actively terminated. If the connection is interrupted, it will not be automatically established again. Only when communication is required of the connection will it be established.
- A hold time of "9999" means that the connection is permanently kept open. If it is interrupted, then the connection will be actively opened up again. This behavior is known as **keep alive**.

Set the hold time to "9999" for connections to the Internet provider (in the corresponding peer list) and backed-up VPN connections (in the VPN connection list) to ensure that the connection is automatically re-established and resumes data transfer after interruption.

14.1.3 High-availability of gateways – redundant gateways with VPN load balancing

Another cause of failure apart from the connection to the provider or to another network may lie with the local gateway. Severe effects can result from the failure of a central VPN gateway that is used, for example, to connect the networks of multiple remote locations with the central network at headquarters.

To ensure that the headquarters remains in contact, multiple VPN endpoints (generally identically configured VPN gateways operated in parallel) can be installed. Should line polling (with dead-peer detection, ICMP line polling) indicate a failure, then a variety of strategies (e.g. the random selection of one of the available gateways) can be used to enable communication to a different VPN end point. At the central headquarters, the new router and the local default gateway are propagated by dynamic routing (RIP V2).

To avoid the situation where the additional VPN gateways remain unused, intelligent load balancing ensures that all of the devices share the load of incoming and outgoing connections also under normal operating conditions.

More information about redundant gateways and load balancing is available under 'VPN connections: High availability with VPN load balancing' → page 314.

14.1.4 High-availability of the Internet access – Multi-PPPoE

The third of the different basic sources of failures is the case where the gateways and connections are in order but the provider's own network is down. Such cases are handled by setting up multiple PPoE connections at the physical interface of a single device (Multi-PPPoE).

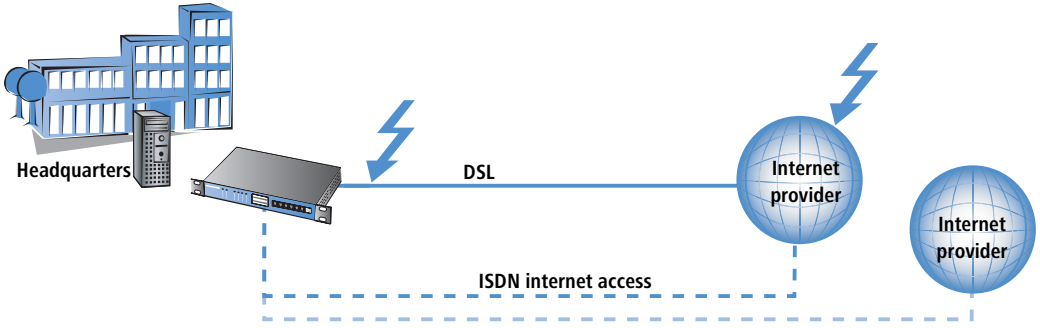
To define these backup solutions as alternative Internet accesses you can use, for example, the Setup Wizard to set up two Internet access accounts one after another. The standard Internet access for normal operations should be set up last. Consequently, the entries in the routing table will be associated with the appropriate remote site.

Additionally, an entry is made in the backup table that defines the alternative Internet access account as the backup to the remote site at the standard provider.

More information about the definition of multiple PPPoE connections is available under 'Multi-PPPoE' → page 129.

14.1.5 Example applications

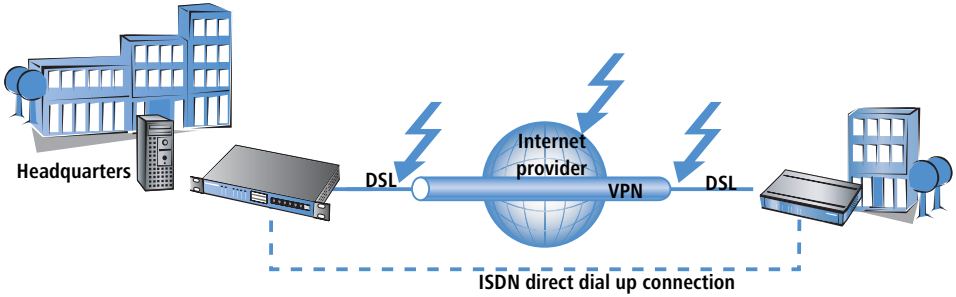
Backup DSL Internet access with ISDN internet access



In this simple backup scenario, Internet access is realized via a DSL connection. An ISDN connection is defined as a backup in case of failure of the DSL Internet access.

This backup solution can be quickly and easily set up with the help of the LANconfig Setup Wizard, for example. A further degree of security is available by defining another Internet provider in addition to the standard provider. This solution caters for the contingency where the provider's network fails and the problem is not caused by the DSL connection.

Backup dynamic VPN network coupling with an ISDN direct dial up connection



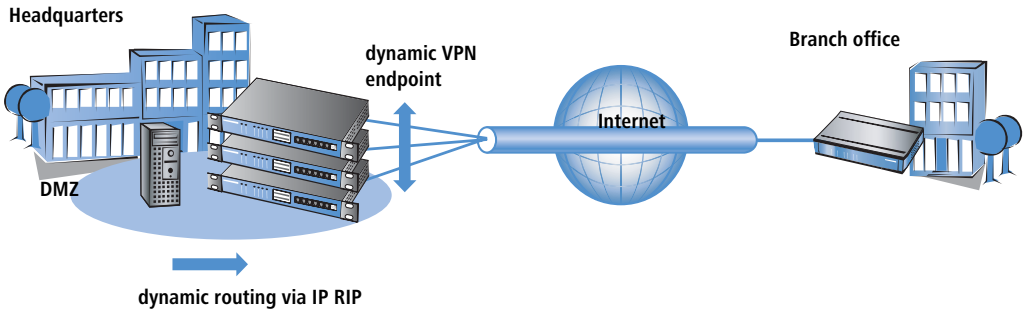
In the case that a branch office is connected to the headquarters via a VPN connection, the Internet-based VPN connection can be backed up by a direct ISDN dial-in connection. Should the Internet connection fail at either of the two routers, the data transmission is transferred to the ISDN link.

In this scenario we are assuming a fully configured VPN connection between the two networks.

- A LAN-LAN coupling via ISDN is additionally set up between the two networks. Do **not** use the Setup Wizard to set up this network coupling! The Wizard would change the entries in the routing table and would thus upset the function of the VPN network connection. Set up the ISDN network coupling in both routers manually—with the appropriate entries for the remote sites in the peer list, the PPP list and with the necessary telephone numbers and access identifiers.
- In the gateway at the headquarters, create an entry in the backup table that acts to backup the VPN remote site via a directly dialled ISDN remote site.
- Further, the router at the headquarters requires an entry for the monitoring of a remote device in the network at the branch office: Typically in the form of the LAN IP address at the remote VPN gateway. This entry ensures that the router at the headquarters can react immediately to a failure of the VPN connection.

Should there be a failure in the connection between the headquarters and branch office (on the way to the Internet provider or at the provider itself) then the ISDN connection takes over the data transfer independent of the Internet.

Redundant VPN gateways



In decentralized company structures that rely on VPN for networking the various locations, the availability of the central VPN gateway is of particular significance. The company-wide communications only remain reliable as long as these central dial-in nodes are working properly.

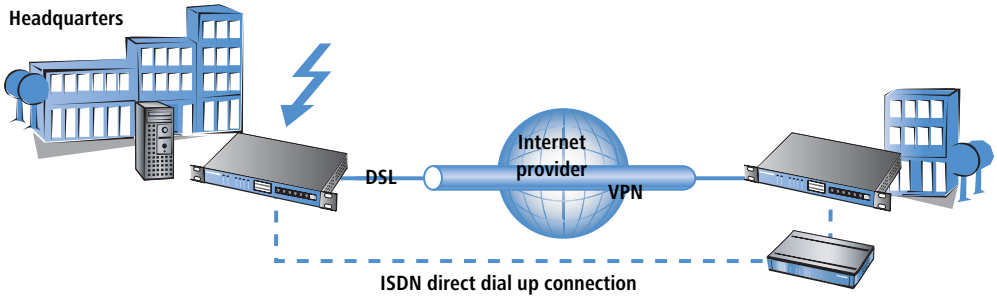
With the option of configuring several "remote gateway" addresses as "dynamic VPN endpoints" for a VPN connection, LANCOM VPN gateways offer a high level of availability by using redundant devices. This involves multiple gateways at the headquarters being set up with identical VPN configurations. On location at the satellite sites, all of these available gateways are entered as possible remote stations for the VPN connection. If one of the gateways is unavailable, the remote router automatically redirects the request to one of the other routers.

To ensure that the computers in the LAN at the headquarters know which VPN gateway it to be used to reach a particular satellite station, the outband router currently connected to the remote site is propagated via RIPv2 to the network at the headquarters.

A powerful mechanism for load balancing between the VPN gateways at the headquarters is attained with the configuration of the satellite stations to select the remote site for VPN connection on a random basis ("VPN load balancing").

Further information to redundant gateways and "VPN Load Balancing" can be found in 'VPN connections: High availability with VPN load balancing' → page 314.

Backup a VPN gateway with an ISDN gateway and RIP



Going a step further, the VPN gateways themselves can be backed up in case of failure. This case assumes the existence of a VPN connection between two gateways. In the event that one of the two VPN devices should fail, an ISDN connection is to take over the data transfer; in this case via a direct dial-in connection.

Regarding the configuration of this solution, we again assume a functional VPN coupling of the two networks. The following additional steps are required:

- A standard ISDN network coupling that routes the same subnets as the VPN connection is set up between the two ISDN routers. In the routing table, however, a distance is entered that is at least 1 higher than the corresponding route in the VPN gateway.
- The local RIP (RIP V2) has to be activated in all routers so that the VPN and ISDN routers can exchange information about the routes with the remote sites. The higher distance of the route via the ISDN gateway is, under normal circumstances, the poorer route.
- It is not necessary to define a backup connection in this case as a different device should take over the data transmission.

If there is a disturbance in the connection between the VPN devices, the value for the distance of the corresponding routes changes automatically: A route which is not available is marked with a distance of 16. Consequently, the route entered into the ISDN router automatically becomes the "better" solution and all data packets will be re-routed over the ISDN connection. As soon as the VPN connection is re-established, the distance changes to a value below that of the ISDN connection and the backup will be terminated as intended.

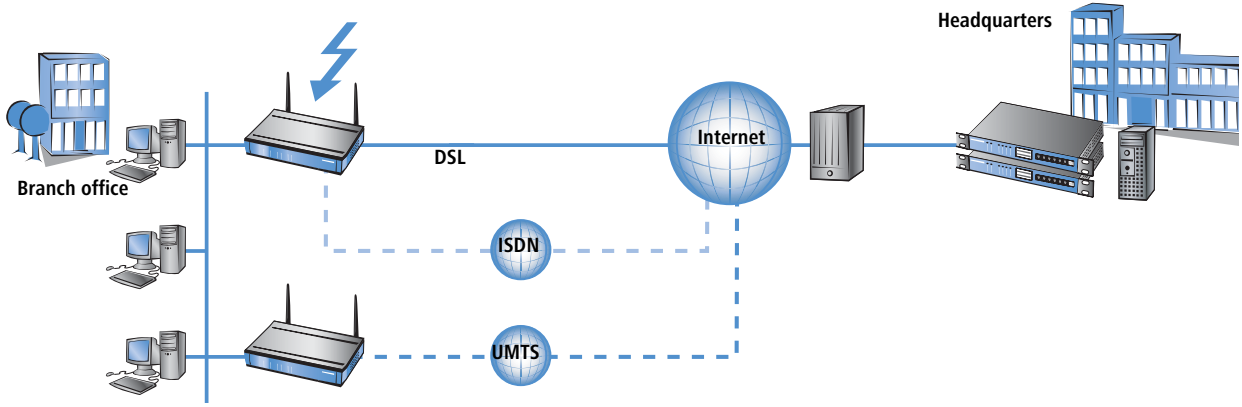
14.2 Backup Solutions and Load Balancing with VRRP

14.2.1 Introduction

For businesses in particular, the high availability of data connections presents an essential requirement of the network components. LANCOM Systems devices provide various mechanisms for securing data transfer as a backup solution:

- Various WAN interfaces (DSL, ISDN, UMTS) enable data transfer over a second physical medium if the primary WAN interface is disturbed or fails.

- In order to provide protection from failure of an Internet provider's network, different Internet access accounts can be configured with Multi-PPoE.
- Two or more VPN gateways in a network can share the VPN tunnels required, thus keeping data traffic alive even in cases of temporary failure of a VPN end point.
- VRRP can now also be used to implement a sophisticated backup system for protection against router hardware failure. Two or more routers are installed in a network, one of which can replace the other in case of device failure.
- In addition to normal VRRP, LANCOM devices can link the backup event triggering function to the availability of a data connection. With this additional feature, LANCOM devices with more than one WAN interface (e.g. DSL and ISDN interface) can be implemented flexibly in backup solutions. The backup event is triggered for example, when the default route is no longer available via the DSL interface. The device's ISDN interface can take its place further along in the backup chain should the the backup router also fail ('Backup chains' → page 507).



14.2.2 Virtual Router Redundancy Protocol

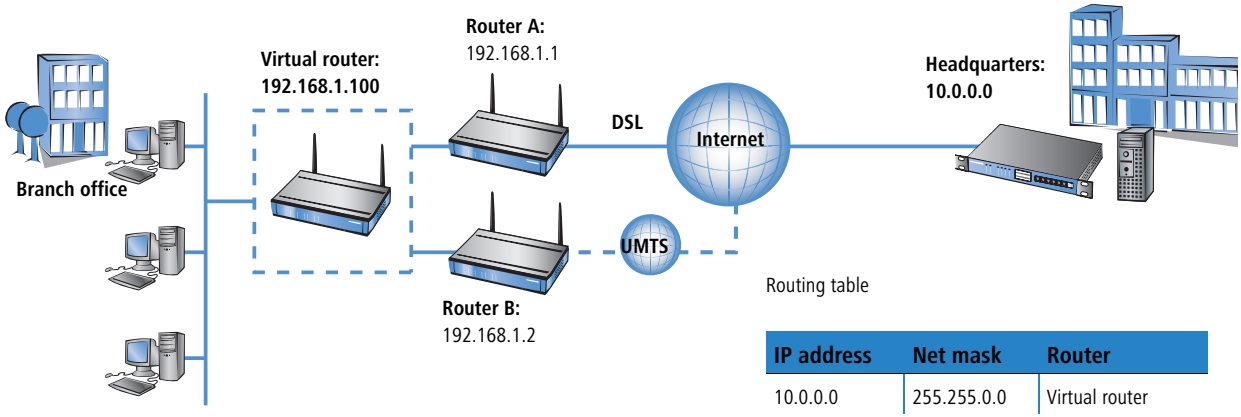
VRRP – Virtual Router Redundancy Protocol – enables multiple physical routers to appear as a single "virtual" router. Of the existing physical routers, one is always the "master". The master is the only router that establishes a data connection to the Internet, for example, and transfers data. The other routers only play a role when the master fails (e.g. due to a hardware defect or because its Internet connection is no longer available). Using the VRRP protocol, which is described in RFC 3768, they negotiate which device should assume the role of master. The new master completely takes over the tasks that were carried out by the previous master.

Virtual and physical routers

Dynamic routing protocols such as RIP adapt the entries in dynamic routing tables when, for example, a route is no longer available. When using VRRP, hosts in the LAN can use a static routing table even though the gateway IP address may change, for example, when a device fails due to a defect and another device takes over its functions. VRRP uses "virtual routers" in the routing tables so that the network users always find the right gateway neverthe-

less. A virtual router is broadcasted in the network with the IP address '192.168.1.100' in the same way as a "normal" router would be and takes over the function of a gateway to certain remote stations. The actual work of data transfer is carried out by the physical routers behind the virtual router.

- Under normal operating conditions, for example, router A with the IP address '192.168.1.1' establishes the connection to the Internet.
- If router A fails, then router B with the IP address '192.168.1.2' takes over the functions of router A. The network clients do not notice this change; for them, the "virtual" router '192.168.1.100' is still the gateway.



Routing table

IP address	Net mask	Router
10.0.0.0	255.255.0.0	Virtual router

From a more technical standpoint, a router in a network requires a unique MAC address in addition to an IP address. Therefore, when defining a virtual router, a virtual MAC address is defined simultaneously which the virtual router reacts to. The virtual MAC address is formed as '00-00-54-00-01-xx', whereby 'xx' stands for the unique router ID.

In order to determine which physical router reacts to the combination of virtual IP and MAC address, priorities are used for the physical routers. For this purpose, every physical router is assigned a priority. The router with the highest priority takes over the functions of the virtual router as master and thus reacts to the virtual IP and MAC addresses. If two physical routers have the same priority, then the router with the "higher" physical IP address is considered to be the master.

All physical routers report their availability on a regular basis so that, should the current master fail, the router with the next highest priority can take over the routing function at the end of this interval at the latest. If a device determines that it cannot complete the tasks required, it can actively log off before the end of the interval thereby triggering the transfer of the master role to the router with the next priority.

The major advantage of virtual routers is that they enable very flexible scenarios with backup and load balancing functions which remain virtually undetected by the LAN. Clients in the local network randomly select a DHCP server from those available and retrieve the required address information from this server.

Address assignment via DHCP with more than one DHCP server in the LAN

Several DHCP servers can be operated parallel to each other in a LAN without disrupting one another's functionality. Upon establishing a network connection, the DHCP clients request an IP address selecting one of the available DHCP servers. The DHCP server receiving the request checks to determine whether the address requested is available or already in use within the LAN before assigning the address. This check prevents address conflicts even when several DHCP servers are in use.

For the clients, it is irrelevant which physical router subsequently establishes the data connection. Similarly, the LAN clients do not notice when a router or WAN interface fails due to the fact that, in this case, another router steps in and is available under the same virtual addresses as before.

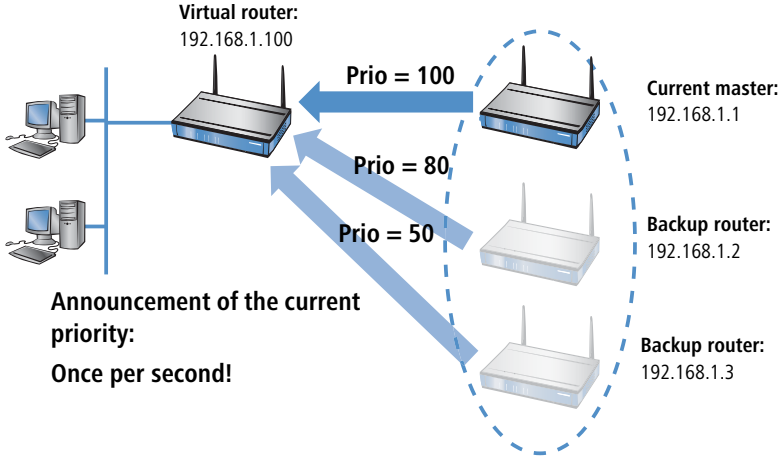
Device, connection or remote station backup

A device can disconnect itself from the VRRP group, an option which indicates that the possibilities offered by VRRP are not restricted only to the failure of a device.

VRRP only provides one backup mechanism which safeguards against device failure. In practice, however, the failure of a physical data transfer medium (e.g. DSL, ISDN or UMTS) or the unavailability of a remote station prevent the router from completing its tasks as planned. For this reason, the LANCOM-specific enhancements to VRRP also offer the ability to define the availability of a remote station as a trigger for the backup event—regardless of whether the data connection is denied due to device, connection or remote station problems.

For the definition of a virtual router, the IP address by which it can be accessed, its priority and its logical router ID are required as a minimum. The router ID serves to ensure that the regular messages from the physical routers can be assigned to the respective virtual routers.

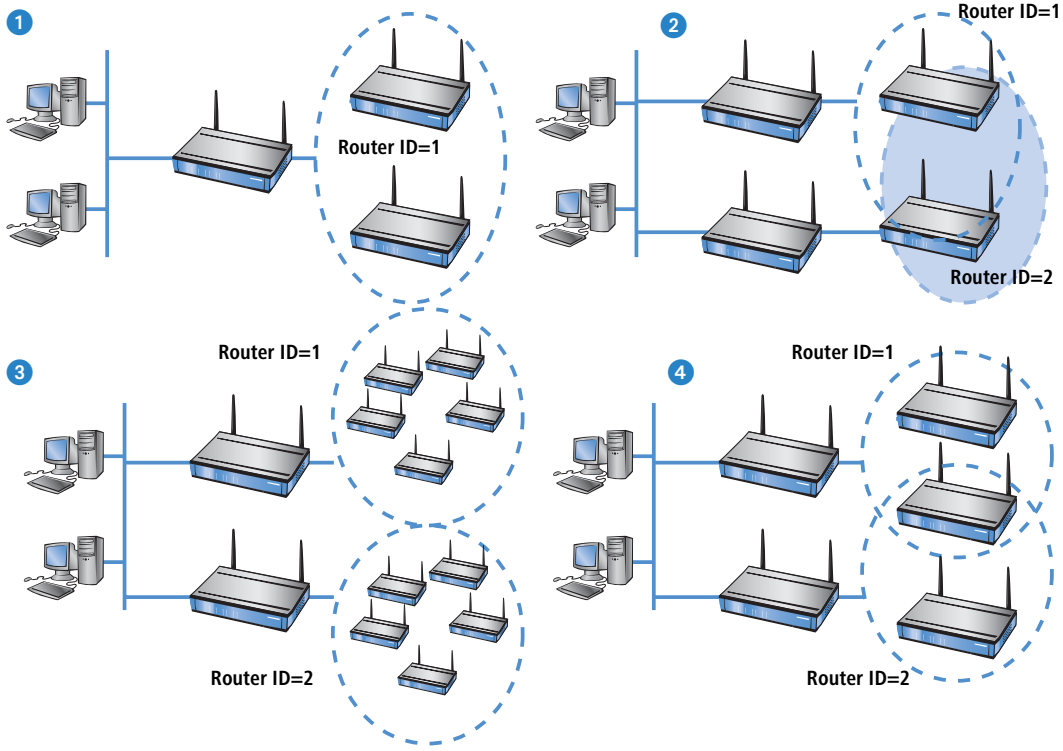
- The router ID can assume a value between 1 and 255. The router ID also reveals the router's virtual MAC address as 00:00:5E:00:01:router ID. The router ID 0 is not permitted.
- The IP address for the virtual router can be chosen freely, however, it must obviously be within the local network. If the virtual router's address is the same as the physical router's address, then the physical router is the "main master" of the system. The main master automatically has the highest priority, that is, when it signals that it is ready for operation, it immediately becomes the active master.
- The priority can assume a value between 1 and 254. The values 0 and 255 have special meanings: With the priority '0', the virtual router is not active, with '255', this virtual router is the main master.



Router ID defines "standby groups"

The physical routers can be assigned to the virtual routers with the router ID that is determined when defining the virtual router. All devices in which virtual routers are set up with the same router ID form a "standby group" in which the devices can act as replacements for one another. There are three different examples of standby groups:

- In a simple backup scenario, two or more routers form **one** standby group. A virtual router with the same router ID and the same virtual IP address is configured in both physical routers (position 1 in the following illustration).
- In order to perform load balancing, the same number of virtual routers with differing IDs and IPs are defined as there are physical routers planned for the VRRP group. For example, two devices would each belong to **two** standby groups 2.
- It is also possible to create more complex combinations with many devices. For example, two devices can form their own standby group with router ID 1 and two other devices can form another group with the ID 2 3. Depending on the requirements, it is also possible to selectively assign certain devices to a single group while other devices remain members of all groups 4.



The Priority System

With the analysis of the priorities, VRRP controls the order in which the physical routers take over the function of the master in a VRRP group. VRRP only considers the failure of an entire device to be a trigger for the backup event.

Since numerous LANCOM devices have more than one WAN interface, the VRRP application in LCOS takes not only the failure of a device but also interruptions to the data connection or the unavailability of a remote station as triggers for the backup event. In order to enable the backup behavior of the LANCOM devices and the formation of backup chains, every virtual LANCOM router is assigned two priorities: a main and a backup priority.

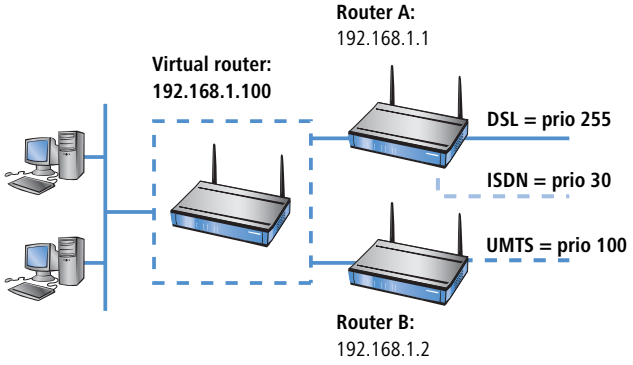
- The main priority is used (propagated into the network) as long as the device is in normal operating condition (i.e. the remote station for the standard connection is still available).
- The backup priority is propagated when the device is in backup mode (i.e. the backup delay has expired and the connection could not be reestablished).
- If '0' is set as the backup priority, the router will not send any signals until the end of the backup event, i.e. the device is not available to the VRRP router group when the remote station is not available.

Since VRRP only knows "priorities" and does not differentiate between main or backup priority, it simply analyzes the priority that is currently being propagated by the device. The device with the currently highest priority is considered to be master.

Normally, priorities are configured so that the main priorities of the devices in a VRRP group are larger than the backup priorities used. However this is a general rule and not a requirement. The main priority of router A can be smaller than the backup priority of another router B. In this case, the backup connection of device B is used **before** the standard connection of router A in the backup chain ('Backup chains' → page 507).

The assignment of priorities to the various WAN interfaces can be determined from the configuration of the backup connections in the backup table (under LANconfig in the configuration area 'Communication' on the 'Call management' tab).

- The main priority refers to the interface on which the standard connection is configured.
- The backup priority refers to the interface on which the backup connection is configured.



VRRP list router A:

Main prio:	Backup prio:	Remote site
255	30	INTERNET DSL

Backup list router A:

Remote site	Backup list

VRRP list router B:

Main prio:	Backup prio:	Remote site
100	0	INTERNET UMTS

A master that has been activated due to the priority status will now attempt to establish a connection if this has been configured as a keep alive connection. If the connection is set up as a normal connection with a hold time, then it will not be established until the next packet is transmitted. If this connection fails, thereby triggering the backup event, then the router will also log off and then propagate itself with its backup priority.

Backup chains

The use of two priorities enables the formation of flexible backup chains by which each physical router does not merely take a single place within the chain but takes a place for every physical WAN interface:

- The first physical router, the main router in the network, has a DSL and an ISDN interface for example, the second router (backup router) has a DSL and a UMTS interface.

- The first router receives the main priority '255'. Consequently, it will become the main router with the value '50' as its backup priority.
- The second router receives the main priority '150' and the value '100' as its backup priority.

Under normal operating conditions, data traffic is processed by the DSL interface on the first router. If the router or this interface fails, the second router attempts (due to the next highest main priority) to establish the connection via its own DSL interface. If this does not succeed, then both devices will propagate their backup priority. Since the second router has the higher backup priority, the connection is established using its UMTS interface. Only when this interface is also unable to establish a connection will the ISDN interface on the first router (with the lower backup priority) be used.

Only keep alive connections return automatically!

The standard connection will only be automatically reestablished after a backup event if the hold time for the connection is configured properly:

- A hold time of "0" means that the connection will not be actively terminated. If the connection is terminated or interrupted due to interference, it will not be automatically established again. The connection will only be reestablished when communication is required of it.
- A hold time of "9999" means that the connection is permanently held open. If it is interrupted, then the connection will be actively opened up again. This behavior is known as **keep alive**.

Set the hold time to "9999" for connections to the Internet provider (in the corresponding name list) and backed-up VPN connections (in the VPN connection list) to ensure that the connection is automatically reestablished and resumes data transfer after interruption.

Return to the VRRP group

After an adjustable amount of time (reconnect delay), a router that has logged off attempts to establish its main or backup connection again without propagating its priority first. If the main connection was successfully established, the backup event is terminated and the router returns to propagating its main priority. If only the backup connection was established, then the router falls back into the normal backup event and begins propagating its backup priority again.

As soon as a device can reestablish its main connection, the router begins propagating with its main priority again and becomes the master:

- Devices that are in backup mode with a lower main priority than the active master can also leave backup mode and propagate their main priority due to the fact that their backup connection is not required in this state.
- Devices that are in backup mode with a higher main priority than the active master can remain in backup mode as long as they are not able to establish their higher-prioritized main connection.
- Devices that have completely logged out of the VRRP group due to the unavailability of a VRRP remote site over the backup connection return to the normal backup mode.

Connection establishment

In order to allow coordinated connection establishment and prevent standby routers from attempting to establish connections, connections from a router are only established when this router:

- is the master **or**
- it is in backup mode and its main connection is configured with a keep alive **or**
- it has completely logged off and the timer for the renewed connection attempt (reconnect delay) expires

This simple rule allows the main connection to be configured as a keep alive connection even in standby routers. It also makes it possible only to use connections with hold time even in the main router.

Connections are always established when all virtual routers connected to the remote site have switched to standby mode. This either happens because another router propagates a higher priority or a LAN connection is lost.

14.2.3 Application scenarios

VRRP is normally employed for two different uses:

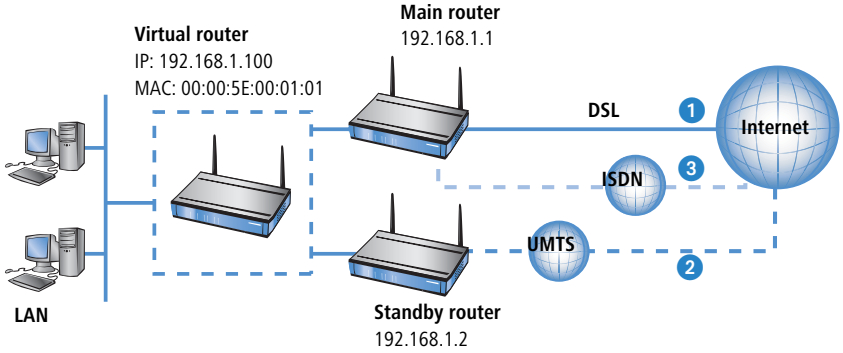
- In the simple backup case with two routers, one device under normal operation establishes the connection to the Internet. The second device is only operated in wait mode as a "standby device" and takes over the function of the main router should it fail.
- In the second case, two or more devices function parallel to each other as routers in the same network and distribute the incoming data connections using static load balancing. If one of these devices fails, the other router in the group can take over the failed device's functions.

Backup solution with VRRP

Possibly the most important application of VRRP is the provision of backup connections in which one or more routers serve as backup for the main router. These routers can use different physical media for the Internet connection, such as DSL in the main router and UMTS or ISDN in the backup routers. A normal backup chain thus resembles the following:

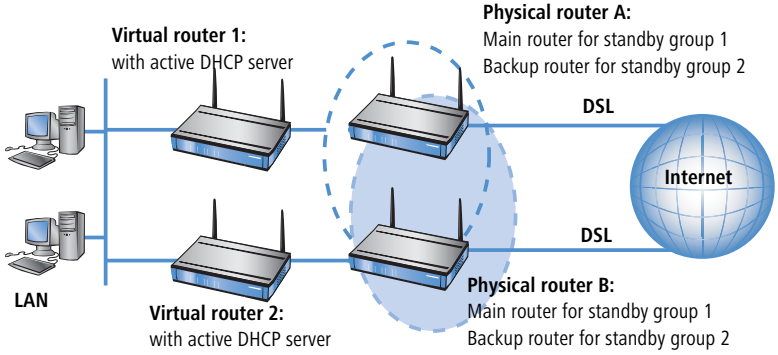
- If the DSL connection fails (1), the UMTS router takes over (2) the function.
- If the UMTS connection fails (2), the ISDN router takes over (3) the function.

