

Reference Manual

© 2004 LANCOM Systems GmbH, Würselen (Germany)

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

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

Trademarks

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

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

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

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

LANCOM Systems GmbH
Adenauertrasse 20 / B2
Adenauerstr. 20/B2
Germany

www.lancom.de

Würselen, March 2004

Contents

1 Preface	8
2 System design	11
3 Configuration and management	13
3.1 Configuration tools and approaches	13
3.2 Configuration software	14
3.2.1 Configuration using LANconfig	14
3.2.2 Configuration with WEBconfig	16
3.2.3 Configuration using Telnet	17
3.2.4 Configuration using SNMP	18
3.3 Remote configuration via Dial-Up Network	18
3.3.1 This is what you need for ISDN remote configuration	19
3.3.2 The first remote connection using Dial-Up Networking	19
3.3.3 The first remote connection using a PPP client and Telnet	20
3.4 LANmonitor—know what's happening	21
3.4.1 Extended display options	22
3.4.2 Monitor Internet connection	22
3.5 Trace information—for advanced users	24
3.5.1 How to start a trace	24
3.5.2 Overview of the keys	25
3.5.3 Overview of the parameters	25
3.5.4 Combination commands	26
3.5.5 Examples	27
3.6 Working with configuration files	27
3.7 New firmware with LANCOM FirmSafe	28
3.7.1 This is how LANCOM FirmSafe works	28
3.7.2 How to load new software	29
3.8 Command line interface	30
3.8.1 Command line reference	31
3.9 Scheduled Events	32

4	Diagnosis	35
4.1	LANmonitor—know what's happening	35
4.1.1	Extended display options	35
4.1.2	Monitor Internet connection	36
4.2	Trace information—for advanced users	37
4.2.1	How to start a trace	37
4.2.2	Overview of the keys	38
4.2.3	Overview of the parameters	38
4.2.4	Combination commands	39
4.2.5	Examples	40
5	Security	41
5.1	Protection for the configuration	41
5.1.1	Password protection	41
5.1.2	Login barring	43
5.1.3	Restriction of the access rights on the configuration	44
5.2	Protecting the ISDN connection	48
5.2.1	Identification control	48
5.2.2	Callback	50
5.3	The security checklist	51
6	Routing and WAN connections	54
6.1	General information on WAN connections	54
6.1.1	Bridges for standard protocols	54
6.1.2	What happens in the case of a request from the LAN?	54
6.2	IP routing	56
6.2.1	The IP routing table	56
6.2.2	Local routing	58
6.2.3	Dynamic routing with IP RIP	59
6.2.4	SYN/ACK speedup	63
6.3	The hiding place—IP masquerading (NAT, PAT)	64
6.3.1	Simple masquerading	64
6.3.2	Inverse masquerading	68
6.3.3	Unmasked Internet access for server in the DMZ	69
6.4	N:N mapping	70
6.4.1	Application examples	72
6.4.2	Configuration	75

6.5	Configuration of remote stations	79
6.5.1	Name list	79
6.5.2	Layer list	80
6.6	Establishing connection with PPP	81
6.6.1	The protocol	82
6.6.2	Everything o.k.? Checking the line with LCP	84
6.6.3	Assignment of IP addresses via PPP	84
6.6.4	Settings in the PPP list	86
6.7	Extended connection for flat rates—Keep-alive	87
6.8	Callback functions	88
6.8.1	Callback for Microsoft CBCP	88
6.8.2	Fast callback using the LANCOM process	89
6.8.3	Callback with RFC 1570 (PPP LCP extensions)	90
6.8.4	Overview of configuration of callback function	91
6.9	Channel bundling with MLPPP	92
7	Firewall	95
7.1	Threat analysis	95
7.1.1	The dangers	95
7.1.2	The ways of the perpetrators	96
7.1.3	The methods	96
7.1.4	The victims	97
7.2	What is a Firewall?	98
7.2.1	Tasks of a Firewall	98
7.2.2	Different types of Firewalls	99
7.3	The LANCOM Firewall	105
7.3.1	How the LANCOM Firewall inspects data packets	106
7.3.2	Special protocols	110
7.3.3	General settings of the Firewall	112
7.3.4	Parameters of Firewall rules	116
7.3.5	Alerting functions of the Firewall	122
7.3.6	Strategies for Firewall settings	126
7.3.7	Hints for setting the Firewall	128
7.3.8	Configuration of Firewall rules	132
7.3.9	Firewall diagnosis	142
7.3.10	Firewall limitations	150
7.4	Protection against break-in attempts: Intrusion Detection	151
7.4.1	Examples for break-in attempts	151

7.4.2	Configuration of the IDS	152
7.5	Protection against “Denial of Service” attacks	153
7.5.1	Examples of Denial of Service attacks	153
7.5.2	Configuration of DoS blocking	156
7.5.3	Configuration of ping blocking and Stealth mode	157
8	Quality of Service	159
8.1	Why QoS?	159
8.2	Which data packets to prefer?	159
8.2.1	Guaranteed minimum bandwidths	162
8.2.2	Limited maximum bandwidths	163
8.3	The queue concept	163
8.3.1	Queues in transmission direction	163
8.3.2	Queues for receiving direction	166
8.4	Reducing the packet length	167
8.5	QoS parameters for Voice over IP applications	169
8.6	QoS in sending or receiving direction	173
8.7	QoS configuration	174
8.7.1	Evaluating ToS and DiffServ fields	174
8.7.2	Defining minimum and maximum bandwidths	176
8.7.3	Adjusting transfer rates for interfaces	178
8.7.4	Sending and receiving direction	180
8.7.5	Reducing the packet length	180
9	Virtual LANs (VLANs)	183
9.1	What is a Virtual LAN?	183
9.2	This is how a VLAN works	183
9.2.1	Frame tagging	184
9.2.2	Conversion within the LAN interconnection	185
9.2.3	Application examples	186
9.3	Configuration of VLANs	189
9.3.1	The network table	189
9.3.2	The port table	190
9.3.3	Configuration with LANconfig	191
9.3.4	Configuration with WEBconfig or Telnet	192

10 Office communications with LANCAPI	194
10.1 What are the advantages of LANCAPI?	194
10.2 The client and server principle	194
10.2.1 Configuring the LANCAPI server	194
10.2.2 Installing the LANCAPI client	197
10.2.3 Configuration of the LANCAPI clients	198
10.3 How to use the LANCAPI	199
10.4 The LANCOM CAPI Faxmodem	199
11 Server services for the LAN	201
11.1 Automatic IP address administration with DHCP	201
11.1.1 The DHCP server	201
11.1.2 DHCP—'on', 'off' or 'auto'?	202
11.1.3 How are the addresses assigned?	203
11.2 DNS	206
11.2.1 What does a DNS server do?	206
11.2.2 DNS forwarding	208
11.2.3 Setting up the DNS server	209
11.2.4 URL blocking	212
11.2.5 Dynamic DNS	213
11.3 Call charge management	214
11.3.1 Charge-based ISDN connection limits	214
11.3.2 Time dependent ISDN connection limit	215
11.3.3 Settings in the charge module	216
11.4 The SYSLOG module	216
11.4.1 Setting up the SYSLOG module	217
11.4.2 Example configuration with LANconfig	217
12 Appendix	220
12.1 SNMP traps	220
12.2 Overview of functions for LANCOM models and LCOS versions	222
13 Index	223

1 Preface

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)
- ▷ Backup solutions
- ▷ 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 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 prod-

ucts. 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' stands as shortened form for the manufacturer, LANCOM Systems GmbH from Würselen, Germany

Validity

The present reference manual applies to all LANCOM routers and LANCOM Wireless Access Points with firmware version 3.32 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 222).

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 41.

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.

Special formatting in body text

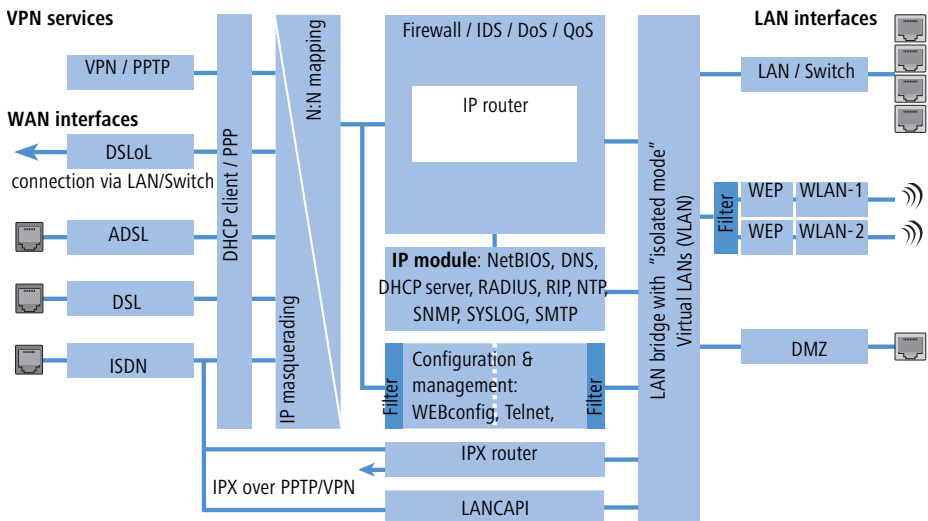
Bold	Menu commands, command buttons, or text boxes
Code	Inputs and outputs for the display mode
<Value>	Placeholder for a specific value

2 System design

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.
- 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.

► Chapter 2: System design

- 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.
- 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

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 to a limited extent also be used within IP networks (inband and remote configuration).



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.

3.2.1 Configuration using 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.

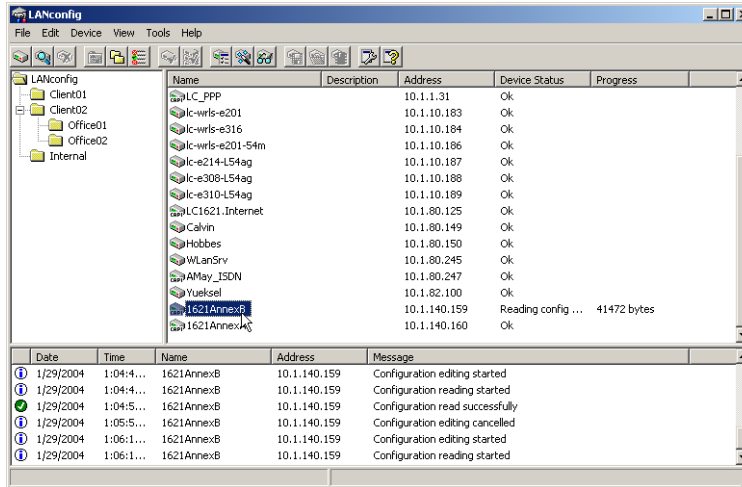
Find new devices



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.

► Chapter 3: Configuration and management

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.

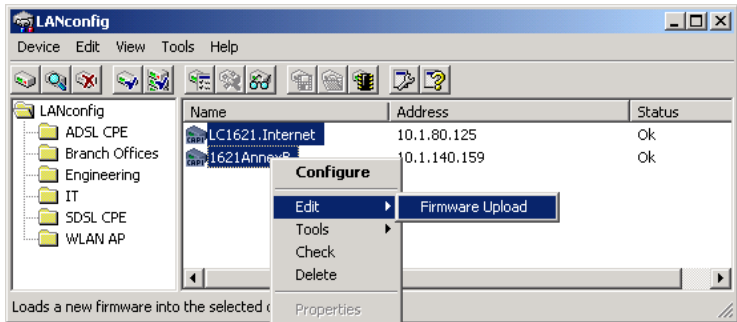
Management of multiple devices

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.



3.2.2 Configuration with 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.

3.2.3 Configuration using 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.

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-module ► Language
Telnet	set /Setup/Config module/Language German

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.

► Chapter 3: Configuration and management

EN

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.

3.2.4 Configuration using 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 (**Management Information Base**) 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

3.3 Remote configuration via Dial-Up Network



The complete section on remote configuration applies only to LANCOM with ISDN interface.

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 WAN interface. This means that you save a lot of time and costs when connecting other networks to your network 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.

3.3.1 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.

3.3.2 The first remote connection using Dial-Up Networking

- ① In the LANconfig program select **Device / New**, enable 'Dial-Up connection' as the connection type and enter the calling number of the WAN 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.

3.3.3 The first remote connection using a PPP client and Telnet

- 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.

The default layer for remote field installations

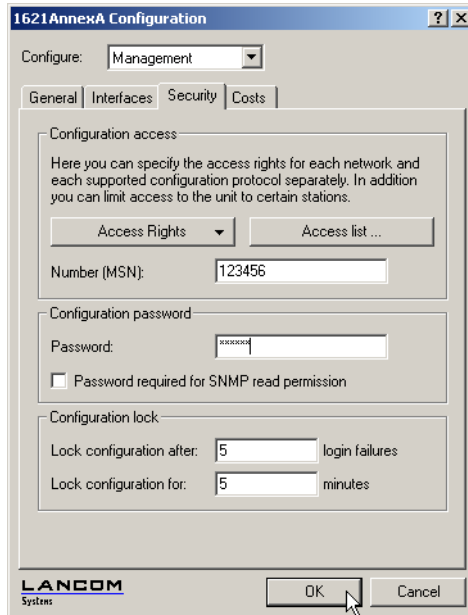
The PPP connection of any other remote site to the router, of course, will only succeed if the device answers every call with the corresponding PPP settings. This is the case using the factory default settings because the default protocol (default layer) is set to PPP.

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 'Security' tab in the 'Management' configuration section.



- ② Enter a number at your location which is not being used for other purposes in the 'Configuration access' area.

Alternatively, enter the following command:

```
set /setup/config-module/Farconfig 123456
```



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.

3.4 LANmonitor—know what's happening

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.

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 the 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.

3.4.1 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.

3.4.2 Monitor Internet connection

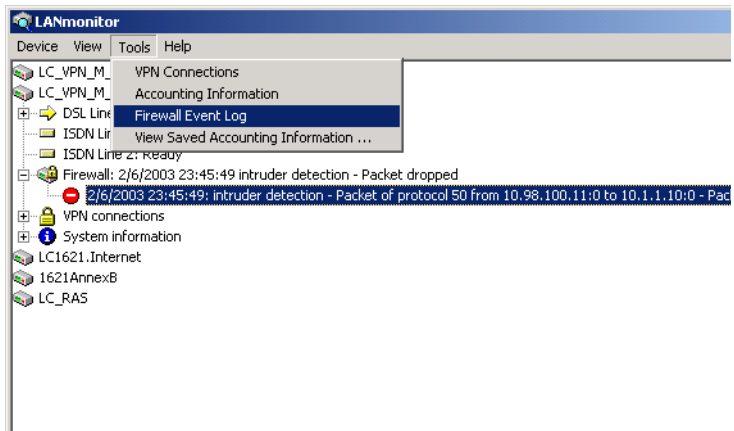
To demonstrate the functions of LANmonitor we will first show you the types of information LANmonitor provides about connections being established to your Internet provider.

- ① To start LANmonitor, go to **Start ► Programs ► LANCOM ► LANmonitor**. Use **Device ► New** 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 **Tools / 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 such 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 ► Properties** and go to the 'Logging' tab. Enable logging and

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

3.5 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 behind 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.

3.5.1 How to start a trace

Trace output can be started in a Telnet session, for example. 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. And what is the meaning of these codes and parameters?

3.5.2 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

EN

3.5.3 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

► Chapter 3: Configuration and management

EN

This parameter...	... brings up the following display for the trace:
NetBIOS	NetBIOS management
DNS	Domain Name Service Protocol
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

3.5.4 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.

3.5.5 Examples

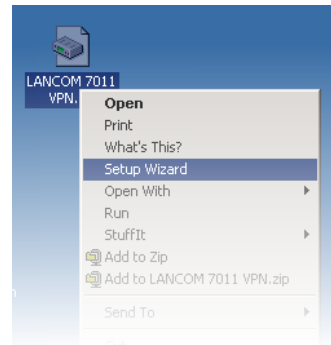
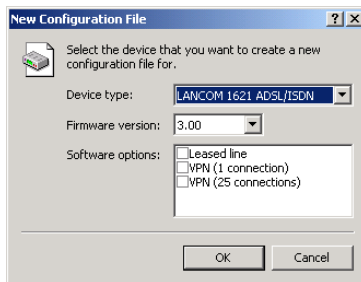
This code...	... in combination with the trace causes the following:
trace	displays all protocols that can generate outputs during the configuration, and the status of each output (ON or OFF)
trace + all	switches on all trace outputs
trace + protocol display	switches on the output for all connection 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 - time	switches off the system time output before the actual trace output

EN

3.6 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. Should your LANCOM (e.g. due to a defect) lose its configuration data, you simply reload the backup copy.

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	Edit ► Save Configuration to File Edit ► Restore Configuration from File Edit ► New Configuration File Edit ► Edit Configuration File Edit ► Print Configuration File
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

3.7 New firmware with LANCOM FirmSafe

The software for devices from LANCOM 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.

