

LANCOM™ reference manual

© 2003 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 Systems shall be liable only to the degree specified in the terms of sale and delivery.

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

Trademarks

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

The LANCOM Systems 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
Adenauertstrasse 20 / B2
52146 Würselen
Germany

www.lancom.de

Würselen, July 2003

Preface

User manual and *LANCOM* reference manual

The documentation of your device consists of two parts: The user manual and the *LANCOM* reference manual.

You are now reading the reference manual. It is supplemental to your user manual and covers topics which apply to several different *LANCOM*. This includes, for example:

- Configuration and management (*LANtools*, *WEBconfig*, remote configuration)
- Advanced security and firewall settings
- Server services (DHCP, DNS, NTP, cost control)
- Quality of Service, Routing and WAN functions

Validity

This reference manual applies to all *LANCOM*: Routers and Access Points with firmware revision 2.90 or better.

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>Code</code>	Inputs and outputs for the display mode
<Value>	Placeholder for a specific value
<i>Italic</i>	Instructions and product names

1 Configuration and management	9
1.1 Configuration tools and approaches	9
1.2 Configuration software	10
1.2.1 Configuration using <i>LANconfig</i>	10
1.2.2 Configuration with <i>WEBconfig</i>	12
1.2.3 Configuration using Telnet	13
1.2.4 Configuration using SNMP	14
1.3 Remote configuration via Dial-Up Network	14
1.3.1 This is what you need for ISDN remote configuration	14
1.3.2 The first remote connection using Dial-Up Networking	15
1.3.3 The first remote connection using a PPP client and Telnet	15
1.4 <i>LANmonitor</i> —know what's happening	17
1.4.1 Extended display options	18
1.4.2 Monitor Internet connection	18
1.5 Trace information—for advanced users	20
1.5.1 How to start a trace	20
1.5.2 Overview of the keys	20
1.5.3 Overview of the parameters	20
1.5.4 Combination commands	22
1.5.5 Examples	22
1.6 Working with configuration files	22
1.7 New firmware with LANCOM FirmSafe	24
1.7.1 This is how LANCOM FirmSafe works	24
1.7.2 How to load new software	25
1.8 Command line interface	26
1.8.1 Command line reference	27
1.9 Scheduled Events	28
2 Security	31
2.1 Protection for the configuration	31
2.1.1 Password protection	32
2.1.2 Login barring	33
2.1.3 Restriction of the access rights on the configuration	34
2.2 Stateful Inspection Firewall	38
2.2.1 Filtering of data packets	39
2.2.2 Stateful Inspection in detail	42
2.2.3 Alerting functions	55
2.2.4 Tips for setting the Firewall	59
2.2.5 Firewall diagnosis	62
2.3 Protection against break-in attempts: Intrusion Detection	67

2.4	Protection against “Denial of Service” attacks	68
2.4.1	Blocking of DoS attacks	69
2.4.2	Denial of Service attacks in detail	69
2.5	Making “Invisible”	72
2.5.1	Ping blocking	73
2.5.2	TCP Stealth mode	73
2.6	The hiding place—IP masquerading (NAT, PAT)	74
2.6.1	Unmasked Internet access for server in the DMZ	78
2.7	Protecting the ISDN connection	80
2.7.1	Identification control	80
2.7.2	Callback	82
2.8	The security checklist	83

3 Quality of Service **87**

3.1	Overview	87
3.1.1	Guaranteed minimum bandwidths	87
3.1.2	Limited maximum bandwidths	88
3.1.3	Type of Service (TOS) and/or DiffServ support	88
3.2	IP Quality of Service in detail	89