Since almost all LANCOM devices with a DSL interface also have an ISDN interface, the main router can also take over ISDN backup functions at the end of the backup chain—as long as the hardware does not fail completely.



Load Balancing

With load balancing, several routers exist which can accomplish the same tasks. These routers are pronounced to be the default gateway and evenly distributed among the computers in the LAN using the DHCP server active in every router (see also 'Address assignment via DHCP with more than one DHCP server in the LAN' → page 504). If one of the routers fails, then another can take over its functions providing both routers work with VRRP. On every router, as many virtual routers are defined as there are actual routers. The computers in the LAN are assigned one of the virtual routers as a gateway. Using the virtual router priorities, it is now defined in which order the other routers take over when a master fails. It is also possible to establish a backup chain using the main and backup priority here.



Example application: Secure Internet access via two DSL/ISDN combination routers

Two load-balancing default gateways that provide security for one another are to be the basis for operating the LAN at two DSL lines. On average, 50% of the LAN stations log in to router 1 and 50% to router 2. The failure of a router or the non-availability of a DSL connection is compensated for by the other router, which the takes over the full load.

Under normal operational circumstances, each router handles on average 50% of users in the LAN (prio 250 for the DSL connection). Should a router or DSL connection fail, then the load is distributed to the other router (prio 100 for the DSL connection of the backup router). If both DSL connections fail, then the traffic is directed over the ISDN connections (each with backup prio 50, ISDN connections not illustrated).

Notes for the configuration of the virtual router

Router A			Router B	
	DHCP= On (10.1.1.x)			DHCP= On (10.1.1.x)
Router ID = 1	Router IP = 10.1.1.1		Router ID=1	Router IP=10.1.1.1
	Prio = 250			Prio = 100
	Backup prio=50			Backup prio=50
	Remote station = DSL-INTERNET			Remote station = DSL-INTERNET
	Comment: Main router for group 1			Comment: Backup router for group 1
Router ID = 2	Router IP = 10.1.1.2		Router ID=2	Router IP=10.1.1.2
	Prio = 100			Prio = 250
	Backup prio=50			Backup prio=50
	Remote station = DSL-INTERNET			Remote station = DSL-INTERNET
	Comment: Backup router for group 2			Comment: Main router for group 2

14.2.4 Interaction with internal services

When using VRRP virtual routers with virtual IP and MAC addresses are used which, in turn, influences the internal services of LANCOM devices. They must behave differently depending on whether a virtual router or a physical router is addressed. Depending on the service or protocol used, the answers to address requests must be changed or completely denied.

ARP

The most important protocol when dealing with virtual routers is ARP (Address Resolution Protocol), which provides the ability to match logical addresses such as IP addresses to hardware addresses such as MAC addresses. The use of virtual and physical IP and MAC addresses means that the router's reaction to ARP requests is of great importance:

- An ARP request to the virtual router's address may only be answered when the LANCOM is the master. This request must be answered with the corresponding virtual MAC address. All other requests must be ignored.
- ARP requests that list a virtual router's address as the sender address must be ignored.
- When using proxy ARP, an ARP request must be checked in order to determine if a virtual router is associated with the remote station through which the requested address can be reached. If so, then the request may only be answered when the LANCOM is the master. This also applies to virtual remote stations (i.e. PPTP or VPN) when they use a remote station that is associated with a virtual router as a physical connection.
- ARP requests sent by the LANCOM itself are always sent with the real sender address, as long as this is not the address of a virtual router. In this event, the virtual MAC address must be entered in the ARP request.

ICMP

When using ICMP, echo requests and replies should be differentiated from error messages. For the error messages, ICMP redirect will require and additional inspection.

- An ICMP echo request directed to the virtual router's address may only be answered by the LANCOM when it is the master.
- ICMP redirects may also be sent from virtual routers but the address of the router to which the packet was sent must be entered as the sender address. This is to be determined from the packet's target MAC address.
- If the LANCOM is addressed via its physical MAC address and the target of the packet is linked to a virtual router, the address of which is connected to the receiving interface, then an ICMP redirect is returned and the sender receives the address of the virtual router.
- For all other error messages, it does not matter whether the virtual router's address or the real address is used as the sender address. To simplify matters, the real address is always used.

With the implementation of VRRP in LANCOM, the previous option 'local routing' in the IP Router menu has been replaced with 'Send ICMP redirects'. If this option is enabled, ICMP redirects are sent, if the option is disabled, the packets are always forwarded.

DHCP

- Gateway address

  Although the computers in the LAN can use ICMP redirects to learn which router is the correct virtual router, it is still advisable to designate the correct router as gateway directly during the DHCP negotiation. This allows the assigning gateway address to be determined as follows:

  - If a gateway is explicitly defined for the interface in the DHCP module, then only this will be assigned.
  - If no explicit gateway is set, then the default route is looked up in the routing table. If the default route exists and is connected to a virtual router which is directly linked to the interface through which the DHCP request is received, then the virtual router's address is assigned as gateway.
  - If other remote sites are linked to virtual routers, then these will not be assigned via DHCP since there can only be one default gateway. A host can only learn the corresponding routers via ICMP redirects.

□ Otherwise, the address corresponding to the address pool or interface (intranet or DMZ) will be assigned.

If more than one virtual router is connected by the default route, then the address of the router with the highest priority will be assigned. This allows for automatic load balancing ('Load Balancing' → page 510) through the selection of the DHCP server by the respective client. The DHCP server is to be activated on all routers involved in load balancing. All routers then define many virtual routers, each with different priorities. If the client randomly selects a DHCP server from those that answer, then it will also be randomly assigned a virtual router.

Example with two routers

LANCOM A defines the following virtual routers:

Router ID	Virt. address	Prio	B Prio	Peer
1	10.0.0.1	100	50	INTERNET
2	10.0.0.2	60	50	INTERNET

and, correspondingly LANCOM B:

Router ID	Virt. address	Prio	B Prio	Peer
1	10.0.0.1	60	30	INTERNET
2	10.0.0.2	100	30	INTERNET

Depending on whether it chooses LANCOM A or LANCOM B, a DHCP client will now be assigned 10.0.0.1 or 10.0.0.2 as gateway and is initially distributed on both LANCOM devices.

Using this example, it becomes clear how load balancing can be combined with backup. If LANCOM A falls into backup mode, then LANCOM B will become the master for all clients. If LANCOM B fails, then LANCOM A will become the master for all clients and will attempt to establish its backup. If this fails, then it is LANCOM B's turn again (this signals the end of the backup chain).

■ Further addresses

If the DHCP server is to assign explicit addresses for certain services which the LANCOM provides, such as DNS and NBNS server, then either the configured addresses or the real addresses are assigned to the respective interfaces. Assigning a virtual router violates the RFC which prohibits a virtual router from offering other services (a device may only react to a virtual address when it is also the "owner" of this address, i.e. when the address is also the real interface address. At the same time, this means that DNS and NBNS must receive special treatment.

DNS server

Since the RFC prohibits a virtual router from offering additional services when the physical router is not the "owner" of the virtual IP address, the LANCOM DNS server requires special treatment. The LANCOM offers two options.

- The solution which conforms to the RFC works in the DNS forwarder. If an external IP address is entered as primary or secondary DNS server, then forwarding to the responsible virtual router functions automatically using the ICMP redirect treatment since the packet is simply forwarded to the virtual router.

  However, if no address is entered and no connection has been made to the remote station to which the packet should be forwarded, then the DNS forwarder checks to see if a virtual router is connected to the remote station.

  - If this is the case and the LANCOM is also the master for one of the virtual routers, then the connection is established and the packet is forwarded to the DNS server assigned to this connection.
  - If the LANCOM is not the master for all connected routers, then the packet is forwarded to the master of the first connected router.

This procedure only works when all routers behave in accordance with the RFC and use port forwarding. If all of the routers involved are LANCOM devices, then this requirement is fulfilled.

- With the second option, a virtual router reacts to DNS requests itself.
  - In order to enable this behavior, the option 'Internal Services' must be enabled. The LANCOM accepts the requests to the internal services (here, for example, DNS) via the virtual addresses as if it had been addressed through one of the physical addresses.
  - In the default setting (Off) the LANCOM behaves in accordance with the RFC and drops the corresponding packets.
  - The default setting is 'On'.

  If a virtual router is connected to the default route when using the internal services, then this will be assigned by the LANCOM DHCP server as the DNS server. If more than one virtual router is connected by the default route, then the router with the highest priority will be assigned (as is the case with gateway addresses).

This option can only guarantee trouble-free operation if all of the routers involved are LANCOM devices.

NBNS/NetBIOS proxy

Since a NetBIOS proxy does not forward packets, the question of the virtual or physical addresses responded to is of no significance here. However, it is important that all routers and backup routers in the VRRP group can store the same host, group and server addresses learned from the remote site in their own database and propagate these upon connection establishment. This is the only method of ensuring that an NBNS request can be answered in every case.

Since the NetBIOS proxy propagates all host, group and server addresses learned from the remote site, it need only be ensured that this information is also recorded by the backup routers in their databases. Under normal circumstances, however, this is prevented by the route verification.

Since the transfer of addresses is usually prevented by the route verification, the addresses are only accepted in VRRP operation when **all** of the following requirements are fulfilled:

- There is a WAN route to the propagated address.

- The corresponding remote site is connected to a virtual router.
- The corresponding address is propagated by the master of this virtual router.
- The switch 'Internal Services' is activated.

Only when all of these requirements are fulfilled, will the respective address be accepted in the database. This ensures that the individual router databases remain consistent and all addresses are immediately recognized when a backup router becomes master.

The position of the 'Internal Services' switch influences the NetBIOS proxy.

- When it is enabled, the NetBIOS proxy accepts NBNS requests that are directed to virtual routers.
- If a virtual router is also connected to the default route, then this will be assigned by the LANCOM DHCP server as the NBNS server.
- If more than one virtual router is connected by the default route, then the router with the highest priority will be assigned (as is the case with gateway addresses).

RIP

The use of VRRP has a particularly strong influence on RIP, through which information on the accessible routes and the corresponding routers is propagated.

- On the one hand, routers must be made known in the network to remote stations which can be reached through a virtual router.
- On the other hand, the routes that are propagated by the virtual routers themselves must be ignored.
- Ultimately, the propagated information is dependent upon the interface which it is to be passed on to.

The announcement of routing information via RIP is governed by the following rules:

- Routes are propagated on all virtual and physical interfaces and every virtual router counts as its own virtual interface.
- If routes are currently being propagated on a physical interface (LAN/DMZ) and a route that must be propagated is connected to a virtual router, then two cases must be differentiated:
  - When the virtual router is active on the interface, i.e. its address is in the address range of the respective interface, then the route will not be propagated.
  - If the virtual router on the interface is not active, then the route will be propagated normally, i.e. the physical interface address will be propagated as the best route.
- If routes are propagated on a virtual router, then only the routes that are connected to this virtual router may be propagated.
- If routes are propagated on a WAN interface, then all routes are propagated.
- Upon receiving a RIP packet, the sender address of the RIP packet must be taken into consideration. The routes contained in the packet must be ignored when they are propagated by a virtual router known by the LANCOM device.
- If the LANCOM cannot establish a connection to the remote site because all channels are occupied, then RIP propagates the routes accessible through this remote site as "unavailable".

- □ In addition, the VRRP module is notified in this case so that it can log off of the router connected to this remote site allowing a new master to be determined.
- □ Similarly, VRRP receives notification when the connection is can be re-established in order to allow the virtual router to propagate with its main or backup priority again.

NTP

When the 'Internal Services' switch is enabled, then the LANCOM also accepts (S)NTP requests that are directed to virtual routers since the exact address of the time source is not relevant for an NTP client.

Other services

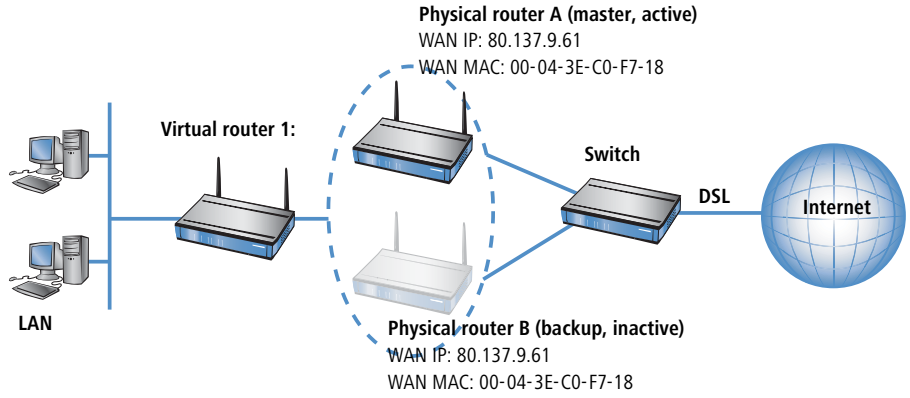
The LANCOM only processes other services when it is addressed via its physical address.

14.2.5 VRRP in the WAN

The description of VRRP is only in regard to the LAN portion of data networks and leaves the regulation of the WAN portion to dynamic routing protocols such as RIP. In order to enable WAN failover all the same, LANCOM VRRP provides two alternatives.

Same IP and MAC addresses

The first possibility entails assigning all of the routers in the VRRP group on the WAN side the same MAC and the same IP address. The routers are then connected to a commonly used DSL line, for example by a switch. In order to avoid address conflicts, only one router may actually react to these addresses on its WAN side, which is achieved through the use of VRRP.



- ■ Due to the fact that the LANCOM terminates its WAN connection when the last virtual router switches to backup mode, this requirement is definitely fulfilled when a total of only one virtual router has been defined.

- In the backup scenario, the necessary requirement is also fulfilled because the main connection is guaranteed to have been terminated or else the backup router would not have become master.

Routing protocols

In the load balancing scenario, however, there are two different WAN connections online simultaneously, which is why the use of the same MAC and IP address is not possible here. In this case, a routing protocol such as RIP, OSPF or BGP must be used as a second option.

In order to accelerate the switch using RIP, which is rather slow, a LANCOM propagates to all networks that it is no longer available before the connection is established, thereby ensuring a quick change of routing priorities.

14.2.6 Configuration

In order to configure failover or load balancing with VRRP, the following parameters can be set:

- **Activation**: The switch 'VRRP activate' enables the VRRP module to be switched on or off (default = off).
- **VRRP list**: In the VRRP list, up to 16 virtual routers can be defined. This table has the following fields:
  - **Router ID**: Unique ID for the virtual router. Values between 1 and 255 are possible. The router ID is used to consolidate several physical routers into a single virtual router or a standby group ('Router ID defines "standby groups"' → page 505).
  - **Router IP**: IP address for the virtual router.

All routers on which the virtual router is set up must assign this router the same IP address.

  - **Main priority**: The main priority of the virtual router with regard to routers with several interfaces refers to the main interface, i.e. with routers with DSL and ISDN support to the DSL interface. Values between 0 and 255 are permitted. The values 0 and 255 have special meanings:

    '0' turns the virtual router off.
  - '255' is only accepted when the virtual router address is identical to the address of the interface that is connected to the router. In other cases, the priority is automatically lowered.
  - **Backup priority**: The backup priority of the virtual router refers to the interface for which a backup connection is configured, i.e. with routers with DSL and ISDN support to the ISDN interface. Here again, values between 0 and 255 are permitted. The values 0 and 255 also have special meanings here:

    0 disables the virtual router in the backup event. Checks are conducted regularly in order to determine whether or not the standard connection can be reestablished. The inspection interval is defined in the reconnect delay.

    '255' is only accepted when the virtual router address is identical to the address of the interface that is connected to the router. In other cases, the priority is automatically lowered.

  When the backup connection cannot be established in backup mode, then the virtual router logs off completely and attempts to reestablish the standard or backup connection in intervals defined by the reconnect delay.

- **Remote site**: Name of the remote station that controls the virtual router behavior. The remote site can also be assigned to other virtual routers.

Entering the remote site is optional. Linking the backup requirement to a remote site allows the use of the LANCOM-specific enhancement to VRRP not only to secure against device failure (VRRP standard) but also against interface failure or disruption at a remote site.

- **Comment**: 64 character-long commentary describing the virtual router.

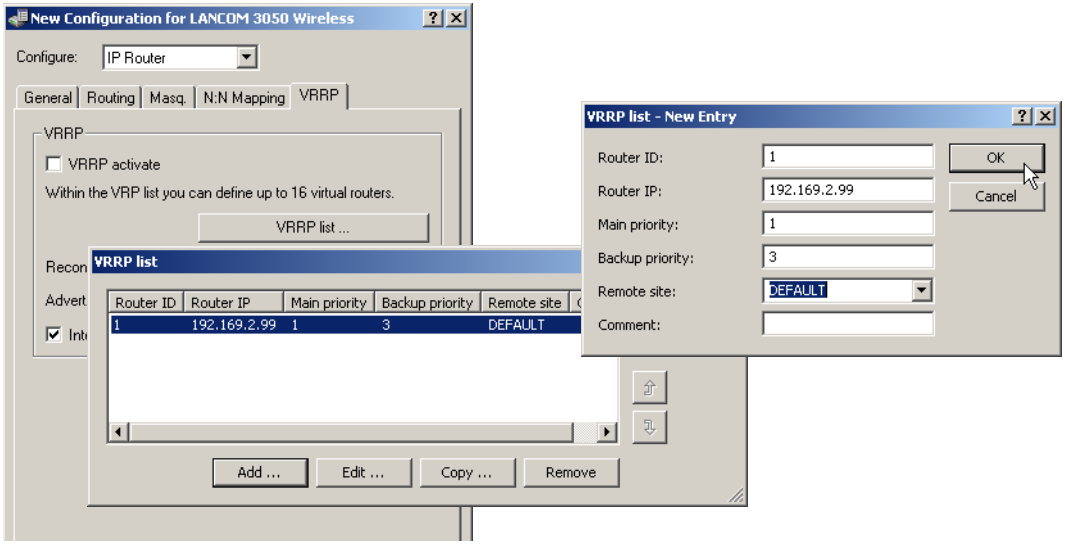
- **Reconnect delay**: The reconnect delay time shows after how many minutes a virtual router that has logged off attempts to reestablish its standard connection. The router remains logged off during this connection attempt. It is only broadcasted with its main or backup priority after the connection has been established successfully. The default value is 30 minutes.
- **Advert. interval**: The advertising interval shows how many seconds until a virtual router is propagated again. The default value is 1 second.

With a propagation time of 1 second, the routers in the VRRP group can change quickly when a device or interface fails. An interruption of this type will usually remain undetected due to the fact that the TCP connection is not interrupted. Other routing protocols require up to 5 minutes or longer in order to conduct the transfer to a backup router.

- **Internal services**: The Internal services check box controls how the device should behave when it is addressed via a virtual router address.
  - In the 'On' position, the LANCOM reacts to certain services exactly as if it had been addressed via its actual address. Naturally, this only occurs when the device itself is the master of the virtual router. The behavior of the DHCP server changes simultaneously ('Interaction with internal services' → page 511).
  - The default setting 'Off' results in behavior in accordance with the RFC, meaning means that the corresponding packets are silently dropped.
  - The default setting is 'On'.

Configuration with LANconfig

The settings for VRRP can be found in the LANconfig in the configuration area 'IP router' on the 'VRRP' tab.



Configuration with WEBconfig, Telnet or SSH

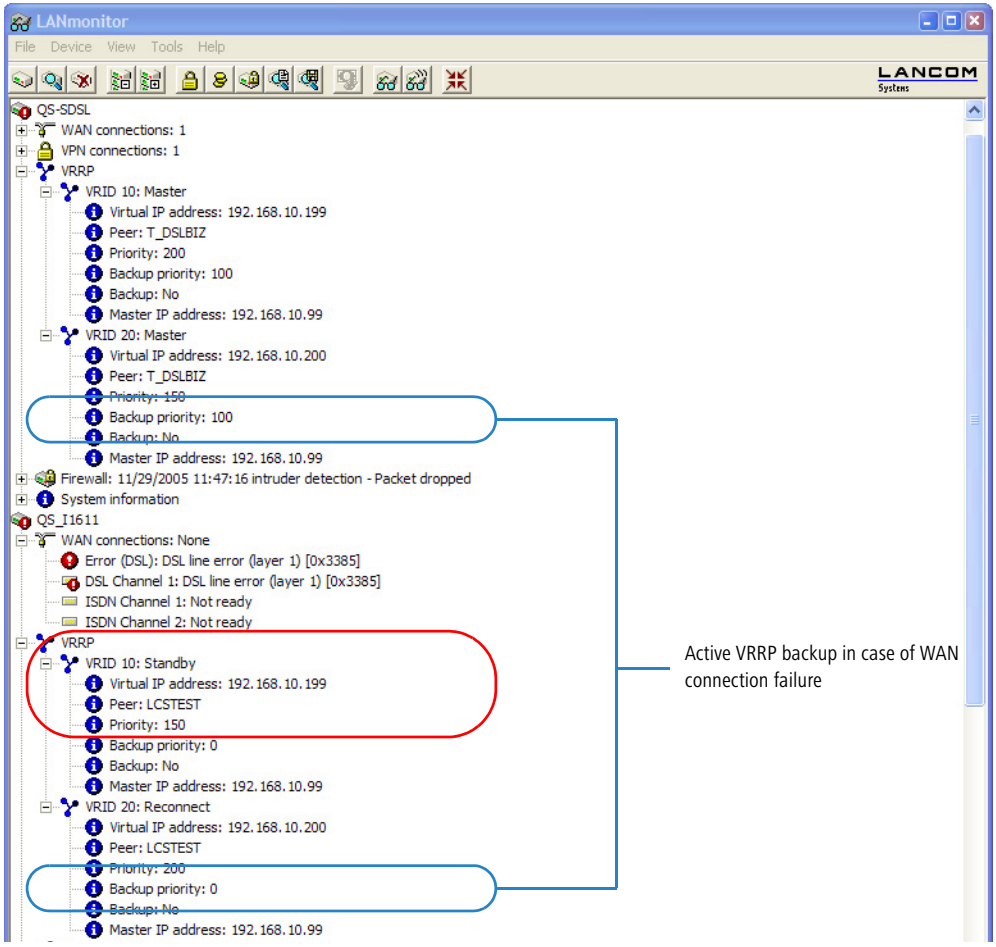
Under WEBconfig, Telnet or SSH client you will find the settings for VRRP under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert Configuration ▶ Setup ▶ IP router ▶ VRRP
Terminal/Telnet	`Setup/IP-router/VRRP`

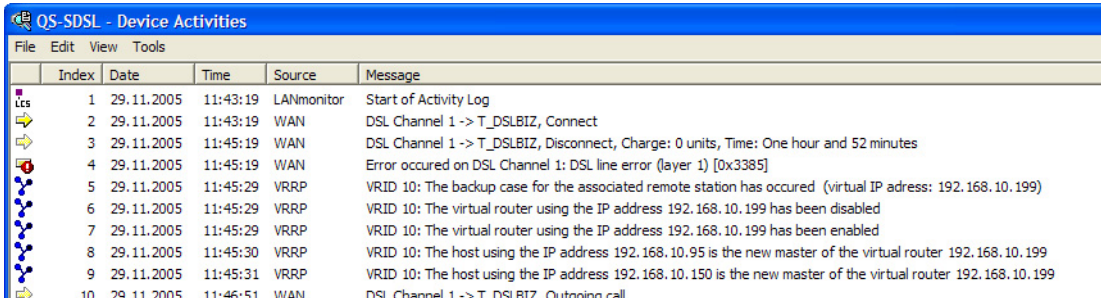
14.2.7 Status Information

Status request with LANmonitor

The current status of the devices in the VRRP group is showed in LANmonitor as long as the VRRP module is activated:



In the device activity log, VRRP events can be viewed in chronological order.



	Index	Date	Time	Source	Message
LCS	1	29.11.2005	11:43:19	LANmonitor	Start of Activity Log
	2	29.11.2005	11:43:19	WAN	DSL Channel 1 -> T_DSLBIZ, Connect
	3	29.11.2005	11:45:19	WAN	DSL Channel 1 -> T_DSLBIZ, Disconnect, Charge: 0 units, Time: One hour and 52 minutes
	4	29.11.2005	11:45:19	WAN	Error occured on DSL Channel 1: DSL line error (layer 1) [0x3385]
	5	29.11.2005	11:45:29	VRRP	VRID 10: The backup case for the associated remote station has occured (virtual IP adress: 192.168.10.199)
	6	29.11.2005	11:45:29	VRRP	VRID 10: The virtual router using the IP address 192.168.10.199 has been disabled
	7	29.11.2005	11:45:29	VRRP	VRID 10: The virtual router using the IP address 192.168.10.199 has been enabled
	8	29.11.2005	11:45:30	VRRP	VRID 10: The host using the IP address 192.168.10.95 is the new master of the virtual router 192.168.10.199
	9	29.11.2005	11:45:31	VRRP	VRID 10: The host using the IP address 192.168.10.150 is the new master of the virtual router 192.168.10.199
	10	29.11.2005	11:46:51	WAN	DSL Channel 1 -> T_DSLBIZ, Outgoing call

Status request with WEBconfig, Telnet or SSH

Status information on VRRP can be found in the IP router's status menu and offers the following entries:

- The values Rx and Tx count the VRRP packets received or sent, respectively.
- Error counts all fatal protocol errors that are logged.
- Drop counts all VRRP packets that are dropped, e.g. when a serious error occurred.

In the Virtual Router table, all active virtual routers are listed with their current status. This table has the following fields:

- **Router ID**: Unique ID for the virtual router.
- **Virt. address**: IP address for the virtual router.
- **Prio**: Main priority for the virtual router.
- **B-Prio**: Backup priority for the virtual router.
- **Remote site**: Name of the remote station that controls the virtual router behavior.
- **State**: State of the virtual router. The following states are possible:
  - Init: The router is currently being set up.
  - Listen: The router is currently learning which device is the master.
  - Standby: The router is the standby router.
  - Master: The router is the master.
  - Down: The router is deactivated.
  - Reconnect: The reconnect timer is running and the router is currently not propagating itself.
- **Backup**: Shows if the remote station (peer) is in backup or not. If the remote station is in backup, then the device will propagate its backup priority, otherwise it will propagate its main priority.
- **Master**: Shows which of the physical routers is currently the master.

The MAC list table displays the MAC addresses for the virtual routers that are currently masters. This table has the following fields:

- **Virt. address**: IP address for the virtual router.
- **MAC address**: MAC address for the virtual router.
- **Router ID**: Unique ID for the virtual router.

15 Office communications with LANCAPI

This section only applies to devices with ISDN interface.

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.

15.1 What are the advantages of LANCAPI?

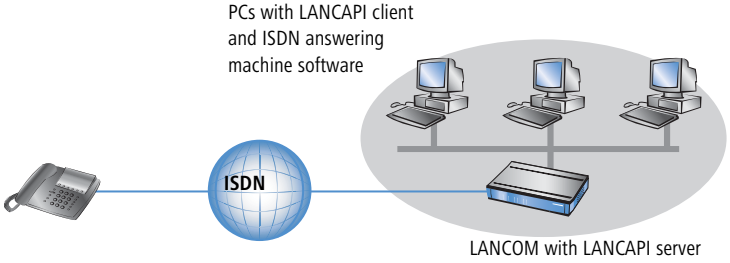
The main advantages of using LANCAPI are economic. LANCAPI provides all Windows workstations integrated in the LAN (local-area network) with unlimited access to office communications functions such as fax machines, answering machines, online banking and eurofile transfer. All functions are supplied via 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.

For example, faxes are sent by simulating a fax machine at the workstation. With LANCAPI, the PC forwards the fax via the network to the router which establishes the connection to the recipient.

Please note: All LANCAPI-based applications access the ISDN directly and do not run across the router of the device. The connect-charge monitoring and firewall functions are thus disabled! The LANCAPI is also independent from all routing or VPN functions.

15.2 The client and server principle

The LANCAPI is made up of two components, a server (in the LANCOM) and a client (on the PCs). The LANCAPI client must be installed on all computers in the LAN that will be using the LANCAPI functions.



15.2.1 Configuring the LANCAPI server

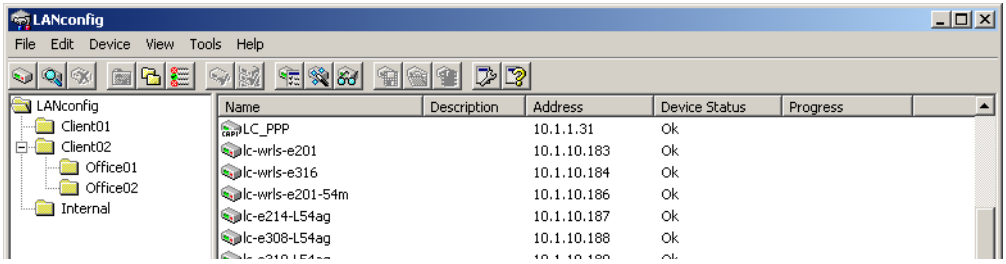
Two basic issues are important when configuring the LANCAPI server:

- What call numbers from the telephone network should LANCAPI respond to?
- Which of the computers in the local network should be able to access the telephone network via LANCAPI?

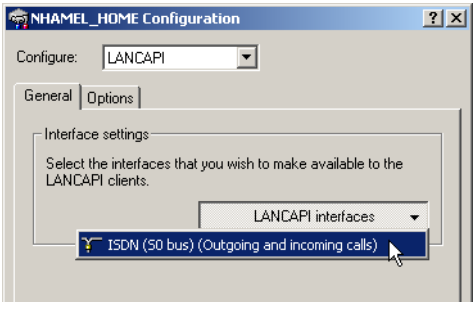
The configuration of the router takes place in the configuration tables of LANconfig or WEBconfig. In the following two sections you can find the instructions for both of these configuration programs.

Configuration with LANconfig

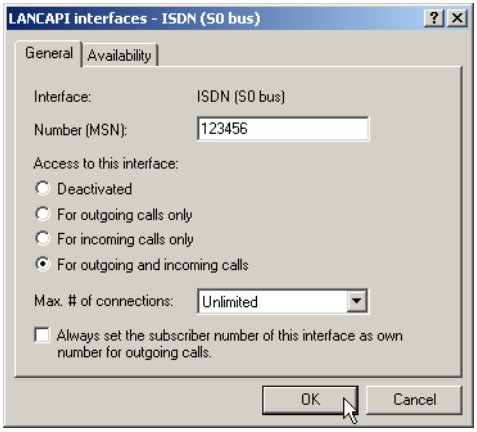
① Open the configuration of the router by double-clicking on the device name in the list and enter your password if requested.



② In the configuration area 'LANCAPI' click on the tab 'General' and select at the **LANCAPI interfaces** the ISDN port you want to set.



③ Activate the LANCAPI server for the outgoing and incoming calls, or allow only outgoing calls.



If the LANCAPI server is supposed to respond to incoming calls, enter the call numbers to which the LANCAPI should respond in the 'Number (MSN)' field. You can enter several call numbers separated by semicolons. If you do not enter a call number here, all incoming calls are reported to LANCAPI.

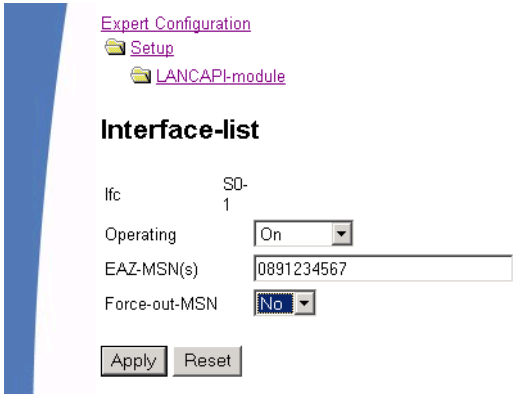
Configuration of WEBconfig

① Select in the main menu the **Expert Configuration**.