3.7.1 This is how LANCOM FirmSafe works

LANCOM 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.

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 five minutes until it has successfully logged on. Only if this login attempt is successful does the new firmware remain active permanently.
 - ▷ If the device no longer responds and it is therefore 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.

3.7.2 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 **Edit ► Save Configuration to File** if using LANconfig, for example).

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 **Edit ► Firmware Management ► Upload New Firmware**, 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 '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**.

TFTP

TFTP can be used to install new firmware on LANCOM. This can be done with the command (or target) **writelflash**. 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 writelflash
```

3.8 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

3.8.1 Command line reference

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

Command	Description
cd <directory>	Change the current directory. Certain abbreviations exists, e.g. "cd ../.." can be abbreviated to "cd ..." etc.
del <name> rm <name>	Delete the table entry with the index <name>
dir [<directory>] ls [<directory>] ll [<directory>]	Display the contents of a directory
do <name> [<parameters>]	Execute the action <name> in the current directory. Parameters can be specified
exit/quit/x	Close the console session
feature <code>	Unlock the feature with the specified feature code
passwd	change password
ping [IP address]	Issues an ICMP echo request to the specified IP address
readconfig	Displays the complete configuration of the device in "readconfig" syntax
readmib	display SNMP Management Information Base
repeat <VALUE> <command>	repeats command every VALUE seconds until terminated by new input
stop	stop ping
set <name> <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.

Command	Description
set [<name>] ?	Show which values are allowed for a configuration item. If <name> is empty, this is displayed for each item in the current directory.
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
trace [...]	Configures the trace output system for several modules, see 'How to start a trace' → page 24
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

- 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.

3.9 Scheduled Events

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 include:

- scheduled connections
- time-dependant firewall rules

► Chapter 3: Configuration and management

► regular firmware or configuration updates

Configuration Tool	Run
WEBconfig	Expert-Configuration ► Config-module ► Cron-table
Terminal/Telnet	setup/config-module/cron-table

The data is stored in a table with the following layout:

Entry	Description
Index	Unambiguously identifies this entry in the table
Base	The <code>Base</code> 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 <code>Minute</code> to <code>Month</code> 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 <code>DayOfWeek</code> 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.

For example, the entry given below would connect the device each weekday at 6 PM with a remote site 'HEADQUARTERS'

Base	Realtime
Minute Hour DayOfWeek Day Month	18 1,2,3,4,5,
Command	do /o/man/con HEADQUARTERS

► *Chapter 3: Configuration and management*



Time-controlled rules will not necessarily be executed at precisely zero seconds of real time, but at some indeterminate point of time in the minute in question.

4 Diagnosis

4.1 LANmonitor—know what's happening

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.

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 the 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.

4.1.1 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.

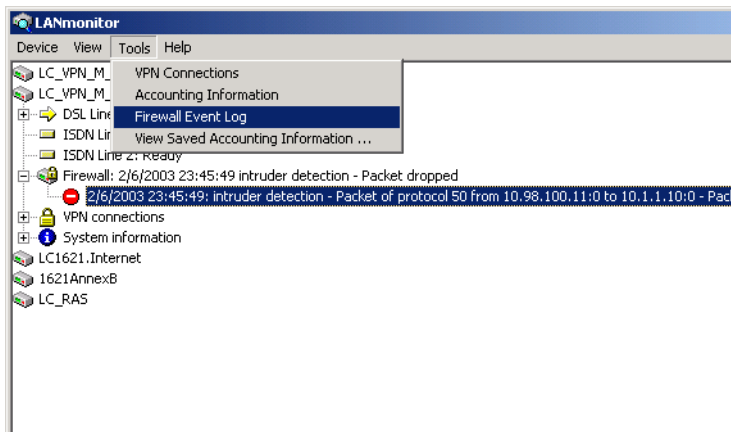
4.1.2 Monitor Internet connection

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 **Device ► New** 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 **Tools / 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 such 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 ► Properties** and go to the 'Logging' tab. Enable logging and specify whether LANmonitor should create a log file daily, monthly, or on an ongoing basis.

4.2 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 behind 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.

4.2.1 How to start a trace

Trace output can be started in a Telnet session, for example. 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. And what is the meaning of these codes and parameters?

4.2.2 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

4.2.3 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

This parameter...	... brings up the following display for the trace:
NetBIOS	NetBIOS management
DNS	Domain Name Service Protocol
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

4.2.4 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.

4.2.5 Examples

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 + 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 - time	switches off the system time output before the actual trace output

5 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 95
- ▷ 'The hiding place—IP masquerading (NAT, PAT)' → page 64
- ▷ 'Virtual LANs (VLANs)' → page 183

5.1 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.

5.1.1 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 informa-

tion could be stolen, or the device could be reconfigured in a way that the protection-mechanisms for the local network could be 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.

► **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 'Security' 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 ► Security ► Configuration password
WEBconfig	Security settings
Terminal/Telnet	<code>passwd</code>

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 ► Security ► Password required for SNMP read permission
WEBconfig	Expert Configuration ► Setup ► SNMP-module ► Password-required-for-SNMP-read-access
Terminal/Telnet	<code>setup/SNMP module/password-required</code>

5.1.2 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 ► Security
WEBconfig	Expert Configuration ► Setup ► Config-module
Terminal/Telnet	Setup/Config module

5.1.3 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
- Network
 - ▷ LAN
 - ▷ WAN

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 internal functions are separately selectable.

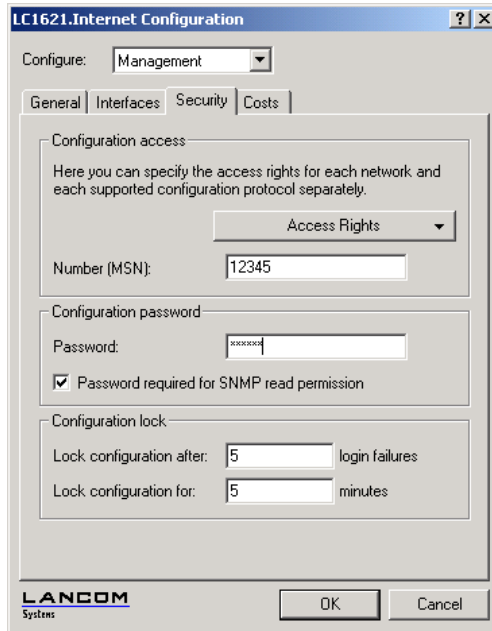
The term 'internal function' denotes configuration sessions via LANconfig (TFTP), WEBconfig (HTTP, HTTPS), SNMP or Terminal/Telnet.

Restrictions on the ISDN administrative account



This paragraph applies only to models with ISDN interface.

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



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

Enter alternatively the following instruction:

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



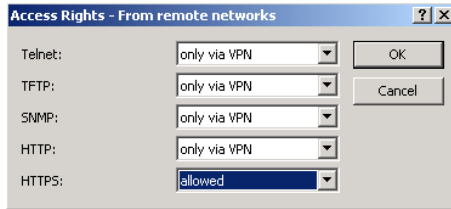
The ISDN administrative account is excluded as only configuration method from in the following described restrictions of network access methods. I.e. all on the Admin MSN incoming connections are not limited by the access restrictions of remote networks



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

Limit the network configuration access

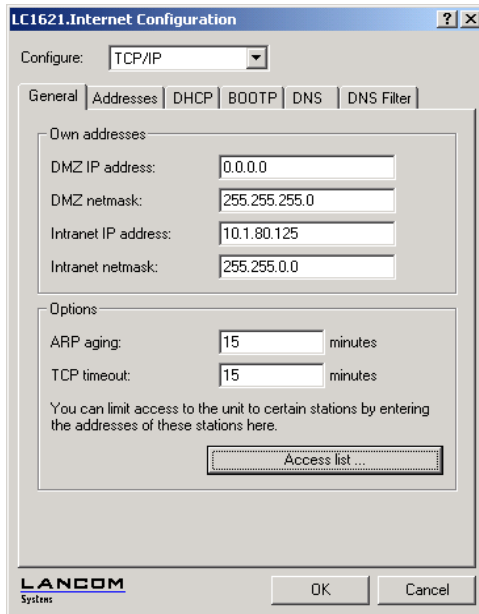
The access to the internal functions can be controlled separately for accesses from the local or from distant networks - for all configuration services separately. The configuration access can generally be permitted or forbidden, a pure read access or - if your model is equipped with VPN - also can be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

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:



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.

Configuration tool	Run
LANconfig	TCP/IP ► General ► Access list
WEBconfig	Expert Configuration ► Setup ► / TCP-IP-module Access-list
Terminal/Telnet	/setup/TCP-IP-module/access-list

5.2 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

5.2.1 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 accepting
WEBconfig	Expert Configuration ► Setup ► WAN-module ► Protect
Terminal/Telnet	setup/WAN-module/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 name 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 establish-

ment. 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-module ► PPP-list
Terminal/Telnet	/setup/WAN-module/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).

5.2.2 Callback

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

Configuration tool	Run
LANconfig	Communications ► Remote site ► Name list (ISDN)
WEBconfig	Expert configuration ► Setup ► WAN module ► ISDN-name-list
Terminal/Telnet	/Setup/WAN-module/Name list

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 name 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 88.

5.3 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.

► **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 – 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 (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 be allowed by a dedicated Firewall rule then. Thus 'Trojans' and certain Email viruses lose 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 129.

► **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.

6 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.

6.1 General information on WAN connections

WAN connections are used for the following applications.

- Internet access
- LAN to LAN coupling
- Remote access

6.1.1 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).

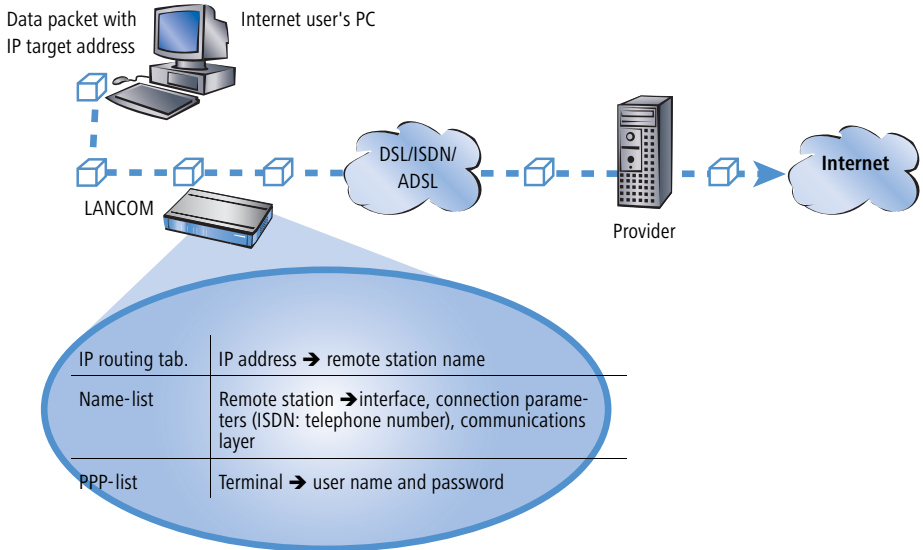
Close cooperation with router modules

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.

6.1.2 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.

6.2 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 router, as well as the additional functions available to support IP routing.

6.2.1 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 static routing table can hold up to 256 entries, the dynamic table can hold 128. The IP router looks at both tables 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). "Unfavourable" 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-module ► IP-routing-table
Terminal/Telnet	<code>cd /setup/IP-router/IP-routing-table</code>

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

IP address	IP netmask	Router	Distance	Masquerading
192.168.120.0	255.255.255.0	MAIN	2	Off
192.168.125.0	255.255.255.0	NODE1	3	Off
192.168.130.0	255.255.255.0	191.168.140.123	0	Off

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.

► Router

The router transmits the appropriate data packets to the IP address and network mask to this remote station. A name is entered at this point if the remote station is a router in another network or an individual workstation computer. This is where the IP address of another router which knows the path to the destination network is entered if the router on the network cannot address the remote station itself.

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

Routes with the router name '0.0.0.0' identify exclusion routes. Data packets for this "zero route" are rejected and are not routed any further.

► Chapter 6: Routing and WAN connections

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 'The hiding place—IP masquerading (NAT, PAT)' → page 64.

6.2.2 Local routing

You know the following behaviour 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-module ► Loc.-routing
Terminal/Telnet	set /setup/IP-router-module/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.

6.2.3 Dynamic routing with IP RIP

In addition to the static routing table, LANCOM 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.

► Chapter 6: Routing and WAN connections

EN

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 LANCAP1).
 - ▷ 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.

Routers without IP RIP support

Routers which do not support the Routing Information Protocol are also occasionally present on the local network. These routers cannot recognize the RIP

packets and look on them as normal broadcast or multicast packets. Connections are continually established by the RIPs if this router holds the default route to a remote router. This can be prevented by entering the RIP port in the filter tables.

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-module ► RIP-config
Terminal/Telnet	setup/IP-router-module/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.

6.2.4 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 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-module ► Routing-method ► SYN/ACK-speedup
Terminal/Telnet	cd /setup/IP-router-module/routing-method set SYN/ACK-speedup OFF

6.3 The hiding place—IP masquerading (NAT, PAT)

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.

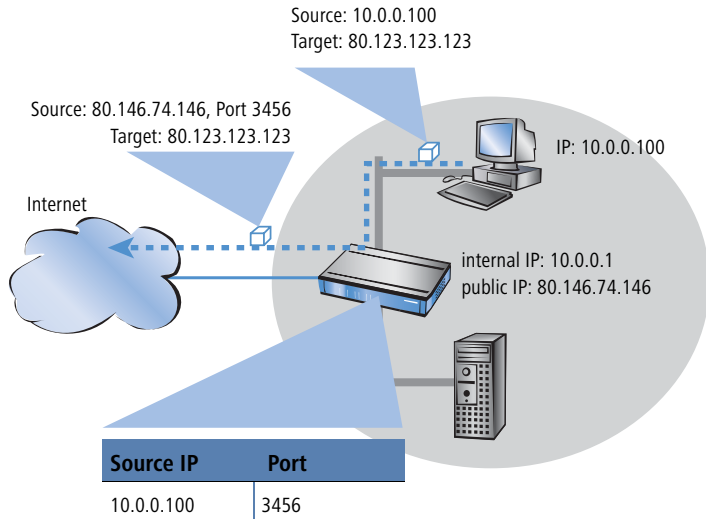
6.3.1 Simple masquerading

IP masquerading provides a hiding place for every computer while connected with the Internet. Only the router module of the LANCOM 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. Thereby, the router separates Internet and Intranet.

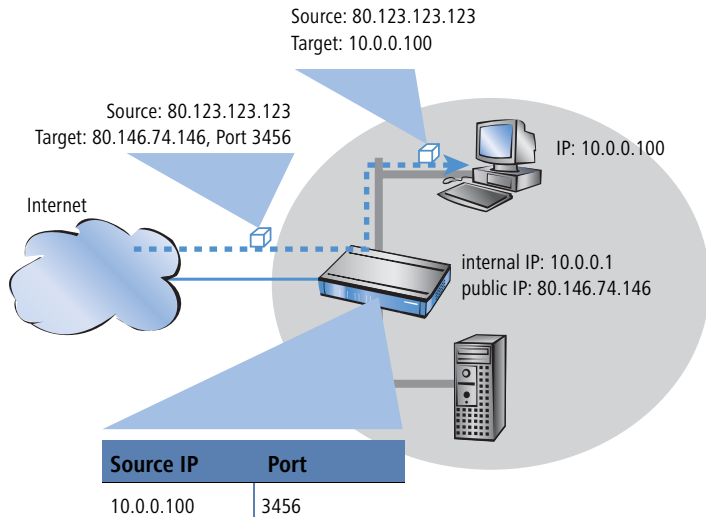
How does IP masquerading work?

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

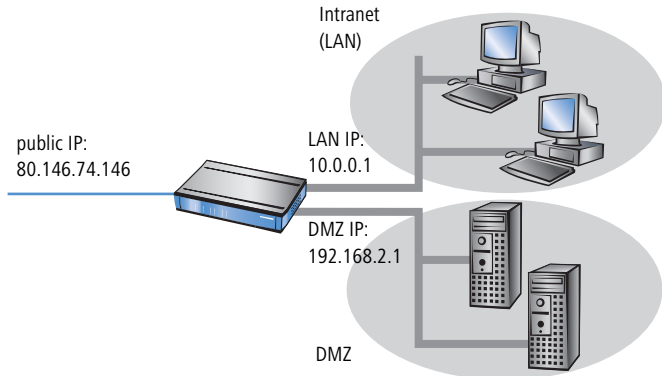
The use of IP masquerading is set individually for each route in the routing table. The routing table can be reached as follows:

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

Multiple addresses for the router

Masquerading pits two opposing requirements of the router against one another: While it must have an IP address which is valid on the local network, it must also have an address valid on the Internet. Since these two addresses may not in principle be located on the same logical network, there is only one solution: two IP addresses are required. Therefore, most standard Internet connections assign the router's Internet IP address dynamically during the PPP negotiation.

On the local side, the router supports two different networks: The **Intranet** and the **DMZ** ('de-militarized zone'). The DMZ marks a distinct, separate local network, usually for servers, that must be accessible from the Internet.



The routing table's **Masquerading** entry informs the router module whether local Intranet or DMZ addresses should be hidden behind the router's Internet IP address or not:

- **IP Masquerading switched off:** No masquerading.
This variant is intended for Internet access with multiple static IP addresses (to be entered under DMZ network address and DMZ netmask). Examples would be to connect servers to the Internet, or to connect two Intranet subnets via VPN.
- **masking Intranet and DMZ (default):** This setting masks all local addresses. Additionally to the Intranet, a second local network (DMZ) with private IP addresses can be connected to the Internet as well.
- **masking Intranet only:** This setting is ideally suited for Internet access with multiple static IP addresses. Other than with 'IP Masquerading switched off': Additionally to the DMZ, an Intranet with private IP addresses is supported simultaneously.

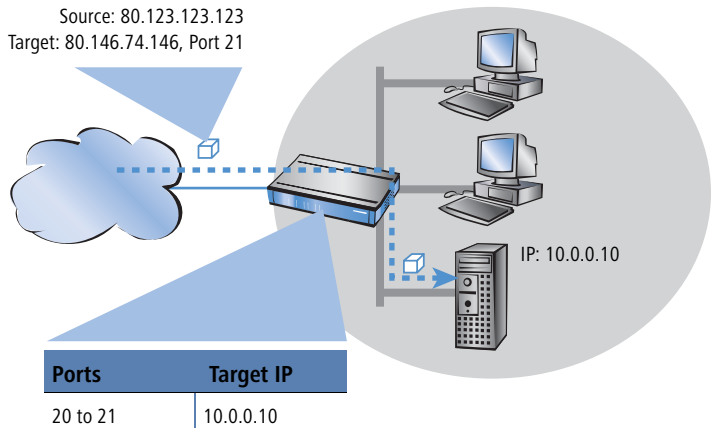
The **DMZ** and **Intranet** address assignment of the LANCOM can be entered at the following places:

Configuration tool	Run
LANconfig	TCP/IP ► General
WEBconfig	Expert Configuration ► Setup ► TCP-IP-Module
Terminal/Telnet	/Setup/TCP-IP-Module