4 Server services for the LAN **91**

4.1	Automatic IP address administration with DHCP	91
4.1.1	The DHCP server	91
4.1.2	DHCP—'on', 'off' or 'auto'?	92
4.1.3	How are the addresses assigned?	93
4.2	DNS	96
4.2.1	What does a DNS server do?	97
4.2.2	DNS forwarding	98
4.2.3	Setting up the DNS server	99
4.2.4	URL blocking	102
4.2.5	Dynamic DNS	103
4.3	Call charge management	104
4.3.1	Charge-based ISDN connection limits	104
4.3.2	Time dependent ISDN connection limit	105
4.3.3	Settings in the charge module	106
4.4	The SYSLOG module	106
4.4.1	Setting up the SYSLOG module	107
4.4.2	Example configuration with <i>LANconfig</i>	107
4.5	<i>Office communications with LANcap</i>	109
4.5.1	What are the advantages of <i>LANcap</i> ?	109

4.5.2	Installing the <i>LANcapi</i> client	110
4.5.3	Configuration of the <i>LANcapi</i> clients	110
4.5.4	Configuring the <i>LANcapi</i> server	111
4.5.5	How to use the <i>LANcapi</i>	114
4.5.6	The LANCOM <i>CAPI Faxmodem</i>	114
5	Routing and WAN connections	117
5.1	General information on WAN connections	117
5.1.1	Bridges for standard protocols	117
5.1.2	What happens in the case of a request from the LAN?	117
5.2	IP routing	119
5.2.1	The IP routing table	119
5.2.2	Local routing	121
5.2.3	Dynamic routing with IP RIP	122
5.2.4	Policy-based routing	126
5.2.5	SYN/ACK speedup	127
5.3	Configuration of remote stations	127
5.3.1	Name list	128
5.3.2	Layer list	128
5.4	Establishing connection with PPP	130
5.4.1	The protocol	130
5.4.2	Everything o.k.? Checking the line with LCP	132
5.4.3	Assignment of IP addresses via PPP	133
5.4.4	Settings in the PPP list	134
5.5	Extended connection for flat rates—Keep-alive	136
5.6	Callback functions	136
5.6.1	Callback for Microsoft CBCP	136
5.6.2	Fast callback using the LANCOM process	138
5.6.3	Callback with RFC 1570 (PPP LCP extensions)	138
5.6.4	Overview of configuration of callback function	139
5.7	Channel bundling with MLPPP	140
6	Index	143

1

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

1.1

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.

1.2 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.

1.2.1 Configuration using *LANconfig*

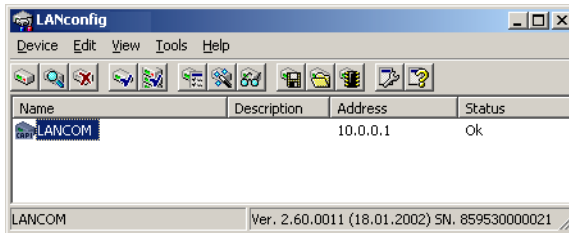
Start *LANconfig* by, for example, using the Windows Start menu: **Start / Programs / LANCOM / LANconfig**. *LANconfig* will now automatically search for devices on the local network. It will automatically launch the setup wizard if a device which has not yet been configured is found on the local area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

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.

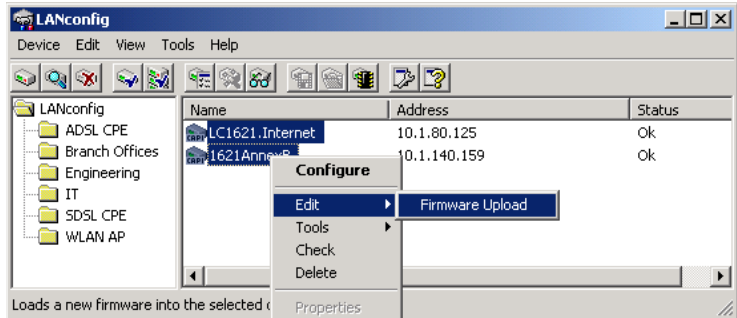
Management of multiple devices

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 and 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.



1.2.2

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.

1.2.3

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)
<i>WEBconfig</i>	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.