② Select in the following menus **Setup** ▶ **LANCAPI-module** ▶ **Interface-list**.

③ Select in the **Interface-list** the (only) entry **S0-1**.

④ Activate the LANCAPI server for outgoing and incoming calls ('On'), or only allow outgoing calls ('Dail-only').



If the LANCAPI server is supposed to respond to incoming calls, enter the call numbers to which the LANCAPI should respond in the 'Number (MSN)' field. You can enter several call numbers separated by semicolons. If you do not enter a call number here, all incoming calls are reported to LANCAPI.

15.2.2 Installing the LANCAPI client

For the installation of the LANCAPI client on a system with Windows XP or Windows 2000 administrator rights are required.

① Place the LANCOM CD in your CD-ROM drive. If the setup program does not automatically start when you insert the CD, simply click 'autorun.exe' in the main directory of the LANCOM CD in the Windows Explorer.

② Select the Install LANCOM software entry.

③ Highlight the **LANCAPI** option. Click **Next** and follow the instructions for the installation routine.

If necessary, the system is restarted and LANCAPI is then ready to accept all jobs from the office communications software. After successful installation, an icon for LANCAPI will be available in the toolbar. A double-click on this icon opens a status window that permits current information on the LANCAPI to be displayed at any time.

The LANCAPI client starts automatically and shows the status in the windows task bar.

15.2.3 Configuration of the LANCAPI clients

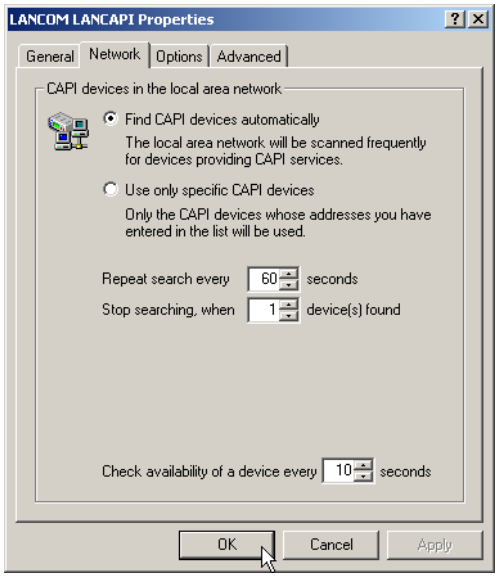
The configuration of the LANCAPI clients is used to determine which LANCAPI servers will be used and how these will be checked. All parameters can remain at their default settings if you are using only one LANCOM in your LAN as an LANCAPI server.

① Start the LANCAPI client in the 'LANCOM' program group. Information regarding the drivers for the available service can be found on the 'General' tab.

② In the LANCAPI client, change to the **Network** tab. First, select whether the PC should find its own LANCAPI server, or specify the use of a particular server.

- For the former, determine the interval at which the client should search for a server. It will continue searching until it has found the number of servers specified in the next field. Once the required number of servers has been found, it will stop searching.
- In the event that the client should not automatically search for servers, list the IP addresses of the servers to be used by the client. This can be useful if you are operating several LANCOM in your LAN as LANCAPI servers and you would like to specify a server for a group of PCs, for example.

□ It is also possible to set the interval at which the client checks whether the found or listed servers are still active.



15.3 How to use the LANCAPI

Two options are available for the use of the LANCAPI:

- You may use software which interacts directly with a CAPI (in this case, the LANCAPI) port. This type of software searches for the CAPI during its installation and uses it automatically.
- Other programs such as LapLink can establish a variety of connection types, for example, using Windows Dial-Up Networking. You may select the installed communications device that you would like to use when creating a new dial-up connection. For the LANCAPI, select the entry 'ISDN WAN Line 1'.

15.4 The LANCOM Systems CAPI Faxmodem

The CAPI Faxmodem provides a Windows fax driver (Fax Class 1) as an interface between the LANCAPI and applications, permitting the use of standard fax programs with an LANCOM. The LANCOM CAPI Faxmodem emulates the modem functions, as well as the fax protocols in the software on the PC. For this purpose an adequate performance (500 MHz Pentium and more) is required.

Installation

The CAPI Faxmodem can be installed from the CD setup. Always install the CAPI Faxmodem together with the current version of LANCAPI. After restarting, the CAPI Faxmodem will be available for you, e.g. in Windows 98 under **Start ▶ Settings ▶ Control Panel ▶ Modems**.

Faxing with the CAPI Faxmodem

Most major fax programs recognize the CAPI Faxmodem automatically during installation and identify it as a 'Class 1' fax modem. Fax transmissions can thus be realized at speeds of up to 14,400 bps. If your fax program offers you a choice (such as WinFax and Talkworks Pro), select the option 'CLASS 1 (Software Flow Control)' when setting up the modem.

Faxing under Windows XP and Windows 2000

Windows XP or Windows 2000 provide with the CAPI Faxmodem full functionality for faxing. An additional fax program is not required.

Thereto start in the Control Panel under “Add or Remove Programs”, “Add/Remove Windows Components” and select “Fax Services”.

After the installation the fax can be found under “Printers and Faxes”, and can be chosen in any Windows program instead of a printer.

The CAPI Faxmodemis only able to transmit fax messages, if the LANCAPI ist active.

15.5 LANCOM Faxmodem option

Additionally to the CAPI Faxmodem some LANCOM models (LANCOM 800, 4000, 4100) have a faxmodem option. With this solution the fax and modem services are implemented in the LANCOM itself, the PCs are released from the load of the modem emulation.

15.6 Provided B channel protocols

Following CAPI-Protocols are provided

Value		Remark
B1 protocol		
	0	64 Kbps with HDLC framing
	1	64 Kbps transparent with byte framing of the network
	2	V.110 asynchron with start-stop-byte framing
	4*	T.30-Modem for fax group 3

Value		Remark
	7*	Modem with full negotiations (B2 has to be 7)
B2-Protocol		
	0	ISO 7776 (X.75 SLP)
	1	Transparent
	4*	T.30 for fax group 3
	7*	Modem with full negotiations (e.g. V.42 bis, MNP 5)
	9	V.120 asynchron
B3-Protocol		
	0	Transparent
	1	T.90NL, compatible with T.70NL in accordance with T.90, Appendix II
	2	ISO 8208 (X.25 DTE-DTE)
	4*	T.30 for fax group 3
	5*	T.30 for fax group 3 extended
	7*	Modem

* = valid only for LANCOM faxmodem option

16 More services

An LANCOM offers a number of services for the PCs in the LAN. These are central functions that can be used by workstation computers. They are in particular:

- Automatic address administration with DHCP
- Name management of computers and networks with DNS
- Logging of network traffic with SYSLOG
- Recording of charges
- Office communications functions with LANCAPI
- Time server

16.1 Automatic IP address administration with DHCP

In order to operate smoothly in a TCP/IP network, all the devices in a local network must have unique IP addresses.

They also need the addresses of DNS-servers and NBNS-servers as well as that of a default gateway through which the data packets are to be routed from addresses that are not available locally.

In a smaller network, it is still conceivable that these addresses could be entered manually in all the computers in the network. In a larger network with many workstation computers, however, this would simply be too enormous of a task.

In such situations, the DHCP (Dynamic Host Configuration Protocol) is the ideal solution. Using this protocol, a DHCP server in a TCP/IP-based LAN can dynamically assign the necessary addresses to the individual stations.

The LANCOM devices have a build in DHCP server, which assigns the IP addresses in the LAN. If a DHCP server already exists in the local network, the device in DHCP client mode can alternatively get the required address information from the other DHCP server.

16.1.1 The DHCP server

As a DHCP server, the LANCOM can administer the IP addresses in its TCP/IP network. In doing so, it passes the following parameters to the workstation computers:

- IP-address
- network mask
- broadcast address
- standard gateway
- DNS server
- NBNS server
- period of validity for the parameters assigned

The DHCP server takes the IP addresses either from a freely defined address pool or determines the addresses automatically from its own IP address (or intranet address).

In DHCP mode, a completely unconfigured device can even automatically assign IP addresses to itself and the computers in the network.

In the simplest case, all that is required is to connect the new device to a network without other DHCP servers and switch it on. The DHCP server then interacts with LANconfig using a wizard and handles all of the address assignments in the local network itself.

16.1.2 DHCP—'on', 'off', 'auto', 'client' or 'forwarding'?

The DHCP server can be set to five different states:

- 'on': The DHCP server is permanently active. The configuration of the server (validity of the address pool) is checked when this value is entered.
  - When correctly configured, the device will be available to the network as a DHCP server.
  - In the event of an incorrect configuration (e.g. invalid pool limits), the DHCP server is disabled and switches to the 'off' state.

Only use this setting if assured, that no further DHCP server is active in the LAN.

- 'off': The DHCP server is permanently disabled.
- 'auto': In this mode, after switching it on, the device automatically looks for other DHCP servers within the local network. This search can be recognized by the LAN-Rx/Tx LED flashing.
  - If at least on other DHCP server is found, the device switches it's own DHCP server off, changes to the DHCP client mode, and obtains the IP address from the DHCP server in the LAN. This prevents the unconfigured device from assigning addresses not in the local network when switched on.
  - The device then enables its own DHCP server if no other DHCP servers are found. If at a later point of time a further DHCP server is switched on in the LAN, the device automatically changes back into the DHCP client mode.
- 'client': The DHCP server is switched off, the device acts like a DHCP client and obtains the address information from a different DHCP server in the LAN.

Only use this setting if assured, that a further DHCP server is active in the LAN and takes over the assigned IP address information.

- 'forwarding': The DHCP server is active and the device accepts the requests from the DHCP clients in the local network. The device does not respond to these requests itself, but forwards them to a central DHCP server.

Whether the DHCP server is active or not can be seen in the DHCP statistics.

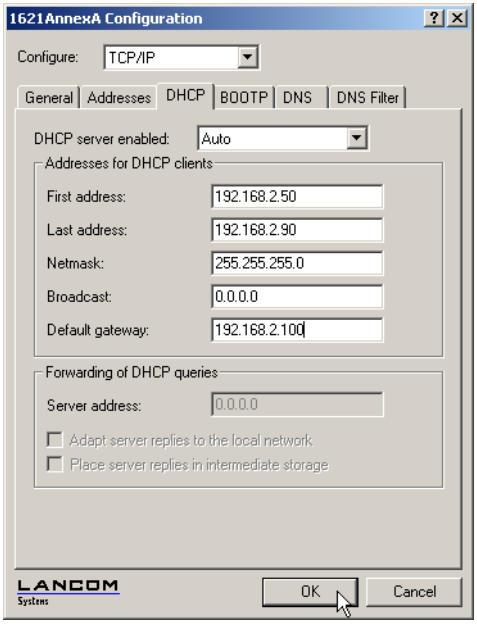
The default setting for this condition is 'auto'.

16.1.3 How are the addresses assigned?

IP address assignment

Before the DHCP server can assign IP addresses to the computers in the network, it first needs to know which addresses are available for assignment. Three options exist for determining the available selection of addresses:

- The IP address can be taken from the address pool selected (start address pool to end address pool). Any valid addresses in the local network can be entered here.



- If '0.0.0.0' is entered instead, the DHCP server automatically determines the particular addresses (start or end) from the IP or intranet address settings in the 'TCP-IP-module' using the following procedure:
  - If only the Intranet address or only the DMZ address is entered, the start or end of the pool is determined by means of the associated network mask.
  - If both addresses have been specified, the Intranet address has priority for determining the pool.

  From the address used (Intranet or DMZ address) and the associated network mask, the DHCP server determines the first and last possible IP address in the local network as a start or end address for the address pool.
- If the router has neither an Intranet address nor an DMZ address, the device has gone into a special operating mode. It then uses the IP address '172.23.56.254' for itself and the address pool '172.23.56.x' for the assignment of IP addresses in the network.

If only one computer in the network is started up that is requesting an IP address via DHCP with its network settings, a device with an activated DHCP module will offer this computer an address assignment. A valid address is taken from the pool as an IP address. If the computer was assigned an IP address at some point in the past, it requests this same address and the DHCP server attempts to reassign it this address if it has not already been assigned to another computer.

The DHCP server also checks whether the address selected is still available in the local network. As soon as the uniqueness of an address has been established, the requesting computer is assigned the address found.

Netmask assignment

The network mask is assigned in the same way as the address. If a network mask is entered in the DHCP module, this mask is used for the assignment. Otherwise, the network mask from the TCP/IP module is used. The order is the same as during the assignment of the addresses.

Broadcast address assignment

Normally, an address yielded from the valid IP addresses and the network mask is used for broadcast packets in the local network. In special cases, however (e.g. when using subnetworks for some of the workstation computers), it may be necessary to use a different broadcast address. In this case, the broadcast address to be used is entered in the DHCP module.

The default setting for the broadcast address should be changed by experienced network specialists only. Incorrect configuration of this section can result in the undesired establishment of connections subject to connect charges!

Standard gateway assignment

The device always assigns the requesting computer its own IP address as a gateway address.

If necessary, this assignment can be overwritten with the settings on the workstation computer.

DNS and NBNS assignment

This assignment is based on the associated entries in the 'TCP/IP-module'.

If no server is specified in the relevant fields, the router passes its own IP address as a DNS address. This address is determined as described under 'IP address assignment'. The router then uses DNS-forwarding (also see 'DNS-forwarding'), to resolve DNS or NBNS requests from the host.

Period of validity for an assignment

The addresses assigned to the computer are valid only for a limited period of time. Once this period of validity has expired, the computer can no longer use these addresses. In order for the computer to keep from constantly losing its addresses (above all its IP address), it applies for an extension ahead of time that it is generally sure to be granted. The computer loses its address only if it is switched off when the period of validity expires.

For each request, a host can ask for a specific period of validity. However, a DHCP server can also assign the host a period of validity that differs from what it requested. The DHCP module provides two settings for influencing the period of validity:

- Maximum lease time in minutes

  Here you can enter the maximum period of validity that the DHCP server assigns a host.

  If a host requests a validity that exceeds the maximum length, this will nevertheless be the maximum available validity!

  The default setting is 6000 minutes (approx. 4 days).

- Default lease time in minutes

  Here you can enter the period of validity that is assigned if the host makes no request. The default setting is 500 minutes (approx. 8 hours).

Precedence for the DHCP server—request assignment

In the default configuration, almost all the settings in the Windows network environment are selected in such a way that the necessary parameters are requested via DHCP. Check the settings by clicking **Start ▶ Settings ▶ Control Panel ▶ Network**. Select the **TCP/IP** entry for your network adapter and open **Properties**.

Check the various tabs for special entries, such as for the IP address or the standard gateway. If you would like all of the values to be assigned by the DHCP server, simply delete the corresponding entries.

On the 'WINS configuration' tab, the 'Use DHCP for WINS Resolution' option must also be selected if you want to use Windows networks over IP with name resolution using NBNS servers. In this case, the DHCP server must also have an NBNS entry.

Priority for computer—overwriting an assignment

If a computer uses parameters other than those assigned to it (e.g. a different default gateway), these parameters must be set directly on the workstation computer. The computer then ignores the corresponding parameters assigned to it by the DHCP server.

Under Windows 98, this is accomplished through the properties of the Network Neighborhood.

Click **Start / Settings / Control Panel / Network**. Select the 'TCP/IP' entry for your network adapter and open **Properties**.

You can now enter the desired values by selecting the various tabs.

Checking of IP addresses in the LAN

Configuration tool	Run/Table
WEBconfig	Expert Configuration Setup / DHCP Table-DHCP
Terminal/Telnet	`setup/DHCP/table-DHCP`

The DHCP table provides a list of the IP addresses in the LAN. This table contains the assigned or used IP address, the MAC address, the validity, the name of the computer (if available) and the type of address assignment.

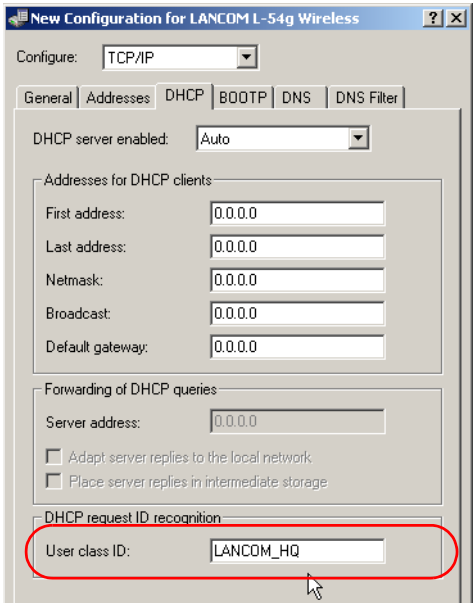
The 'Type' field specifies how the address was assigned. This field can assume the following values:

- 'new'
  The computer has made its initial request. The DHCP server verifies the uniqueness of the address that is to be assigned to the computer.
- 'unknown'
  While verifying uniqueness, it was determined that the address has already been assigned to another computer. Unfortunately, the DHCP server has no means of obtaining additional information on this computer.
- 'static'
  A computer has informed the DHCP server that it has a fixed IP address. This address can no longer be used.
- 'dynamic'
  The DHCP server assigned the computer an address.

16.2 Vendor Class and User Class Identifier on the DHCP Client

The DHCP client in LANCOM can insert additional information in the DHCP request sent, which simplify request recognition within the network.

- The vendor class identifier (DHCP option 60) shows the device type, e.g. 'LANCOM L-54'. The vendor class ID is always transmitted.
- The user class identifier (DHCP option 77) displays a user-defined string, which can be entered under `Setup/DHCP` or in LANconfig in the configuration area under 'TCP/IP' on the 'DHCP' tab in the 'User Class ID' field (default: empty). The user class ID is only transmitted when the user has configured a value.



16.3 DNS

The domain name service (DNS) is responsible in TCP/IP networks for associating computer names and/or network (domains) and IP addresses. This service is required for Internet communications, to return the correct IP address for a request such as 'www.lancom.de' for example. However, it's also useful to be able to clearly associate IP addresses to computer names within a local network or in a LAN interconnection.

16.3.1 What does a DNS server do?

The names used in DNS server requests are made up of several parts: one part consists of the actual name of the host or service to be addressed; another part specifies the domain. Specifying the domain is optional within a local network. These names could thus be 'www.domain.com' or 'ftp.domain.com', for example.

If there is no DNS server in the local network, all locally unknown names will be searched for using the default route. By using a DNS server, it's possible to immediately go to the correct remote station for all of the names with known IP addresses. In principle, the DNS server can be a separate computer in the network. However, the following reasons speak for locating the DNS server directly in the LANCOM:

- LANCOM can automatically distribute IP addresses for the computers in the local network when in DHCP server mode. In other words, the DHCP server already knows the names and IP addresses of all of the computers in its own network that were assigned IP addresses via DHCP. With the dynamic address assignments of a DHCP server, an external DNS server might have difficulties in keeping the associations between the names and IP addresses current.

- When routing Microsoft Networks via NetBIOS, the LANCOM also knows the computer names and IP addresses in the other connected NetBIOS networks. In addition, computers with fixed IP addresses can also enter themselves in the NetBIOS table and thus be known by their names and addresses.
- The DNS server in the LANCOM can also be used as an extremely convenient filter mechanism. Requests for domains can be prohibited throughout the LAN, for subnetworks, or even for individual computers—simply by specifying the domain name.

How does the DNS server react to the request?

When processing requests for specific names, the DNS server takes advantage of all of the information available to it:

- First, the DNS server checks whether access to the name is not prohibited by the filter list. If that is the case, an error message is returned to the requesting computer stating that access to the address has been denied.
- Next, it searches in its own static DNS table for suitable entries.
- If the address cannot be found in the DNS table, it searches the dynamic DHCP table. The use of DHCP information can be disabled if required.
- If no information on the name can be located in the previous tables, the DNS server then searches the lists of the NetBIOS module. The use of the NetBIOS information can also be disabled if necessary.
- Finally, the DNS server checks whether the request to another DNS server is to be forwarded to another DNS server via a WAN interface (special DNS forwarding via the DNS destination table).

If the requested name cannot be found in any of the information sources available to it, the DNS server sends the request to another server—that of the Internet provider, for example—using the general DNS forwarding mechanism, or returns an error message to the requesting computer.

16.3.2 DNS forwarding

If it cannot serve the request from its own DNS tables, the DNS server forwards the request to other DNS servers. This process is called DNS forwarding.

Here a distinction is made between

- special DNS forwarding
  Requests for certain name areas are forwarded to certain DNS servers.
- general DNS forwarding
  All other names not specified in detail are forwarded to the "higher-level" DNS server.

Special DNS forwarding

With "special DNS forwarding" name areas can be defined for the resolution of which specified DNS server are addressed.

A typical application for special DNS forwarding results for a home workstation: The user wants to be able to connect to the company intranet and directly to the Internet at the same time. The requests sent into the intranet must be routed to the company DNS server, and all other requests to the DNS server of the provider.

General DNS forwarding

All DNS requests that cannot be resolved in another way are forwarded to a DNS server. This DNS server is determined according to the following rules:

- Initially the router checks whether a DNS server has been entered in its own settings. If it is successful there, it obtains the desired information from this server. Up to two higher-level DNS servers can be specified.

LANconfig	TCP/IP ▶ Addresses ▶ Primary DNS / Secondary DNS
WEBconfig	Expert Configuration ▶ Setup ▶ TCP-IP ▶ DNS-default ▶ DNS-backup
Terminal/Telnet	`/setup/TCP-IP/DNS-default` `/setup/TCP-IP/DNS-backup`

- If no DNS server is entered in the router, it will attempt to reach a DNS server over a PPP connection (e.g. from the Internet provider) to get the IP address assigned to the name from there. This can only succeed if the address of a DNS server is sent to the router during PPP negotiation.
- The default route is established and the DNS server searched for there if no connection exists.

This procedure does not require you to have any knowledge of the DNS server address. Entering the Intranet address of your router as the DNS server for the workstation computers is sufficient to enable you obtain the name assignment. This procedure also automatically updates the address of the DNS server. Your local network always receives the most current information even if, for example, the provider sending the address changes the name of his DNS server or you change to another provider.

16.3.3 Setting up the DNS server

The settings for the DNS server are contained in the following menu or list:

Configuration tool	Run/Table
LANconfig	TCP/IP ▶ DNS
WEBconfig	Expert Configuration ▶ Setup ▶ DNS
Terminal/Telnet	`cd /setup/DNS`

Proceed as follows to set the DNS server:

① Switch the DNS server on.

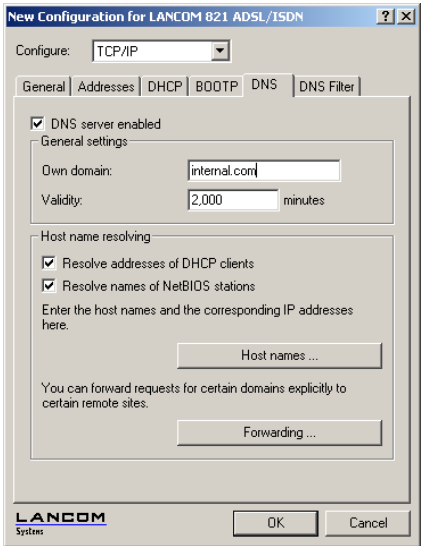
WEBconfig	… ▶ Operating
Terminal/Telnet	`set operating on`

② Enter the domain in which the DNS server is located. The DNS server uses this domain to determine whether the requested name is located in the LAN. Entering the domain is optional.

WEBconfig	… ▶ Domain
Terminal/Telnet	`set domain yourdomain.com`

③ Specify whether information from the DHCP server and the NetBIOS module should be used.

WEBconfig	… ▶ DHCP-usage … ▶ NetBIOS-usage
Terminal/Telnet	`set DHCP-usage yes` `set NetBIOS-usage yes`



Activated DNS server in the TCP IP configuration

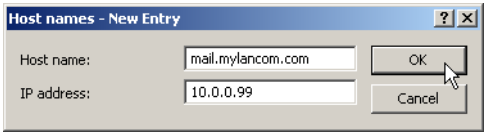
④ The main task of the DNS server is to distinguish requests for names in the Internet from those for other remote stations. Therefore, enter all computers in the Host names table,

- □ for which you know the name and IP address,
- □ that are not located in your own LAN,
- □ that are not on the Internet and
- □ that are accessible via the router.

With the following commands you add stations to the Host names table:

LANconfig	TCP/IP ▶ DNS ▶ Host names ▶ Add
WEBconfig	… ▶ DNS-table ▶ Add
Terminal/Telnet	`cd setup/DNS/DNS-table set mail.yourdomain.com 10.0.0.99`

For example, if would like to access the mail server at your headquarters (name: mail.yourdomain.com, IP: 10.0.0.99) via the router from a branch office, enter:



Stating the domain is optional but recommended.

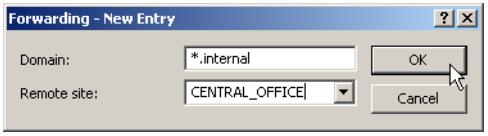
When you now start your mail program, it will probably automatically look for the server 'mail.yourdomain.com'. The DNS server thereupon returns the IP address '10.0.0.99'. The mail program will then look for that IP address. With the proper entries in the IP routing table and peer list, a connection is automatically established to the network in the headquarters, and finally to the mail server.

⑤ To resolve entire name areas of another DNS server, add a forwarding entry consisting of a name area and remote station:

LANconfig	TCP/IP ▶ DNS ▶ Forwarding ▶ Add
WEBconfig	… ▶ DNS destination table ▶ Add
Terminal/Telnet	`cd setup/DNS/DNS-destination- table set *.intern COMPANY`

When entering the name areas, the wildcards '?' (for individual characters) and '*' (for multiple characters) may be used.

To reroute all domains with the ending '.intern' to a DNS server in the LAN of the remote station 'COMPANY', create the following entry:



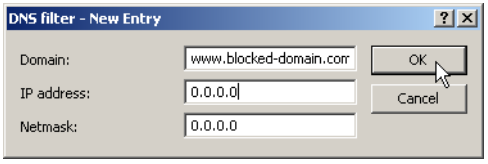
The DNS server may either be specified by the remote site name (for automatic setting via PPP), or by an explicit IP address of the according name server.

16.3.4 URL blocking

① Finally, one can restrict access to certain names or domains with the filter list.

To block the domain (in this case the web server) 'www.offlimits.com' for all computers in the LAN, the following commands and entries are required:

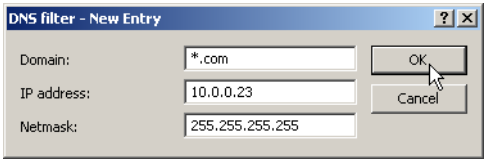
LANconfig	TCP/IP ▶ DNS Filter ▶ DNS filter... ▶ Add
WEBconfig	... ▶ Filter-list ▶ Add
Terminal/Telnet	`cd setup/DNS/filter-list` `set 001 www.blocked.com 0.0.0.0 0.0.0.0`



The index '001' in the console command can be selected as desired and is used only for clarity.

When entering the domains, the wildcards '?' (represents exactly one character) and '*' (for any number of characters) are permitted.

To only block the access of a certain computer (e.g. with IP 10.0.0.123) to COM domains, enter the following values:



In the console mode the command is:

```
set 002 *.com 10.0.0.123 255.255.255.255
```

The hit list in the DNS statistics contains the 64 most frequently requested names and provides a good basis for setting up the filter list.

If your LAN uses subnetting, you can also apply filters to individual departments by carefully selecting the IP addresses and subnet masks. The IP address '0.0.0.0' stands for all computers in the network, and the subnet mask '0.0.0.0' for all networks.

16.3.5 Dynamic DNS

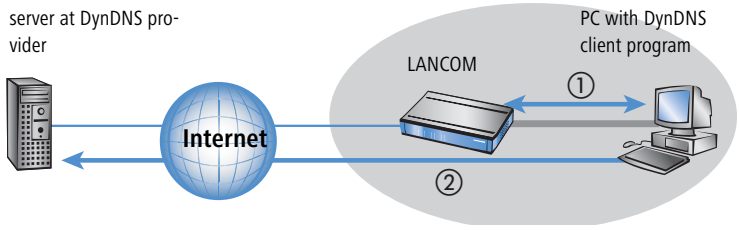
Systems with dynamic IP addresses become accessible over the WAN - for example over the Internet - via so-called Dynamic DNS service providers, e.g. www.dynDNS.org.

Thereby a LANCOM becomes available under a certain DNS-resolvable name (FQDN - 'fully qualified Domain Name', for example "http://MyLANCOM.dynDNS.org").

The advantage is obvious: If you want to accomplish e.g. remote maintenance for a remote site without ISDN available (e.g. over WEBconfig/HTTPS), or to connect with the LANCOM VPN Client to a branch office with dynamic IP address, then you just need to know the appropriate Dynamic DNS name.

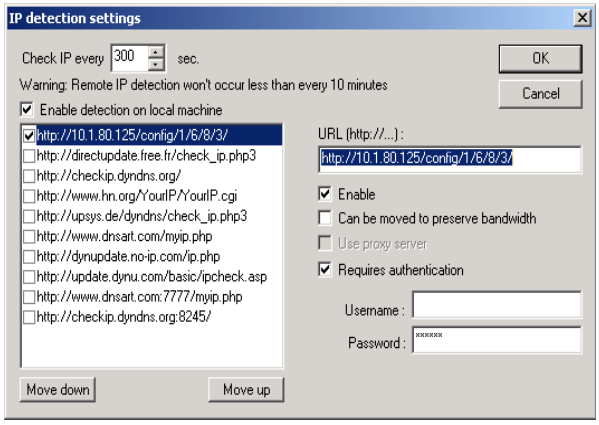
How to deposit the current IP address at the Dynamic DNS server?

All Dynamic DNS provider support a set of client programs, which can determine the current assigned WAN IP address of a LANCOM via different methods ①, and transfer this address - in case of a change - to their respective Dynamic DNS server ②.

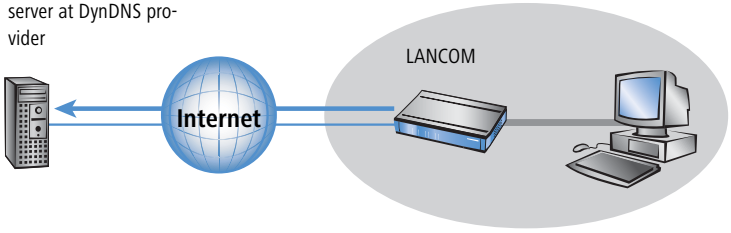


The current WAN IP address of a LANCOM can be picked under the following address:

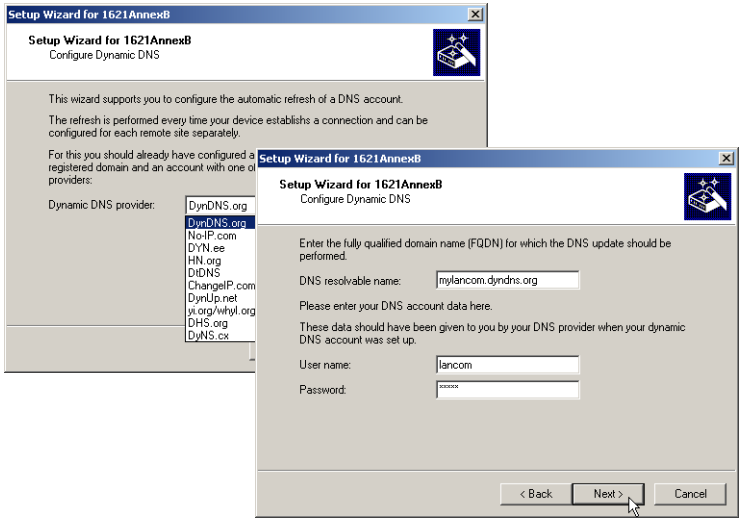
```
http://<address of LANCOM>/config/1/6/8/3/
```



Alternatively the LANCOM can directly transmit the present WAN IP to the DynDNS provider.