6.3.2 Inverse masquerading

This masking operates in both directions: The local network behind the IP address of the router is masked if a computer from the LAN sends a packet to the Internet (simple masquerading).

If, on the other hand, a computer sends a packet from the Internet to, for example, an FTP server on the LAN ('exposed host'), 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

Configuration tool	Run
LANconfig	IP router ► Masq. ► Service list
WEBconfig	Expert Configuration ► Setup ► IP-router-module ► Masquerading ► Service-table
Terminal/Telnet	/setup/IP-router-module/masquerading/ service-table

EN

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.

6.3.3 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 and LANCOM 1621 ADSL/ISDN with the Switch set to 'Private Mode').

Two local networks - operating servers in a DMZ

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

Example: You are assigned the IP network address 123.45.67.0 with the net-mask 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 129): Allow access from "All stations in local network" to 123.45.67.2

6.4 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 ('The hiding place—IP masquerading (NAT, PAT)' → page 64) 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 68).

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.

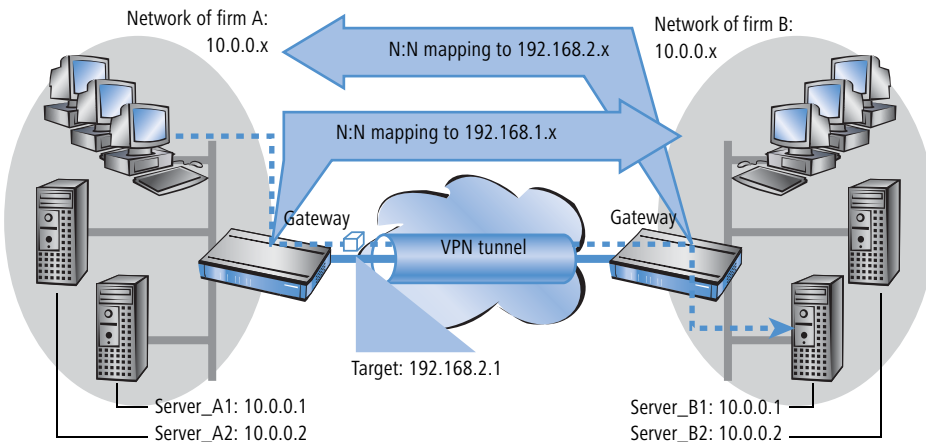
6.4.1 Application examples

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:



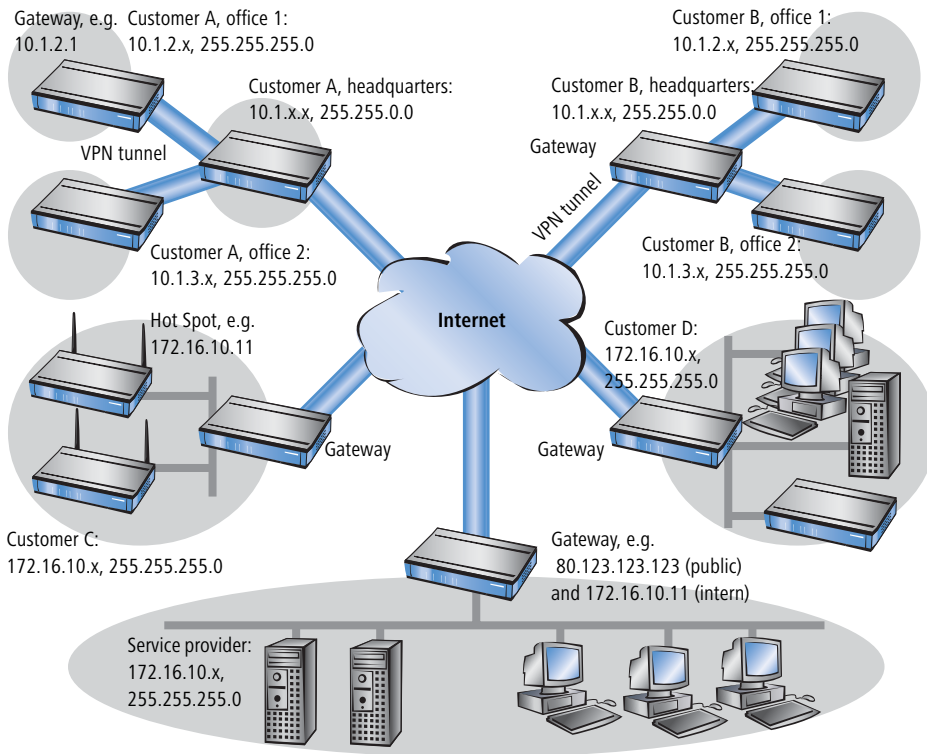
In this example network servers of company A and B should have access over a VPN tunnel to the respective other network. All stations of the LAN should have access to the server of the remote network. For the time being, there is no access possible to the other network, because both networks use the 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

► Chapter 6: Routing and WAN connections

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 220).

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:

- 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".

Loopback:
decentralized
1:1 mapping



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.

6.4.2 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.

► Chapter 6: Routing and WAN connections

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 112)!

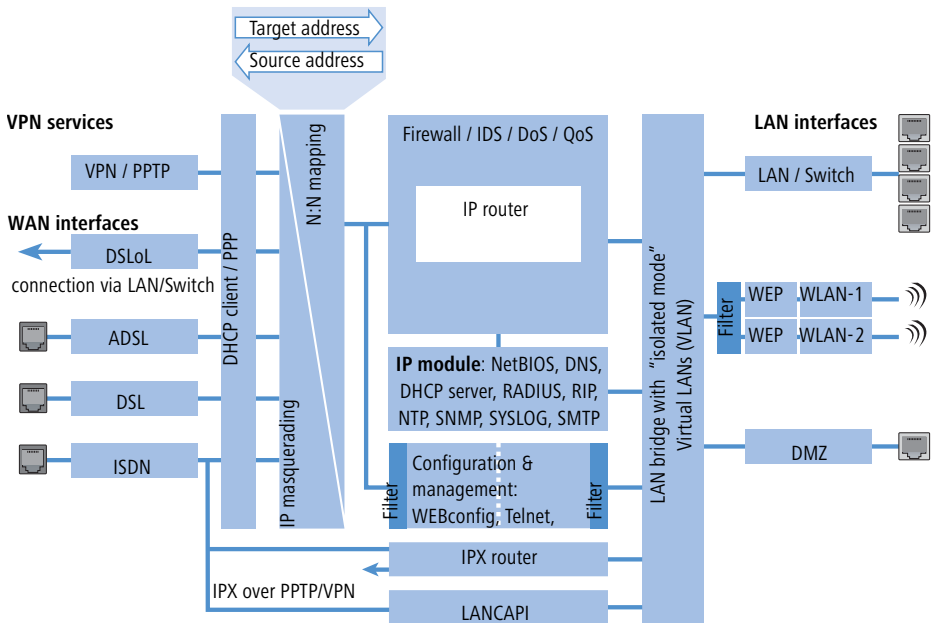
Additional configuration hints

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 208).
- 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.



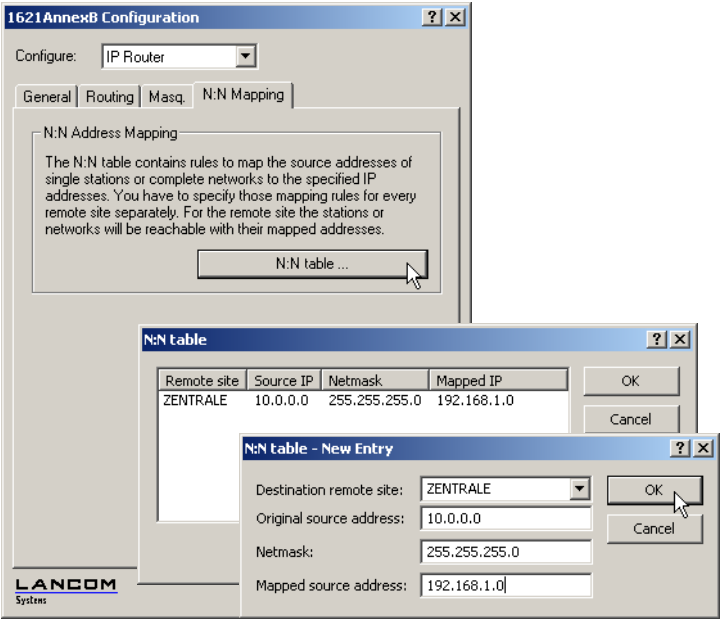
The IP address translation takes place in the LANCOM between firewall and IP router on one hand, and the VPN module on the other hand. All rules related to the own network use therefore the “unmapped” original addresses. The entries of the remote network use the “mapped” addresses of the remote side, valid on the VPN connection.



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 module / NAT table

When starting a new entry under WEBconfig, the NAT table shows up as follows:

Expert Configuration
 Setup
 IP-router-module

NAT-table

Idx.
 Src-Address
 Src-Mask
 Dst-Station
 Mapped-Network

6.5 Configuration of remote stations

Remote stations are configured in two tables:

- In the name 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 81.

6.5.1 Name list

The available remote stations are created in the name list with a suitable name and additional parameters.

Configuration tool	Menu/table
LANconfig	Communication ► Remote sites ► Name list
WEBconfig	Expert configuration ► Setup ► WAN module ► Name-list
Terminal/Telnet	cd /Setup/WAN module set name list[...]

6.5.2 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-module ► Layer-list
Terminal/Telnet	<code>cd /setup/WAN</code> <code>module/ set layer-list [...]</code>

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 name 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.

Parameter	Meaning
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.
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 'Channel bundling with MLPPP' → page 92.
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)

6.6 Establishing connection with PPP

LANCOM 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.

6.6.1 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).
- Verification of the connection through the LCP (Link Control Protocol)
- Combining several ISDN channels (MultiLink PPP)

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.

6.6.2 Everything o.k.? Checking the line with LCP

The devices involved in the establishment of a connection through PPP negotiate a common behaviour 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 behaviour 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'.

6.6.3 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.

EN

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.

EN

6.6.4 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-module ► PPP-list
Terminal/Telnet	<code>cd /setup/WAN module</code> <code>set PPP-list [...]</code>

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!

6.7 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 name 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').

6.8 Callback functions

The LANCOM supports automatic callback via its ISDN port.

In addition to callback via the D channel, the CBCP (Callback Control Protocol) 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.

6.8.1 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 name list via the callback entry as well as the calling number entry.

Name list (ISDN) - New Entry

Name:

Phonenummer:

Short hold time: seconds

Short hold time (bundle): seconds

Layer name:

Automatic callback:

- ☒ No callback
- ☐ Call back the remote site
- ☐ Call back the remote site (fast procedure)
- ☐ Call back the remote site after name verification
- ☐ Wait for callback from remote site

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

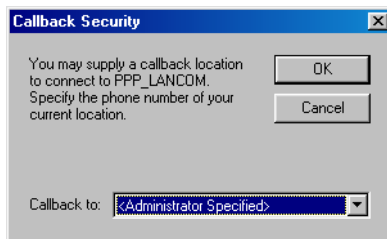
For this setting the callback entry must be set to 'Call back the remote site after name verification' (or must have the value 'Name' in WEBconfig or in the console). In the name list **no** telephone number may be specified.

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 name 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.

6.8.2 Fast callback using the LANCOM process

This fast, LANCOM-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 name list (or 'Looser' when configuring via WEBconfig, terminal program or Telnet).

► *Chapter 6: Routing and WAN connections*

- The callback party selects 'Call back the remote site (fast procedure)' in the name list and enters the calling number ('LANCOM' when configuring via WEBconfig, terminal program or Telnet).



For fast callback using the LANCOM method, the number list for answering calls must be kept up to date at both ends.

6.8.3 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.

6.8.4 Overview of configuration of callback function

The following options are available in the name 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 name 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.
'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 routers.



With Windows remote stations, the 'Name' setting **must** be selected.

6.9 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 **P**PP) 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.

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+compr** uses both (compression and channel bundling) and provides the maximum possible data transmission performance.
- ② Now create a new entry in the name 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-module ► Router-interface-list
Terminal/Telnet	cd /setup/WAN-module 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

► *Chapter 6: Routing and WAN connections*

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 LANCAPAPI are possible! So you should only use channel bundling if the double transmission capacity can really be used in full.

7 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.

7.1 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”.

7.1.1 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.

► *Chapter 7: Firewall*

- Modify data of LAN workstations, e. g. to obtain even further ways for access.
- Destroy data on the workstations of the LAN.
- Paralyse 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.

7.1.2 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.

7.1.3 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.

7.1.4 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:

- Particularily 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 organisations 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.

7.2 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 151 and 'Protection against "Denial of Service" attacks' → page 153.

7.2.1 Tasks of a Firewall

Checking data packets

How does the Firewall supervise 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.

7.2.2 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

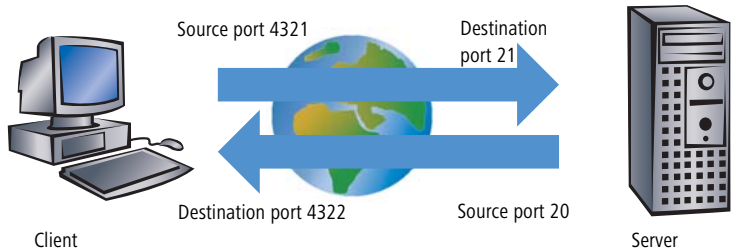
The rules defined in a packet filter-orientated Firewall determine e.g., whether the packets may pass on by a special IP address range into the local network, or whether packets should be filtered for special services (i.e. with special port numbers). By these measures, the communication with certain 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 unfavourable 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

► Chapter 7: Firewall

packets that do not belong to one of the tracked session of the connection state table will be automatically discarded.

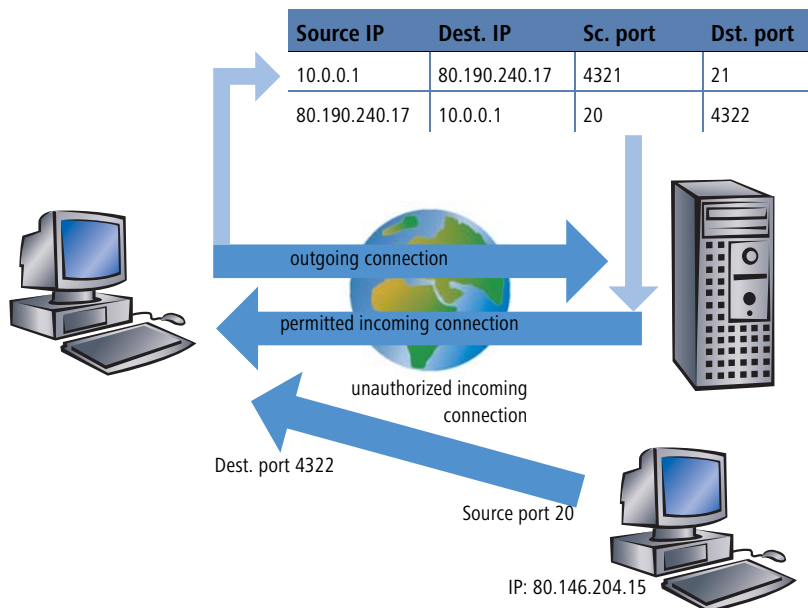
Stateful Inspection: direction-dependent checking

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.

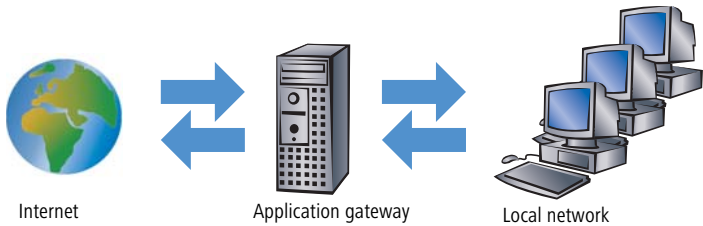
Moreover, a Firewall with Stateful Inspection is mostly able to re-assemble the received data packets, that means to buffer the individual parts and to assemble them again to an complete packet. Therefore, complete IP packets can be checked by the Firewall, rather than individual parts only.

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.

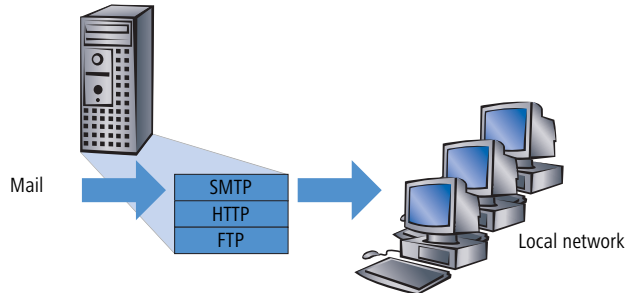
Application Gateway

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.

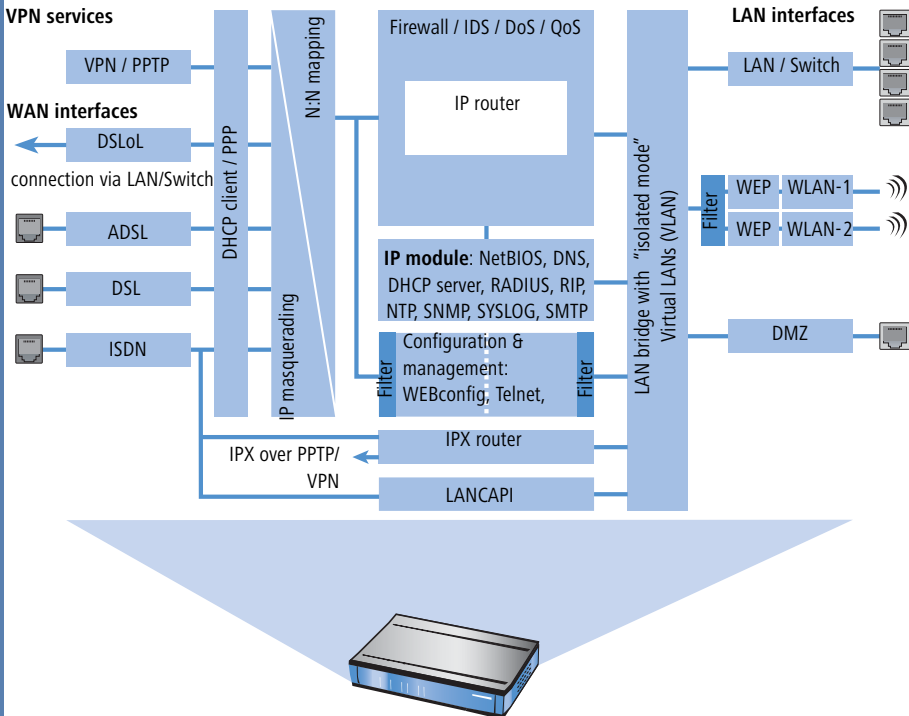
7.3 The LANCOM Firewall

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.

7.3.1 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.

► Chapter 7: Firewall

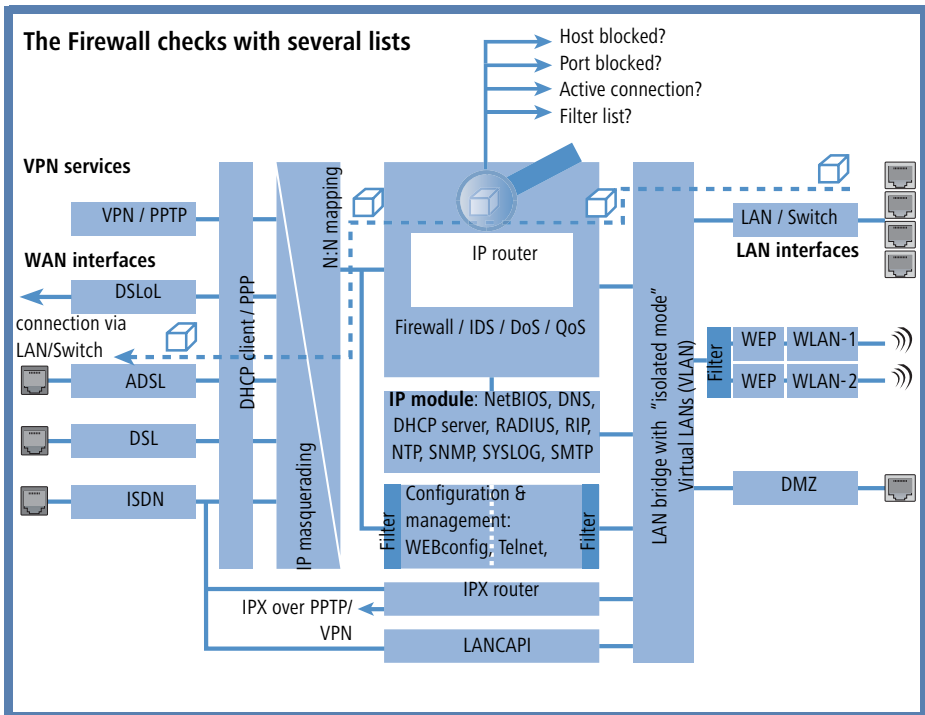
The LANCOM Firewall uses several lists for checking data packets, which are automatically generated from Firewall rules, resulting Firewall actions or by active data connections:

- 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 129.

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 116).

7.3.2 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 99.

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 remapped 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".

7.3.3 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
- Default VPN rules (→ page 113)
- Administrator email (→ page 113)
- Fragments (→ page 113)
- Re-establishing of the session (→ page 114)
- Ping blocking (→ page 114)
- Stealth mode(→ page 115)
- Mask authentication port (→ page 115)

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 70) are only active when the Firewall has been switched on!

Default VPN rules

A VPN rule consists, apart from some VPN specific information and among other things, of the definition of source and destination networks. The information about source and destination can get in principle from the IP routing table, the TCP/IP settings (Intranet addresses and DMZ addresses), or from the Firewall rules.

Similar to Quality of Service functions, VPN connections also use existing Firewall functions in order to classify e. g. the packets according to their subnetworks. Therefore, the Firewall is a central source for the VPN rules. It can be defined in the Firewall whether further sources should be used for the VPN rules or not. The according option can take on the following values:

- **Create automatically:** With this setting, all available sources for generating VPN rules will be consulted, i.e. IP routing table, TCP/IP settings and Firewall rules.
- **Specify manually:** With this setting only the manually specified Firewall rules are used as base for creating VPN rules.



For detailed information about VPN rules, please see the appropriate VPN documentation.

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 behaviour of the Firewall. The following options are available:

- **Filter:** Fragmented packets are directly discarded by the Firewall.

► Chapter 7: 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 behaviour 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 behaviour 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 behaviour 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 115).

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 behaviour 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. e-mails 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.

7.3.4 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 132.

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 117)
- **Observe further rules:** Should further Firewall rules be observed when this rule applies to a data packet? (→ page 117)

- **Create VPN rule:** Is this Firewall rule also used to create a VPN rule? (→ page 118)

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 behaviour 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 142.

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 follow-

ing 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 sub-network 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

As described in section 'Default VPN rules' → page 113, 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.



For detailed information about VPN rules please see the appropriate VPN documentation.

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:

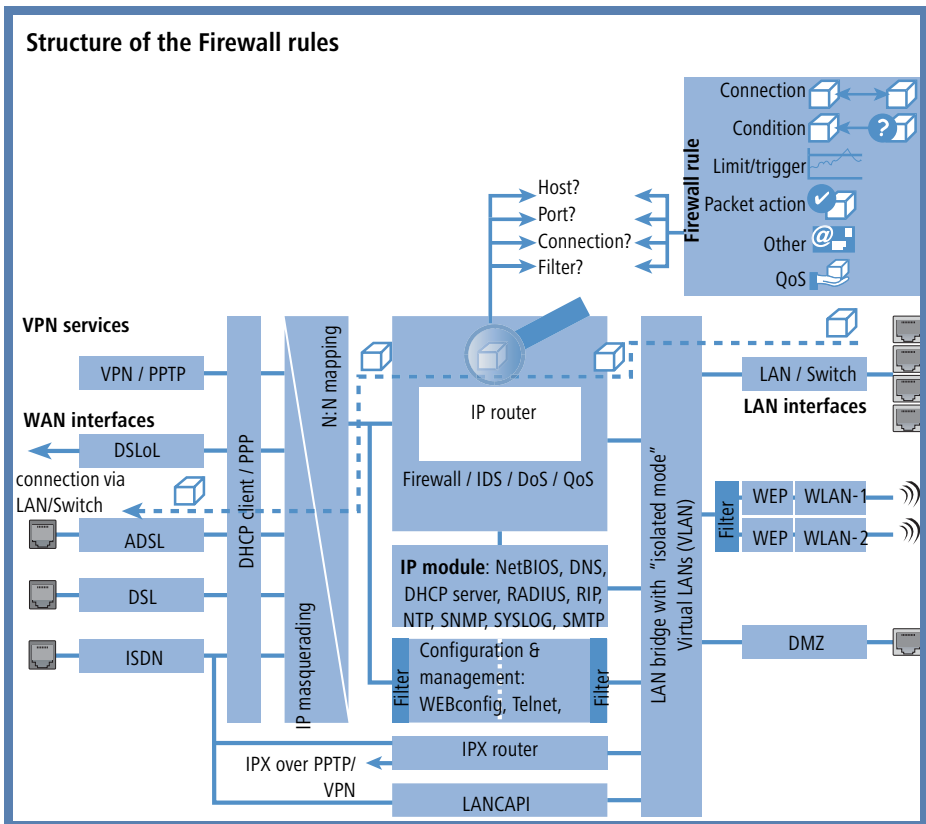
- **Stations / Service:** To which stations/networks and services/protocols does the rule refer to? (→ page 119)
- **Conditions:** Is the effectiveness of the rule reduced by other conditions? (→ page 120)
- **Trigger:** On exceeding of which threshold shall the rule being triggered? (→ page 121)
- **Action:** What should happen to the data packets when the condition applies and the limit is reached? (→ page 121)
- **Further measures:** Should further measures be initiated apart from the packet action? (→ page 121)
- **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 122)



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 106 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:

EN



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

► Chapter 7: Firewall

EN

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 name list)
- Certain stations of the LAN described by the host name)
- Certain MAC¹ 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.

1. MAC is the abbreviation for **Media Access Control** 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).



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.



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”.

► Chapter 7: Firewall

EN

- **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 159.

7.3.5 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 217) 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:

```
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

Notification by SNMP trap

If as notification method dispatching SNMP traps was activated (see also 'Configuration using SNMP' → page 18), 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.

7.3.6 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 be reached any more etc.

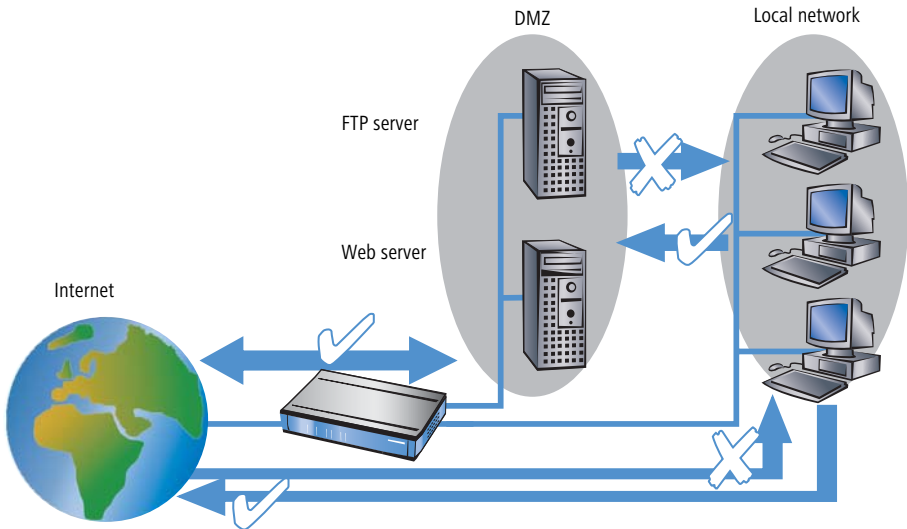
Firewall with DMZ

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.

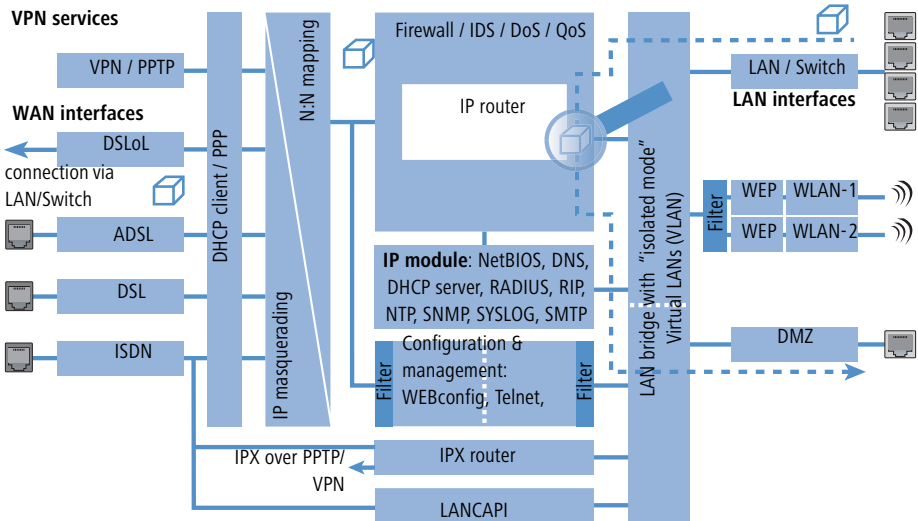
- The stations of the LAN can access the Internet, as well as servers in the DMZ.
- Servers of the DMZ have no access to the stations of the LAN. That guarantees that no “cracked” server of the DMZ becomes a security risk for the LAN.



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

► Chapter 7: Firewall

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.

7.3.7 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.

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.



If you operate a web server in your LAN, that has been permitted access to this service from the outside (see 'The hiding place—IP masquerading (NAT, PAT)' → page 64), 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.

Some typical applications are shown in the following.

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.



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 79):

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.

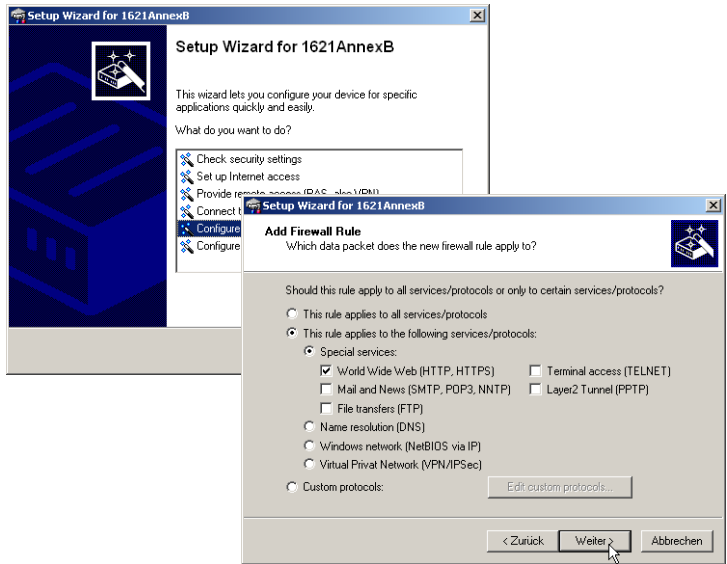


The LANCOM automatically sorts Firewall rules when creating the filter list. Thereby, the rules are sorted into the filter list on the basis of their level of detail. First all specific rules are considered, afterwards the general ones (e.g. Deny All). Examine the filter list in case of complex rule sets, as described in the following section.