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.

1.2.4

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 (**M**anagement **I**nformation **B**ase) for use in SNMP programs.

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

1.3

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.

1.3.1

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.

1.3.2

The first remote connection using Dial-Up Networking

- 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.
- 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.
- 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.

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



1.3.3

The first remote connection using a PPP client and Telnet

- 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
- 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'.

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

The default layer for remote field installations

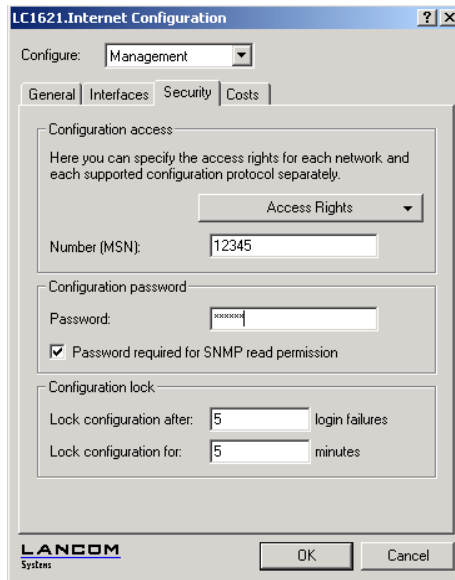
The PPP connection of any other remote site to the router, of course, will only succeed if the device answers every call with the corresponding PPP settings. This is the case using the factory default settings because the default protocol (default layer) is set to PPP.

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:

a Switch to the 'Security' tab in the 'Management' configuration section.



- b 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.

1.4

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.

1.4.1

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.

1.4.2

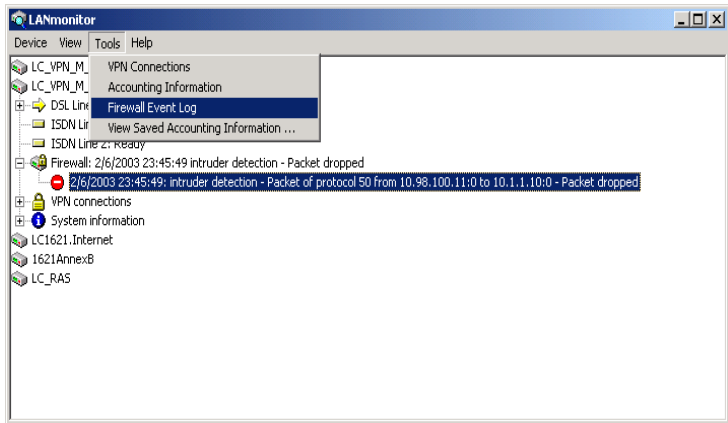
Monitor Internet connection

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.

- a 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**.

- b *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.

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

1.5

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.



1.5.1

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?

1.5.2

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

1.5.3

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
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

1.5.4

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.

1.5.5

Examples

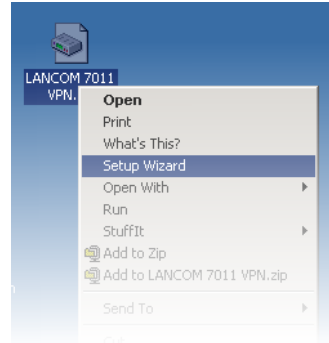
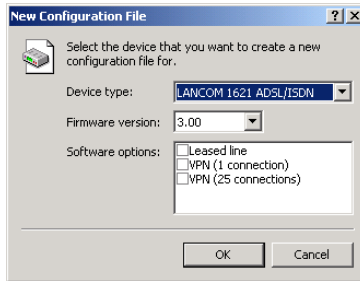
This code...	... in combination with the trace causes the following:
trace	displays all protocols that can generate outputs during the configuration, and the status of each output (ON or OFF)
trace + all	switches on all trace outputs
trace + protocol display	switches on the output for all connection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

1.6

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
<i>LANconfig</i>	Edit / Save Configuration to File Edit / Restore Configuration from File Edit / New Configuration File Edit / Edit Configuration File Edit / Print Configuration File
<i>WEBconfig</i>	Save Configuration/ Load Configuration (in main menu)
TFTP	tftp 10.0.0.1 get readconfig file1 tftp 10.0.0.1 put file1 writeconfig

1.7 New firmware with LANCOM FirmSafe

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

1.7.1 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.