The required settings can be changed comfortably with the Setup Wizard:



16.4 Call charge management

The capability of the router to automatically establish connections to all desired remote sites and to close them again when no longer required provides users with extremely convenient access, e.g. to the Internet. However, quite substantial costs may be incurred by data transfer over paid lines if the router is not configured properly (e.g. in the filter configuration) or by excessive use of the communications opportunities (e.g. extended surfing in the Internet).

To reduce these costs, the software provides various options:

- The available online minutes can be restricted to a specific period.
- For ISDN connections, a limit on time or charges can be set for a particular period.

16.4.1 Connection limits for DSL and cable modem

Even though a DSL or cable modem connection behaves like a leased line, which is always online, depending on the provider connection charges can be accounted by the time.

In this section all connections over a ethernet WAN port of the LANCOM, e. g. cable modem connection, will be referred as DSL connection.

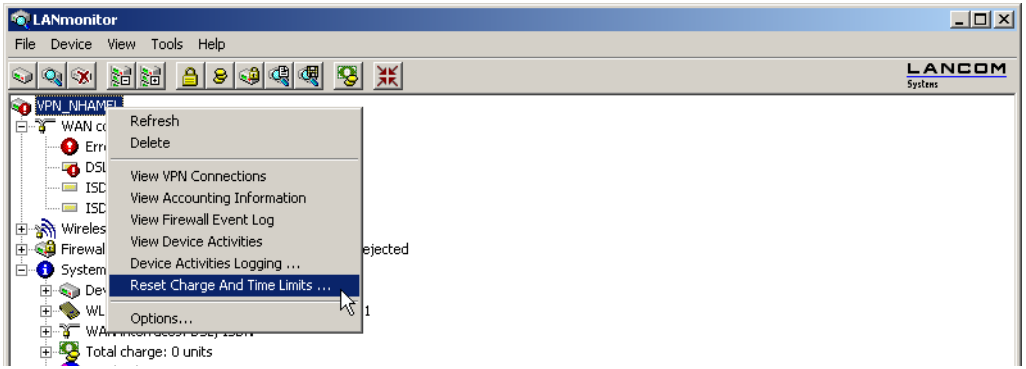
To limit the costs, the maximal connection duration can be controlled with time, by arranging a time limit for DSL connections for a period of time. By default the DSL connections can only be used for a maximum of 600 minutes in six days.

If the limit is reached, all DSL connections are automatically terminated. As soon as the current period has passed the time count is reset and the connection enabled. The administrator can of course reset the time count and enable the connection beforehand.

If the connection has a charge limit and a short hold of '0' or '9999' seconds, the charge control is switched off and the connection is kept even if the limit is exceeded.

If in an exceptional case you would like to extend the online budget, e.g. to download a large file from the internet, you do not necessarily have to change the time limit. In this case you can manually reset the limit.

Click with the right mouse button on the error in LANmonitor and select in the menu the entry 'Reset Charge And Time Limit'



If you cannot see the system information in LANmonitor, activate the view with **View ▶ Show Details ▶ System Information**.

In WEBconfig and Telnet the commands to activate the additional time limit are as follows:

Configuration tool	Call
WEBconfig	Expert Configuration ▶ Setup ▶ Charges ▶ Activate-additional-budget
Terminal/Telnet	`cd /Setup/Charges` `do activate-additional-budget`

The additional time limit is activated for the current period, in the following period normal time limit is set.

16.4.2 Charge-based ISDN connection limits

If charge information is sent to an ISDN connection, the resulting connection charges can be limited quite easily. For example, in its default state, a maximum of 830 charge units may be used in six days. The router will not permit the establishment of any further connections once this limit has been reached.

The best way to use the router's call charge monitoring function is if you have "call charge information enabled **during** the connection" to the ISDN network (i.e. AOCD). If necessary, subscribe to this facility from your telecommunications carrier. Charge monitoring with the "Charge information **after** connection" feature is also possible in principle, but in this case continuous connections may not be detected!

If you have enabled least-cost routing on the router modules, connections may be established to providers who do not transmit any charge information!

16.4.3 Time dependent ISDN connection limit

However, this mechanism of ISDN connection monitoring will not work if the ISDN connection does not provide charge information. That may be the case, for example, if the provision of charge information was not requested for the connection, or if the telecommunications provider generally does not supply this information.

To reduce the costs of ISDN connections even if no call charge information is available, maximum connection lengths based on time can be regulated. This requires setting up a time budget for a specified period. In the router's default state, for example, connections may only be established for a maximum of 210 minutes within six days.

When the limit of a budget is reached, all open connections that were initiated by the router itself will be shut down automatically.The budgets will not be reset to permit the establishment of connections until the current period has elapsed. Needless to say, the administrator can reset the budgets at any time if required!

The charge and time monitoring of the router functions can be disabled by entering a budget of 0 units or 0 minutes.

Only the router functions are protected by the charge and time monitoring functions! Connections via LANCAPI are not affected.

16.4.4 Settings in the charge module

Configuration tool	Run/table
LANconfig	Management ▶ Costs
WEBconfig	Expert Configuration ▶ Setup ▶ Charges
Terminal/Telnet	`cd /setup/charges`

In the charges module, the online time can be monitored and used to control call establishment.

- Day(s)/Period
  The duration of the monitoring period in days can be specified here.
- Budget units, Online minutes budget
  The maximum number of ISDN units or online minutes in a monitoring period

The current charge and connect-time information is retained when rebooting (e.g. when installing new firmware) is not lost until the unit is switched off. All the time references here are in minutes.

16.5 The SYSLOG module

The SYSLOG module gives the option of recording accesses to the LANCOM. This function is of particular interest to system administrators, because it allows a full history of all activities to be kept.

To be able to receive the SYSLOG messages, you will need an appropriate SYSLOG client or daemon. In UNIX/Linux the SYSLOG daemon, which is installed by default, generally does the recording. It reports either directly through the console or writes the protocol to a SYSLOG file.

In Linux the file `/etc/syslog.conf` directs which facilities (this expression will be explained later) should be written to which log file. Check in the configuration of the daemon whether network connections are explicitly monitored.

Windows does not have any corresponding system functions. You will need special software that fulfills the function of a SYSLOG daemon.

16.5.1 Setting up the SYSLOG module

Configuration tool	Run/Table
LANconfig	Management ▶ Log & Trace
WEBconfig	Expert Configuration ▶ Setup ▶ SYSLOG
Terminal/Telnet	`cd /setup/SYSLOG`

16.5.2 Example configuration with LANconfig

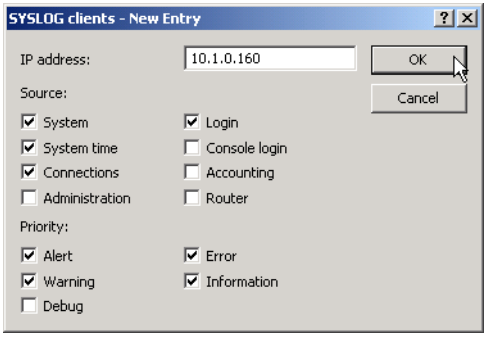
Create SYSLOG client

① Start LANconfig. Under 'Management', select the 'Log & Trace' tab.

② Turn the module on and click **SYSLOG clients**.

③ In the next window click **Add...**.

④ First enter the IP address of the SYSLOG client, and then set the sources and priorities.



SYSLOG comes from the UNIX world, in which specified sources are predefined. LANCOM assigns its own internal sources to these predefined SYSLOG sources, the so-called “facilities”.

The following table provides an overview of the significance of all news sources that can be set in the LANCOM. The last column of the table also shows the alignment between the internal sources of the LANCOM and the SYSLOG facilities.

Source	Meaning	Facility
System	system messages (boot processes, timer system etc.)	KERNEL
Login	messages regarding login and logout of a user during the PPP negotiation and errors occurring during this process	AUTH
System time	messages regarding changes to the system time	CRON
Console login	messages regarding console logins (Telnet, outband, etc.), logouts and errors occurring during this process	AUTHPRIV
Connections	messages regarding establishing and releasing connections and errors occurring during this process (display trace)	LOCAL0
Accounting	accounting information after release of a connection (user, online time, transfer volume)	LOCAL1
Administration	messages regarding configuration changes, remotely executed commands etc.	LOCAL2
Router	regular statistics on the most frequently used services (sorted by port numbers) and messages regarding filtered packets, routing errors etc.	LOCAL3

The eight priority stages defined initially in the SYSLOG are reduced to five stages in the LANCOM. The following table shows the relationship of alarm level, significance and SYSLOG priorities.

Priority	Meaning	SYSLOG priority
Alert	All messages requiring the attention of the administrator are collected under this heading.	PANIC, ALERT, CRIT
Error	All error messages that can occur during normal operation without requiring administrative intervention are sent to this level (e.g. connection errors).	ERROR
Warning	Error messages that do not affect normal operation of the device are sent to this level.	WARNING
Information	All messages that are purely informative in character are sent to this level (e.g. accounting information).	NOTICE, INFORM
Debug	Transfer of all debug messages. Debug messages generate a high data volume and interfere with the normal operation of the device. They should therefore be disabled during normal operation and should only be activated for troubleshooting.	DEBUG

⑤ After you have set all the parameters, confirm the entries with **OK**. The SYSLOG client is then entered with its parameters into the SYSLOG table.

Facilities

All messages from LANCOM can be assigned to a facility with the **Facility mapping** button and then are written to a special log file by the SYSLOG client with no additional input.

Example

All facilities are set to 'local7'. Under Linux in the file `/etc/syslog.conf` the entry

```
local7.* /var/log/lancom.log
```

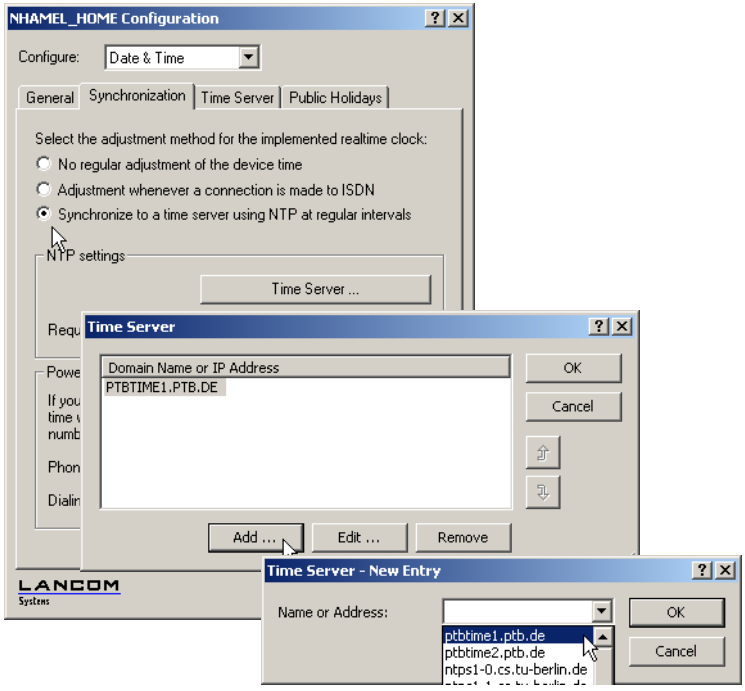
writes all outputs of the LANCOM to the file `/var/log/lancom.log`.

16.6 Time server for the local net

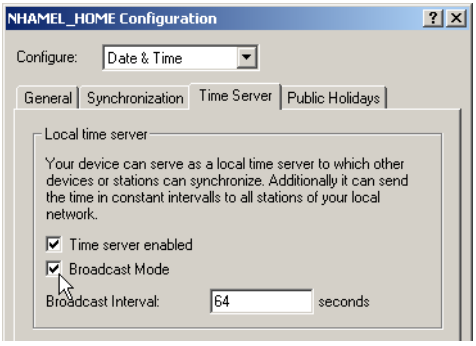
LANCOM routers can apply exact information of time either over ISDN or over public time servers on the internet (NTP-Server with 'Open Access' policy). The LANCOM can then provide the detected time for all stations in the local network.

16.6.1 Configuration of the time server under LANconfig

To provide the current time in the local network your LANCOM has to regularly apply the time from a time server. For this so called real time clock click in the configuration area 'Date & time' on the tab 'Synchronization'. Under 'NTP settings' open the list of time servers by clicking on the button **Time Server ...**. With the button **Add...** you can extend the list.



With these settings only the LANCOM applies the time from public time servers. To provide the real time for the remaining device enable the local time server under the tab 'Time Server'. Furthermore activate the broadcast mode and enter the broadcast interval.



16.6.2 Configuration of the time server with WEBconfig or Telnet

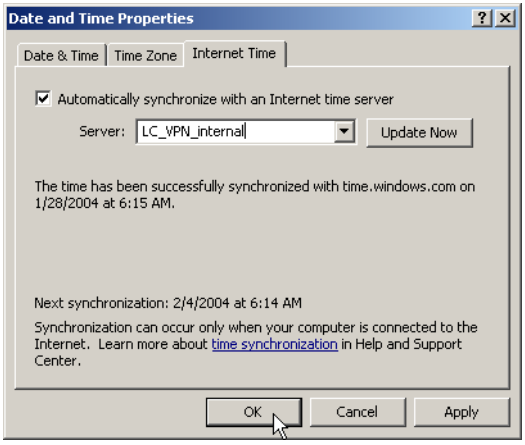
When configuring with WEBconfig or Telnet you can find the required parameters in the following areas:

Configuration tool	Run
WEBconfig	Expert Configuration ▶ Setup ▶ NTP
Terminal/Telnet	`cd /Setup/NTP-Modul`

16.6.3 Configuring the NTP clients

The NTP clients must be configured so that they use the time information from the LANCOM. Not all operating systems provide an integrated NTP client: Windows XP does so, for other Windows operating systems a separate NTP client is required, Linux distributions have to be installed with NTP.

The settings of date and time in a XP system can be opened with a double click on the time at the bottom left, where you can select the server for synchronization.



16.7 Scheduled Events

16.7.1 Regular Execution of Commands

This feature is intended to allow the device to execute predefined commands in a telnet-like environment, at times defined by the user. The functionality is equivalent to the UNIX cron service. Subject of execution can be any LANCOM command line command. Therefore, the full feature set of all LANCOM devices can be controlled by this facility.

Application examples:

- scheduled connection

  Many leased lines disconnect automatically after 24 hours of continuous operation. This enforced disconnection can have some unwanted side-effects for example if it happens to an unsuitable time during the day, because e.g. the VPN tunnel is disconnected and the IP address of the LANCOM is changed. To control the disconnecting time a manual disconnection can be set e.g. at midnight, so it can not happen at an unsuitable time.

  As a second example devices with a distributed network with only dynamic IP addresses can build up a connection at a certain time to a VPN gateway, so that data can be transferred safely. This way a protected access is even possible without an ISDN connection.

- time-dependant firewall or QoS rules

  The firewall and QoS rules are at first temporally constant. But it can be useful to make variable settings for different daytimes or weekdays. At e. g. off-hours or weekends different priorities for guaranteed bandwidths can be set than at business hours.

- regular firmware or configuration updates

  Time-controlled rules do not only provide the settings of particular values, it is even possible to switch to a whole different configuration. This possibility allows you to pool a whole string of settings and change them all at once with one command. Therefore changing the configuration of the device with completely different values at the weekend and switching back on monday mornings can be done with just one command.

  Additionally the regular update of the newest firmware from one single source is adjustable.

- Email messages

  With the time-controlled rules you have the option that the LANCOM informs the administrator by email not only about specific firewall events, but even to set times. The email can e.g. inform about building up an internet connection successfully after an enforced disconnection or after booting the device because of a restart.

- time-dependant interfaces

  The time dependant use of interfaces for a set duration is also provided by the time-controlled rules. Therewith e.g. a WLAN interface can permit the wireless access to the network only at certain times.

- Deleting certain tables

  It can be useful to delete the content of some tables in LCOS regularly. If your internet access for example has a monthly limited transfer volume, you can delete your accounting table monthly to have a survey of the present transferred data volume.

16.7.2 The cron table

The parameters for the time-controlled rules are stored in the cron table with the following layout:

Entry	Description
Index	Unambiguously identifies this entry in the table
Base	The `Base` field rules whether the time check is done against the device's operation time or the real time. Rules based on real time are only executed if the device has acquired the current time, e.g. via NTP. For real-time based rules, all four columns have a meaning, while operation-time based rules only take the minute/hour fields into account.
Minute Hour DayOfWeek Day Month	The entries `Minute` to `Month` form a mask that lets the user define at which times a command will be executed. Entries in the mask field may be blank to mark that the respective component shall not be part of the compare operation; otherwise, a field may contain a list of comma-separated items that may either be a single number or a number range, given as minimum and maximum concatenated with a hyphen. For the DayOfWeek field, the usual cron interpretation applies: 0 Sunday 1 Monday 2 Tuesday 3 Wednesday 4 Thursday 5 Friday 6 Saturday
Command	The command itself may be a list of command line commands, separated by semicolons.

Realtime-controlled rules can only be executed if the device has a valid time reference e.g. via NTP ('Time server for the local net' → page 548).

Examples:

Time base	min.	hrs.	W.-days	M.-days	month	command
Realtime	0	4	0-6	1-31	1-12	do /oth/man/disconnect internet
Realtime	59	3	0-6	1-31	1-12	mailto:admin@mylancom.de?subject=Enforced disconnection?body=Manual disconnecting the interface
Realtime	0	0		1		do /setup/accounting/Delete-Accounting-list
Realtime	0	18	1,2,3,4,5			do /so/man/connect HEADQUARTERS

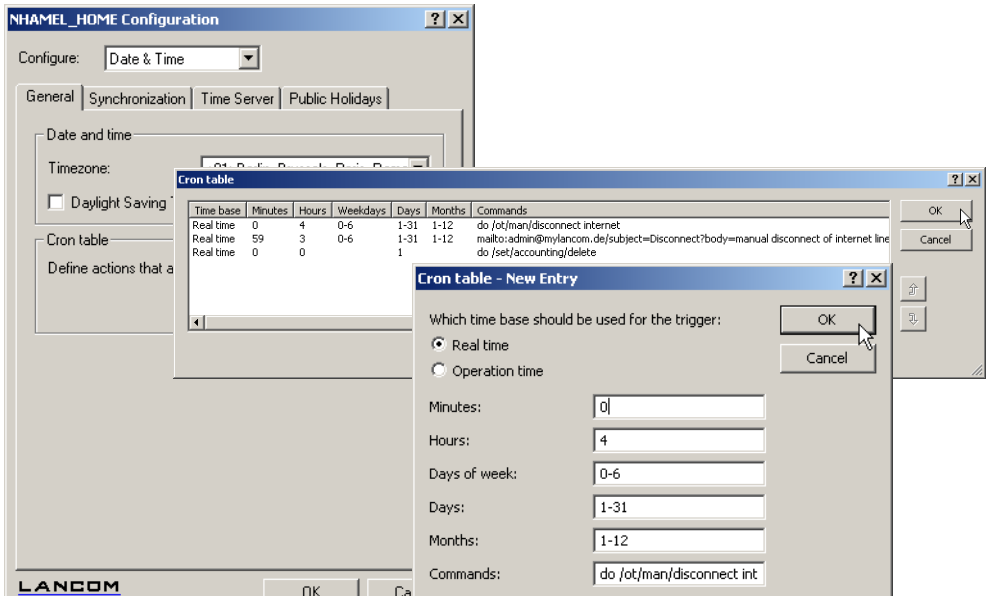
- The first entry will enforce a disconnection to the internet provider every morning at 4 AM.
- The second entry will inform the admin every morning at 3:59 AM by email, shortly before the enforced disconnection.
- The third entry will delete on the first of every month the accounting table.
- The fifth entry will connect the device every weekday at 6 PM to the headquarters.

Time-controlled rules will not necessarily be executed at precisely zero seconds of real time.
Please note that the language of the commands must be identical to the set language of the console, oth-

erwise they will not be executed. The display language of your LANCOM is set to english by default. The language can be changed if desired ('Change the language of the display.' → page 29).

16.7.3 Configuring the time-controlled rules

Under LANconfig you can find the Cron table in the configuration area 'Date & Time' on the tab 'General':



Under WEBconfig or Telnet you can find the Cron table as follows:

Configuration Tool	Run
WEBconfig	Expert-Configuration ▶ Config ▶ Cron-table
Terminal/Telnet	`setup/config/cron-table`

16.8 Port mapping

16.8.1 Free translation of TCP/IP ports on masked connections

If IP masquerading is used over a connection, the IP address of the computer in the local network is hidden behind the IP address of the router. So that individual computers in a LAN can still be contacted, inverse masquerading is used whereby an incoming port range in the service table is assigned to a particular IP address in the LAN.

On occasion it is desirable for the "exposed" host not to be contacted over this standard port, e.g. when security reasons demand the use of another port. In this case it is not only necessary to map the ports to an IP address, but to translate between ports as well. Another example of port mapping is the translation of multiple WAN ports to one common port in the LAN, but to different IP addresses (N-IP mapping).

16.8.2 Configuration

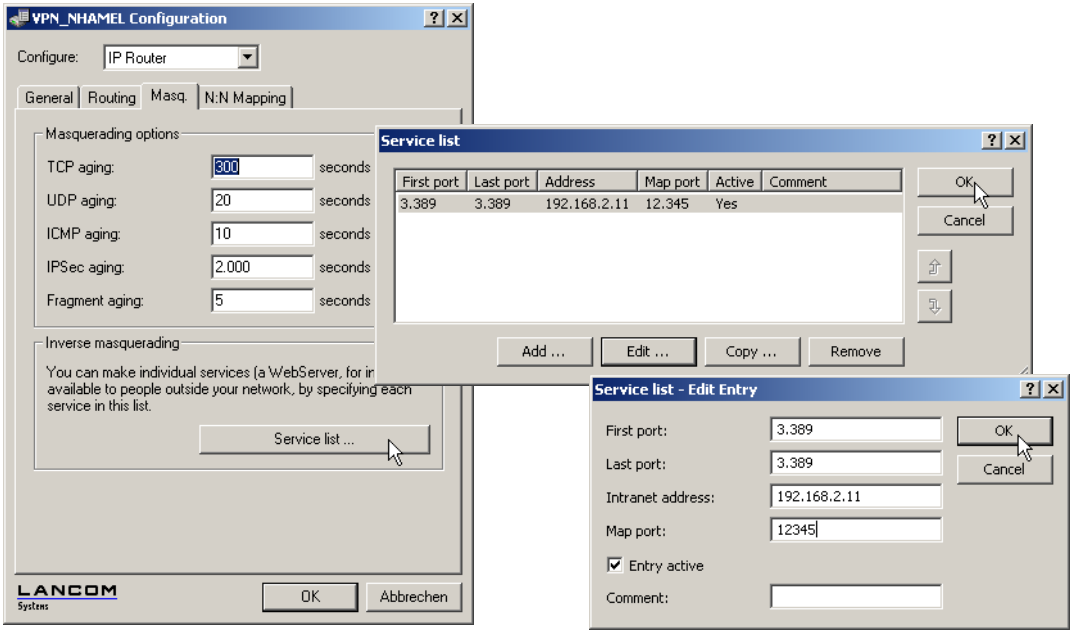
The configuration of port mapping involves the assignment of a port or port range (start port to end port) to an IP address from the LAN as the target and the port (map port) to be used in the LAN.

If "0" is entered for the map port, the ports used in the LAN will be the same as those used in the WAN. If a port range is to be mapped, then the map port identifies the first LAN port to be used. For example, mapping the port range '1200' to '1205' to the internal map port '1000' means that the ports 1000 to 1005 will be used for data transfer in the LAN.

Port mapping is static, meaning that two ports or port ranges cannot be mapped to the same map port of a target computer in the LAN. The same port mapping can be used for different target computers.

LANconfig

When using LANconfig for the configuration, you will find the service list in the configuration area 'IP Router' on the 'Masq.' tab under the button **Service list**.



WEBconfig, Telnet or terminal program

Under WEBconfig, Telnet or a terminal program, you will find the service list for the wireless network under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ IP-router ▶ Masquerading ▶ Service-table
Terminal/Telnet	`Setup/IP-router/Masquerading/Service-table`

16.9 PPPoE Servers

16.9.1 Introduction

In accordance with the widespread availability of DSL, PPPoE clients have now been widely integrated into all operating systems. These can be used to "log on to the network" as well as to manage access rights to services such as the Internet, e-mail or remote stations.

PPPoE can only be used on a network segment.

As it is what is known as a "Layer 2" technology, PPPoE can only be used within a network segment, i.e. it cannot be used across IP subnets. The PPPoE connection cannot be established across network segment limits, such as via a router.

After a user logs on to the LAN (e.g. username: 'Purchasing', password: 'secret') using a specified PPPoE logon, further rights can be regulated via the firewall. This enters the PPPoE user name as a 'remote station' in the firewall. With a deny all rule, and a PPPoE rule in the following format, user Anyone can be permitted to use the Internet with Web and FTP:

- Source: Anyone
- Target: All stations

Services: WWW, FTP

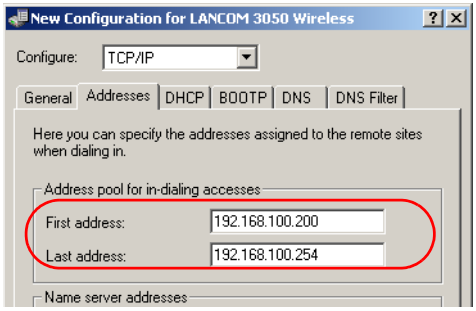
16.9.2 Example application

All employees in the 'Purchasing' department must first authenticate themselves to the LANCOM using PPoE (IP routing, PAP check) in order to access the Internet.

Constraint: The LANCOM can be accessed directly by the users in the LAN as a router, firewall and gateway, i.e. there are no other routers in between them.

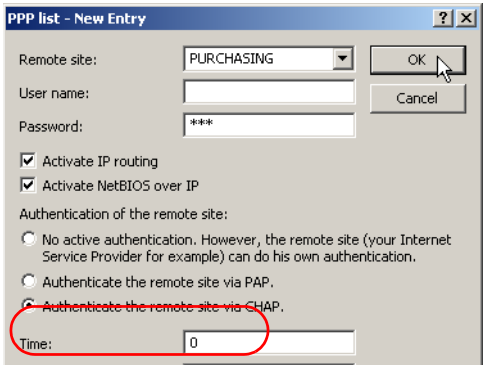
The computers in Purchasing are assigned with an IP address from a certain address range (e.g. 192.168.100.200 to 192.168.100.254) from the list of addresses for dial-in connections (LANconfig▶ TCP/IP ▶ Addresses).

The LANCOM itself is in a different IP address range!

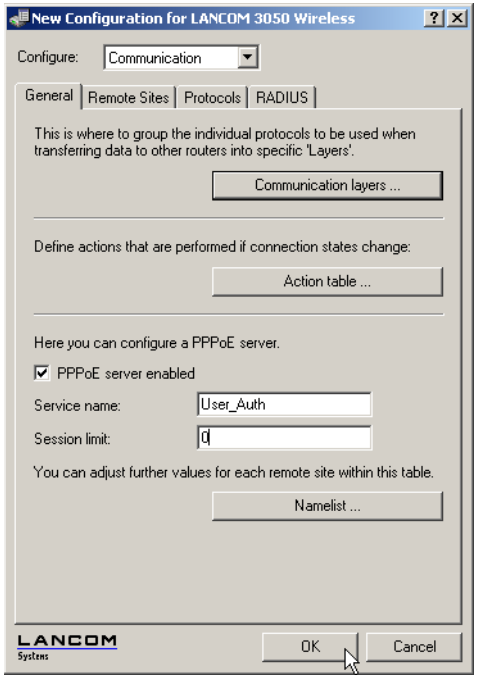


To prevent users from bypassing the authentication, a DENY ALL rule is defined in the firewall to stop local connections from being established.

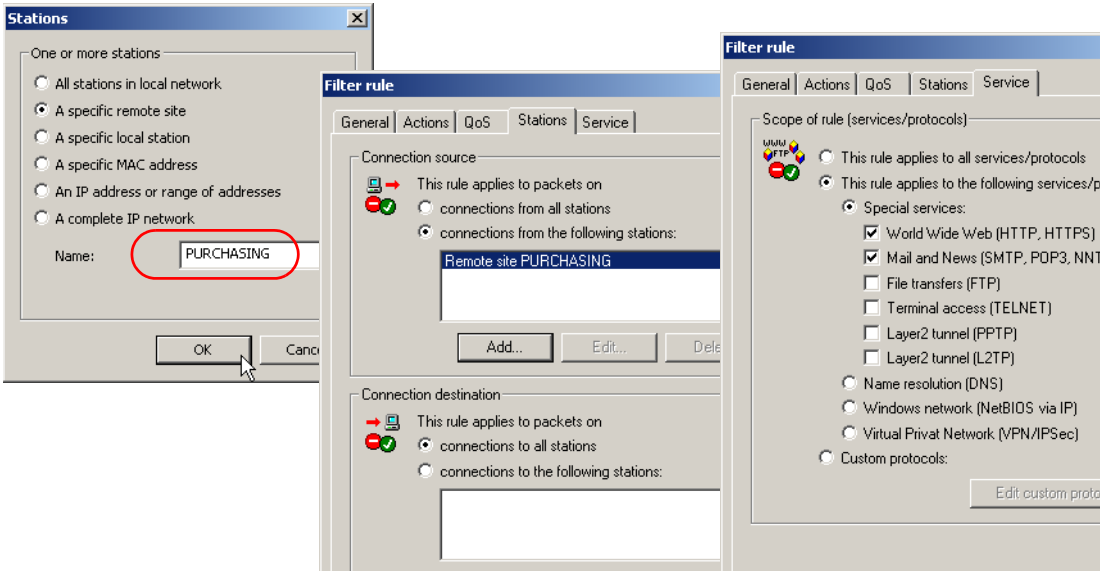
The user 'Purchasing' is then entered into the PPP list (LANconfig ▶ Communication ▶ Protocols) without a user name but with a password which is to be used by all staff members in the department, and authentication (encrypted) is set up as CHAP. Both IP routing and NetBIOS (Windows Networking) are to be activated for this PPP user:



Along with the activation of the PPPoE server (LANconfig ▶ Communication ▶ General), further limitations (e.g. permissible MAC addresses) can also be defined in the PPPoE server. The example uses the existing entry 'DEFAULT' with the MAC address '00.00.00.00.00.00', thereby permitting all MAC addresses.