7.3.8 Configuration of Firewall rules

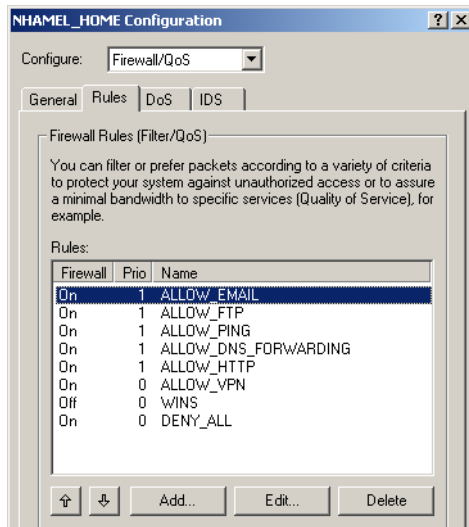
Firewall wizard

The fastest method to configure the Firewall is provided by the Firewall wizard in LANconfig:



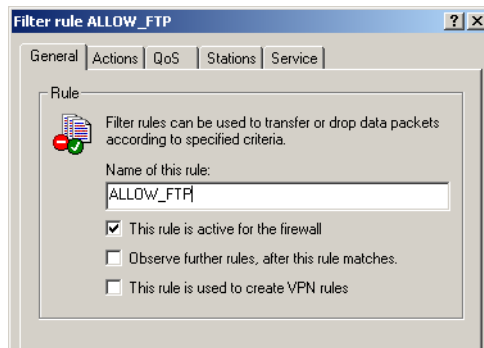
LANconfig

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:



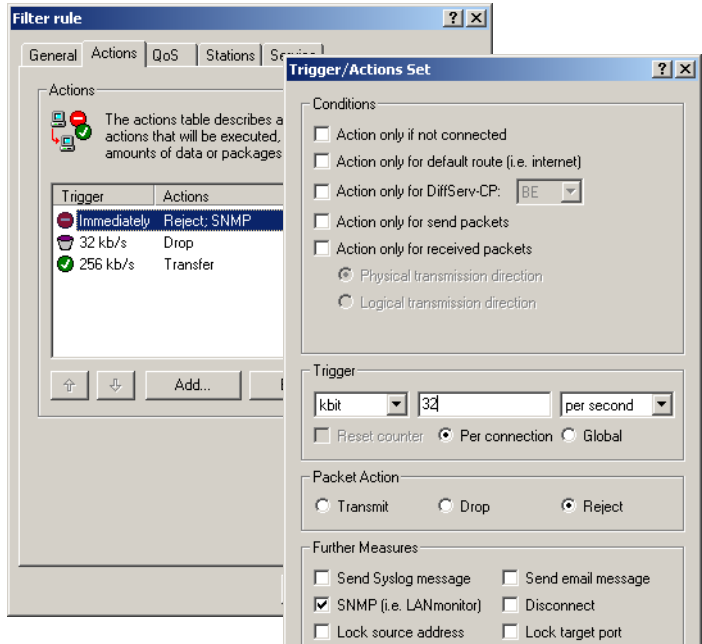
Within the dialogue for the definition of filter rules, the following options can be found on different index cards:

- **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.

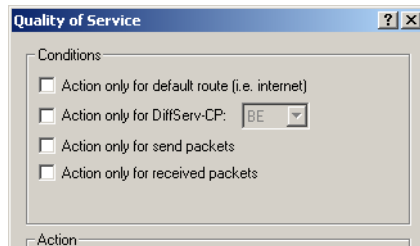


► Chapter 7: Firewall

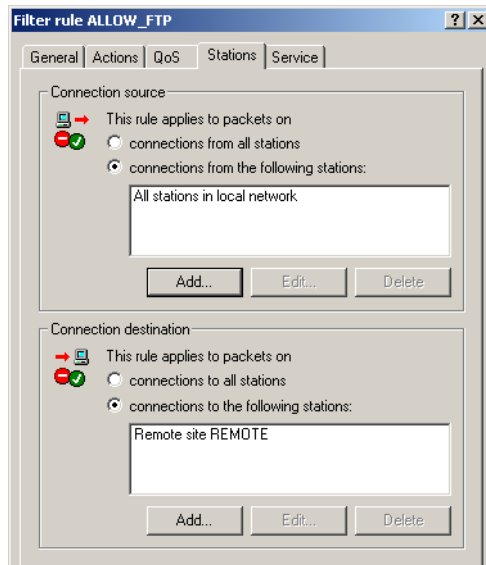
- The option 'Observe further rules ...' can be used to create complex functions ensuring e.g. certain bandwidths with QoS ('Connection' → page 119)
- The option 'This rule is used to create VPN rules' enables to utilize the information about source and destination networks of this rule also to define VPN networks ('Default VPN rules' → page 113).
- **Actions:** Here the Firewall actions are defined, consisting of condition, trigger, packet action and further measures.



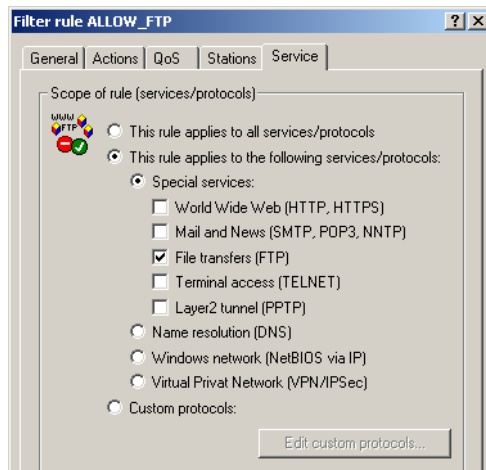
- **QoS:** Here you can assign minimum bandwidths for data packets specified by according Firewall rules (see also 'Defining minimum and maximum bandwidths' → page 176).



- **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 116.

The definition of the Firewall rules can be composed of entries of the object table for protocols, services, stations (→ page 137), and of entries of the

action table for Firewall actions(→ page 138). It can also contain direct descriptions in the appropriate LCOS syntax (e. g. %P6 for TCP).

[Expert Configuration](#)
[Setup](#)
[IP-router-module](#)
[Firewall](#)

Rule-table

Name	ALLOW_HTTP
Prot.	TCP
Source	LOCALNET
Destination	ANYHOST %S80,443,591,808,8080
Action	%Lcds0 %A
Linked	No
Prio	0
Active	Yes
VPN-rule	No

Done Internet



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.

► Chapter 7: Firewall

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 name list
Host name	%D	Note advice for host names (→ page 120)
MAC address	%E	00:A0:57:01:02:03
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.

[Expert Configuration](#)
 Setup
 IP-router-module
 Firewall

Object-table
Name
Description

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 174.	@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

Limit	Description	Object ID
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:

The screenshot shows a configuration window for a Firewall. At the top, there are three tabs: 'Setup', 'IP-router-module', and 'Firewall'. Below the tabs is the title 'Object-table'. There are two input fields: 'Name' with the value 'CLOSE_ON_FLOODING' and 'Description' with the value '%a %\cds8%d%\gbs100%h10%m'. At the bottom, there are two buttons: 'Apply' and 'Reset'.

- 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 (%\cds8) 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 (%\gbs100) 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.

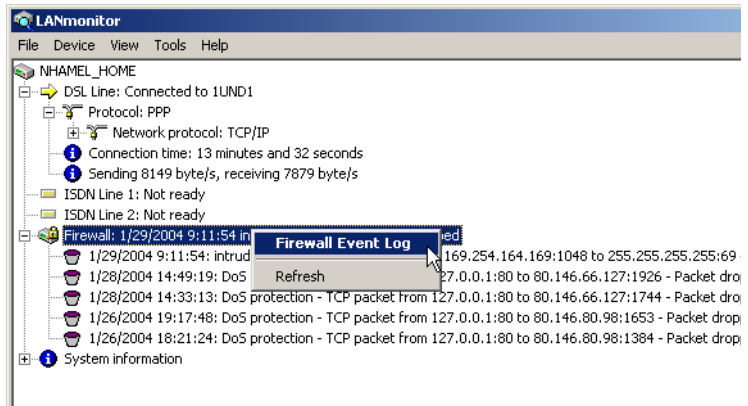
When building the actual filter table, action objects get minimized similarly to the address and service objects to the smallest necessary number, i.e. multiple definitions of an action get eliminated, and contradictory actions are turned into the "safest". Thus e.g. %a (accept) and %d (drop) becomes only %d, and %r (reject) and %d becomes %r.

7.3.9 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 143).

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.

► Chapter 7: Firewall

If you call up the logging table via LANmonitor, it looks like the following depiction:

LC_VPN_M_LCSTEST - Firewall Event Log									
Event Log View									
Idx.	System time	Source address	Dest. address	Prot	Source ...	Dest. p...	Filter rule	Limit	Ac
1	2/4/2004 12:12:41	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Pa
2	2/4/2004 12:11:40	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Pa
3	2/4/2004 12:06:45	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Pa
4	2/4/2004 12:05:44	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Pa
5	2/4/2004 12:02:32	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Pa
6	2/4/2004 12:01:31	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Pa
7	2/4/2004 12:00:04	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Pa
8	2/4/2004 11:59:03	10.1.1.11	10.1.255.255	17 (U...	137 (n...	137 (n...	intruder de...	Immediately	Pa
9	2/4/2004 11:55:08	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Pa
10	2/4/2004 11:54:07	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Pa
11	2/4/2004 11:48:05	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Pa
12	2/4/2004 11:47:04	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Pa
13	2/4/2004 11:45:00	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Pa

If you call up the logging table via WEBconfig, it looks like the following depiction:

[Expert Configuration](#)

[Status](#)

[IP-router-statistics](#)

Log-table

Idx.	System-time	Src-address	Dst-address	Prot.	Src-port	Dst-port	Filter-rule	Limit	
0001	1/29/2004 16:10:53	169.254.164.169	224.0.0.2	2	0	0	intruder detection	00000001	I
0002	1/29/2004 16:09:43	169.254.164.169	234.1.4.9	2	0	0	intruder detection	00000001	I
0003	1/29/2004 9:11:58	169.254.164.169	255.255.255.255	17	1048	69	intruder detection	00000001	I
0004	1/28/2004 14:49:23	127.0.0.1	80.146.66.127	6	80	1926	DoS protection	00000001	I
0005	1/28/2004 14:33:17	127.0.0.1	80.146.66.127	6	80	1744	DoS protection	00000001	I
0006	1/26/2004 19:17:52	127.0.0.1	80.146.80.98	6	80	1653	DoS protection	00000001	I
0007	1/26/2004 18:21:28	127.0.0.1	80.146.80.98	6	80	1384	DoS protection	00000001	I
0008	1/26/2004 17:38:41	127.0.0.1	80.146.80.98	6	80	1972	DoS protection	00000001	I

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

Element	Element meaning
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.
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 37). 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`:



```
D:\WINNT.4\System32\telnet.exe
Password:
LC1621.Internet:/
> show filter

Filter 0001 from Rule WINS:
  Protocol: 17
  Src: 00:00:00:00:00:00 0.0.0.0 0.0.0.0 137-139
  Dst: 00:00:00:00:00:00 0.0.0.0 0.0.0.0 0-0
  UPN-Flags: none
  Limit per conn.: after transmitting or receiving of 0 packets
  actions after exceeding the limit:
    reject if on default route

Filter 0002 from Rule WINS:
  Protocol: 6
  Src: 00:00:00:00:00:00 0.0.0.0 0.0.0.0 137-139
  Dst: 00:00:00:00:00:00 0.0.0.0 0.0.0.0 0-0
  UPN-Flags: none
  Limit per conn.: after transmitting or receiving of 0 packets
  actions after exceeding the limit:
    reject if on default route

LC1621.Internet:/
>
```

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
0001	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0
0002	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0
0003	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0
0004	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0
0005	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0
0006	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0
0007	1	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0

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.

Entry	Description
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.
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:

[Expert Configuration](#)

 [Status](#)

 [IP-router-statistics](#)

Connection-list

	Src-address	Dst-address	Prot.	Src-port	Dst-port	Timeout	Flags	Filter-rule	Src-route C
	192.168.2.60	80.190.240.17	6	3617	80	295	00020008	ALLOW_HTTP	1
	192.168.2.60	80.190.240.17	6	3618	80	296	00020008	ALLOW_HTTP	1
	192.168.2.60	212.227.15.181	6	3610	110	1	00020038	ALLOW_EMAIL	1
	192.168.2.60	212.227.15.181	6	3612	110	2	00020038	ALLOW_EMAIL	1
	192.168.2.60	212.227.15.181	6	3614	110	3	00020038	ALLOW_EMAIL	1

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.
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 149) 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
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.

7.3.10 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 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 information such as contracts, passwords, development information etc. should be transmitted only over protected connections, i.e. by using suitable data encryption and VPN connections.

7.4 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.

7.4.1 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 153): 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.

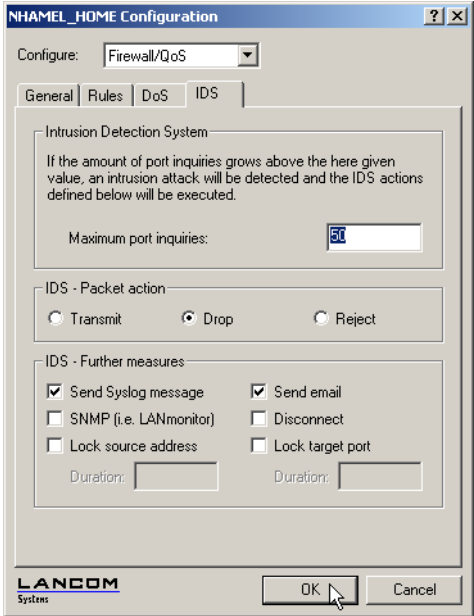
If a certain number of half-open connections between the scanned and the scanning computer exist, then this is reported as a port scan.

Likewise, the receipt of empty UDP packets is interpreted as an attempted port scan.

7.4.2 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 behaviour 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

7.5 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.

7.5.1 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.

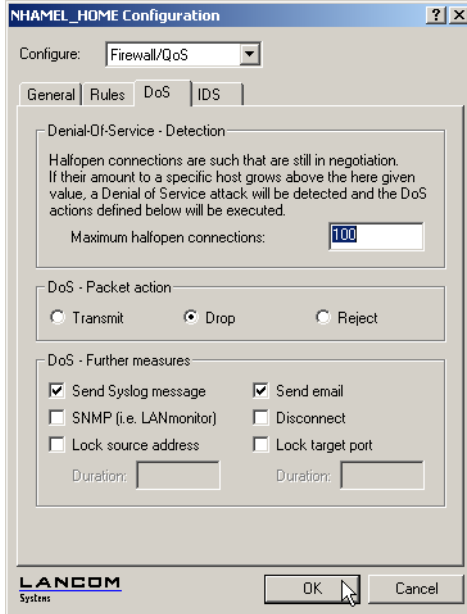


By default installation all items are configured as "secure", i.e. maximal 100 permissible half-open connections by different workstations (see SYN Flooding), at most 50 half-open connections of a single computer (see Portscan) of fragmented packets to be reassembled.

7.5.2 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 behaviour 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

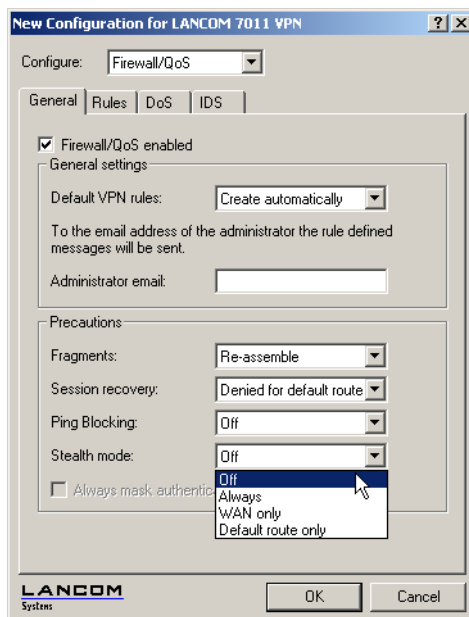
However, always active are the following protection mechanisms:

- Address examination (against IP Spoofing)
- Blocking of broadcasts into local area network (against Smurf and Co).

7.5.3 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':



► Chapter 7: Firewall

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

8 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.

8.1 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 another 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.

8.2 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

► Chapter 8: Quality of Service

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 prioritisation 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
CS5	101000	40
CS6	110000	48
CS7	111000	56

Code point	DSCP bits	Dec.
AF11	001010	10
AF12	001100	12
AF13	001110	14
AF21	010010	18
AF22	010100	20
AF23	010110	22
AF31	011010	26
AF32	011100	28

Code point	DSCP bits	Dec.
AF33	011110	30
AF41	100010	34
AF42	100100	36
AF43	100110	38
EF	101110	46

8.2.1 Guaranteed minimum bandwidths

Hereby you give priority to enterprise-critical applications, e.g. Voice-over-IP (VoIP) PBX systems or certain user groups.