1.7.2

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
```

1.8 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

1.8.1

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>] list [<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' on page 20
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.

1.9

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
- regular firmware or configuration updates

Configuration Tool	Run
<i>WEBconfig</i>	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	18
DayOfWeek	1,2,3,4,5,
Day	
Month	
Command	do /o/man/con HEADQUARTERS



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.

2

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
- The Stateful Inspection firewall
 - Filtering of data packets
 - Stateful Inspection in detail
 - Alerting functions
 - Tips for firewall configuration
 - Firewall diagnosis
- Protection from break-in attempts: Intrusion Detection
- Protection from Denial of Service attacks
- Making 'invisible'
- 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.

2.1

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.

2.1.1

Password protection

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



As long as a password hasn't been set, anyone can change the configuration of the device. For example, your Internet account information could be stolen, or the device could be reconfigured in a way that the protection-mechanisms 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
<i>LANconfig</i>	Management / Security / Configuration password
<i>WEBconfig</i>	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
<i>LANconfig</i>	Management / Security / Password required for SNMP read permission
<i>WEBconfig</i>	Expert Configuration / Setup / SNMP-module / Password-required-for-SNMP-read-access
Terminal/Telnet	<code>setup/SNMP module/password-required</code>

2.1.2

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
<i>LANconfig</i>	Management / Security
<i>WEBconfig</i>	Expert Configuration / Setup / Config-module
Terminal/Telnet	Setup/Config module

2.1.3

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.

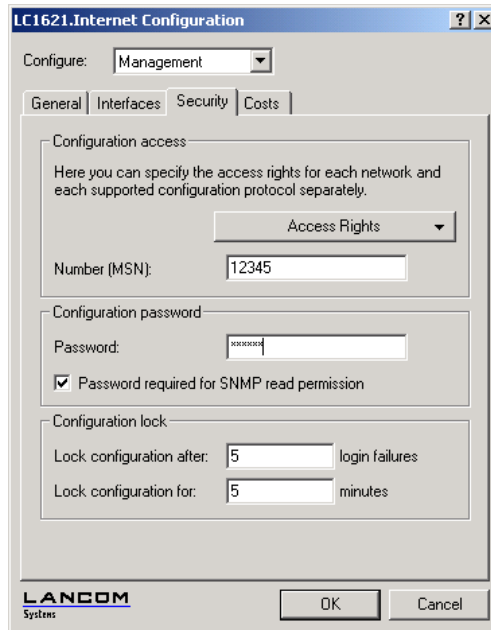
The term 'internal function' denotes configuration sessions via *LANconfig* (TFTP), *WEBconfig* (HTTP, HTTPS), SNMP or Terminal/Telnet.

Restrictions on the ISDN administrative account

This paragraph applies only to models with ISDN interface.



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



LC1621.Internet Configuration

Configure: Management

General Interfaces Security Costs