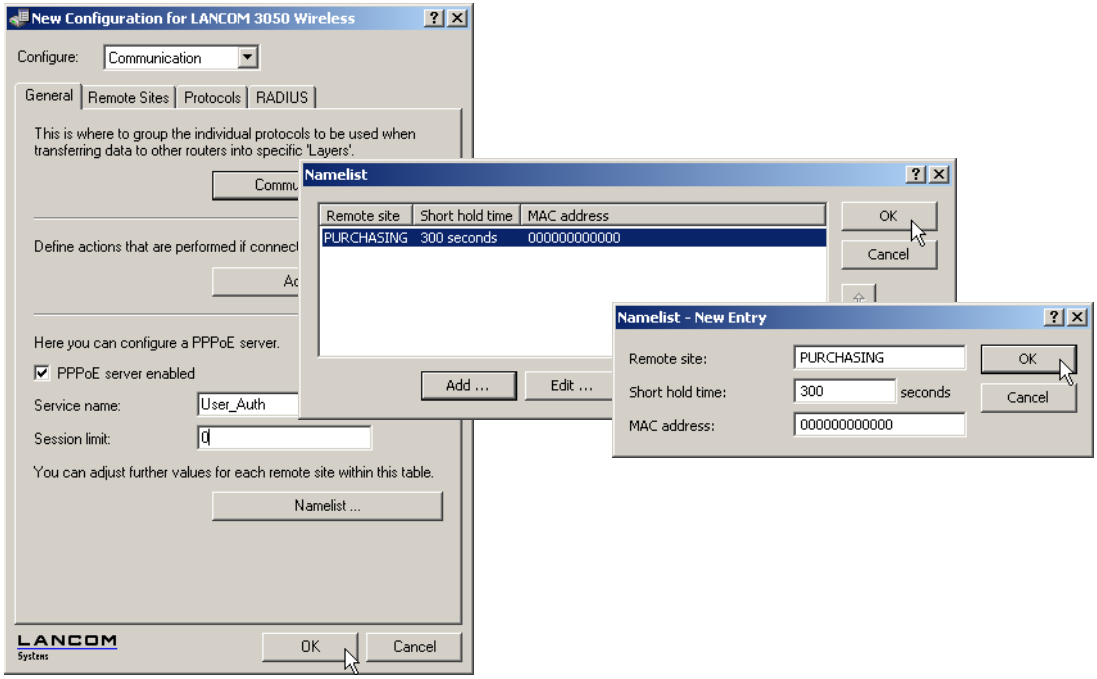
The firewall (LANconfig ▶ Firewall/QoS ▶ Rules) can be used to control which services are available to the employees in Purchasing (e.g. release of HTTP and EMAIL only).



16.9.3 Configuration

Configuration with LANconfig

The settings for the PPPoE server can be found in LANconfig in the configuration area 'Communication' on the 'General' tab.



Configuration with WEBconfig, Telnet or SSH

Under WEBconfig, Telnet or SSH client you will find the settings for the PPPoE server under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ PPPoE server
Terminal/Telnet	`Setup/PPPoE servers`

- **Operating**: The 'Operating' button switches the server on or off. The default value is 'Off'.
- **Service**: The name of the service offered is entered under 'Service'. This enables a PPPoE client to select a certain PPPoE server that is entered for the client.
- **Session limit**: The 'Session limit' specifies how often a client can be logged on simultaneously with the same MAC address. Once the limit has been reached, the server no longer responds to the client queries that are received. Default value is '1', maximum value '99'. A Session limit of '0' stands for an unlimited number of sessions.
- **Name list**: Different parameters (such as shorthold time and MAC address) can be assigned to users in the name list:

A MAC address of '000000000000' means that the user may log on with any MAC address. If a MAC address is entered, then the PPP negotiation is terminated if the user logs on from a different MAC address. The user's shorthold time is set after the logon. If no entry exists, then the time belonging to user 'DEFAULT' is used.

In addition to this table, an entry has to be made in the PPP table in which the password, the rights (IP, IPX,NetBIOS) and other PPP parameters (LCP polling) are entered. The user can therefore also be authenticated using a RADIUS server.

16.10RADIUS

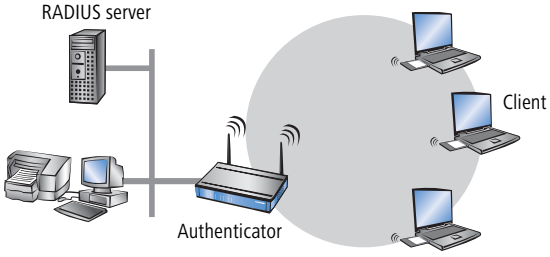
RADIUS stands for "Remote Authentication Dial-In User Service" and is referred to as a "triple-A" protocol. The three "A"s stand for

- Authentication
- Authorization
- Accounting (billing)

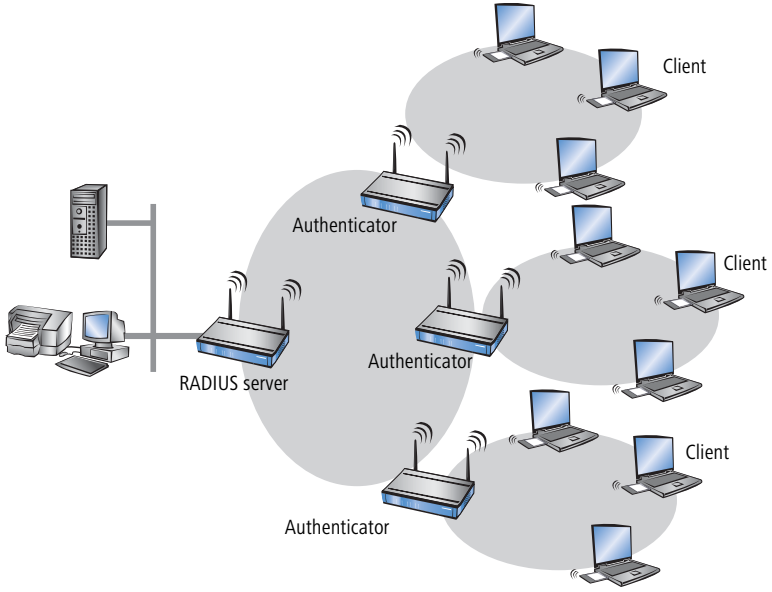
This protocol allow you to grant users access to a network, to assign them certain rights and to track their actions. Where necessary, the RADIUS server can also be used in the billing of user services such as WLAN hot spots. For every action performed by the user, the RADIUS server can run an authorization procedure releasing or blocking access to network resources on a per user basis.

3 different devices are required for RADIUS to work.

- Client: This is a device (PC, notebook etc.) from which the user wishes to dial in to the network.
- Authenticator: A network component positioned between network and client and which forwards on the authorization. This task can be performed by an LANCOM Access Point for example. The authenticator is referred to as the Network Access Server (NAS).



- Authentication server: RADIUS server on which user data is configured. This is usually located within the same network for which it issues access authorizations. It is accessible to the client via the authenticator. Some scenarios may also allow the use of a LANCOM access point for this task.



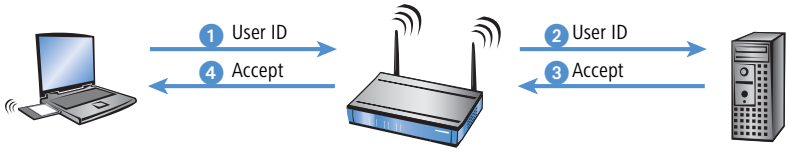
The authenticator has no initial information on the clients wanting to register. This is all stored in a database on the RADIUS server. The registration information the RADIUS server needs for the authentication process is stored in the database there and can vary from network to network. The authenticator has just the one task, that of transferring the information between the client and the RADIUS server.

Access to a RADIUS server can be configured in several ways:

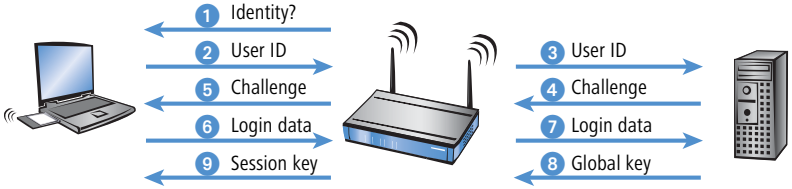
- Using PPP when dialing into a network (see 'Dial-in using PPP and RADIUS' → page 565)
- Via WLAN (see 'Dial-in using WLAN and RADIUS' → page 567)
- Via a public spot for users who register using a browser (see 'Dial-in using a public spot and RADIUS' → page 568
- Via the 802.1x protocol (see 'Dial-in using 802.1x and RADIUS' → page 569)

16.10.1How RADIUS works

The authentication process of a client using the authenticator on a RADIUS server can vary in complexity and is implementation dependent. In a simplified application, the client sends its registration data to the RADIUS server via the authenticator and receives back either an "Accept" or a "Reject".



In more complicated applications, the RADIUS server can request additional registration data using what is known as a "Challenge". The handshake sequence looks something like this:

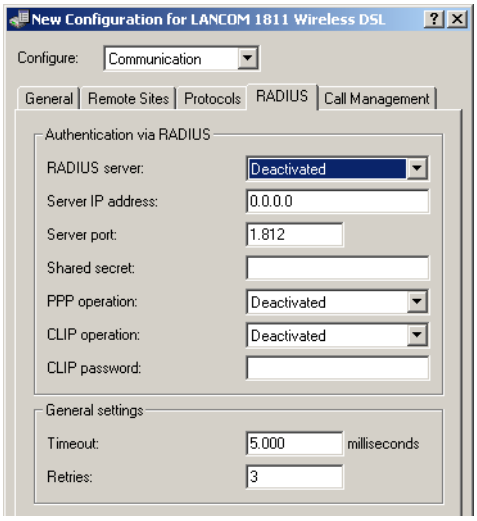


16.10.2Configuration of RADIUS as authenticator or NAS

The RADIUS protocol is supported by LANCOM devices in a range of different applications. For each of these cases there is a specific set of parameters which may be configured independently of other applications. There are also general parameters which need to be configured for each of these applications. Not all devices support all applications.

General settings

General settings apply to all RADIUS applications. Default values have been selected such that they need not usually be changed.



Configuration tool	Call
LANconfig	Communication ▶ RADIUS
WEBconfig, Telnet	Expert configuration > Setup > RADIUS module

- **Timeout [default: 5.000]**

  This value specifies how many milliseconds should elapse before retrying RADIUS authentication.

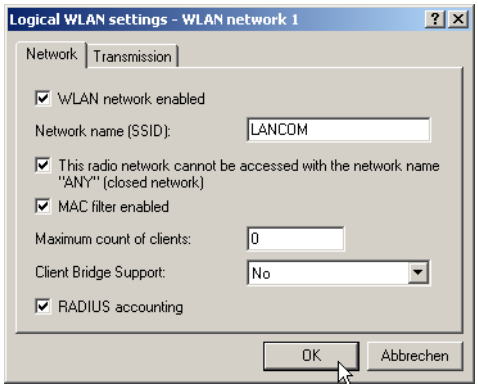
With PPP authentication using RADIUS, please note that the device dialing accepts the RADIUS timeout configured here.

- **Retries [default: 3]**

  This value specifies how many authentication attempts are made in total before a Reject is issued.

RADIUS accounting

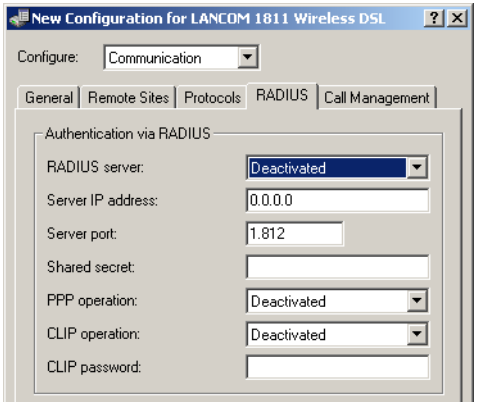
Accounting for a logical WLAN network can be enabled from a RADIUS server by enabling the "RADIUS Accounting" option in the logical WLAN settings for the network.



Configuration tool	Call
LANconfig	Interfaces ▶ Wireless LAN ▶ Logical WLAN settings
WEBconfig, Telnet	Expert configuration > Setup > RADIUS module

Dial-in using PPP and RADIUS

When dialing-in using the PPP protocol (Point-to-Point protocol), RADIUS can be used to check client access authorizations. A client can dial-in to the network from anywhere. The resulting data transmission between client and authenticator is encrypted.



Configuration tool	Call
LANconfig	Communication ▶ RADIUS
WEBconfig, Telnet	Expert configuration > Setup > WAN > RADIUS

- **Radius server [default: disabled]**

  When authenticating using RADIUS, the user administration and authentication tasks are passed on to a RADIUS server.

  - Disabled: The functionality of RADIUS is disabled and no requests are forwarded to the RADIUS server.
  - Enabled: The functionality of RADIUS is enabled and requests may be forwarded to the configured RADIUS server. Depending on the setting, other sources may be used for the authentication process (e.g. PPP list).
  - Exclusive: RADIUS functionality is enabled and the authentication process is run exclusively by RADIUS.

  The appropriate RADIUS server must be configured to use the functionality of RADIUS. All user data, such as user name and password, is entered on the RADIUS server.

- **Server IP address**

  Specify here the IP address of your RADIUS server from which users are managed centrally.

- **Server port [default: 1.812]**

  Specify here the port used for communication to your RADIUS server.

- **Key (shared secret)**

  Specify here the key to be used for coding data. The key must also be configured on the RADIUS server.

■ **PPP mode [default: disabled]**

A RADIUS server may be used for the authentication process when dialing-in using PPP.

- □ Disabled: PPP clients are not authenticated using RADIUS. They are checked **exclusively** using the PPP list.
- □ Enabled: RADIUS authentication for PPP clients is enabled. User data supplied by clients is **first** checked using the PPP list. If no matching entry is found in the PPP list, the client is checked by the RADIUS server. Authentication is successful if the PPP list check**or** RADIUS server check returns as positive.
- □ Exclusive: RADIUS authentication for PPP clients is enabled. User data supplied by clients is checked **exclusively** by the RADIUS server. In this mode, it is just the advanced settings of the PPP list for the user which are interpreted (e.g. check for PAP/CHAP – or the allowed protocols IP, IPX and/or NetBIOS).

■ **CLIP mode [default: disabled]**

A RADIUS server may be used for control of a return call when dialing-in using PPP.

- □ Disabled: The return call function is not controlled by RADIUS. **Only** those entries in the name list are used.
- □ Enabled: The RADIUS function for the return call is enabled. Telephone numbers reported by clients are **first** checked using the name list. If no matching entry is found in the name list, the telephone number is checked by the RADIUS server. If the name list check **or** RADIUS server check returns as positive, a return call can be established.

If the telephone number communicated is in the name list, but no return call is active there, RADIUS ceases checking.

- □ Exclusive: The RADIUS function for the return call is enabled. User data reported by clients is checked **exclusively** by the RADIUS server.

In order to use the return call control from RADIUS, a user must be set up on the RADIUS server for each telephone number to be authenticated. The user name corresponds to the telephone number and the user password is the CLIP password specified here.

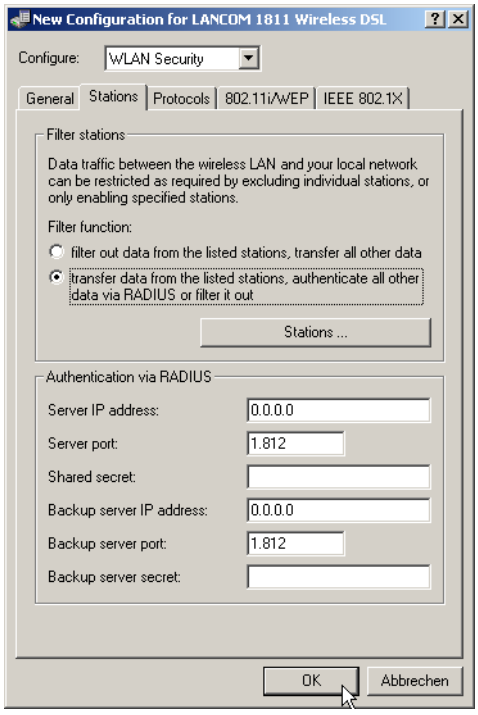
■ **CLIP password**

Password for return call control.

The generic values for retry and timeout must also be configured (see 'Configuration of RADIUS as authenticator or NAS' → page 562). They are under PPP on the same page as PPP parameters.

Dial-in using WLAN and RADIUS

When using a RADIUS server for the authentication of WLAN clients, the RADIUS server uses the MAC address to check client authorizations.



Configuration tool	Call
LANconfig	WLAN Security ▶ Stations
WEBconfig, Telnet	Expert configuration > Setup > WLAN > RADIUS access check

To use the RADIUS functionality for WLAN clients, the option "Transfer data from the listed stations, authenticate all others via RADIUS or filter them out" must be selected for the "Filter stations" parameter.

- **Server IP address**

  Specify here the IP address of your RADIUS server from which users are managed centrally.

- **Server port [default: 1.812]**

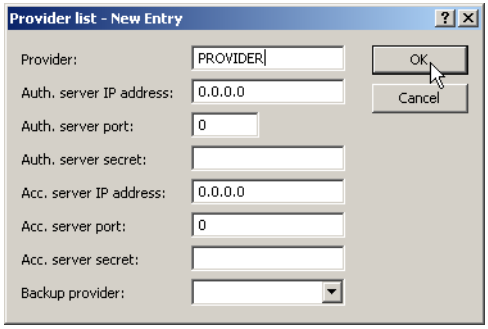
  Specify here the port used for communication to your RADIUS server.

- **Key (shared secret)**
  Specify here the key to be used for coding data. The key must also be configured on the RADIUS server.
- **Backup server IP address [default: 1.812]**
  Specify here the IP address of your backup RADIUS server from which users are managed centrally.
- **Backup server port**
  Specify here the port used for communication to your backup RADIUS server.
- **Backup key**
  Specify here the key to be used for coding data. The key must also be configured on the backup RADIUS server.

The generic values for retry and timeout must also be configured (see 'Configuration of RADIUS as authenticator or NAS' → page 562).

Dial-in using a public spot and RADIUS

When configuring a public spot (enable using software option for the LANCOM access points), user registration data can be forwarded to one or more RADIUS servers. These are configured in the provider list. The registration data individual RADIUS servers require from the clients is not important to the LANCOM access point since this data is passed on transparently to the RADIUS server.



Configuration tool	Call
LANconfig	Public Spot ▶ Public Spot Users ▶ Provider list
WEBconfig, Telnet	Expert configuration > Setup > WLAN > RADIUS accounting

- **Provider**
  Name of the provider for whom the RADIUS server is defined.
- **Auth. server IP address**
  The IP address of the RADIUS server for this provider.

- **Auth. server port**

  The port over which the LANCOM access point can communicate with the RADIUS server for this provider.

- **Auth. server secret**

  Key (shared secret) for access to the RADIUS server of the provider. The key must also be configured on the appropriate RADIUS server.

- **Acc. Server IP address**

  IP address of the Accounting server for accesses to the public spot.

- **Acc. server port**

  The port over which the LANCOM access point can communicate with the accounting server.

- **Acc server secret**

  Key (shared secret) for access to the Accounting server. The key must also be configured on the Accounting server.

- **Backup provider**

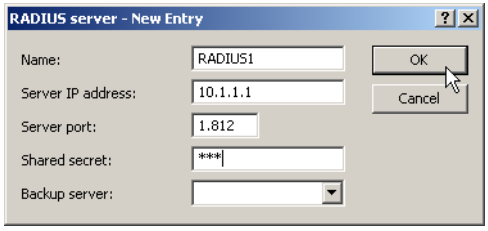
  The name of a different provider can be selected as the backup from the current table. Using these types of entries, backup chains linking several RADIUS servers can be easily configured.

The generic values for retry and timeout must also be configured (see 'Configuration of RADIUS as authenticator or NAS' → page 562).

Dial-in using 802.1x and RADIUS

WLAN clients can use the 802.1x protocol for network registration. The LANCOM access point can use this protocol to forward the registration to the RADIUS server. The MAC address is used for user identification.

Please refer to 'EAP and 802.1x' → page 349 for further information on the 802.1 x protocol.



Configuration tool	Call
LANconfig	WLAN Security ▶ IEEE 802.1X ▶ RADIUS server
WEBconfig, Telnet	Expert configuration -->Setup -->IEEE802.1x > Radius server

- **Name**

  In this table, each RADIUS server needs a unique name. The name 'DEFAULT' is reserved for all WLAN networks that use an authentication process in line with IEEE 802.1x and that have not specified their own RADIUS server.

  By using the name defined in the 'Key 1/passphrase' field, each WLAN network using authentication in line with IEEE 802.1x can be assigned its own RADIUS server.

- **Server IP address**

  Specify here the IP address of your RADIUS server from which users are managed centrally.

- **Server port**

  Specify here the port used for communication to your RADIUS server.

- **Key (shared secret)**

  Specify here the key to be used for coding data. The key must also be configured on the RADIUS server.

- **Backup server**

  Name of the backup server from the list of RADIUS servers configured so far.

The generic values for retry and timeout must also be configured (see 'Configuration of RADIUS as authenticator or NAS' → page 562).

WLAN clients must be entered as follows on the RADIUS server:

The user name is the MAC address in the format AABBCC-DDEEFF. The password for all users is identical to the key (shared secret) for the RADIUS server.

16.10.3Configuring RADIUS as server

In addition to its function as RADIUS authenticator or NAS, an LANCOM access point can also operate as a RADIUS server. When in this mode, information in the device on users authorized to register is made available to other access points in Authenticator mode.

RADIUS server parameters

When configuring the RADIUS server, a definition is needed of which authenticator can access the RADIUS server, the password required for this access, and the open port that is to be used to communicate with the RADIUS server. The authentication port applies globally for all authenticators.

Configuration tool	Call
LANconfig	WLAN security ▶ RADIUS
WEBconfig, Telnet	Expert configuration > Setup > Radius > Server

- **Authentication port [default: 0]**

  Specify here the port used by the authenticators to communicate with the RADIUS server in the LANCOM access point. Port '1812' is normally used.

  Port '0' disables the RADIUS server.

In addition to the port, 16 authenticators that are allowed to communicate with the RADIUS server may be entered here. Entries are made in the corresponding table and with the following parameters:

- **IP address**

  IP address of the authenticator which may communicate with the RADIUS server in the LANCOM access point.

- **Secret**

  Password required by the authenticator for access to the RADIUS server in the LANCOM access point.

In addition to the configuration of the RADIUS server, the client information source must also be defined 'WLAN access list as a basis for RADIUS information' → page 571.

WLAN access list as a basis for RADIUS information

512 WLAN clients, all able to register with the LANCOM access point, may be entered in the access list. When operating in RADIUS server mode, this list can also be used to check on RADIUS clients wanting to register at other access points. In an installation having several access points, client access authorizations can be maintained centrally.

Configuration tool	Call
LANconfig	WLAN security ▶ RADIUS
WEBconfig, Telnet	Expert configuration > Setup > WLAN > RADIUS access check

- **Provide server database [default: yes]**

  This parameter specifies whether the WLAN access list is to be used as an information source for the RADIUS server in the LANCOM access point.

  The WLAN access list contains the user name in the form of the MAC address and the password ('WPA passphrase'). In addition to this access data, the access list provides information such as bandwidth restriction and association to a specific VLAN.

- **Recheck cycle [default: 0]**

  Once a WLAN client is logged on after authentication by RADIUS, it remains active until it logs off itself or is logged off by the RADIUS server. By specifying a recheck cycle [minutes], the RADIUS server can regularly check whether the WLAN clients logged in are still in the access list. If a WLAN client is removed from the access list, it remains logged in to the WLAN up to the point when the recheck cycle runs again.

A recheck cycle of '0' disables regular checking. WLAN clients remain logged in until they log themselves out.

16.11Operating printers at the USB connector of the LANCOM

With the USB port of various LANCOM models, printers can be connected up and made available to the entire network. The LANCOM provides a print server to manage the printing jobs from the network. Supported protocols are RawIP and LPR/LPD.

Parallel print jobs arriving from different stations are saved on the respective computer. The print server in the LANCOM processes the waiting jobs one after the other.

16.11.1Configuring the printer server in the LANCOM

When configuring the USB port for the connection of a printer, the first thing is to define the ports which will receive the print jobs as transported by the various protocols.

Printer table

The printer table contains the settings for the connected printer.

Configuration tool	Call
WEBconfig, Telnet	Expert-Configuration > Setup > Printer > Printer

Normally there will be no need to adjust the printer settings. With the default settings, the print server works with RawIP and LPR/LPD and reacts to the standard ports as suggested by Windows when the printer connection is being configured. If printer operation does not work with these settings, the printing parameters can be adjusted.

- **Printer [Default: *]**
  Printer name.
- **RawIP-Port [Default: 9100]**
  This port can be used to accept print jobs over RawIP.

RawIP is used by Windows as standard and is recommended for operating printers at a USB port.

- **LDP-Port [Default: 515]**
  This port can be used to accept print jobs over LDP.

The protocol and port options entered here must agree with the settings for the printer connection in the corresponding computer's operating system.

- **Active [Default: No]**
  - □ Yes: The print server is active.
  - □ No: The print server is not active.

- **Bidirectional [Default: No]**
  - □ Yes: The LANCOM transmits the printer's status information at regular intervals to the connected computers.
  - □ No: The LANCOM does not transmit and status information.

Access list:

Up to 16 networks that have access to the configured printer can be entered into the access list.

Configuration tool	Call
LANconfig	Printer ▶ General ▶ Access list
WEBconfig, Telnet	Expert-Configuration > Setup > Printer > Access-List

- **IP address**

  IP address of the network with clients requiring access to the printer.
- **Net mask**

  Netmask of the permitted networks.

If the access list is empty, any computer with any IP address can use the printer at the LANCOM's USB port.

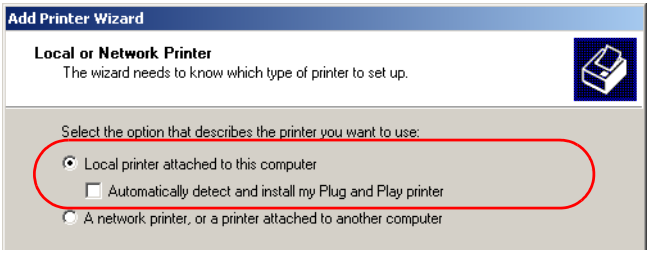
For reasons of security, access from the WAN to the printer at the USB port of the LANCOM is not permitted.

16.11.2Printer configuration at the computer

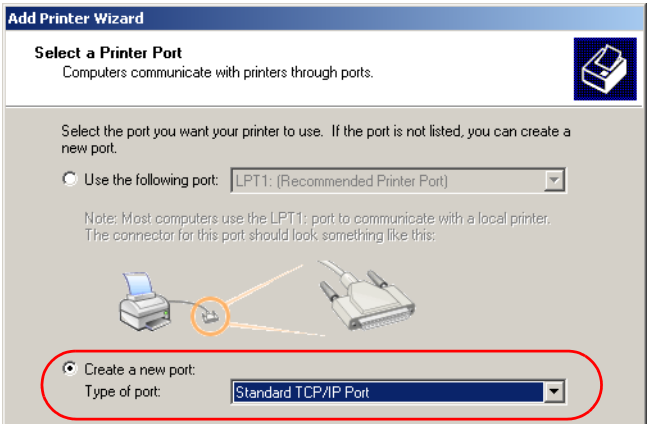
To use the printer at the USB port over the network, the printer drivers on the computers have to be connected with a corresponding printer connection. The following is a description of the setup under Windows XP; the configuration under Windows 2000 is similar. Controlling printers via TCP/IP ports with older version of Windows is rather unsatisfactory.

① In the Control Panel, open the dialog for the configuration of a new printer and start the Wizard to add a new printer.

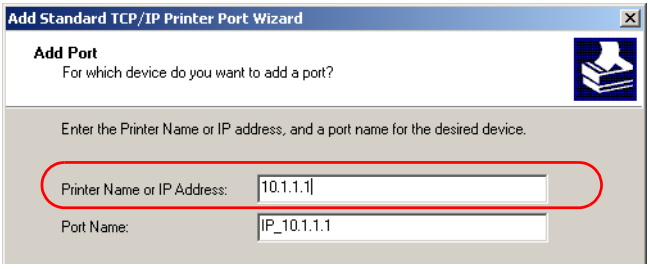
② Select the option for a local printer and deactivate Plug&Play.



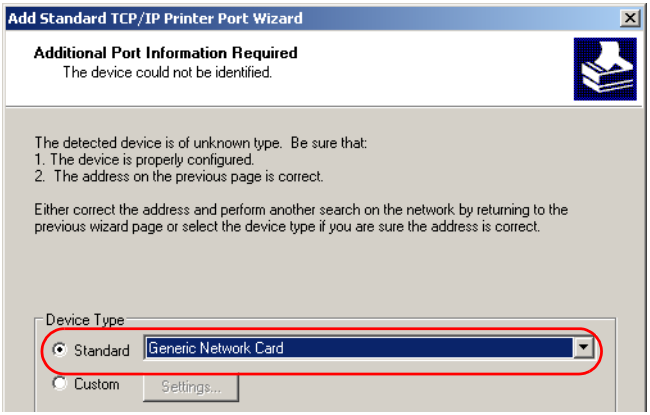
③ Select the option to add a new printer port.



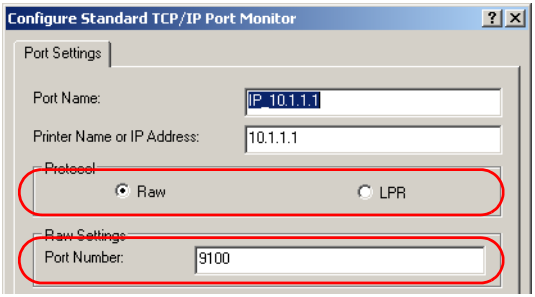
④ Enter the IP address of the LANCOM as the IP address of the printer port. The name for the printer port will automatically be filled out with 'IP_<IP address of the LANCOM>'.



⑤ As the device type, select the option 'Standard' for a 'Generic Network Card'. If you wish to keep the standard settings (recommended), press on **Next** to proceed to the next dialog.



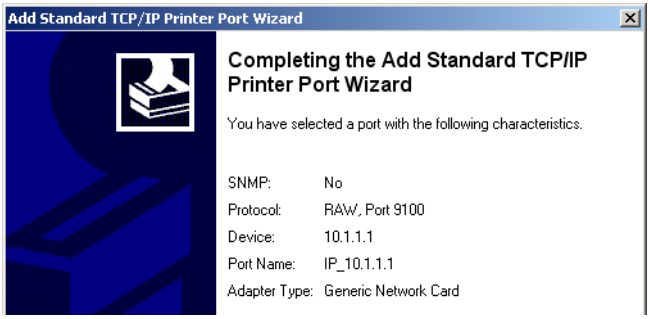
⑥ Alternatively, you can select 'Custom' and press on the **Settings** button to open an additional dialog. In diesem Dialog können Sie das Protokoll auswählen, das für die Übertragung der Druckaufträge zum Drucker am USB-Port des LANCOM verwendet werden soll ('Raw' – RawIP oder 'LPR'). The port to be used can be entered here too (for RawIP only). For LPR, port '515' is always used as standard.



The protocol and port options entered here must agree with the settings for the printer in the LANCOM configuration.

The dialog for selecting the protocol and port can also be accesses via the Control Panel by opening the Printer Properties and accessing the 'Ports' tab.

⑦ Once the settings have been made, the printer port is set up. The Wizard now goes on with the selection of the printer driver.



Further information about the installation of a printer driver is available in the documentation for the printer.

□ Operating printers at the USB connector of the LANCOM

17 Appendix

17.1 Error messages in LANmonitor

It is possible to read out VPN error messages over the LANmonitor.

17.1.1 General error messages

Connection attempt cancelled	
Connection establishment failed (D-channel layer 1)	Bus activation failed
Connection establishment failed (D-channel layer 2)	no UA on SABME
Connection establishment failed (Layer 1)	a/b ports
Connection establishment failed (Layer 2)	a/b ports
ISDN line error (Layer 1)	Cable not connected
Connection aborted (layer 2)	X.75 / V.110
Local error	Required resource not available -> ISDN problem; boot tele-communications system
PP login at remote site - PAP rejected	Remote device can only handle PAP, but CHAP is required
PPP login from remote site - timeout (PPP-PAP RX)	Remote did not send PAP request
PPP login at remote site - timeout (PPP-PAP TX)	Remote did not respond to PAP request
PPP login from remote site - CHAP rejected	a CHAP reject was received after a CHAP challenge
PPP login from remote site - timeout (PPP-CHAP RX)	Remote did not send CHAP response
PPP login at remote site - timeout (PPP-CHAP TX)	Remote did not respond to CHAP response
Time limit exceeded	exactly like fee limit... .
Connection establishment failed (Layer 1)	no HDLC flags found
Connection establishment failed (Layer 2)	X.75 / V.110 not working
DSL line error (Layer 1)	Cable not connected

17.1.2 VPN error messages

For correct evaluation of error messages for VPN connections, at least LCOS version 3.22 must be installed on both LANCOM devices.