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.

8.2.2 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.

8.3 The queue concept

8.3.1 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 63).

► Urgent queue II

This is for all packets that have been assigned a guaranteed minimum bandwidth, but whose connection has exceeded this minimum bandwidth.

► Chapter 8: Quality of Service

EN

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"

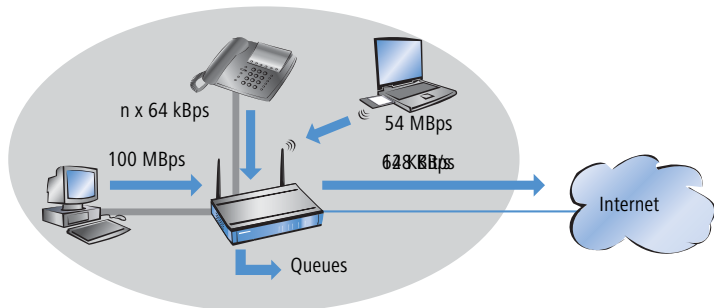
▷ Packets with DiffServ "Assured Forwarding"

► 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.

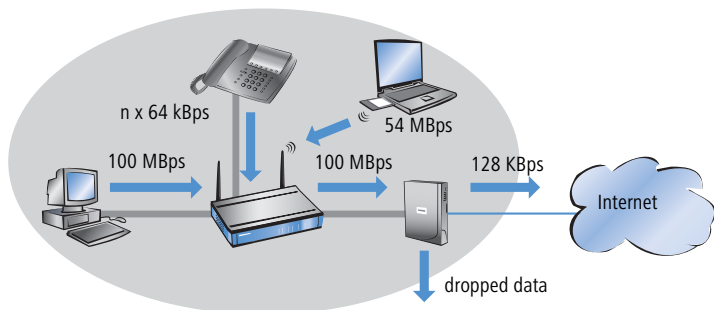
The queue concept can, however, only work out when a "traffic congestion" of data packets has been accumulated at the interface from LAN to the WAN. Such a congestion is created when the interface within the LANCOM can submit fewer data to the WAN than data are delivered in peak periods from the LAN. 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.



EN

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 happen within the broadband modem. But because no queues are deployed therein, surplus data will be lost. Thus a prioritisation 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!

8.3.2 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 receiveable. All data packets received on the WAN interface are transferred to the LAN with equal rights.

In order to be able to prioritise 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

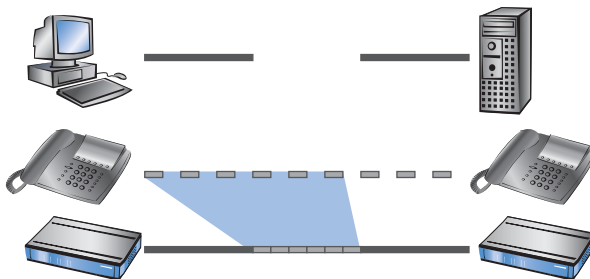
All packets that do not need special treatment because of an active QoS rule on the receiving side end up here. Packets of this queue are directly passed on resp. confirmed without consideration of maximum bandwidths.

8.4 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.



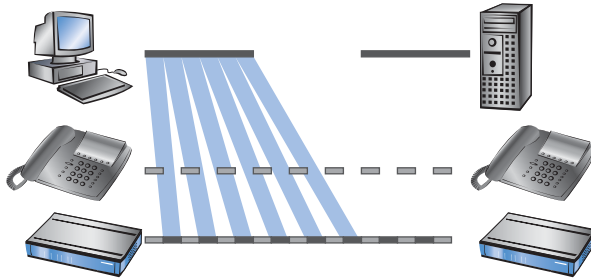
The FTP transfer uses quite large data packets of 1500 byte, whereas, the Voice over IP connection sends packets of e.g. 24 byte net in relatively short intervals. If FTP packets are in the sending queue of the LANCOM just at the moment when a VoIP packet is to be transferred, then the VoIP packet can 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 behaviour 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.

► Chapter 8: Quality of Service

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.

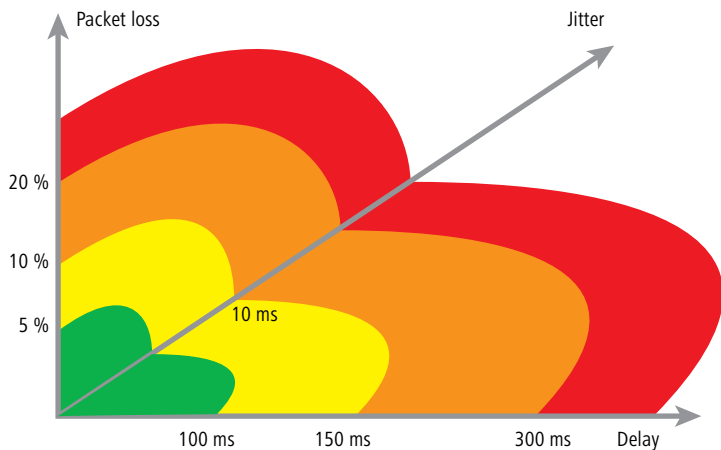
- The LANCOM is able to split packets to be sent above an adjustable maximum size (e.g. 256 byte) into smaller units itself. But such a procedure called "fragmentation" is not supported by all servers of the Internet, because dealing with fragmented packets is considered as a security risk, and therefore 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.

8.5 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.



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.

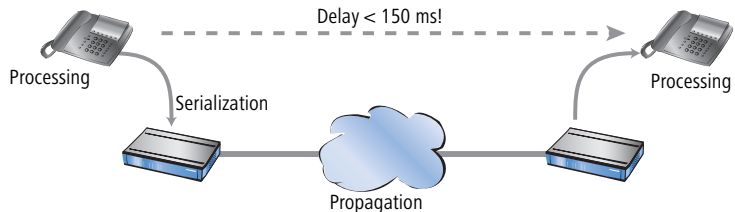
Apart from the average delay time, also a variation in this delay is perceived by the human ear. Delay differences of the voice information from sender to addressee (jitter) are still tolerated up to 10 ms, and values beyond considered as irritating.

► Chapter 8: Quality of Service

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.

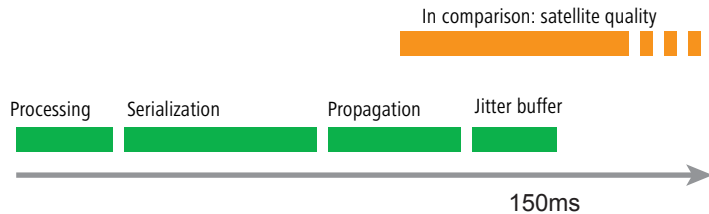
- Jitter can be removed in the receiving station by an appropriate buffer. In this buffer (jitter buffer) the packets are stored intermediately, and passed on at a constant rate to the addressee. By this intermediate buffering, the delay variations due to individual transmission times of the individual 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

► Chapter 8: Quality of Service

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

EN

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	Processing	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.

8.6 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 reduc-

tion always the physical data transfer via the respective interface applies as the direction!

8.7 QoS configuration

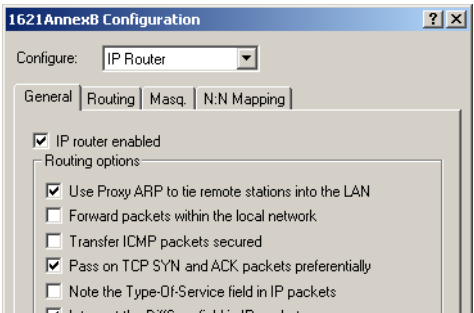
8.7.1 Evaluating ToS and DiffServ fields

EN

LANconfig

ToS or DiffServ?

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 prioritisation 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 module/Routing method
Telnet	Setup/IP router module/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:

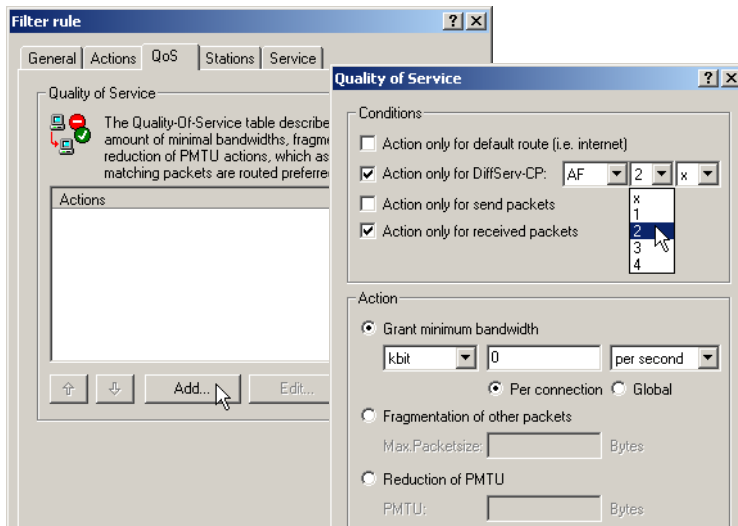
DSCP code points	Kind of transmission
CSx (including CS0 = BE)	normal transmission
AFxx	secured transmission
EF	preferred transmission

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 161.

► Chapter 8: Quality of Service

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 module/Firewall/Rule list
Telnet	Setup/IP router module/Firewall/Rule list

EN

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 95.

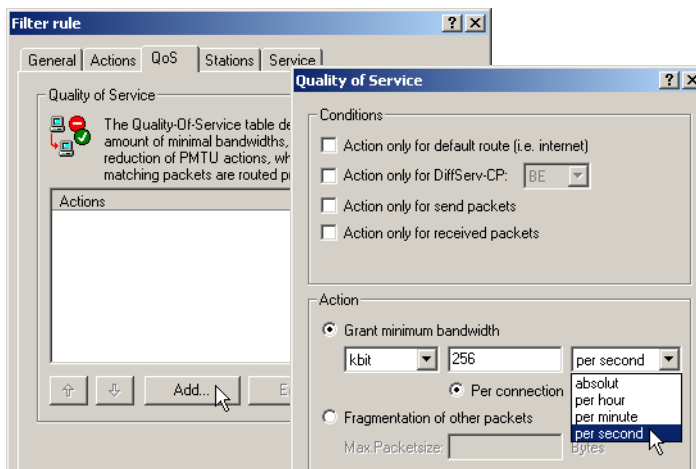
8.7.2 Defining minimum and maximum bandwidths

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 '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 module/Firewall/Rule list
Telnet	Setup/IP router module/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.

► Chapter 8: Quality of Service

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 95.

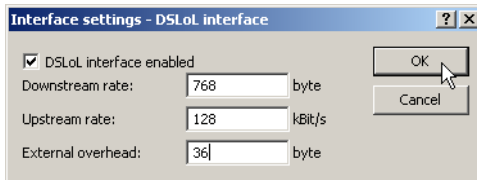
8.7.3 Adjusting transfer rates for interfaces



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 'Management' on index card 'Interfaces' within the settings for the different WAN interfaces:



- An Ethernet WAN (DSL/cable) and DSLoL 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 163).
- 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

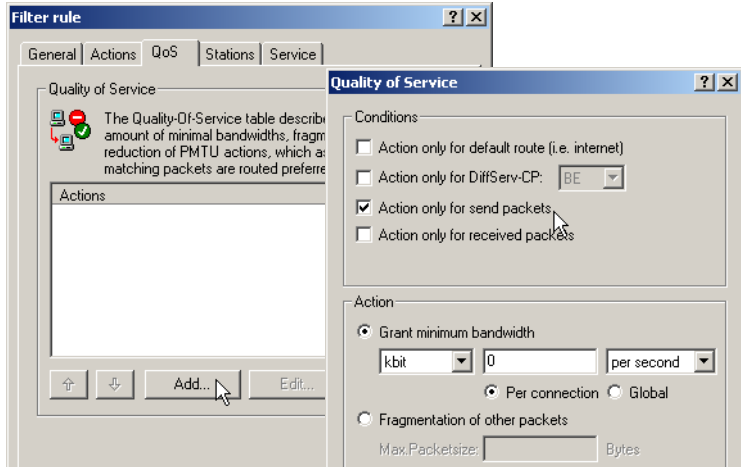


Only upstream and downstream rates are indicated by Kbps, external overhead in bytes/packet.

8.7.4 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 module/Firewall/Rule list
Telnet	Setup/IP router module/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%

8.7.5 Reducing the packet length

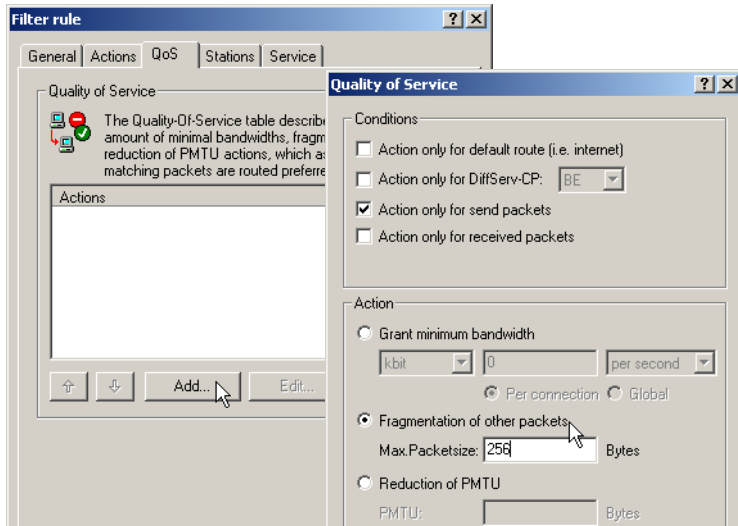
The length reduction of the data packets is defined by a Firewall rule according to the following conditions:

► 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.

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 module/Firewall/Rule list
Telnet	Setup/IP router module/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 Virtual LANs (VLANs)

9.1 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 be 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.

9.2 This is how a VLAN works

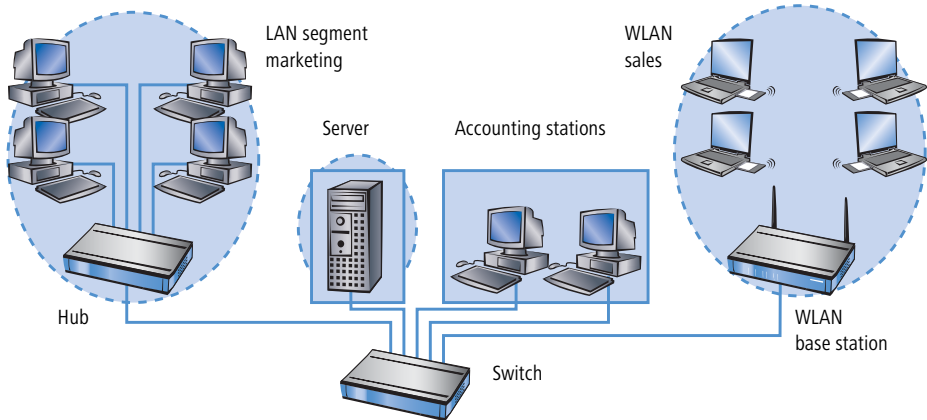
By defining VLANs on a LAN the following goals should be achieved:

- 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.

► Chapter 9: Virtual LANs (VLANs)

- 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.

9.2.1 Frame tagging

In order to shield or, if necessary, to prioritise 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 190).

- **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 behaviour 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.

9.2.2 Conversion within the LAN interconnection

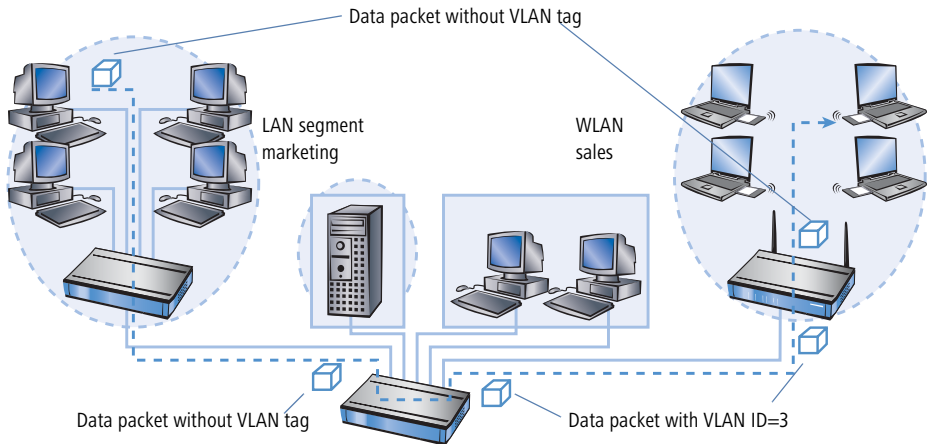
Certain stations shall be grouped to logical units by virtual LANs. But the stations themselves are usually neither able to generate the required VLAN tags, nor able to handle them.

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

► Chapter 9: Virtual LANs (VLANs)

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.