Configuration access

Here you can specify the access rights for each network and each supported configuration protocol separately.

Access Rights

Number (MSN): 12345

Configuration password

Password: xxxxxx

☒ Password required for SNMP read permission

Configuration lock

Lock configuration after: 5 login failures

Lock configuration for: 5 minutes

LANCOM Systems

OK Cancel

- b 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-(EAS-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

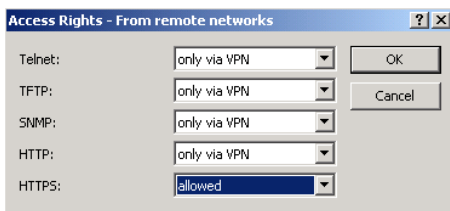


If you want to completely switch off the ISDN remote management, leave the field with Admin MSN empty.

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,

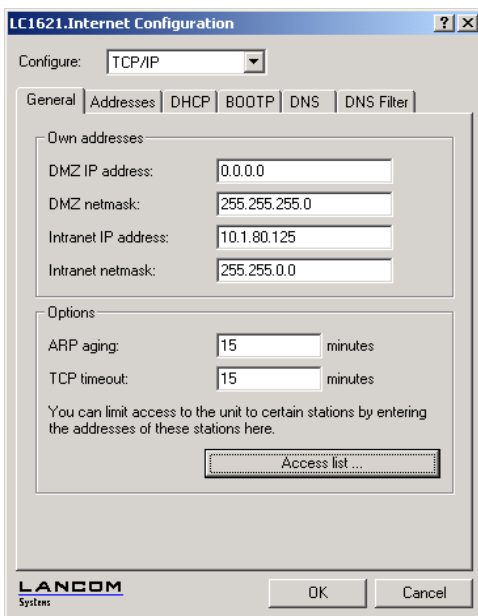
a pure read access or - if your model is equipped with VPN - also can be permitted only over VPN.



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.

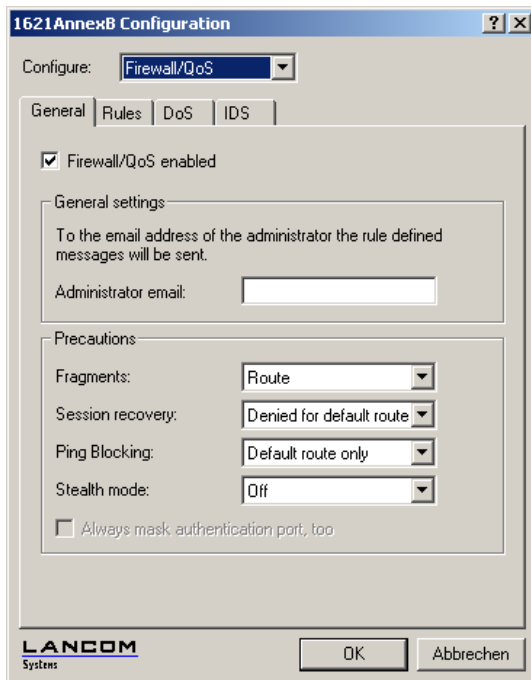
Configuration tool	Run
<i>LANconfig</i>	TCP/IP / General / Access list
<i>WEBconfig</i>	Expert Configuration / Setup / TCP-IP-module / Access-list
Terminal/Telnet	/setup/TCP-IP-module/access-list

2.2 Stateful Inspection Firewall

The main requirement for broadband connections is a safety-functionality, which guarantees an absolutely secure "always-on" operation of entire networks. This can be accomplished with the *LANCOM* integrated Firewall.

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. 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.

In opposite to simple port filter Firewalls, it is possible to control dynamically opened ports (e.g. like with FTP or H.323) as well. The Stateful Inspection Firewall controls these protocols in detail, and is opening solely the individually required ports - instead of releasing all ports unnecessarily.





Affected by the Firewall are always just the "passing" data packets through the LANCOM. The restrictions concerning the access for internal services to configure the LANCOM (e.g. HTTP, HTTPS, TFTP and Telnet) have been described in the preceding paragraph.

2.2.1

Filtering of data packets

The LANCOM Firewall filters offer filter functions for single computers as well as for entire networks. They ensure an effective protection against undesired intrusion in your network.

What can be filtered?

Important are the source and destination filters for single ports or port ranges. Single protocols or any protocol combination (TCP/UDP/ICMP) may be filtered as well. IP address ranges or complete IP networks are suitable objects, just as certain stations or remote sites.