A VPN connection is always either an outgoing or an incoming connection. To make searching for the error faster and more efficient, the error messages are different for the initiator and the responder. The initiator is the remote

device which initiates the connection. The responder is the device which receives the connection. After the error message is read out, look in the appropriate menu item on the corresponding remote.

Example:

For the error message 'IKE or IPSec establishment timeout (Initiator)', no direct error can be determined. The responder, however, has determined an error like 'No proposal matched (Responder, IPSec)', which it send to an SNMP client (LANmonitor) using an SNMP trap. Using this error message, the corresponding parameter in the configuration can be checked and changed if necessary. Thus is it always necessary to verify the error messages on both sides.

Message	Initiator	Responder	
License exceeded - no more VPN tunnels available (Responder, IKE)	x	x	The maximum number of possible VPN channels has been reached.
No route to remote gateway	x	x	The router to the remote gateway could not be found. Please check the public IP address or the DynDNS name of the remote device.
Dynamic VPN - no PPP table entry matched	x		In dynamic VPN, the outgoing call could not be authenticated with the PPP data sent. Please check the PPP username and PPP password on both sides under "Configure --> Communication --> Protocols --> PPP list --> Remote site".
Dynamic VPN - no PPP table entry matched		x	The incoming call cannot be authenticated with the PPP data received. Please check the PPP username and PPP password on both sides under "Configure --> Communication --> Protocols --> PPP list --> Remote site".
IKE or IPSec establishment timeout	x	x	A time limit was reached. The router on the remote side is no longer responding. Please check the VPN error message in the LANmonitor on the remote device.
Line polling to remote gateway failed			The LCP polling failed. Please check on the remote device whether ping blocking is enabled in the firewall menu under "Configure --> Firewall --> General --> Ping blocking"
No entry in polling table and keep alive in configured			The holding time of the VPN tunnel under "Configure --> VPN --> Connection list --> Names" is set to Short hold (9999 sec.). However, the required ICMP polling is missing. Please add them under "Configure --> Communication --> Remote Sites --> Polling Table". As remote site, enter the VPN remote device, for the IP address enter an IP address from the LAN at the remote site.
Dynamic VPN - predefined charge limit exceeded	x		The fee limit under "Configure --> Costs --> Fees - Limit (ISDN)" was reached. Please reboot the device.
Dynamic VPN - preset time limit exceeded	x		The time limit under "Configure --> Costs --> Time limit (ISDN)" was reached. Please reboot the device.
Dynamic VPN - no ISDN call number for negotiator channel	x		The ISDN call number for the remote device for dynamic VPN is missing. Please enter the call number under "Configure --> Communication --> Remote sites --> Name list (ISDN) --> Name".

Message	Initiator	Responder	
Dynamic VPN - Multiple connections on ISDN interface for negotiator channel not allowed			While establishing multiple ISDN connections, a limit was reached. Please check under "Configure --> Management --> Interfaces --> Interface Settings --> ISDN --> Max. outgoing calls".
Predefined charging limit exceeded	x		The fee limit under "Configure --> Management --> Costs --> Charge limit (ISDN)" was reached. Indicated by a synchronized blinking of the Power LED.
Predefined time limit exceeded	x		The time limit under "Configure --> Management --> Costs --> Time Limit (ISDN)" was reached. Indicated by a synchronized blinking of the Power LED.
No IP address for PPTP server	x		The IP address of the PPTP selected has not been entered. Enter the IP address under "Configure --> Communication --> Protocols --> PPTP list". Also see .
Exchange type mismatch (Main or Aggressive mode)		x (IKE)	The exchange type does not match that of the remote device. Please check the value under "Configure --> VPN --> Connection list --> Edit VPN remote site entry --> IKE Exchange"
No proposal matched	x (IKE)		The IKE proposals do not match. -- > Check VPN rules
No proposal matched		x (IKE)	The IKE proposals do not match. -- > Check VPN rules
IKE group mismatch		x (IKE)	Please check the IKE groups on both sides under "Configure --> VPN --> Connection parameters --> VPN remote site identification --> IKE Group"
Life type unsupported (other than Kbytes or seconds?)		x (IKE)	The value for the lifetime is not supported. Please use a life type in "sec = seconds" or "kb = kilobytes". Check this entry under "Configure --> VPN --> Parameters --> Lifetime"
Lifetime mismatched		x (IKE)	The lifetime specified does not match that of the remote device. Check this entry under "Configure --> VPN --> Parameters --> Lifetime"
ID type value unsupported (other than IP network, domain, or email)		x (IKE)	False entry of identity. Please correct your entry under "Configure --> VPN --> IKE --> IKE key"
ID type mismatch (e.g. IP network, domain, or email)		x (IKE)	The two sites are using different identities. Compare the identification at both sites under "Configure --> VPN --> IKE --> IKE key"
No rule matched ID - unknown connection or wrong ID (e.g. remote gateway definition)		x (IKE)	The incoming VPN connection could not be assigned to a remote device.
IKE key mismatch	x (IKE)		Please compare the preshared keys under "Configure --> VPN --> IKE --> IKE key"
IKE key mismatch		x (IKE)	Please compare the preshared keys under "Configure --> VPN --> IKE --> IKE key"
Out of memory	x (IKE)		The number of VPN connections has overloaded the device's memory. To maintain the stability of the device, no further VPN connections should be established.

Message	Initiator	Responder	
Out of memory		x (IKE)	The number of VPN connections has overloaded the device's memory. To maintain the stability of the device, no further VPN connections should be established.
No rule matched IDs - unknown connection or wrong ID (e.g. IP network definition)		x (IKE)	The incoming VPN connection could not be assigned to a remote device. Please check the following parameters: ID type does not match (see this document), incorrect network definition, VPN rules do not match (see VPN RULES).
No proposal matched	x (IPsec)	x (IPsec)	The devices cannot agree on a matching proposal. Please check the settings under "Configure --> VPN --> IKE --> IKE Proposals" and under "Configure --> VPN --> IPSec parameters --> IPSec proposal lists".
IPSec PFS group mismatch			Please check the PFS (Perfect Forward Sequence) under "Configure --> VPN --> Connection parameters --> VPN remote identification --> PFS Group"

17.2 SNMP Traps

MIB2 Traps	Explanation
coldstart	Device was restarted by switching power off and on.
warmstart	LCOS was restarted, for instance by a software reboot
authentication failed (= console login failed)	Login failed during access to the configuration

Enterprise specific Traps	Explanation
Firmware upload started	Firmware upload was started
Configuration upload started	The reading of the firmware or configuration was started
Upload succeeded	The reading of the firmware or configuration was successful
Upload failed (timeout)	The reading of the firmware or configuration failed: maximum time was exceeded
Upload failed (incomplete)	The reading of the firmware or configuration failed: incomplete configuration
Upload failed (bad device)	The reading of the firmware or configuration failed: wrong device
Configuration download started	Output of the configuration was started
Download succeeded	Output of the configuration was successful
Console login	Login to configuration successful
Console logout	Logout from configuration was successful
Firewall trap	Information about a firewall event
Connection status	WAN connection status
VPN Connection status	Status of VPN connection
WAN-Ethernet UP/DOWN	WAN interface available or not available

WLAN traps	Operating mode	Explanation
WLAN Scan started	Access point or client	The WLAN station has started a scan for free radio channels
Started WLAN BSS ID	Access point	The WLAN station has created a new radio cell
Joined WLAN BSS ID	Client	The WLAN station has found a radio cell
Authenticated WLAN station	Access point	The authentication of a client WLAN station was successful
Deauthenticated WLAN station	Access point	The client WLAN station has signed off
Associated WLAN station	Access point	Client WLAN station connected
Reassociated WLAN station	Access point	Client WLAN station has reconnected, was previously signed in to another access point

WLAN traps	Operating mode	Explanation
RADIUS access check for WLAN station succeeded	Access point	Checking of RADIUS access to the WLAN station was successful
RADIUS access check for WLAN station failed	Access point	Checking of RADIUS access to the WLAN station was unsuccessful
Disassociated WLAN station due to station request	Access point	WLAN station was signed off due to a request from the station
Rejected association from WLAN station	Access point	The sign on of the WLAN station was rejected
WLAN card hung, resetting	Access point or client	WLAN card stopped, reset

17.3 Radio channels

17.3.1 Radio channels in the 2,4 GHz frequency band

In the frequency range from 2400 to 2483 MHz are up to 13 channels available. The following overview shows which channels are supported by the different regions (EU/WORLD). The last column shows which channels can be used without overlapping.

Frequency range	2400–2500 MHz		no overlapping with
Channel No.	EU (ETSI)	WORLD (ETSI + FCC)	
1	2412	2412	6, 11
2	2417	2417	7
3	2422	2422	8
4	2427	2427	9
5	2432	2432	10
6	2437	2437	1, 11
7	2442	2442	2
8	2447	2447	3
9	2452	2452	4
10	2457	2457	5
11	**2462**	**2462**	1, 6
12	2467	–	–
13	2472	–	–

Bold values indicate the default setting of the *LANCOM DSL/I-10 Office* radio adapters when utilized in a base station.

17.3.2 Radio channels in the 5 GHz frequency band

In the frequency range from 5,13 to 5,805 GHz up to 19 non-overlapping channels are available in Europe, defined as the sub-bands as follows:

- Band 1: 5150 - 5350 MHz (channels 36, 40, 44, 48, 52, 56, 60 and 64)
- Band 2: 5470 - 5725 MHz (channels 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 and 140)
- Band 3: 5725 - 5875 MHz (channels 147, 151, 155, 167)

Please note that frequency ranges an radio channels in band 3 are reserved for operation in UK only!

The following overview shows which channels are allowed in different regions.

	Channel No.	Frequency	ETSI (EU)	FCC (US)
Band 1	36	5,180 GHz	yes	yes
	40	5,200 GHz	yes	yes
	44	5,220 GHz	yes	yes
	48	5,240 GHz	yes	yes
	52	5,260 GHz	yes	yes
	56	5,280 GHz	yes	yes
	60	5,300 GHz	yes	yes
	64	5,320 GHz	yes	yes
Band 2	100	5,500 GHz	yes	no
	104	5,520 GHz	yes	no
	108	5,540 GHz	yes	no
	112	5,560 GHz	yes	no
	116	5,580 GHz	yes	no
	120	5,600 GHz	yes	no
	124	5,620 GHz	yes	no
	128	5,640 GHz	yes	no
	132	5,660 GHz	yes	no
	136	5,680 GHz	yes	no
	140	5,700 GHz	yes	no

	Channel No.	Frequency	ETSI (EU)	FCC (US)
Band 3 (UK only)	147	5,735 GHz	no	yes
	151	5,755 GHz	no	yes
	155	5,775 GHz	no	yes
	167	5,835 GHz	no	yes

17.3.3 Radio channels and frequency ranges for Indoor and Outdoor operating

In several countries specific regulations are valid concerning the use of frequency ranges and radio channels for indoor and outdoor operating. The following table gives information on the permitted application:

Country	Band (GHz)	Sub band	Frequency	Channels	Turbo channels	Emitted power (dBm)	Indoor/ Outdoor
Germany, Austria, Switzerland, Netherlands, Belgium, Luxembourg, Italy, Malta	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	200/23	I
		2	5,470-5,725	100-140	106-130	1000/30	I+O
UK	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	200/23	I
		2	5,470-5,725	100-140	106-130	1000/30	I+O
		3	5,725-5,585	147, 151, 155, 167	–	2000/33,1	(only fixed WLAN outdoor installations!)
Czechia	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	200/23	I
France	2,4	1	2,4-2,4835	1-13	6	100/20	I
	2,4	1	2,4-2,454	1-9	6 (up to max. 10 dBm only!)	100/20	O
	2,4	1	2,454-2,4835	10-13		10/10	O
	5	1	5,15-5,35	36-64	42-58	200/23	I

Further details to the restrictions for the use of wlan adapters within the EU can be found in the internet:

Country	Organization	Link
Belgium	Institut Belge des Postes et Telecommunications (BIPT)	www.bipt.be
Denmark	National Telecom Agency	www.tst.dk
Germany	Regulierungsbehörde für Telekommunikation und Post	www.regtp.de

Country	Organization	Link
Finland	Finnish Communications Regulatory Authority (FICORA)	www.ficora.fi
France	Autorité de Régulation des Télécommunications (ART)	www.art-telecom.fr
Greece	National Telecommunications Commission (EET)	www.eett.gr
Great Britain	Office of Telecommunications (Oftel)	www.oftel.gov.uk
	Postal Services Commission (Postcomm)	www.postcomm.gov.uk/
	Radiocommunications Agency	www.open.gov.uk/radiocom
Ireland	Commission for Communications Regulation (ComReg)	www.comreg.ie
Iceland	Post and Telecom Administration (PTA)	www.pta.is
Italy	L'Autorità per le garanzie nelle communicazioni (AGC)	www.agcom.it
Latvia	Telecommunication State Inspection	www.vei.lv
Liechtenstein	Amt für Kommunikation (AK)	www.ak.li
Lithuania	Radio Administration	www.rrt.lt/
Luxembourg	Institut Luxembourgeois des Télécommunications (ILT)	www.etat.lu/ILT
Netherlands	Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA)	www.opta.nl
	Agentschap Telecom	www.agentschap-telecom.nl
	Ministerie Economische Zaken	www.ez.nl
Norway	Norwegian Post and Telecommunications Authority (NPT)	www.npt.no
Austria	Rundfunk und Telekom Regulierungs-GmbH	www.rtr.at
	Bundesministerium für Verkehr, Innovation und Technologie	www.bmvit.gv.at
Poland	Urzad Regulacji Telekomunikacji (URT)	www.urt.gov.pl
Portugal	Autoridad Nacional De Comunicaçòes (ICP-Anacom)	www.anacom.pt
Sweden	National Post and Telecom Agency	www.pts.se
Switzerland	Bundesamt für Kommunikation	www.bakom.ch
Slowenia	Agencija za telekomunikacije, radiodifuzijo in pošto	www.atrp.si
Spain	Comision del Mercado de las Telecomunicaciones (CMT)	www.cmt.es
Czechia	Czech Telecommunication Office	www.ctu.cz
Hungary	Communication Authority (HIF)	www.hif.hu

Please inform yourself about the current radio regulations of the country you want to operate a Wireless LAN device.

17.4 RFCs supported

RFC	Title
1058	Routing Information Protocol
1331	The Point-to-Point Protocol (PPP) for the Transmission of Multi-protocol Datagrams over Point-to-Point Links
1334	PPP Authentication Protocols
1389	RIP Version 2 MIB Extensions
1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
1542	Clarifications and Extensions for the Bootstrap Protocol
1552	The PPP Internetworking Packet Exchange Control Protocol (IPXCP)
1577	Classical IP and ARP over ATM
1631	The IP Network Address Translator (NAT)
1877	PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
1974	PPP Stack LZS Compression Protocol
2284	Extensible Authentication Protocol
2104	HMAC: Keyed-Hashing for Message Authentication
2131	Dynamic Host Configuration Protocol
2132	DHCP Options and BOOTP Vendor Extensions
2225	Classical IP and ARP over ATM
2364	PPP Over AAL5
2401	Security Architecture for the Internet Protocol
2402	IP Authentication Header
2403	The Use of HMAC-MD5-96 within ESP and AH
2404	The Use of HMAC-SHA-1-96 within ESP and AH
2405	The ESP DES-CBC Cipher Algorithm With Explicit IV
2406	IP Encapsulating Security Payload (ESP)
2407	The Internet IP Security Domain of Interpretation for ISAKMP
2408	Internet Security Association and Key Management Protocol (ISAKMP)
2409	The Internet Key Exchange (IKE)
2410	The NULL Encryption Algorithm and Its Use With IPsec
2412	The OAKLEY Key Determination Protocol
2451	The ESP CBC-Mode Cipher Algorithms

□ RFCs supported

RFC	Title
2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5
3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

17.5 Glossary

802.11	Wireless LAN specification of the IEEE; data rate up to 2 Mbps; in 2.4 GHz ISM band; FHSS and DSSS; infrared spectrum communications also planned
802.11a	Extension to 802.11; data rate up to 54 Mbit/s; in 5 GHz band; OFDM
802.11b	Extension to 802.11; data rate up to 11 Mbit/s; in 2.4 GHz band; high market penetration; DSSS/CCK
802.11g	Extension to 802.11; data rate up to 54 Mbit/s; in 2.4 GHz band; OFDM and DSSS
802.11h	802.11a customization, data rate up to 54 Mbit/s; in 5 GHz band; in area of transmission power and frequency management; for use in Europe; OFDM
802.11i	Future 802.11 extension with additional security features
802.1x	Specification of a port-based authentication mechanism from the IEEE
AES	Advanced Encryption Standard
Access point	Base station in a wireless LAN; independent LAN-WLAN bridge; connects stations of a LAN (local network) with a WLAN (wireless network) in a point-to-multipoint mode; connects two networks over a wireless network in point-to-point mode
Access router	Active network component for connection of a local network to the Internet or a company network
ADSL	Asymmetrical Digital Subscriber Line - transmission process for high-speed data transmission over normal telephone lines. With ADSL, transmissions (downstream) of up to 6 Mbps can be implemented over normal telephone lines; for bidirectional transmission there is a second frequency band with transmission speeds of up to 640 kbps (upstream) - hence the name "asymmetric".
Bandwidth	Data rate with which a user can surf the Internet; the higher the bandwidth, the faster the connection
Broadband	Service which provides high bandwidth; e.g.: DSL or WLAN
Bridge	Transport protocol-independent, transparent network component; transmits all packets which are identified as "not local" and only understands the difference between "local" and "remote". Works on Layer 2 of the OSI model
Broadcast	Broadcasts are packets to all stations of a local network; bridges transmit broadcasts; routers do not transmit broadcasts
BSS	Basic Service Set
CAPI	Common ISDN Application Programming Interface - CAPI is a standard for control of ISDN adapters
CCK	Code Complementary Keying; type of modulation used by DSSS
Client	Any computer equipped with a wireless LAN adapter (wireless LAN card), which uses services provided by other participants in the wireless network
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance; access procedure to the radio channel used under 802.11
CRC	Cyclic Redundancy Check; process for detecting bit errors
Data throughput	Speed at which you can surf on the Internet; depends on the bandwidth and the number of users
DHCP	Dynamic Host Configuration Protocol

DNS	Domain Name Service - computers communicate with computers in remote networks using IP addresses; DNS servers translate names into IP addresses; without DNS servers, you would have to remember all IP addresses and couldn't work with names (e.g. www.lancom.de)
Domain	area of network closed to outside; => Intranet
Download / Downstream	Download / downstream denotes the direction of dataflow in a WAN. Downstream is the direction from the head end or Internet to the participant connected to the network.
DS	Distribution System
DSL	Digital Subscriber Line - DSL procedures include all procedures for digital-broadband use of telephone lines, such as ADSL, HDSL, SDSL, VDSL and so on, which are also called xDSL.
DSSS	Direct Sequence Spread Spectrum; code multiplex -- band spreading process
Dynamic DNS	IPsec-VPN implementation which allows the transparent connection of local networks into a VPN solution, even when their routers work with dynamic addresses (dial-up)
EAP	Extensible Authentication Protocol
EAP-MD5	EAP variant which uses password for one-sided authentication
EAP-TLS	EAP Transport Layer Security; EAP variant which uses certificates for mutual authentication
EAP-TTLS	EAP Tunneled Transport Layer Security; EAP variant which uses certificates for mutual authentication
EIRP	Effective Isotropic Radiated Power
ESS	Extended Service Set
ESSID	Extended Service Set Identity; "network name" of the wireless LAN
Ethernet	Strand or star-formed physical transport medium; all stations can send simultaneously; collisions are detected and corrected through the network protocol
FHSS	Frequency Hopping Spread Spectrum; frequency skipping band spread procedure
Firewall	Protective mechanism for an Intranet against attacks from outside
Frequency	Number of oscillations per second (given in Hertz; 1 Hz = 1 oscillation per second; GHz = Gigahertz = 1 billion Hertz or oscillations per second)
FTP	File Transfer Protocol enables data transfer between different systems and simple file manipulation; FTP is based on the TCP transmission protocol
Frequency band	Contiguous frequency range which has the same transmission properties
Radio frequency	Every radio application uses globally regulated radio frequencies
Gateway	Network component which provides access to other network components on a layer of the => OSI model. Packets which do not go to a local partner are sent to the gateway. The gateway takes care of communication with remote networks.
Hub	Network component; distributor; collector; also used to translate from one connection type to another
HotSpot	Locally limited wireless network with a base station with Internet access; public wireless Internet access
IAPP roaming	Roaming between the cells of a wireless network using IAPP (Inter Access Point Protocol)
IBSS	Independent Basic Service Set

IDS	Intrusion Detection System -- earliest possible detection of attacks on the network
IEEE	Institute of Electrical and Electronics Engineers, New York - www.ieee.org
IP	Internet Protocol
IP masquerading	Combination of PAT (Port Address Translation) and NAT (Network Address Translation) from LANCOM Systems process used for connection of an intranet (multiple workstations) to the Internet over a single IP address; simultaneously, the internal computers are protected from attacks from outside
IPSec	Internet Protocol Security
IP Quality of Service	These functions give precedence to enterprise-critical applications, particular services, or user groups
ISDN	Integrated Services Digital Network -- fast connection; two independent channels; higher transmission rates than analog (up to 128 Kbit/s); uses the old analog lines; comfort features (call forwarding, callback on busy, etc.); supports both analog and digital services
ISM frequency band	Industrial-Scientific-Medical, license-free frequency bands which can be used for industrial, scientific, and medical purposes.
ISP	Internet Service Provider -- service provider with a connection to the Internet (backbone) who provides connection points for end customers
LCOS	LANCOM Operating System - uniform operating system for LANCOM products
LAN	Local Area Network - local network limited to one site
LANcapi	Virtual CAPI which is provided over the network; with LANcapi, which is implemented in all LANCOM routers with ISDN interfaces, a PC connected to the LAN can use ISDN telematic services
LANconfig	Software for configuration of LANCOM devices under Windows
LANtools	Diverse, user-friendly set of tools for the management and monitoring of LANCOM products and systems
MAC	Media Access Control; radio access protocol on ISO Layer 2 data link; it defines packet format, packet addressing, and error detection
MAC address	Serial number of a network component which is assigned by the manufacturer
Mbit	Megabit: standard unit for the specification of data quantities in the context of bandwidths
MIC	Message Integrity Check, cryptographic integrity protection mechanism
NetBIOS	Network Basic Input/Output System. Non-routable network protocol for local networks developed by IBM and later taken over by Microsoft.
NTBA	Network Termination Basic Adaptor . The NTBA (network termination adapter) is responsible in an ISDN base connection for the translation of the connection created by the telephone company to the S0 bus.
OFDM	Orthogonal Frequency Divison Multiplex
PEAP	Protected EAP, EAP variant for mutual authentication
PKI	Public Key Infrastructure
PPP	Point to Point Protocol: network protocol for connections between two computers. PPP is based on TCP/IP.
PPTP	Point to Point Tunneling Protocol: Network protocol for the construction of virtual private networks over the Internet.

Point-to-Multipoint (WLAN)	Multiple WLAN stations log into a base station and constitute a common network with the wired stations
Point-to-Point (WLAN)	Two base stations connect two wired networks over WLAN; point-to-point operation enables coupling of networks even across streets without cables
QoS	Quality of Service (see also IP Quality of Service)
RADIUS	Remote Authentication Dial-In User Service; authentication and monitoring protocol on the application level for authentication, integrity protection, and accounting for network access
RC4	Streaming cipher process by Ron Rivest, "Ron's Code"
RFC	Request for Comments
Router	Intelligent network components; comparable with a post office, which can determine from the logical destination address of a packet which next network component should transmit the packet; knows the overall topology of the network
SDSL	Single Line Digital Subscriber Line - downstream and upstream with 2.048 Mbit/s (two-strand wire)
Server	Computer which provides services over the network (e.g. files, news, email, WWW pages)
SINA	Secure Inter-Network Architecture
SMTP	Simple Mail Transfer Protocol - SMTP protocol is the Internet standard for distribution of electronic mail; the protocol is based on the TCP protocol
SNMPv3	Simple Network Management Protocol Version 3
SSID	Service Set Identity; “network name" of the wireless LAN
SSL	Secure Socket Layer
Splitter	The splitter is comparable with an audio frequency filter; in an ADSL connection, the splitter separates the ISDN signals from the DSL signals; the ISDN signals go to the NTBA and the DSL signals go to the DSL modem
Switch	A central distributor in a star-shaped network; each station has the entire bandwidth available; if a station fails, the rest of the network is not affected; is used for collision prevention; increases the overall throughput of the network; switches are cascadable
TAE	Telephone connection unit used in Germany. Plug for the connection of analog devices like a telephone or modem into the telephone network.
TCP/IP	Transmission Control Protocol/Internet Protocol; family of protocols (ARP, ICMP, IP, UDP, TCP, HTTP, FTP, TFTP) used mainly in the Internet, although it is making headway in intranets as well
TKIP	Temporal Key Integrity
TLS	Transport Layer Security
TPC	Transmission Power Control
Upload/Upstream	Upload / upstream denotes the direction of dataflow in a WAN; upstream is the direction from the node connected to the network to the head end/Internet
Chaining	Concatenation of bit sequences
VPN	Virtual Private Network - a VPN is a network consisting of virtual connections over which non-public or company internal data can be transmitted securely, even if public network infrastructures are used

WAN	Wide Area Network - network connection over long distances (e.g. over ISDN with a LANCOM router)
WECA	Wireless Ethernet Compatibility Alliance; alliance of manufacturers of wireless LAN components based on IEEE 802.11; renamed the WiFi Alliance
WEBconfig	Web-based configuration interface for LANCOM devices.
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity; marketing concept generated by the WECA
WiFi-Alliance	Alliance of manufacturers of wireless LAN components based on IEEE 802.11; formerly the WECA
WLAN	Wireless Local Area Network - local radio network
WPA	WiFi Protected Access; name for security mechanisms beyond IEEE 802.11; generated by the WiFi Alliance
WISP	Wireless Internet Service Provider
xDSL	xDSL stands for the family of Digital Subscriber Line technologies
XOR	Logical operation "exclusive OR"

18 Index

□

A Addendum to LCOS Version 6.20

A.1 Overview

This addendum describes the new functions within LCOS version 6.20 and the modifications since release 6.10:

A.2 Wireless LAN

A.2.1 Background WLAN scanning

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

Background scanning is mainly used for the following tasks:

- Rogue AP detection
- Fast roaming for WLAN clients

Rogue AP detection

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

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

Fast roaming for WLAN clients

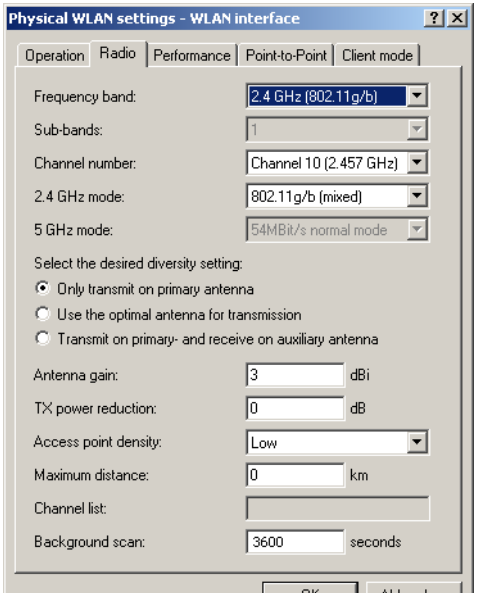
However, the background scanning method can be used for objectives other than rogue AP detection. A LANCOM Wireless Router in client mode that logs itself on to another access point can also use the roaming procedure in a mobile installation. This is the case, for example, when a LANCOM Wireless Router used in an industrial application scenario is mounted to a forklift that navigates its way through multiple warehouses with separate access points. Under normal circumstances, the WLAN client would only log on to another access point when the connection to the access point it had been using until that moment was lost. With the background scanning function, the LANCOM Wireless Router using the client mode can collect information about other available access points in advance. Then the client is not switched to another access point when the existing connection has been completely lost, but rather when another access point within its range has a stronger signal.

Evaluating the background scan

The information on the access points found can be viewed in the LANCOM Wireless Router statistics. The WLANmonitor presents the scan results quite conveniently and also offers additional functions such as access point grouping or automatic notification via e-mail whenever a new WLAN device appears.

Configuring the background scan

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



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

■ **Background scan interval [default: 0 seconds]**

If a value is entered here, the LANCOM Wireless Router searches the frequencies in the active band that are currently not in use in cycles within this interval in order to find available access points.

- The background scan function is usually deployed for rogue AP detection for the LANCOM Wireless Router in access point mode. Here, the scan interval should be adjusted to correspond to the time span in which unauthorized access points should be recognized, e.g. 1 hour.
- Conversely, for the LANCOM Wireless Router in client mode, the background scan function is generally used for improved mobile WLAN client roaming. In order to achieve fast roaming, the scan time is limited here, for example, to 120 seconds. Shorter scan intervals may result in noticeable losses in throughput on connections that are otherwise stable; for longer intervals, the support of fast roaming is limited.
- When the background scan time is '0' the background scanning function is deactivated.

Background scanning can be limited to a lower number of channels when indoor mode is activated. This allows roaming for the mobile LANCOM Wireless Router in client mode to be improved even further.

A.2.2 Rogue AP and rogue client detection with the WLANmonitor

WLAN devices that make unauthorized attempts at accessing a WLAN by posing as an access point or client are called rogues.

- Rogue clients are computers equipped with WLAN adapters that are located within the range of a WLAN and attempt to log on to one of the access points, for example, in order to use the Internet connection or in order to receive access to secured areas on the network.
- An example of rogue APs are access points that a company's employees connect to the network without the knowledge or permission of the system administrators, thereby consciously or unconsciously making the network vulnerable to potential attackers via unsecured WLAN access. Not quite as dangerous, but disruptive all the same are access points that belong to third-party networks yet are within the range of the local WLAN. If such devices also use the same SSID and channel as the local AP (default settings), then local clients could attempt to log on to external networks.

Unidentified access points within the range of the local network frequently pose a possible threat and security gap. At the very least they are a disturbance, and so they need to be identified to decide whether further measures in securing the local network need to be introduced. Information about the clients within range of your network is automatically stored to an internal table in the LANCOM Wireless Router. Once activated, background scanning records neighboring access points and records them to the scan table. WLANmonitor presents this information visually. The access points and clients found can be categorized in groups such as 'known', 'unknown' or 'rogue'.

Rogue AP detection

The WLANmonitor sorts all of the access points found into predefined subgroups under 'Rogue AP Detection' while displaying the following information:

- Time of first and last detection
- BSSID, the MAC addresse of the AP for this WLAN network
- Network name
- Type of encryption used
- Frequency band used
- Radio channel used
- Use of 108Mbps mode

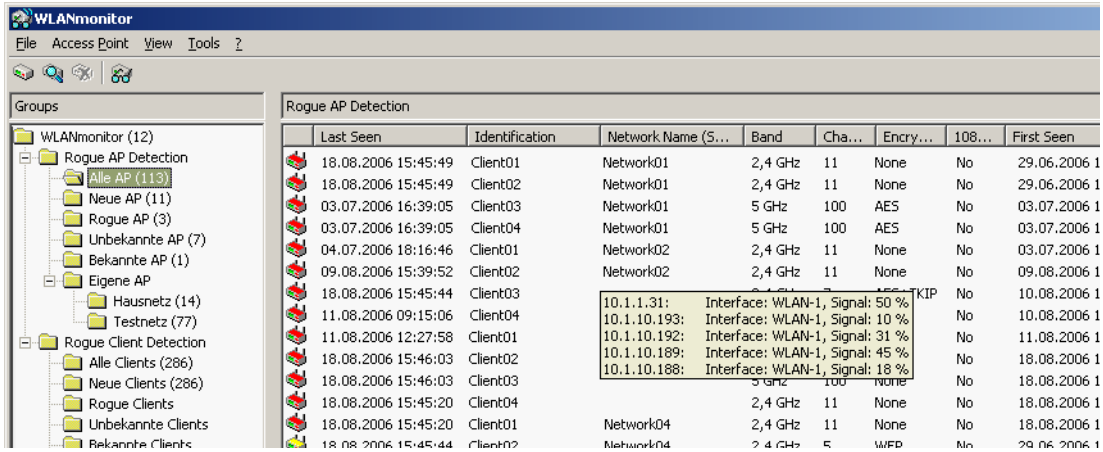
To use rogue AP detection, background scanning has to be activated in the LANCOM Wireless Router.