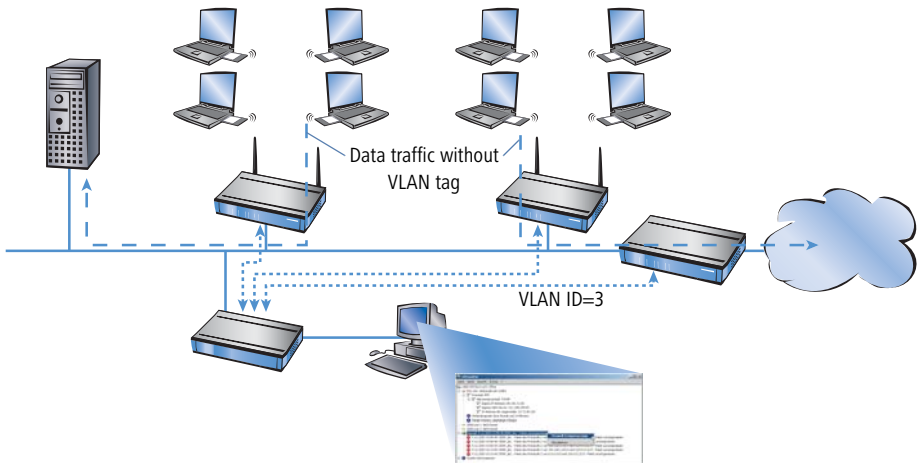
9.2.3 Application examples

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.



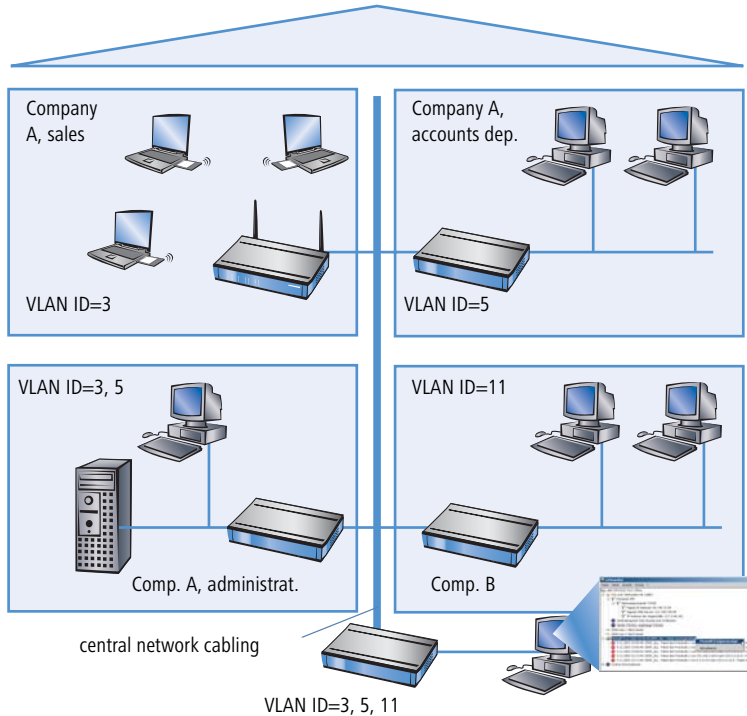
By setting up a virtual LAN between the base stations and the administrator's switch, management data is shielded against all "public" traffic on the LAN.

Different organisations 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.

► Chapter 9: Virtual LANs (VLANs)

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.

9.3 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.

9.3.1 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 (→ page 190).

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

EN

9.3.2 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.

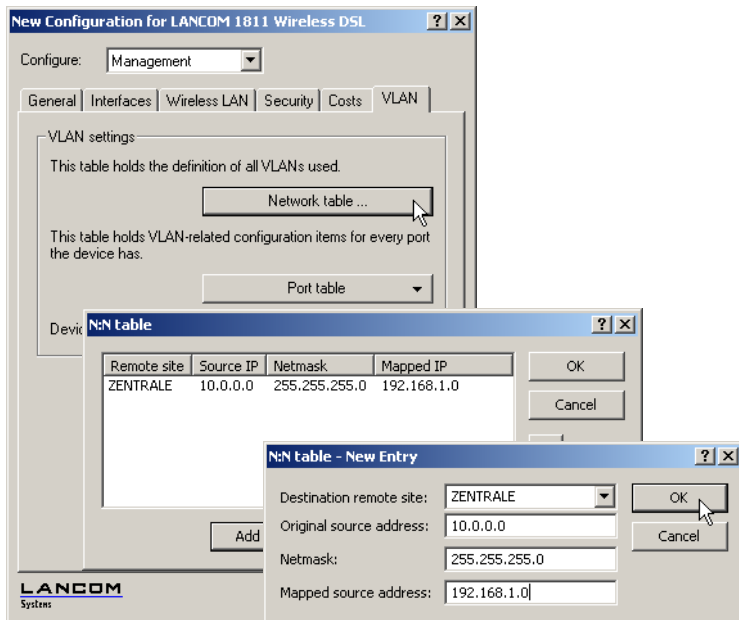
Example for a port table:

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

Port	Use tagging	Allow untagged frames	Allow all VLANs	Default ID
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

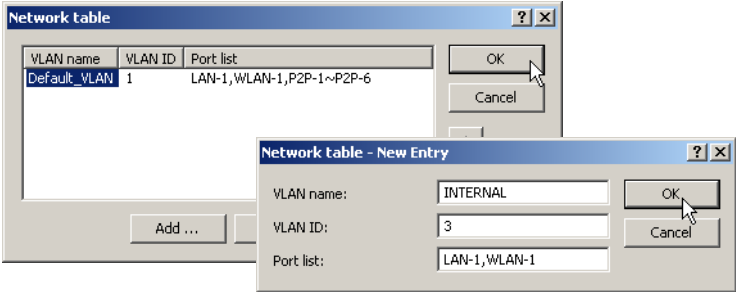
9.3.3 Configuration with LANconfig

Parameters for virtual networks can be set with LANconfig under 'Management' on the register card 'VLAN':

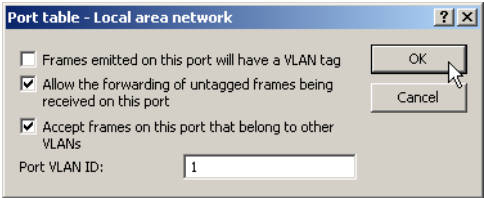


► Chapter 9: Virtual LANs (VLANs)

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:

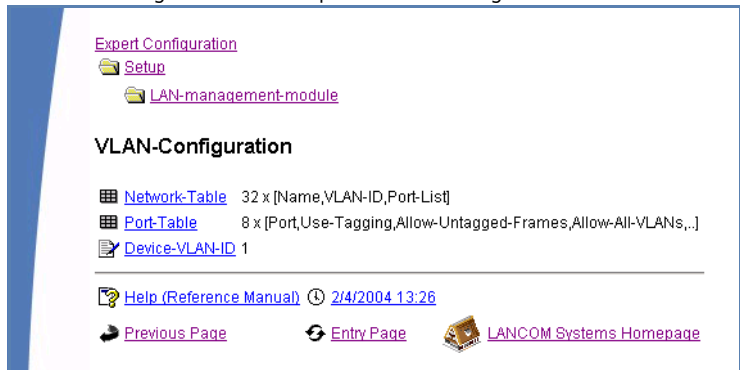


9.3.4 Configuration with WEBconfig or Telnet

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 module ► VLAN Configuration
Terminal/Telnet	cd /Setup/LAN Management module/VLAN Configuration

The VLAN configuration shows up under WEBconfig as follows:





Expert Configuration


Setup



LAN-management-module




VLAN-Configuration

 [Network-Table](#) 32 x [Name,VLAN-ID,Port-List]

 [Port-Table](#) 8 x [Port,Use-Tagging,Allow-Untagged-Frames,Allow-All-VLANs,...]

 [Device-VLAN-ID](#) 1

 [Help \(Reference Manual\)](#)  2/4/2004 13:26

 [Previous Page](#)  [Entry Page](#)  [LANCOM Systems Homepage](#)

10 Office communications with LANCAP

LANCAP from LANCOM 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.

This section briefly introduces the LANCAP and its use for office communications tasks.

10.1 What are the advantages of LANCAP?

The main advantages of using LANCAP are economic. LANCAP 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 LANCAP, the PC forwards the fax via the network to the router which establishes the connection to the recipient.



Please note: All LANCAP-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!

10.2 The client and server principle

The LANCAP is made up of two components, a server (in the LANCOM) and a client (on the PCs). The LANCAP client must be installed on all computers in the LAN that will be using the LANCAP functions.

10.2.1 Configuring the LANCAP server

Two basic issues are important when configuring the LANCAP server:

- What call numbers from the telephone network should LANCAP respond to?

► Chapter 10: Office communications with LANCAPi

- Which of the computers in the local network should be able to access the telephone network via LANCAPi?

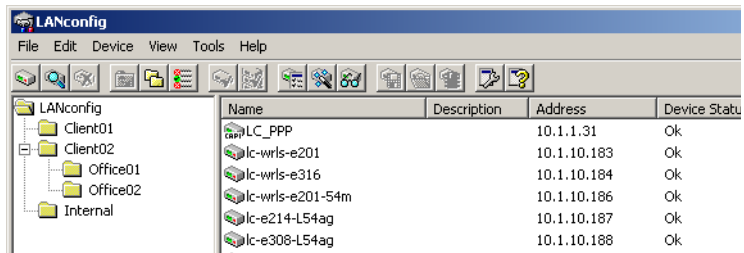
The LANCAPi server is configured in the following menus:

Configuration tool	Run command/menu
LANconfig	LANCAPi
WEBconfig	Expert Configuration / Setup / LANCAPi-module
Terminal/Telnet	cd /setup/LANCAPi-module

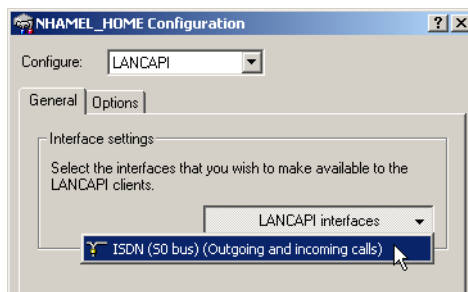
EN

Example configuration with LANconfig

- ① Open the configuration of the router by double-clicking on the device name in the list and select the configuration area **LANCAPi**.

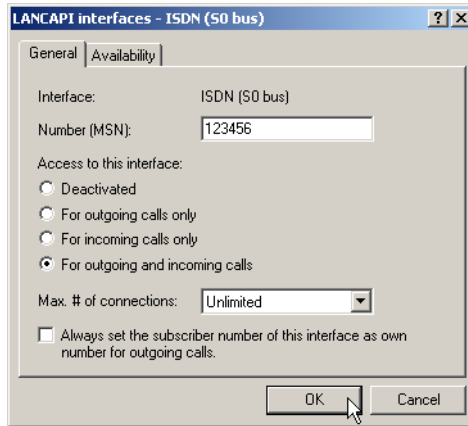


- ② Select the ISDN port you want to set.



► Chapter 10: Office communications with LANCAP1

- ③ Activate the LANCAP1 server for the outgoing and incoming calls, or allow only outgoing calls.

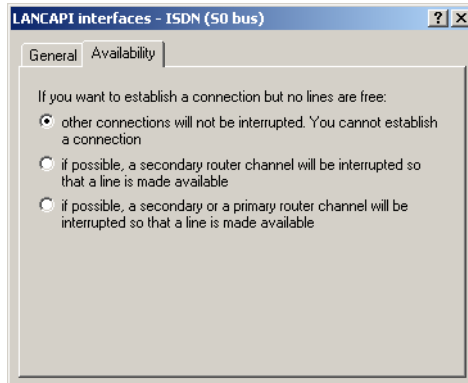


- ④ In the latter case, the LANCAP1 will not respond to incoming calls—to receive faxes, for example. Permitting outgoing calls only is useful if you do not have a specific call number available for the LANCAP1.
- ⑤ When the LANCAP1 server is activated, enter the call numbers to which the LANCAP1 should 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 LANCAP1.
- ⑥ LANCAP1 is preset to use IP port '75' (any private telephony service). Do not change this setting unless this port is already in use by a different service in your LAN.
- ⑦ If you do not wish all the computers in the local network to be able to access the LANCAP1 functions, you can define all the authorized users (by means of their IP addresses) by entering them in the access list.



If you enter more than one call number for the LANCAP1, you can, for example, provide each individual workstation with a personal fax machine or personal answering machine. Proceed as follows: When installing communications programs on the different workstations, specify the various call numbers to which the program should respond.

- ⑧ Switch to the 'Availability' tab. Here you can determine how the LANCOM should respond if a connection is to be established via the LANCAP (incoming or outgoing) when both B channels are already busy (priority control).



The meaning of the options offered here:

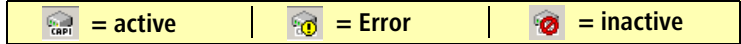
- The connection via *LANCAP* can not be performed. A fax program using the *LANCAP* will then probably attempt to send again at a later time.
- The connection via the LANCAP can then be established when a main channel is free. A main channel is the first B channel used when a router connection is established. Secondary channels are used for channel bundling. The LANCAP must wait if two router connections are established to separate remote stations (two main channels busy).
- A connection via LANCAP can always be established; an existing router connection will be terminated for the duration of the call if required. This can be used to ensure the permanent availability of the fax function, for example.

10.2.2 Installing the LANCAP client

- 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 **LANCAP** 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.



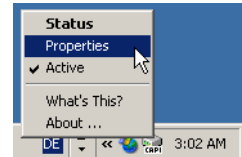
10.2.3 Configuration of the LANCAPI clients

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.

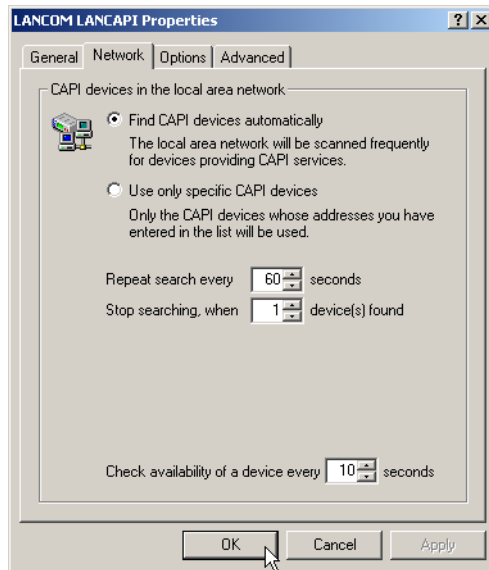


You can also run the LANCAPI client through the Windows task bar. To do this, simply click with the right mouse button on the LANCAPI symbol in the Windows task bar next to the clock and select **Properties**.



- 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.



10.3 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'.

10.4 The LANCOM 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.

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.



The LANCOM CAPI Faxmodem requires LANCAPI for the transmission of fax messages. A small CAPI icon in the lower right corner of your screen confirms that LANCAPI is enabled. Please also take care with the settings of the LANCAPI itself.

11 Server services for the LAN

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

11.1 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.

11.1.1 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

► Chapter 11: Server services for the LAN

- 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.

11.1.2 DHCP—'on', 'off' or 'auto'?

The DHCP server can be set to three 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.
- '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.
 - ▷ The device then disables its own DHCP server if any other DHCP servers are found. 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.

Whether the DHCP server is active or not can be seen in the DHCP statistics.

The default setting for this condition is 'auto'.

11.1.3 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 Neighbourhood.

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-module Table-DHCP
Terminal/Telnet	setup/DHCP-module/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.

11.2 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.

11.2.1 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.

► Chapter 11: Server services for the LAN

- 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.

EN

11.2.2 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-module ► DNS-default ► DNS-backup
Terminal/Telnet	/setup/TCP-IP-module/DNS-default /setup/TCP-IP-module/DNS-backup

EN

- 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.

11.2.3 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-module
Terminal/Telnet	cd /setup/DNS-module

Proceed as follows to set the DNS server:

- ① Switch the DNS server on.

WEBconfig	... ► Operating
Terminal/Telnet	set operating on

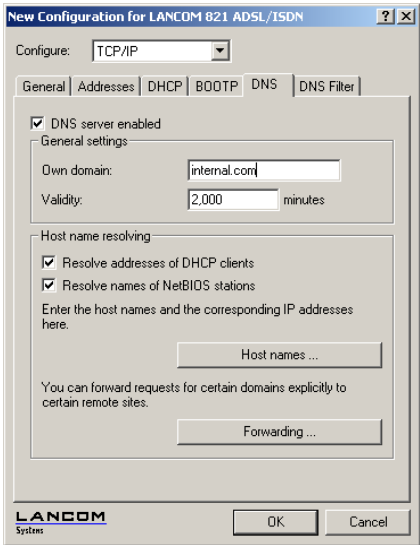
► Chapter 11: Server services for the LAN

- 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

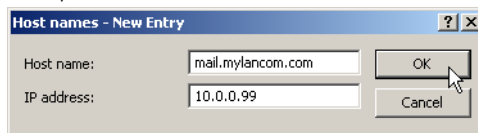
- ④ The main task of the DNS server is to distinguish requests for names in the Internet from those for other remote stations. Therefore, enter all computers in the Host names table,
- ▷ for which you know the name and IP address,
 - ▷ that are not located in your own LAN,
 - ▷ that are not on the Internet 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	<pre>cd setup/DNS-module/DNS- table set mail.yourdomain.com 10.0.0.99</pre>

For example, if you 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.