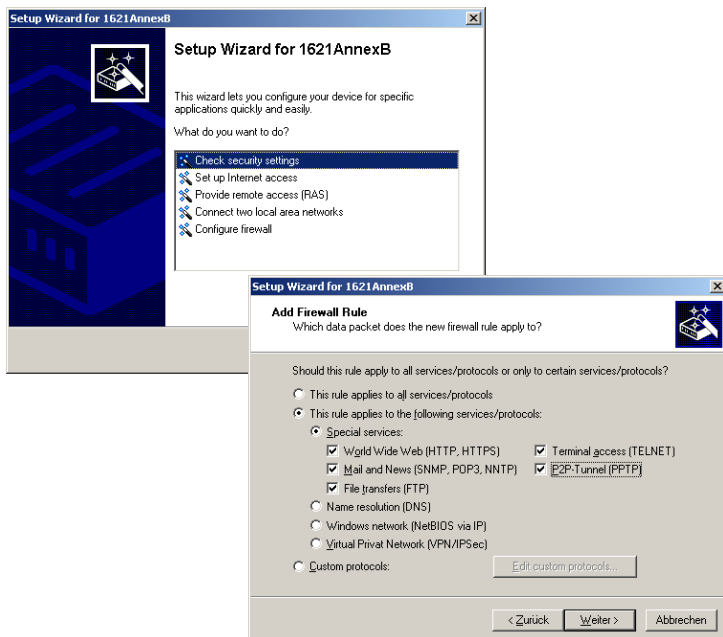
Besides to these IP-level objects, certain stations from the LAN could also be selected via their MAC address. MAC is the abbreviation for **M**edia **A**ccess **C**ontrol and it is the crucial factor for communication inside of a LAN.

Every network device has its own MAC address. MAC addresses are worldwide unique, similar to serial numbers.

MAC addresses allow distinguishing between the PCs in order to give or withdraw them dedicated rights on an IP level. MAC addresses can be found on most networking devices in a hexadecimal form (e.g. 00:A0:57:01:02:03).

Filter Installation

The Firewall assistant in LANconfig is the easiest and fastest tool to configure the Firewall:

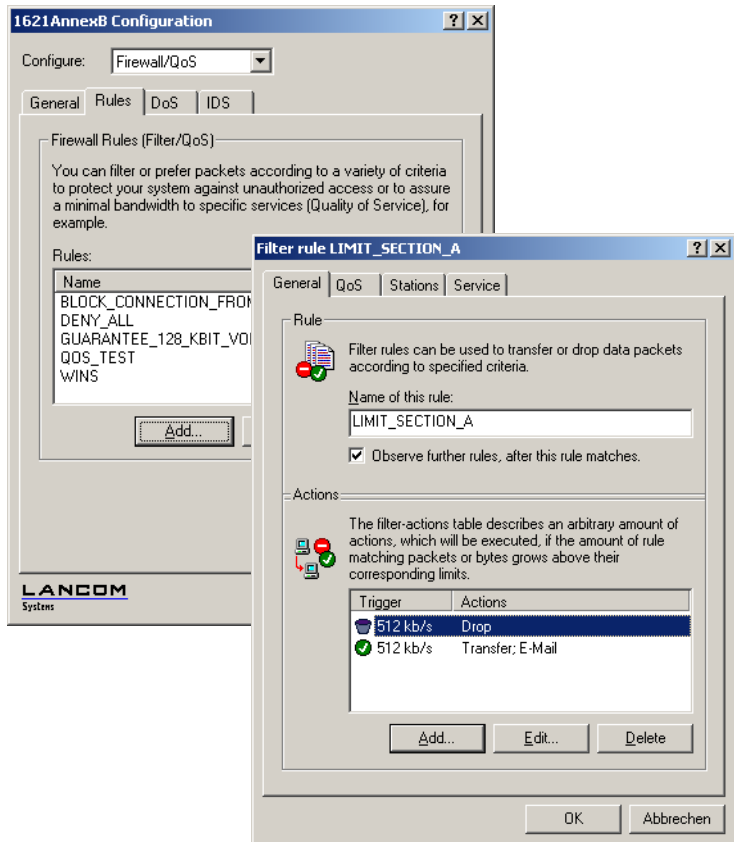


With the other configuration tools, the Firewall filters are configured in the following menus and lists.

Configuration tool	Run
<i>LANconfig</i>	Firewall/QoS / Rules / Add
<i>WEBconfig</i>	Expert Configuration / Setup / IP-Router-Module / Firewall / Rule-Tabelle
Terminal/Telnet	/Setup/IP-Router-Module/Firewall/Rule-Table

Filter installation with LANconfig

The filter installation with LANconfig is absolutely easy. You will find the following register cards which help you to define filter rules under "Firewall / QoS / Rules":



Starting from the general register card "Firewall / QoS / Rules", you will reach after "Add" or "Edit" the dialog to define filter rules:

- "Rules"
The name of the filter service is entered here, as well as whether further rules have to be considered after this rule has matched.
- "Actions"
Here you can define the trigger conditions and the appropriate Firewall actions for this rule (see also 'Action objects' on page 46).

- "QoS"
Here you can set minimum bandwidths for dedicated data packets, which are specified by their respective Firewall rule. (See "'Quality of Service objects' on page 50 and 'Quality of Service' on page 87)
- "Stations"
Here you define the stations - as sender or addressee of the packets - for which the filter rule is valid. (See 'Source and destination objects' on page 44)
- "Services"
Under "Services" you have to decide for which IP protocols, source and destination ports the filter rule is applicable. You can declare and permit for example an access solely to web pages and e-mails.
- "VPN"
This register card defines the rules for handling encoded packets, e.g. if only the transmission of encoded packets should be allowed (only if your router supports VPN).