The WLANmonitor uses the following groups for sorting the APs that are found:

- All APs: List of all scanned WLAN networks grouped as follows

- New APs: New unknown and unconfigured WLAN networks are automatically grouped here (APs displayed in yellow)
- Rogue APs: WLAN networks identified as rogue and in need of urgent observation (APs displayed in red)
- Unknown APs: WLAN networks which are to be further analyzed (APs displayed in gray)
- Known APs: WLAN networks which are not a threat (APs displayed in gray)
- Own APs: New affiliated WLAN networks from access points monitored by WLANmonitor are automatically grouped here (APs displayed in green)

The WLANs that have been found can be placed into a corresponding group depending on their status. You can set up your own network groups within the individual groups by using the context menu (right mouse button) (except for the group 'All APs').



If a parameter is changed on an AP, e.g. the security settings, then it is displayed again as a newly discovered AP.

Rogue client detection

The WLANmonitor presents all of the clients found into predefined subgroups under 'Rogue Client Detection' while displaying the following information:

- Time of first and last detection
- MAC address of the client
- Network name

No configuration of the LANCOM Wireless Router is necessary to make use of rogue client detection.

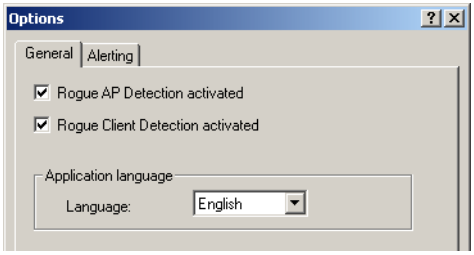
The WLANmonitor uses the following groups for sorting the clients that are found:

- All clients: List of all found clients grouped as follows (clients are colored according to their group)
- New clients: New unknown clients are automatically grouped here (clients displayed in yellow)
- Rogue clients: Clients identified as rogue and in need of urgent observation (clients displayed in red)
- Unknown clients: Clients which are to be further analyzed (clients displayed in gray)
- Known clients: Clients which are not a threat (clients displayed in gray)
- Own clients: New affiliated clients associated with access points monitored by WLAN monitor are automatically grouped here (APs displayed in green)

The clients that have been found can be placed into a corresponding group depending on their status. You can set up your own network groups within the individual groups by using the context menu (right mouse button) (except for the group 'All clients').

Activating rogue-AP and rogue-client detection

The functions for rogue-AP and rogue-client detection can be switched on or off in WLANmonitor.



Configuration tool	Call
WLANmonitor	Tools ▶ Options ▶ General

- **Rogue AP detection activated**

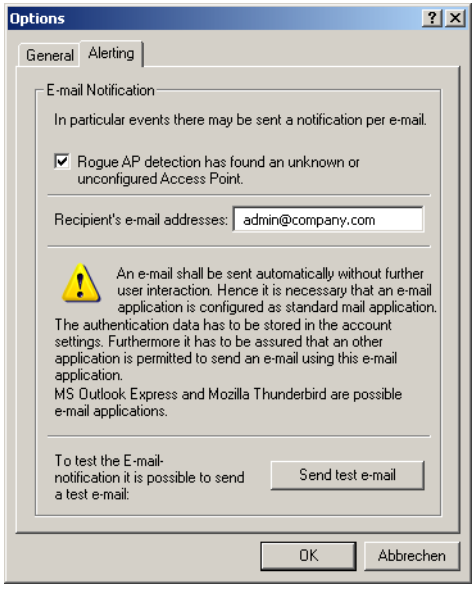
  Activate this option if WLANmonitor is to display unknown or unconfigured access points.

- **Rogue client detection activated**

  Activate this option if WLANmonitor is to display unknown or unconfigured clients.

Configuring the alert function in the WLANmonitor

The WLANmonitor can inform the administrator automatically via e-mail whenever an unknown or unconfigured access point is discovered.



Configuration tool	Call
WLANmonitor	Tools ▶ Options ▶ Alerts

- **E-mail messaging**

  Activate this option if you would like the WLANmonitor to report unknown or unconfigured access points via e-mail.

- **Recipient e-mail addresses**

  Enter the e-mail address(es) of the administrators here that should be informed in the event of rogue AP detection. Multiple e-mail addresses should be separated by commas.

In order to send e-mail alerts, the computer on which WLANmonitor is running requires a standard e-mail client (MS Outlook Express or Mozilla Thunderbird) that allows automatic mail transmission to be configured and running.

■ **Send a test e-mail**

Some mail clients require a confirmation from the user before sending via third-party applications. Test the alarm function with this button.

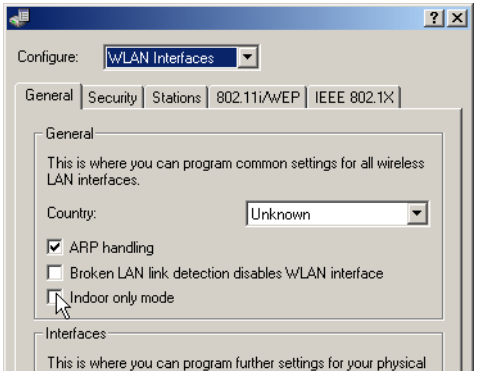
A.2.3 Indoor function for WLAN channels

When selecting the frequency band (2.4 or 5 GHz), among other things, you must determine the channels which may possibly be used for transmission. From these possible channels, under automatic channel selection, a LANCOM Wireless Router selects a free channel, for example, in order to avoid interference with other radio signals.

In some countries, there are special regulations on the frequency bands and channels which may be used for WLAN for indoor and outdoor operation. For example, in France, not all available channels in the 2.4 GHz band may be used in outdoor operation. In some countries the DFS procedure is required for outdoor operation in the 5 GHz band in order to avoid interference from radar systems.

Configuring the indoor-only option

With the option 'indoor-only' a LANCOM Wireless Router can be restricted exclusively to operation in closed buildings. This restriction on the other hand allows the channels to be managed more flexibly under automatic channel selection.



Configuration tool	Call
LANconfig	WLAN interfaces ▶ General
WEBconfig, Telnet	Expert configuration > Setup > WLAN

■ **Indoor-only [default: off]**

□ In the 5 GHz band in ETSI countries, the channel selection is limited to the channels 36, 40, 44 and 48 in the frequency range 5.15 to 5.25 GHz. At the same time, the DFS function is turned off and the mandatory interruption after 24 hours is no longer in effect. This restriction reduces the risk of interruption due to false radar detections.

□ In the 2.4 GHz band in France, the channels 8 to 13 are also permitted, although these channels are permitted solely for indoor operation.

Activating the indoor-only function can only be relied upon if the country in which the access point is being operated has been set.

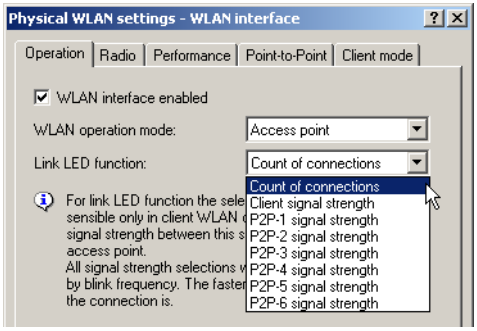
Activating the indoor-only function is only permitted when the access point and all connected clients are located in a closed space.

A.2.4 Signal-quality display via LEDs

When setting up point-to-point connections or operating the device as a WLAN client, the best possible positioning of the antennas is facilitated if the signal strength can be recognized at different positions. The WLAN link LED can be used for displaying the signal quality during the set-up phase. In the corresponding operation mode, the WLAN link LED blinks faster the better the reception quality in the respective antenna position is.

Configuration of WLAN link LED

When configuring the WLAN link LED, the operation mode in which the LED is to be used must be set.



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

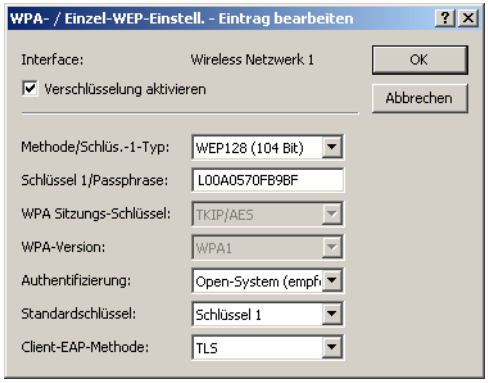
■ **Link LED function [default: number of connections]**

□ Number of connections: In this operation mode, the LED uses "inverse flashing" in order to display the number of WLAN clients that are logged on to this access point as clients. There is a short pause after the number of flashes for each client. Select this operation mode when you are operating the LANCOM Wireless Router in access point mode.

- □ Client signal strength: In this operation mode, this LED displays the signal strength of the access point with which the LANCOM Wireless Router has registered itself as a client. The faster the LED blinks, the better the signal. Select this operation mode only if you are operating the LANCOM Wireless Router in client mode.
- □ P2P1 to P2P6 signal strength: In this operation mode, the LED displays the signal strength of respective P2P partner with which the LANCOM Wireless Router forms a P2P path. The faster the LED blinks, the better the signal.

A.2.5 Authentication with EAP/802.1X for LANCOM Wireless Router in client mode

In WLAN client operation mode, the LANCOM Wireless Router can authenticate to another access point using EAP/802.1X. To activate the EAP/802.1X authentication in client mode, the client EAP method is selected as the encryption method for the first logical WLAN network.



Configuration tool	Call
LANconfig	Wireless LAN ▶ 802.11i/WEP ▶ WPA or private WEP settings ▶ Wireless network 1
WEBconfig, Telnet	Expert configuration > Setup > Interfaces > WLAN > Encryption > WLAN 1

■ **Client EAP method**

Select the desired client EAP method here. Please observe that the selected client EAP method must match the settings on the access point that the LANCOM Wireless Router is attempting to log onto. The following values are available:

- □ TLS
- □ TTLS/PAP
- □ TTLS/CHAP
- □ TTLS/MSCHAP
- □ TTLS/MSCHAPv2
- □ TTLS/MD5

□ PEAP/MSCHAPv2

In addition to setting the client EAP method, also be sure to observe the corresponding setting for the WLAN client operation mode!
The client EAP method setting has no function on logical WLAN networks other than WLAN 1.

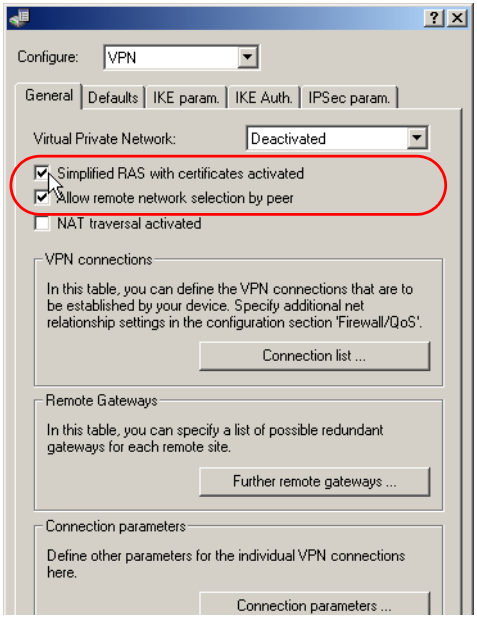
A.3 VPN

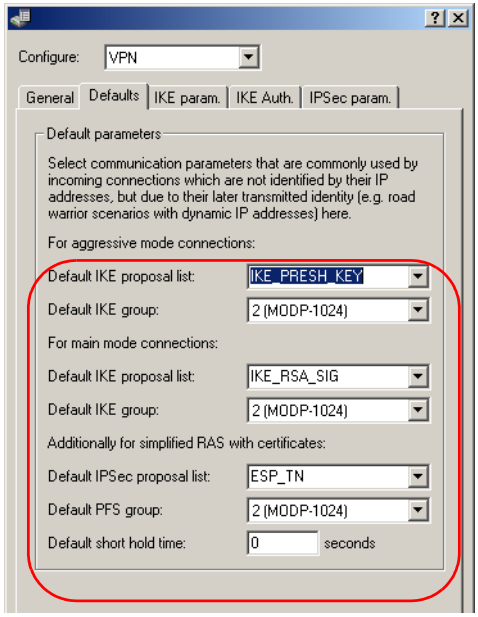
A.3.1 Simplified network connection with certificates – proadaptive VPN

In cases where large network infrastructures are coupled via VPN, it is advantageous for the costs and effort in configuring a new subnetwork to be limited to the local VPN router and that the central dial-in router configuration remains unchanged. In order to achieve this simplified network connection, the dial-in devices transmit their identity with the help of a digital certificate.

If simplified dial-in with certificates is activated for the LANCOM Router at the headquarters, then the remote routers can suggest a network to be used for the connection during the IKE negotiation in phase 2 This network is entered, for example, when setting up the VPN connection on the remote router. The LANCOM Router at the headquarters accepts the suggested network when the option 'Allow remote station to select the remote network' is activated. Moreover, the parameters used by the client during dial in must agree with the default values in the VPN router.

When configuring the dial-in remote stations, be sure to note that each remote station requests a specific network so that no network address conflicts arise.





Configuration tool	Call
LANconfig	VPN ▶ General and VPN ▶ General ▶ Defaults
WEBconfig, Telnet	Expert configuration > Setup > VPN

By activating the simplified RAS dial in, **all** remote routers that have a valid certificate signed by the publisher of the device's root certificate can dial in to the corresponding network. No further configuration of the router is necessary! Unwanted dial-in connections are then prevented exclusively by blocking the certificates and using a CRL.
The simplified connection of networks with certificates is therefore limited to LANCOM Router models that support certificate revocation lists (CRL).

A.3.2 Request certificates using CERTREQ

During IPSec negotiations authenticated with the use of RSA signatures, some VPN gateways expect the remote station to request the certificates to be exchanged via a "certificate request" (CERTREQ). Among other things, this allows the gateway to select the certificate to be used providing that the gateway trusts more than one CA.

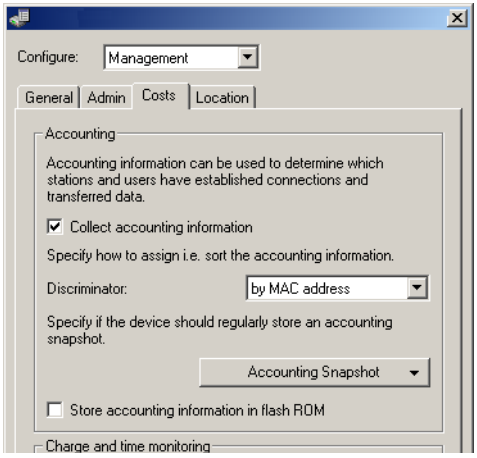
In order to establish a connection to these VPN gateways, the LANCOM VPN Router sends a corresponding CERTREQ when the connection is initiated. This is received by the publisher of the root certificate stored in the LANCOM.

A.3.3 Targeted VPN accounting with intermediate storage

Information on connections between clients in the local network and various remote stations is saved in the accounting table with entries for the connection time and the transferred data volume. Using accounting snapshots, accounting data can be regularly saved at specific times for later evaluation.

Configuring accounting

When configuring accounting, the general parameters must be defined:



Configuration tool	Call
LANconfig	Management ▶ Costs
WEBconfig, Telnet	Expert configuration > Setup > Accounting

- **Collect accounting information**
  - Turn accounting on or off.
- **Store accounting information in flash ROM**
  - Turn accounting data in flash memory on or off. Accounting data saved to flash will not be lost in the event of a power outage.
- **Discriminator**

  Selection of the feature according to which the accounting data are to be gathered:
  - MAC address: The data are collected according to the client's MAC address.
  - IP address: The data are collected according to the client's IP address.

When varying IP addresses are in use, e.g. when using a DHCP server, the option 'IP address' can lead to inaccurate accounting data. In this case, it may not be possible to accurately assign the data to users.

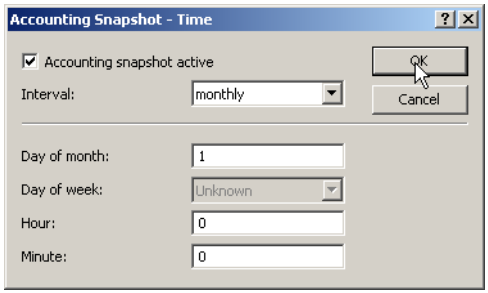
Conversely, with this setting, data can be separated from clients that are behind another router and therefore appear with the same MAC address as the router in the accounting list.

■ **Sort according to**

Select here whether the data should be sorted in the accounting table according to connection times or data volume.

Snapshot configuration

When configuring the snapshot, the interval is set in which the accounting data are temporarily saved into a snapshot:



Configuration tool	Call
LANconfig	Management ▶ Costs ▶ Accounting Snapshot
WEBconfig, Telnet	Expert configuration > Setup > Accounting > Time snapshot

The snapshot function can only be used when the device is set with the correct system time.

■ **Accounting snapshot active**

□ Turn intermediate storage of accounting data on or off.

■ **Interval**

□ Daily, weekly or monthly

■ **Day of month**

The day of the month on which caching will take place: Only relevant if the interval is 'monthly'.

■ **Day of week**

The weekday on which caching will take place. Only relevant if the interval is 'weekly'.

■ **Hour**

The hour on which caching will take place:

□ '0' to '23'

■ **Minute**

The minute in which caching will take place:

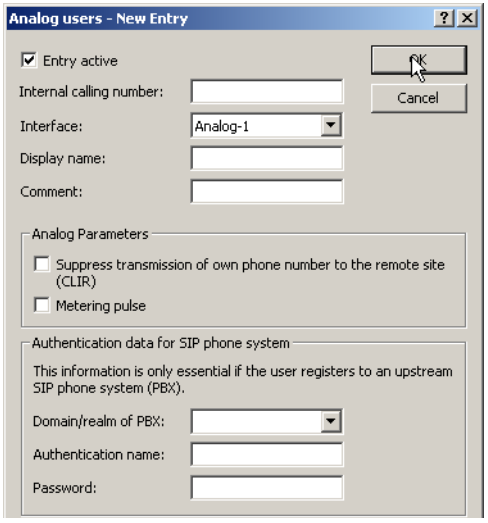
□ '0' to '59'

A.4 VoIP

A.4.1 Analog lines and users

Some LANCOM VoIP Routers are equipped with interfaces for connection to analog exchange lines and for connecting analog terminal equipment. To use these over VoIP, analog users and analog lines can be set up.

Configuring analog users



■ **Internal telephone number**

Internal number of the analog telephone or name of the user (SIP URL).

■ **Display name**

Name for display on the telephone being called.

■ **Interface**

Analog interface that should be used to establish the connection.

■ **Hide your telephone number from the person being called (CLIR)**

This option stops your own number from being transmitted to the remote station.

- **Metering pulse**

  The metering pulse is used in analog telephone networks to inform callers of the costs of their calls. With appropriate terminal equipment (e.g. telephone with charge display), the metering pulse is filtered out from the overall signal and this information is converted to display the call charge.

  This option allows the metering pulse to be passed on to the analog user/equipment. It is possible for charge information from the ISDN telephone network to be transferred to an ISDN line and converted into an analog metering pulse.

- **Domain/realm**

  Domain of the upstream SIP PBX.

  Only required when the user registers at an upstream SIP PBX.

- **Authentication name**

  Name for the authentication during registration to the SIP proxy.

  Only required when the user registers at an upstream SIP PBX.

- **Password**

  User password.

  Only required when the user registers at an upstream SIP PBX.

- **Entry active**

  User is active / not active

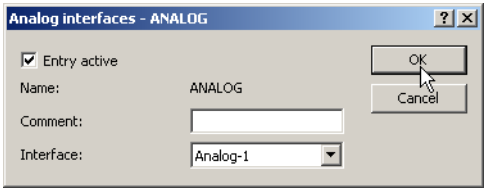
- **Comment**

  Comment on the user

Configuration tool	Call
LANconfig	Voice Call Manager ▶ User ▶ Analog User
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > User > Analog User

Configuring internal analog interfaces

The internal analog interfaces (a/b ports) require configuration if they are to be used by local users (connection of terminal equipment).



- **Interface**

  An internal interface to which the analog subscribers are connected.

- **Entry active**

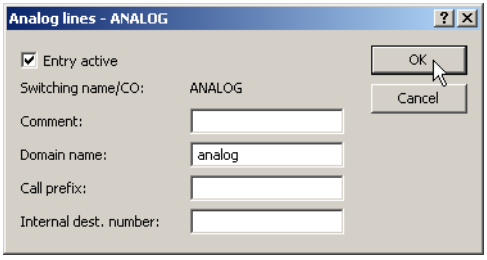
  Interface is active / not active.

- **Comment**

  Comment about analog interface

Configuration tool	Call
LANconfig	Voice Call Manager ▶ User ▶ Analog interfaces
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > User > Analog User > Interfaces

Configuring analog lines



- **Switching name/CO**

  Name of the line; may not be identical to another line that is configured in the device.

- **Domain name**

  Domain in which the calls from/to the analog line are managed in LANCOM's SIP world.

- **Call prefix**

  With incoming calls using this line, this prefix is placed in front of the calling number so that the correct line is automatically selected for a return call.

■ **Internal destination number**

Incoming calls on this line are transferred to the call router with this destination number. The call router switches this call either in accordance with the call-routing table or to an internal user with this internal number.

■ **Entry active**

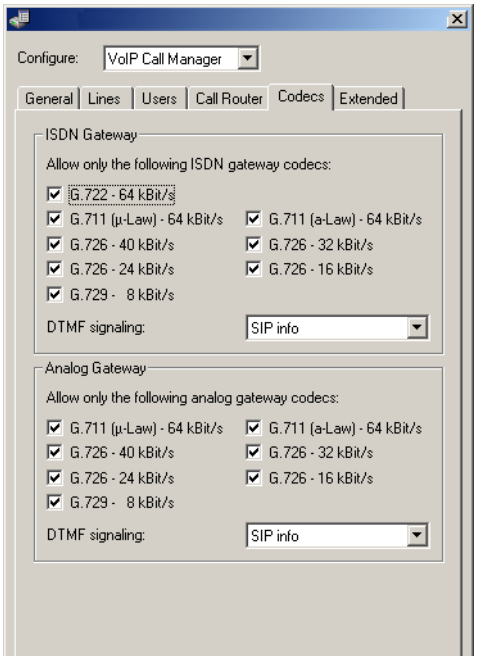
Line is active / not active.

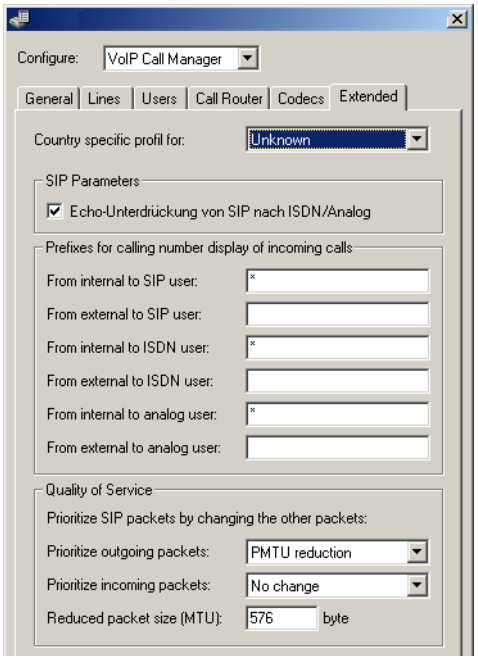
■ **Comment**

Comment on the line

Configuration tool	Call
LANconfig	Voice Call Manager ▶ User ▶ Lines ▶ Analog lines
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > Line > Analog > Interfaces

Configuring the advanced analog settings





Configuration tool	Call
LANconfig	Voice Call Manager ▶ Gateways
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > General

■ **Analog gateway codecs**

The VoIP Call Manager offers the codecs activated here when negotiating calls to/from SIP remote stations.

■ **Prefix from external to analog user**

This prefix is added to the calling party ID, if available, for an incoming, **external** call if the call is directed to a analog user.

Configuration tool	Call
LANconfig	Voice Call Manager ▶ Extended
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > Analog User

- **Prefix from internal to analog user**

  This prefix is added to the calling party ID, if available, for an incoming, **internal** call if the call is directed to a analog user.

Configuration tool	Call
LANconfig	Voice Call Manager ▶ Extended
WEBconfig, Telnet etc.	Expert Configuration > Setup > Voice Call Manager > Analog User

A.4.2 Call hold, transfer call, connect call

LANCOM VoIP Routers support various services which are familiar to users of the ISDN network:

- With **call hold** the user can place an active call into a wait state. In this state, the user can for example make a call to another person.
- With **transfer call**, the user can switch to and fro between two connections. The user is only connected with one caller at a time, while the other caller is put on hold.
- With **connect call** the user switches an active call over to another call which is on hold. The two callers are then connected and the user is no longer involved in the call.

The services call hold, transfer call and connect call are available to all local SIP, ISDN and analog users, and also to subscribers at an upstream SIP PBX; however, they can only be initiated by a SIP user.

A.4.3 New voice transmission codecs

Along with the codecs supported for the SIP gateway function to date, LANCOM VoIP Routers now additionally support the following:

- G.722 - 64 kbps (high-quality codec for ISDN to SIP an vice versa only)
- G.729 - 8 kbps (codec with higher compression for lower bandwidths)

These codecs are available to the devices LANCOM 1722 VoIP, LANCOM 1723 VoIP, LANCOM 1724 VoIP and LANCOM 1823 VoIP, and also for all LANCOM models with the LANCOM Advanced VoIP Option.

A.4.4 Transfer of DTMF tones

ISDN telephone networks introduced the possibility of transmitting information on which button was pushed on the telephone using DTMF tones (Dual Tone Multiple Frequency). With the help of DTMF tones, the telephone user can communicate with voice mailboxes and computer telephony systems, for example.

In VoIP applications, special mechanisms are required to assume the DTMF tone function. If, for example, during a telephone call, a button is pressed on a VoIP telephone or a VoIP softphone, this should trigger the same action as a call with an ISDN telephone.

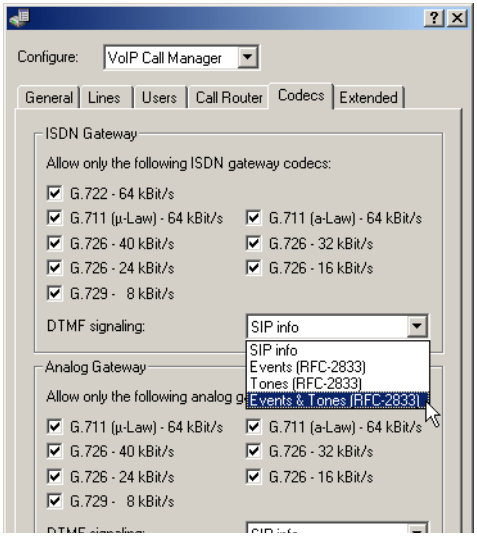
Generally, DTMF tones are transmitted in VoIP applications in one of two ways:

- In-band describes the transmission of the DTMF tones in the same data stream in which the voice data are transferred. However, this procedure is relatively unreliable because the DTMF tones in the IP datastream can easily be mistaken for voice data, particularly when using compression codecs.
- Out-of-band describes the transmission of the DTMF tones in a stream that runs parallel to the actual voice data. Two standards are generally used for out-of-band transmission:
  - SIP INFO (RFC 2976)
  - RC 2833 (RTP payload for DTMF digits)

  Both variations can wrap information, e.g. on buttons pressed, their tone frequency and the length of time the button was pressed into the signaling datastream. In addition, events that should be transmitted with DTMF tones can also be transmitted in cleartext in the SIP data.

DTMF signaling configuration

When configuring DTMF signaling, the type of transmission to be used for the DTMF tones must be set:



Configuration tool	Call
LANconfig	VoIP Call Manager ▶ Extended
WEBconfig, Telnet	Expert Configuration > Setup > Voice Call Manager > General

- **DTMF signaling**
  - SIP info: Transmits the DTMF tones according to the SIP info standard
  - Events (RFC 2833): Transmits the events in cleartext according to the RFC 2833 standard

- □ Tones (RFC 2833): Transmits the tones according to the RFC 2833 standard
- □ Events&tones (RFC 2833): Transmits the events in cleartext and tones according to the RFC 2833 standard

The DTMF signaling settings must match the SIP provider requirements. Defective DTMF signaling settings could make it impossible to establish a connection via the SIP provider.

A.4.5 Transfer toll information to the internal ISDN buses

LANCOM VoIP Routers support two variants of the AOC (Advice Of Charge) service:

- AOC-D refers to the transmission of charge information during the call.
- AOC-E refers to the transmission of charge information at the end of the call.

LANCOM VoIP Routers transmit charge information from both types of AOC service between internal and external busses. AOC-D charge information can be converted into a metering pulse for analog users at the internal analog interfaces if the corresponding option has been activated.

A.4.6 Bandwidth demand of VoIP codecs

The following table is an overview of bit rates for various VoIP codecs for voice connections over VPN:

VoIP codec	Packets/s	Voice payload		IP payload		IPSec payload	
		kbps	Bytes	kbps	Bytes	kbps	Bytes
G.729 30ms	33,3	8	30	32	70	36	136
G.726 30ms	33,3	32	120	42,7	160	62	232
G.711 30ms	33,3	64	240	74,7	280	92	344
G.711 20ms	50	64	160	80,0	200	106	264
G.722 20ms	50	64	160	80,0	200	106	264

- IP payload: Voice payload + 40 byte header (12 byte RTP; 8 byte UDP; 20 byte IP header)
- IPSec payload: IP paket + padding + 2 byte (padding length & next header) = multiple of the IPSec initialization vector

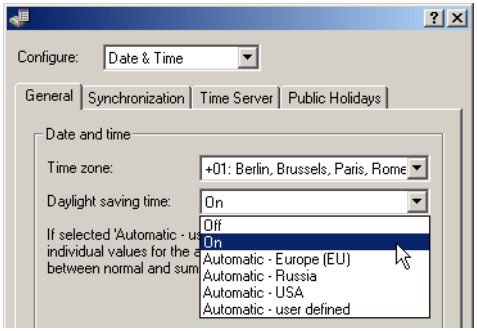
For further information on bandwidth requirements for Voice over IP with IPSec is available in the LANCOM techpaper Performance Analysis of LANCOM Routers.

A.5 Management

A.5.1 Time change according to UTC

Configuring daylight-saving time change

LANCOM devices work internally with the coordinated world time (UTC). For protocol displays and time-related settings (e.g. cron jobs), the local time is taken as calculated from the defined time zone. To take local daylight-saving time into account, settings can be configured according to requirements.