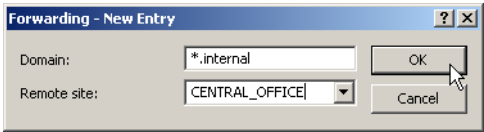
When you now start your mail program, it will probably automatically look for the server 'mail.yourdomain.com'. The DNS server thereupon returns the IP address '10.0.0.99'. The mail program will then look for that IP address. With the proper entries in the IP routing table and name list, a connection 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	<pre>cd setup/DNS-module/ DNS-destination- table set *.intern COMPANY</pre>

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.

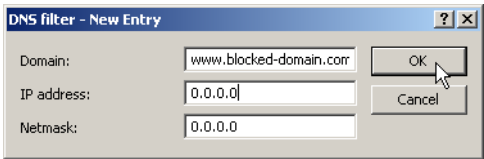
11.2.4 URL blocking



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	<pre>cd setup/DNS-module/filter-list set 001 www.blocked.com 0.0.0.0 0.0.0.0</pre>



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:



DNS filter - New Entry

Domain: *.com

IP address: 10.0.0.23

Netmask: 255.255.255.255

OK Cancel

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.

11.2.5 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://MyLAN-COM.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, and transfer this address - in case of a change - to their respective Dynamic DNS server.

► Chapter 11: Server services for the LAN

The current WAN IP address of a LANCOM can be picked under the following address:

`http://<address of LANCOM>/config/1/6/8/3/`

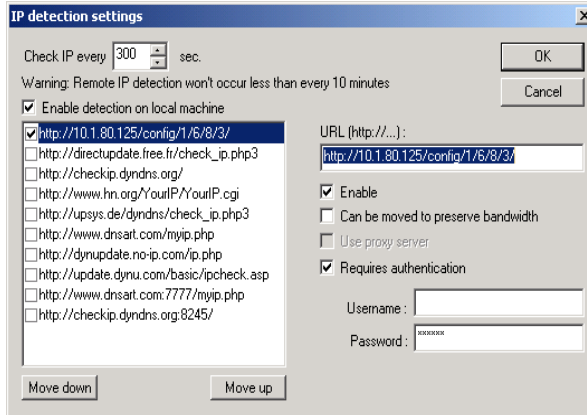


Figure: Picking the current IP address out of a LANCOM

11.3 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.

11.3.1 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 maxi-

mum 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!

11.3.2 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 LANCAPAPI are not affected.

11.3.3 Settings in the charge module

Configuration tool	Run/table
LANconfig	Management ► Costs
WEBconfig	Expert Configuration ► Setup ► Charges-module
Terminal/Telnet	<code>cd /setup/charges-module</code>

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.

11.4 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.

11.4.1 Setting up the SYSLOG module

Configuration tool	Run/Table
LANconfig	Management ► Log & Trace
WEBconfig	Expert Configuration ► Setup ► SYSLOG-module
Terminal/Telnet	cd /setup/SYSLOG-module

11.4.2 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 clients - New Entry

IP address: 10.1.0.160

Source:

- ☒ System
- ☒ System time
- ☒ Connections
- ☐ Administration
- ☒ Login
- ☐ Console login
- ☐ Accounting
- ☐ Router

Priority:

- ☒ Alert
- ☒ Warning
- ☐ Debug
- ☒ Error
- ☒ Information

OK Cancel

SYSLOG comes from the UNIX world, in which specified sources are pre-defined. 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

► Chapter 11: Server services for the LAN

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

Priority	Meaning	SYSLOG priority
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`.

12 Appendix

12.1 SNMP traps

MIB2:-Traps	
coldstart	
warmstart	
authentication failed (= Console login failed)	
enterprise specific	

enterprise pecific Traps:	
Firmware upload started	
Configuration upload started	
Upload succeeded	
Upload failed (timeout)	
Upload failed (incomplete)	
Upload failed (bad device)	
Configuration download started	
Download succeeded	
Console login	
Console logout	
Firewall-Traps	
Connection status (=> LAN-monitor)	
VPN Connection status	
WAN-Ethernet UP/DOWN Link Trap	

WLAN-Traps

WLAN Scan started	
Started WLAN BSS ID	
Joined WLAN BSS ID	
Authenticated WLAN station	
Deauthenticated WLAN station	
Associated WLAN station	
Reassociated WLAN station	
RADIUS access check for WLAN station succeeded	
RADIUS access check for WLAN station failed	
Disassociated WLAN station due to station request	
Rejected Association from WLAN station	
WLAN card hung, resetting	

12.2 Overview of functions for LANCOM models and LCOS versions

	800 1000 1100	I-10	821	1511	1521	1611	1621	1811	1821	3050 3550	4000 4100	6000 6001 6021	7011	L-2	IL-2	L-11	IL-11	L-54g	L-54ag
Stateful Inspection	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80
DoS	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80
IDS	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80
QoS	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30
N:N mapping						3.30		3.30	3.30	3.30	3.30	3.30	3.30						
VLAN				3.30	3.30			3.30	3.30	3.30						3.30	3.30	3.30	3.30
DMZ port			1)	1)	1)		1)	1)	1)				✓						
DES, 3-DES, Blowfish						✓ ²⁾	✓ ²⁾	✓ ²⁾	✓ ²⁾	✓ ²⁾	✓ ²⁾	✓	✓						
AES						3.20 ²⁾	3.20 ²⁾	3.20 ²⁾	3.20 ²⁾	3.20 ²⁾	3.20 ²⁾	3.20	3.20						
VPN-5 option						integrated with 3.32	integrated with 3.32	integrated with 3.32	integrated with 3.32	✓	✓								
VPN hardware accelerator								in association with VPN-25	in association with VPN-25										
VPN-25 option						✓	✓	✓	✓	✓	✓								
VPN-100												✓							
VPN-200													✓						
ADSL modem			✓		✓		✓		✓										
4-port switch			✓	✓	✓		✓	✓	✓										
ISDN leased line option	✓	✓	✓	✓	✓	✓	✓	✓	✓		integrated	integrated	integrated		✓		✓		
Fax modem option	✓	—	—	—	—	—	—	—	—	—	integrated	✓	—	—	✓		✓	—	—
Dynamic DNS	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10			3.10	3.10	3.10	3.10
DSLolL			3.10				3.10									3.10	3.10	3.10	3.10
CRON	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10

¹⁾ Port separation (Private mode)

²⁾ only, if the respective VPN options of the devices are activated.

13 Index

Numerics

1:1 mapping	74
3-DES	222
4-port switch	222

A

AAL-5	81
Access protection	48
for the configuration	48
by name or number	48
by number	48
via TCP/IP	44

Address administration	
IP address administration	201

Address pool	203
--------------	-----

ADSL	26, 39
------	--------

ADSL modem	222
------------	-----

AES	222
-----	-----

AOCD	215
------	-----

ATM	26, 39
-----	--------

ATM adaptation layer	81
----------------------	----

Auth.	89
-------	----

Authentication	86
----------------	----

auto reconnect	88
----------------	----

Availability	197
--------------	-----

B

B-channel	
protocol	49

Bonk	155
------	-----

Brute force	43
-------------	----

Bruttodatenrate	166
-----------------	-----

C

Call charge	
information	215
limit	214
management	194, 214

Callback	48, 50
----------	--------

according to RFC 1570	90
-----------------------	----

Fast callback	50
---------------	----

for Microsoft CBCP	88
--------------------	----

Callback procedure	
fast callback	89

Caller ID	48
-----------	----

Calling Line Identifier Protocol	50
----------------------------------	----

Capab.	206
--------	-----

CAPI Faxmodem	199
---------------	-----

CAPI interface	194
----------------	-----

Channel bundling	92
------------------	----

dynamic	92
---------	----

static	92
--------	----

Charge limiting	214
-----------------	-----

Charges	
---------	--

information	92
-------------	----

units	92, 215
-------	---------

CLIP	49, 50
------	--------

Collision domain	183
------------------	-----

Command line interface	30
------------------------	----

Command line reference	31
------------------------	----

Common ISDN Application	
-------------------------	--

Programming Interface (CAPI)	194
------------------------------	-----

Computer names	206
----------------	-----

Conf	87
------	----

Configuration	
---------------	--

procedure	13
-----------	----

SNMP	18
------	----

Configuration files	27
---------------------	----

Configuration interface	13
-------------------------	----

Connection limit	215
------------------	-----

Cost reduction	214
----------------	-----

CRON	222
------	-----

D

D channel	26, 39, 49
-----------	------------

Data compression procedure	
----------------------------	--

LZS	93
-----	----

► Index

Data transfer	92	available information	208
Denial of Service attacks		filter mechanism	207
Bonk	155	DNS-table	211, 212
Ping of Death	154	Dynamic DNS	213
Teardrop	155	Domain	206, 212
Denial-of-Service-Angriffe	153	deny access	213
Fragrouter	155	Domain name service (DNS)	
LAND	154	DNS	206
Smurf	153	DoS	222
SYN Flooding	153	Downstream rate	166
Device-name	86	DSCP	161
DHCP	25, 38, 81, 201	DSLol	222
assignment		Dynamic channel bundling	92
broadcast address	204	Dynamic DNS	213, 222
DNS and NBNS server	204	Dynamic Host Configuration	
network mask	203	Protocol (DHCP)	201
standard gateway	204	Dynamic routing	56
DHCP server	201, 207	E	
mode	202	E-mail virus	129
for WINS resolution	205	Encapsulation	80
period of validity	204	End address	203
Dial-Up Network	18	ETH-10	81
Dial-Up Networking	49	Exclusion routes	57
Differentiated Services –		exposed host	69
see DiffServ		F	
Differentiated Services Code Point –		Fail	87
see DSCP		Fast callback	50
DiffServ	160, 161	Fax	199
Assured Forwarding	160, 161	Fax Class 1	199
Best Effort	161	Fax driver	199
Class Selector	161	Fax modem option	222
Expedited Forwarding	160, 161, 163	Fax transmission	200
IPSec	160	Filter	64
Distance of a route	58	Firewall	64, 194
DMZ	67, 70	Firmware-upload	29
IP address assignment	203	with LANconfig	29
DMZ port	222	with terminal program	30
DNS	26, 39, 206	with TFTP	30
DNS forwarding	208	with WEBconfig	30
DNS server	201, 204, 206		

Flash ROM memory	28	IP-Spoofing	151
Flat rate	87	Inverse masquerading	68, 71
Fragrouter	155	IP broadcast	62
Frame tagging	184	IP header	160
FTP		IP masquerading	25, 38, 64, 71
active FTP	173	simple masquerading	68
passive FTP	173	IP multicast	62
TCP-secured transfer	168	IP routing	
FTP data transfer	167	standard router	58
FTP download	159	IP telephony	167
G		IP4 address	71
Gateway	64, 201	IP-address	23, 36, 64, 84
Gross data rate	166	IP-routing-table	56
H		IP-Spoofing	151
HDLC	81	ISDN	
High telephone costs	214	D channel	50
Host	206	ISDN leased line option	222
Host name table	210	K	
HTTPS	17	Keep-Alive	87
I		L	
ICMP	131	LAN	
Identification control	48	Different organisations on one	
Identifying the caller	48	LAN	187
IDS	222	LANCOM FirmSafe	28
IEEE 802.1p/q	183	LANconfig	14, 19, 29
IEEE 802.3	81	Management of multiple devices	16
Inband	13	LAND	154
inband		LANmonitor	21, 35
Configuration via Inband	13	display options	22, 35
with Telnet	17	monitor Internet connection	22, 36
Install software	28	system information	22, 35
Internet	64	Layer-2	81
Internet access	85	Layer-2-switch	183
Intranet		Layer-3	81
IP address assignment	203	LCOS	8, 222
Intranet address	67	LCP echo reply	84
Intrusion Detection	151	LCP echo request	84
Intrusion-Detection		LCR	215
		Least-cost routing	215

► Index

- LLC-MUX 80
 Logging table 143
 Logical LAN 185
 Logical sending direction 173
 Login 29, 43
 Login barring 43
 Loopback address 74
 LZS data compression 93
- M**
- MAC frame 185
 Mail server 211
 Maximum bandwidth 161, 163
 Microsoft Network 205
 Minimum bandwidth 160, 162, 163
 Reception 162
 Sending 162
 Modem 81
 Monitoring 21, 35
 MS-CHAP 82, 83
 Multilink PPP (MLPPP) 82, 92
- N**
- N:N mapping 71, 222
 Configuration 75
 Decentralized mapping 74
 Firewall 76
 Loopback address 76
 NAT table 75
 Network coupling via VPN 72
 Routing table 76
 VPN rule 76
 Central mapping 75
 DNS forwarding 76
 NAT 64, 70
 NBNS server 201, 205
 Net data rate 166
 NetBIOS 26, 39, 207
 NetBIOS networks 207
 NetBIOS proxy 129
 Nettodatenrate 166
- Network Address Translation 70
 Network coupling 72
 Network names 206
 No charge information 215
- O**
- Office communications 194
 Online minutes 214
 Outband 13
 configuration via Outband 13
 Overhead 159
- P**
- Packet dump 26, 39
 passwd 43
 Password 21, 23, 36, 41, 48, 49, 86
 PAT 64
 Period 214
 Period of validity 202, 204
 Physical LAN 184
 Physical sending direction 173
 Ping 131
 Ping blocking 114
 Ping of Death 154
 Ping-Blocking 114
 PMTU reduction 168
 Port 68
 IP port 196
 Port Address Translation 71
 Port separation 222
 PPP 23, 36, 48, 81, 92
 callback functions 88
 checking the line with LCP 84
 handshake 20
 IP address assignment 84
 LCP Extensions 90
 PPP client 19
 PPP connection 20
 PPPoE 81
 Precedence 161
 Priority control 197

Protection			
for the configuration	41		
for the LAN	64		
Q			
QoS	167, 222		
Direction of data transfer	173		
QoS –			
siehe Quality-of-Service			
Quality of Service	159		
Quality-of-Service	159		
Queue	163		
Queues	163		
Secured queue	164		
Standard queue	164		
Urgent queue I	163		
Urgent queue II	163		
R			
Remote access	18, 85		
Remote configuration	13		
Remote connection	19		
Remote control	72		
Remote maintenance			
with N:N mapping	73		
Remote-ID	86		
Repetitions	87		
RIP	25, 38		
Router-interface-list	93		
Router-name	57		
S			
Security	41, 64		
Security checklist	51		
Security procedures	49		
Security settings	9, 43		
Serial port	13		
Single user access	64		
Smurf	153		
SNMP	18		
SNMP trap	73		
Stac data compression	93		
Standard fax programs	199		
Start address	203		
Stateful Inspection	222		
Static channel bundling	92		
Static routing	56		
SYN Flooding	153		
SYN/ACK speedup	63		
SYSLOG	216		
T			
TCP	159		
TCP- control packets	163		
TCP Stealth mode	115		
TCP/IP	56		
TCP/IP networks	206		
TCP-Stealth-Modus	115		
Teardrop	155		
Telnet	19		
Term	87		
Terminal program	29		
TFTP	17		
Throughput	92		
Time	87		
Time budget	215		
Time dependent connection-			
limit	215		
Time-out	92, 93		
ToS	160, 161		
High Reliability	160		
IPSec	160		
Low Delay	160, 163		
Priority	161		
Trace			
examples	27, 40		
keys and parameters	24, 37		
outputs	24, 37		
starting	24, 37		
Transmission rates	23, 37		
Trojans	129		

► *Index*

Troubleshooting 22, 35
 Type-of-Service –
 see ToS

U

UDP 159
 Upload 28
 Upstream rate 166
 User name 20, 49, 86

V

V.110 81
 VC-MUX 80
 Virtual LAN 183
 VLAN 183, 222
 Allow all VLANs 190
 Allow untagged frames 190
 Connection of WLAN stations 187
 Conversion in the interfaces 185
 Default ID 190
 Default-VLAN ID 185
 ID 185
 Management of LAN traffic 187
 Network table 189
 Port 190
 Port list 189
 Port table 190

Priority 185
 Shielding of SNMP traffic 187
 Use of a central cabling 188
 Use tagging 190
 VLAN D 189
 VLAN ID 185
 Voice-over-IP 159, 162
 VoIP 69

VoIP –

siehe Voice-over-IP

VPN 222
 Client 131
 Gateway 130
 Network coupling with
 N:N mapping 72
 Remote maintenance via
 N:N mapping 73

W

WAN-layer 80
 WEBconfig 14, 16, 29
 HTTPS 17
 Wildcards 212
 WINS Address 205

Y

Y connection 93