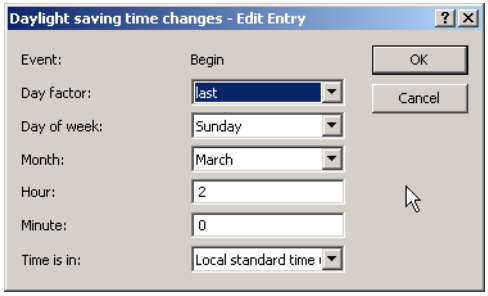
Configuration tool	Call
LANconfig	Date & time ▶ General
WEBconfig, Telnet	Expert configuration > Setup > Time > Daylight-saving time

■ **Daylight-saving time**

- □ Off: The system time will not be adjusted to daylight-saving time.
- □ On: As long as this option is enabled, one hour is added statically to the current system time (comprised of UTC and time zone).
- □ Automatic (EU, USA, Russia): In this setting, the daylight-saving time change is performed automatically in conformance with the time zone of the device's location.
- □ Automatic (user-defined): If the device is located in an area that is not listed here, then the daylight-saving time change options can be manually defined by the user.

User-defined daylight-saving time change

User-defined values can be set for the beginning and the end of the automatic daylight-saving time change.



Configuration tool	Call
LANconfig	Date & time ▶ General ▶ Daylight-saving time
WEBconfig, Telnet	Expert configuration > Setup > Time > DST clock changes

- **Index**
  - First, second, third, fourth, last, second to last, third to last, fourth to last: The time change will take place on this recurring day of the month.
- **Day of week**
  - Monday to Sunday: The day on which the change will take place.
- **Month**
  - January to December: The month on which the change will take place.
- **Hour**
  - 0 to 23: The hour in which the change will take place.
- **Minute**
  - 0 to 59: The minute in which the change will take place.
- **Time type**
  - Local standard time or UTC: Defines the time zone the data refers to.

In the last hour of daylight-saving time or the first hour that follows in standard time, it is possible for time entries to be ambiguous. If the time is acquired via ISDN or set manually during this time, then it is always assumed that the time entry is in daylight-saving time.

A.5.2 SSH authentication

The SSH protocol generally allows two different authentication mechanisms:

- With user name and password

■ With the help of a public key

In the public key method, a key pair is used that is made up of a private and public key – a digital certificate. Detailed information about the keys mentioned here can be found under the section 'Digital certificates' in the chapter on VPN in the reference manual. The private part of the key pair is saved on the client (frequently protected with a password), the public part is loaded into the LANCOM Router.

The LANCOM Router supports both RSA and DSS/DSA keys. RSA keys are somewhat smaller, thereby allowing somewhat faster operation.

Generating key pairs

The pairs consisting of public and private keys can be generated with the help of OpenSource software OpenSSH, for example. The following command from a Linux operating system creates a key pair from the public part '`id_rsa.pub`' and the private part '`id_rsa`':

```
ssh-keygen -t rsa
```

Entering users into the public key

The public keys are generated in the following syntax:

```
<Encryption algorithm> <Public key> <User> [Further users]
```

In order to grant access to additional users with this key, the respective user names are simply attached to the existing key file.

Installing the private key on the SSH client

The private part of the key must be installed on the SSH client. Refer to the documentation for information on the steps required for your SSH client.

Load public key into the LANCOM Router

The public key(s) can be uploaded to the LANCOM Router using WEBconfig. For this, select the entry **Upload certificate or file** on the WEBconfig start page. In the following dialog, select the type of key ('SSH RSA key' or 'SSH DSA key'), select the file and enter the password if required. Entering the Upload command initiates the transfer to LANCOM.

Configuring the authentication methods

The authentication methods permitted for SSH access can be set separately for LAN, WAN and WLAN.

Configuration tool	Call
WEBconfig, Telnet	Expert configuration > Setup > Config > SSH authentication methods

■ **Methods**

□ All: Allows authentication using password and digital certificate.

- □ Password: Allows authentication with a password.
- □ Public key: Only allows authentication with a digital certificate.

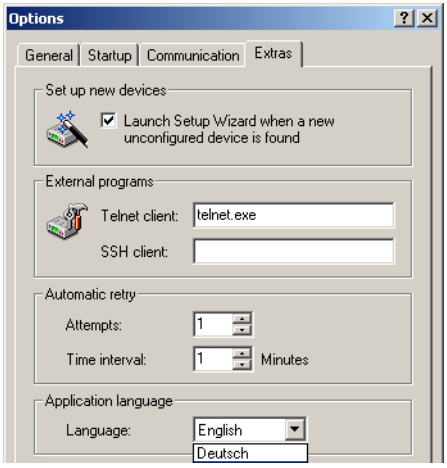
Certificate check on SSH access

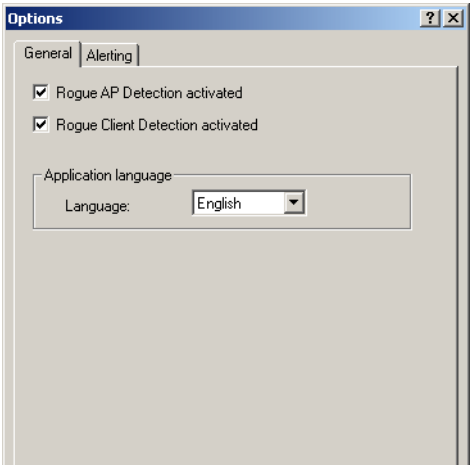
When establishing the SSH connection, the client first asks the LANCOM Router which authentication methods are permitted for this connection. If the public key method is allowed, the client searches for private keys that have been installed and transfers these with the user name to the LANCOM Router. When the LANCOM Router finds an entry in the list that includes the user name that corresponds to its public SSH key, the SSH connection is permitted. If the client does not have a suitable private key installed or if the LANCOM Router does not have a corresponding entry with the user name or public key, the SSH client can revert to authentication with user name/password – as long as this authentication method is permitted.

A.6 Extensions in LANconfig, LANmonitor and WLANmonitor

A.6.1 Graphical user interface language switchable

The language for the LANconfig, LANmonitor or WLANmonitor graphical user interface can be set to 'German' or 'English'.





Configuration tool	Call
LANconfig	Tools ▶ Options ▶ Extras
LANmonitor and WLANmonitor	Tools ▶ Options ▶ General

A.6.2 Download script from device

Installations with multiple LANCOM devices often profit from the automatic execution of certain configuration tasks. The scripting function in LANCOM enables entire sets of commands for device configuration to be stored in a single file—a script—for transfer to one or more devices in one step.

Detailed information about scripting can be found under the section 'scripting' in the chapter on Network Management with LANtools in the reference manual.

In addition to manually setting a script and console read-outs, script files can also be read out from a device with the help of LANconfig. For this, right click on the corresponding entry in the device list and select the entry **Configuration management ▶ Save script to file** from the context menu. Select the following options here:

- **Numeric sections**

  Enable this option if you do not want the configuration sections in the script to be displayed in cleartext (e.g. `/setup/wlan/ppp`), but numerically (`/2/2/5`).

- **Default parameters**

  Unless defined otherwise, the only parameters saved in a script are those that deviate from the default values. Enable this option if the standard values should also be entered into the script.

- **Column names**

  Unless defined otherwise, the fields of a table are initially entered as column names in the scripts and, thereafter, only the respective values are inserted into the rows. Enable this option when every value in the table should explicitly receive the description of the column in which it is inserted.

- **Comments**

  Activate this option when additional comments should be included in the script file.

- **Compact formatting**

  □ Enable this option if spaces and tabs should be suppressed.

- **Download only selected sections**

  Without further entries, the entire device configuration will always be saved in the script. In contrast, entering the sections also makes it possible to save partial configurations. Enter the sections to which the script should be transferred into this field, e.g. `/setup/wlan`.

A.6.3 WLAN functions reorganized

The configuration parameters for the WLAN area under LANconfig were reorganized with the release of the LCOS Version 6.20:

- All parameters that were formerly located under the 'Wireless LAN' tab in the configuration area 'Interfaces' are now under the 'General' tab on the 'WLAN Interfaces' tab.
- The parameters that were located under 'WLAN Security' on the 'General' and 'Protocols' tabs are now located under the 'Security' tab on the 'WLAN Interfaces' tab.

- The parameters for the 'Stations', '802.11i/WEP' and 'IEEE 802.1X' tabs have also been moved to the configuration area 'WLAN Interfaces'.

These changes have no effect on the configuration paths via WEBconfig or console access (Telnet, SSH, etc.).

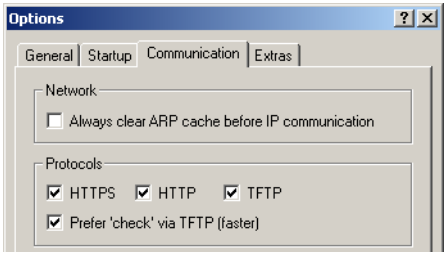
A.6.4 Device-specific settings for communications protocols

With LANconfig, all device actions are conducted using the TFTP protocol. Since this protocol has disadvantages compared to other protocols when transmitting large volumes of data, the protocols HTTPS and HTTP can also be used as alternatives.

The use of the protocols can be set either globally for all devices managed by a LANconfig or specifically for each individual device. The global settings overwrite the specific settings here – therefore, in the specific device settings, only the settings allowed in the global configuration can take effect.

Configuration of the global communication settings

When setting up the communications protocols, one must differentiate between the protocol that is used solely for checking the device and for other operations such as a firmware upload, etc.:



Configuration tool	Call
LANconfig	Tools ▶ Options ▶ Communication

- **HTTPS, HTTP, TFPT**

  When this is selected, the individual protocols are enabled for the operations firmware upload, configuration up/download, and script up/download. In these operations, LANconfig attempts to use these protocols in the order HTTPS, HTTP and TFTP. If the transfer fails when using a selected protocol, then the next protocol is automatically attempted.

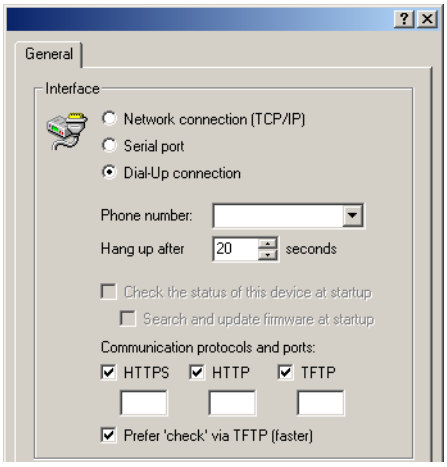
- **Prefer checks via TFTP**

  When checking the devices, only small amounts of data are transferred with the system information. As such, device checks could be performed using the TFTP protocol, particularly in the LAN. When this option is activated, the TFTP protocol is used to check the device first, regardless of the previously set communications protocols. If the check via TFTP fails, then the protocols HTTPS, HTTP and TFTP are attempted in that order.

The device-specific settings are subordinate to the global communications settings. This allows, for example, the use of a protocol to be restricted centrally.

Configuration of the specific communication settings

For configuring the specific communications settings, the properties dialog of a device is opened via the context menu (right-click on mouse):



- **HTTPS, HTTP, TFPT**

  Select the communications protocols as described in the global settings:

  In the fields under the protocols, the port to be used can be entered using the following default values:

  - HTTPS: 443
  - HTTP: 80
  - TFTP: 69

- **Prefer checks via TFTP**

  Preferred checking via TFTP as described in the global settings.

For all specific communications settings, the global settings are considered to be superordinate. A protocol can therefore only be used for operating a device when it is also activated in the global settings.

A.7 Overview of functions by model and LCOS* version

	800/1000/1100	I-10 HW-Rv. A	I-10 HW-Rv. C	DSL/I-10+	800+	821	821+	1511	1521
Interfaces									
ADSL modem						✔	✔		✔
ADSL 2+							5.20		ADSL 2
VLAN								3.30	✔
DMZ port				5.20	5.20	1)	5.20	5.20	5.20
Switch ports				3	4	4	4	4	4
Ethernet port mapping				5.00			✔	5.00	5.00
DSLoL						3.10			
Security									
Stateful Inspection, DoS, IDS	2.80	2.80	2.80	✔	✔	2.80	✔	✔	✔
IP QoS, Traffic Shaping	3.30	3.30	3.30	✔	✔	3.30	✔	3.30	✔
SSH configuration access				✔	✔	4.00	✔	4.00	4.00
ISDN-based anti-theft device				5.00	5.00	5.00	✔	5.00	5.00
Management									
Rights management for admins				✔	✔	4.00	✔	4.00	4.00
Multiple loopback addresses				✔	✔	4.00	✔	4.00	4.00
Modem operation at serial interface				4.10	4.10	4.10	✔	4.10	4.10
Scripting				5.00	5.00	5.00	✔	5.00	5.00
CRON	3.10	3.10	3.10	✔	✔	3.10	✔	✔	✔
Port sniffer				5.00	5.00		✔	5.00	5.00
Other functions									
DHCP auto client mode	3.42	3.42	3.42	✔	✔	3.42	✔	3.42	3.42
N:N mapping				4.10	4.10	4.10	✔	✔	4.10
Dynamic DNS	3.10	3.10	3.10	✔	✔	3.10	✔	✔	✔
Free port mapping				✔	✔	4.00	✔	4.00	4.00
Multi-PPPoE				✔		4.00	✔	4.00	4.00
Load balancing (4 channels)				2 5.00		2 5.00	4	2 5.00	2 5.00
Policy-based routing				5.00	5.00	5.00	✔	5.00	5.00
VRRP				5.20	5.20	5.20	5.20	5.20	5.20
PPPoE servers				5.20	5.20	5.20	5.20	5.20	5.20
WAN RIP				5.20	5.20	5.20	5.20	5.20	5.20
Spanning Tree Protocol								5.20	5.20
Layer 2 QoS tagging							6.10	6.10	6.10

	800/1000/1100	I-10 HW-Rv. A	I-10 HW-Rv. C	DSL/I-10+	800+	821	821+	1511	1521
VPN functions									
AES, 3-DES, DES, Blowfish, CAST									
VPN-5 option available									
VPN-25 option available									
VPN hardware acceleration									
VPN-100									
VPN-200									
Digital certificates (X.509) incl. PKCS #12									
Certificate revocation list - CRL									
Simplified RAS with certificates									
AES 256 / IPCOMP									
Redundant VPN gateways									
NAT Traversal (NAT-T)									
IKE config mode									
WLAN functions									
WLAN-802.11b								✔	✔
WLAN-802.11g								✔	✔
WLAN-802.11a (incl. turbo mode)									
LEPS								4.00	4.00
Multi-SSID, IP-redirect								3.42	3.42
Super A/G								3.42	3.42
Standard WEP encryption								4.00	4.00
802.11i with HW-AES								3.50	3.50
802.11i for P2P in WLAN								4.00	4.00
WLANmonitor								5.00	5.00
Group configuration								5.00	5.00
Fully transparent client bridge mode								5.00	5.00
Bandwidth limitations in the WLAN								5.20	5.20
QoS for WLAN (IEEE 802.11e, WMM/WME)								6.10	6.10
RADIUS server								6.10	6.10
VoIP functions (detailed information about your device's VoIP functions can be found in the user manual)									
SIP users				4 [7)]			4 [7)]	4 [7)]	4 [7)]
ISDN users				40			40	40	40
SIP lines				16			16	16	16
Lines to SIP PBXs				4			4	4	4
External ISDN busses for VoIP				1			1	1	1
Internal ISDN busses for VoIP									
Analog exchange line connections									
Connectors for analog terminal equipment									

□ *Overview of functions by model and LCOS* version*

	800/1000/1100	I-10 HW-Rv. A	I-10 HW-Rv. C	DSL/I-10+	800+	821	821+	1511	1521
Software options									
ISDN leased line option	Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10
Public spot option								✔	✔
Fax modem option	✔	✔							
UMTS/VPN option									

* The numbers in the table indicate the LCOS version in which the function was implemented

[1] Port separation (private mode)

[2] Only if the VPN options have been activated for the device

[3] No Multi-SSID with 11-Mbit WLAN cards

[4] Optional VPN-500 and VPN-1000 available

[5] Compatible with ADSL and ADSL2

[6] 3050; only with external MC-54 card

[7] depending on VoIP option (Basic/Advanced)

	1611	1611+	1620	1621	1711	1721	1722	1723	1724
Interfaces									
ADSL modem			✔	✔		✔	✔	✔	✔
ADSL 2+			✔			✔	✔	✔	✔
VLAN		6.10	6.10		6.10	6.10	6.10	✔	✔
DMZ port		5.20	✔	1)	5.20	5.20	✔	✔	✔
Switch ports		4	4	4	4	4	4	2	2
Ethernet port mapping		✔	✔		5.00	✔	✔	✔	✔
DSLoL				3.10					
Security									
Stateful Inspection, DoS, IDS	2.80	✔	✔	2.80	✔	✔	✔	✔	✔
IP QoS, Traffic Shaping	3.30	✔	✔	3.30	✔	✔	✔	✔	✔
SSH configuration access	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔
ISDN-based anti-theft device	5.00	✔		5.00	5.00	✔	✔	✔	✔
Management									
Rights management for admins	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔
Multiple loopback addresses	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔
Modem operation at serial interface	4.10	4.10	✔	4.10	4.10	✔	✔	✔	✔
Scripting	5.00	✔	✔	5.00	5.00	✔	✔	✔	✔
CRON	3.10	✔	✔	3.10	✔	✔	✔	✔	✔
Port sniffer		✔	✔		5.00	✔	✔	✔	✔
Other functions									
DHCP auto client mode	3.42	3.42	✔	3.42	3.42	✔	✔	✔	✔
N:N mapping	3.30	✔	✔	3.30	✔	✔	✔	✔	✔
Dynamic DNS	3.10	✔	✔	3.10	✔	✔	✔	✔	✔
Free port mapping	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔
Multi-PPPoE	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔
Load balancing		4	2	2 5.00	4 channels 5.00	4 channels	4 channels	2 channels	2 channels
Policy-based routing	5.00	✔	✔	5.00	5.00	✔	✔	✔	✔
VRRP	5.20	5.20	✔	5.20	5.20	✔	✔	✔	✔
PPPoE servers	5.20	5.20	✔	5.20	5.20	✔	✔	✔	✔
WAN RIP	5.20	5.20	✔	5.20	5.20	✔	✔	✔	✔
Spanning Tree Protocol									
Layer 2 QoS tagging		6.10	6.10		6.10	6.10	6.10	✔	✔

□ Overview of functions by model and LCOS* version

	1611	1611+	1620	1621	1711	1721	1722	1723	1724
VPN functions									
AES, 3-DES, DES, Blowfish, CAST	3.32	✔	✔	3.32	✔	✔	✔	✔	✔
VPN-5 option available	Integrated from 3.32	Integr.	Integrated	Integrated from 3.32	Integrated	Integrated	Integrated	Integrated	Integrated
VPN-25 option available	✔	✔	✔	✔	✔	✔	✔	✔	✔
VPN hardware acceleration					with VPN-25	with VPN-25	with VPN-25	with VPN-25	with VPN-25
VPN-100									
VPN-200									
Digitale certificates (X.509) incl. PKCS #12	5.00	✔	✔	5.00	5.00	✔	✔	✔	✔
Certificate revocation list - CRL					6.10	6.10	6.10	✔	✔
Simplified RAS with certificates					6.20	6.20	6.20	6.20	6.20
AES 256 / IPCOMP	5.00	✔	✔	5.00	5.00	✔	✔	✔	✔
Redundant VPN gateways	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔
NAT Traversal (NAT-T)	5.20	5.20	✔	5.20	5.20	✔	✔	✔	✔
IKE config mode	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔
WLAN functions									
WLAN-802.11b									
WLAN-802.11g									
WLAN-802.11a (incl. turbo mode)									
LEPS									
Multi-SSID, IP-redirect									
Super A/G									
Standard WEP encryption									
802.11i with HW-AES									
802.11i for P2P in WLAN									
WLANmonitor									
Group configuration									
Fully transparent client bridge mode									
Bandwidth limitations in the WLAN									
QoS for WLAN (IEEE 802.11e, WMM/WME)									
RADIUS server									
VoIP functions (detailed information about your device's VoIP functions can be found in the user manual)									
SIP users		4 [7)]			4/32 [7)]	4/32 [7)]	32	32	32
ISDN users		40			40	40	40	40	40
SIP lines		16			16	16	16	16	16
Lines to SIP PBXs		4			4	4	4	4	4
External ISDN busses for VoIP		1			1	1	0-2	0-1	0-4
Internal ISDN busses for VoIP							0-2	0-2	0-4
Analog exchange line connections								1	

	1611	1611+	1620	1621	1711	1721	1722	1723	1724
Connectors for analog terminal equipment							0-2	2	0-4
Software options									
ISDN leased line option	Integr. as of 6.10	Integr. as of 6.10		Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10	Integr.	Integr.
Public spot option									
Fax modem option									
UMTS/VPN option									

* The numbers in the table indicate the LCOS version in which the function was implemented

1) Port separation (private mode)

2) Only if the VPN options have been activated for the device

3) No Multi-SSID with 11-Mbit WLAN cards

4) Optional VPN-500 and VPN-1000 available

5) Compatible with ADSL and ADSL2

6) 3050; only with external MC-54 card

7) depending on VoIP option (Basic/Advanced)

□ Overview of functions by model and LCOS* version

	1811	1821	1823	3050 3550	4000 4100	6000 6001 6021	7011	7111	8011
Interfaces									
ADSL modem		✔	✔						
ADSL 2+		From hardware release E	✔						
VLAN	3.30	✔	✔	3.30			6.10	6.10	6.10
DMZ port	5.20	5.20	✔				✔	5.20	5.20
Switch ports	4	4	2					4	4
Ethernet port mapping	5.00	5.00	✔					5.00	5.00
DSLoL									
Security									
Stateful Inspection, DoS, IDS	✔	✔	✔	2.80	2.80	2.80	2.80	✔	✔
IP QoS, Traffic Shaping	✔	✔	✔	3.30	3.30	3.30	3.30	✔	✔
SSH configuration access	4.00	4.00	✔	4.00	4.00	4.00	4.00	✔	4.00
ISDN-based anti-theft device	5.00	5.00	✔		5.00	5.00	5.00	5.00	5.00
Management									
Rights management for admins	4.00	4.00	✔	4.00	4.00	4.00	4.00	✔	4.00
Multiple loopback addresses	4.00	4.00	✔	4.00	4.00	4.00	4.00	✔	4.00
Modem operation at serial interface	4.10	4.10	✔						
Scripting	5.00	5.00	✔	5.00	5.00	5.00	5.00	5.00	5.00
CRON	✔	✔	✔	3.10	3.10	3.10	3.10	✔	3.10
Port sniffer	5.00	5.00	✔					5.00	5.00
Other functions									
DHCP auto client mode	3.42	3.42	✔	3.42	3.42	3.42	3.42	✔	3.42
N:N mapping	3.30	✔	✔	3.30	3.30	3.30	3.30	✔	✔
Dynamic DNS	✔	✔	✔	3.10	3.10	3.10	3.10	✔	✔
Free port mapping	4.00	4.00	✔	4.00	4.00	4.00	4.00	✔	4.00
Multi-PPPoE	4.00	4.00	✔	4.00			4.00	✔	4.00
Load balancing	4 channels 5.00	4 channels 5.00	2 channels					4 channels 5.00	4 channels 5.00
Policy-based routing	5.00	5.00	✔	5.00	5.00	5.00	5.00	5.00	5.00
VRRP	5.20	5.20	✔	5.20	5.20	5.20	5.20	5.20	5.20
PPPoE servers	5.20	5.20	✔	5.20	5.20	5.20	5.20	5.20	5.20
WAN RIP	5.20	5.20	✔	5.20	5.20	5.20	5.20	5.20	5.20
Spanning Tree Protocol	5.20	5.20	✔	5.20					
Layer 2 QoS tagging	6.10	6.10	✔	6.10	6.10	6.10	6.10	6.10	6.10

	1811	1821	1823	3050 3550	4000 4100	6000 6001 6021	7011	7111	8011
VPN functions									
AES, 3-DES, DES, Blowfish, CAST	3.32	✔	✔	✔	✔	✔	✔	✔	✔
VPN-5 option available	Integrated from 3.32	Integrated	Integrated	✔	✔				
VPN-25 option available	✔	✔	✔	✔	✔				
VPN hardware acceleration	with VPN-25	with VPN-25	with VPN-25					✔	✔
VPN-100						✔		✔	
VPN-200							✔		✔
Digitale certificates (X.509) incl. PKCS #12	5.00	5.00	✔					5.00	5.00
Certificate revocation list - CRL								6.10	6.10
Simplified RAS with certificates								6.20	6.20
AES 256 / IPCOMP	5.00	5.00	✔	5.00	5.00	5.00	5.00	5.00	5.00
Redundant VPN gateways	4.00	4.00	✔	4.00 [2)]	4.00	4.00	4.00	✔	4.00
NAT Traversal (NAT-T)	5.20	5.20	✔	5.20	5.20	5.20	5.20	5.20	5.20
IKE config mode	4.00	4.00	✔	4.00	4.00	4.00	4.00	✔	4.00
WLAN functions									
WLAN-802.11b	✔	✔	✔	✔					
WLAN-802.11g	✔	✔	✔	✔ [6)]					
WLAN-802.11a (incl. turbo mode)	✔	✔	✔	✔ [6)]					
LEPS	4.00	4.00	✔	4.00					
Multi-SSID, IP-redirect	3.42	3.42	✔	3.42 [3)]					
Super A/G	3.42	3.42	✔	3.42 [3)]					
Standard WEP encryption	4.00	4.00	✔	4.00					
802.11i with HW-AES	3.50	3.50	✔	- / 3.50					
802.11i for P2P in WLAN	4.00	4.00	✔	4.00					
WLANmonitor	5.00	5.00	✔	5.00					
Group configuration	5.00	5.00	✔	5.00					
Fully transparent client bridge mode	5.00	5.00	✔	5.00					
Bandwidth limitations in the WLAN	5.20	5.20	✔	5.20					
QoS for WLAN (IEEE 802.11e, WMM/WME)	6.10	6.10	✔	6.10					
RADIUS server	6.10	6.10	✔	6.10					
VoIP functions (detailed information about your device's VoIP functions can be found in the user manual)									
SIP users	4/32 [7)]	4/32 [7)]	32					4/32 [7)]	4/32 [7)]
ISDN users	40	40	40					40	40
SIP lines	16	16	16					16	16

□ *Overview of functions by model and LCOS* version*

	1811	1821	1823	3050 3550	4000 4100	6000 6001 6021	7011	7111	8011
Lines to SIP PBXs	4	4	4					4	4
External ISDN busses for VoIP	1	1	0-1					1	1
Internal ISDN busses for VoIP			0-2					0	0
Analog exchange line connections			1						
Connectors for analog terminal equipment			2						
Software options									
ISDN leased line option	Integr. as of 6.10	Integr. as of 6.10	Integrated		Integrated	Integrated	Integrated	Integrated	Integrated
Public spot option	✔	✔	✔	✔					
Fax modem option									
UMTS/VPN option				3550: As of 6.20 Integrated					

* The numbers in the table indicate the LCOS version in which the function was implemented

1) Port separation (private mode)

2) Only if the VPN options have been activated for the device

3) No Multi-SSID with 11-Mbit WLAN cards

4) Optional VPN-500 and VPN-1000 available

5) Compatible with ADSL and ADSL2

6) 3050; only with external MC-54 card

7) depending on VoIP option (Basic/Advanced)

	L-2	IL-2	L-11	IL-11	L-54g	L-54ag IAP	L-54 dual	OAP	XAP
Interfaces									
ADSL modem									
ADSL 2+									
VLAN			3.30	3.30	3.30	3.30	3.30	✔	✔
DMZ port									
Switch ports									
Ethernet port mapping								5.00	5.00
DSLoL	3.10	3.10	3.10	3.10	3.10	3.10	3.10		
Security									
Stateful Inspection, DoS, IDS	2.80	2.80	2.80	2.80	2.80	2.80	2.80	✔	✔
IP QoS, Traffic Shaping	3.30	3.30	3.30	3.30	3.30	3.30	3.30	✔	✔
SSH configuration access					4.00	4.00	4.00	✔	✔
ISDN-based anti-theft device									
Management									
Rights management for admins					4.00	4.00	4.00	✔	✔
Multiple loopback addresses					4.00	4.00	4.00	✔	✔
Modem operation at serial interface					4.10	4.10	4.10		
Scripting					5.00	5.00	5.00	5.00	5.00
CRON	3.10	3.10	3.10	3.10	3.10	3.10	3.10	✔	✔
Port sniffer								5.00	5.00
Other functions									
DHCP auto client mode					3.42	3.42	3.42	✔	✔
N:N mapping					4.10	4.10	4.10	✔	✔
Dynamic DNS	3.10	3.10	3.10	3.10	3.10	3.10	3.10	✔	✔
Free port mapping					4.00	4.00	4.00	✔	✔
Multi-PPPoE					4.00	4.00	4.00	✔	✔
Load balancing									
Policy-based routing					5.00	5.00	5.00	5.00	5.00
VRRP					5.20	5.20	5.20	5.20	5.20
PPPoE servers					5.20	5.20	5.20	5.20	5.20
WAN RIP					5.20	5.20	5.20	5.20	5.20
Spanning Tree Protocol					5.20	5.20	5.20	5.20	5.20
Layer 2 QoS tagging					6.10	6.10	6.10	6.10	6.10
VPN functions									
AES, 3-DES, DES, Blowfish, CAST									
VPN-5 option available									
VPN-25 option available								✔	✔

□ Overview of functions by model and LCOS* version

	L-2	IL-2	L-11	IL-11	L-54g	L-54ag IAP	L-54 dual	OAP	XAP
VPN hardware acceleration								In combination with VPN -25	
VPN-100									
VPN-200									
Digital certificates (X.509) incl. PKCS #12								5.00	
Certificate revocation list - CRL									
Simplified RAS with certificates									
AES 256 / IPCOMP								5.00	
Redundant VPN gateways								✔	
NAT Traversal (NAT-T)								5.20	
IKE config mode								✔	
WLAN functions									
WLAN-802.11b	✔	✔	✔	✔	✔	✔	✔	✔	✔
WLAN-802.11g					✔	✔	✔	✔	✔
WLAN-802.11a (incl. turbo mode)						✔	✔	✔	✔
LEPS					4.00	4.00	✔	✔	✔
Multi-SSID, IP-redirect					3.42	3.42	✔	✔	✔
Super A/G					3.42	3.42	✔	✔	✔
Standard WEP encryption					4.00	4.00	✔	✔	✔
802.11i with HW-AES					3.50	3.50	✔	✔	✔
802.11i for P2P in WLAN					4.00	4.00	✔	✔	✔
WLANmonitor					5.00	5.00	✔	5.00	✔
Group configuration					5.00	5.00	✔	5.00	✔
Fully transparent client bridge mode					5.00	5.00	✔	5.00	✔
Bandwidth limitations in the WLAN					5.20	5.20	✔	5.20	✔
QoS for WLAN (IEEE 802.11e, WMM/WME)					6.10	6.10	✔	6.10	✔
RADIUS server					6.10	6.10	✔	6.10	✔
VoIP functions (detailed information about your device's VoIP functions can be found in the user manual)									
SIP users									
ISDN users									
SIP lines									
Lines to SIP PBXs									
External ISDN busses for VoIP									
Internal ISDN busses for VoIP									
Analog exchange line connections									
Connectors for analog terminal equipment									

	L-2	IL-2	L-11	IL-11	L-54g	L-54ag IAP	L-54 dual	OAP	XAP
Software options									
ISDN leased line option		Integr. as of 6.10		Integr. as of 6.10					
Public spot option	✔	✔	✔	✔	✔	✔	✔	✔	✔
Fax modem option									
UMTS/VPN option									

* The numbers in the table indicate the LCOS version in which the function was implemented

1) Port separation (private mode)

2) Only if the VPN options have been activated for the device

3) No Multi-SSID with 11-Mbit WLAN cards

4) Optional VPN-500 and VPN-1000 available

5) Compatible with ADSL and ADSL2

6) 3050; only with external MC-54 card

7) depending on VoIP option (Basic/Advanced)