Filter Installation with WEBconfig or via terminal/Telnet

A little more difficult as with LANconfig is the configuration via WEBconfig or via a terminal or Telnet connection. Nevertheless, these methods of configuration unveil the most detailed configuration options to expert users.

Here the filter function is described by the filter list, which is based on three tables: Object table, action table and rule table. The object table defines items like PCs, networks and protocols. The action table defines items like limitations, minimum bandwidths and alerts. Finally, the rule table combines objects and actions to Firewall rules. The filter list is created automatically from the rule table, showing the resulting filter settings.

2.2.2

Stateful Inspection in detail

This paragraph presents detailed background information concerning functions and features of the LANCOM Firewall.



If you want to skip this information right now, you can continue directly with the chapter "'Tips for setting the Firewall' on page 59.

The main requirement to a Stateful Inspection Firewall is the control of permitted connections. The Stateful Inspection Firewall is using two databases for working. These are the port filter database and connection state database (the real "Stateful Inspection"), where all active connections



and blocked ports, hosts and others are filed. When a packet arrives, the program is checking immediately if an entry for this connection exists in the state database. If such an entry exists, the handling of the packet will be like described in the database. If no entry has been found for the packet, the search for an entry continues in the port filter database and the action will be executed as specified. When the action implies to accept the packet, an entry will be added in the state database, and eventual further actions will be added as well.

If no explicit Firewall rule exists for a data packet, the packet will be accepted ("Allow-All"). So a backward-compatibility to present installations is realized in this way. For maximum protection through the Stateful Inspection, please pay attention to paragraph 'Set-up of an explicit "Deny All" strategy' on page 59.

Object table

The object table defines the elements and objects that apply to the rule table of the Firewall. Objects can be:

- Protocols
- Single PCs (MAC or IP address, host name)
- Entire networks
- Services (ports or port ranges, e.g. HTTP, Mail & News, FTP, ...)
- Trigger conditions - global and per connection
- Notifications (E-mail, SYSLOG/SNMP/Log)
- Actions for hosts and connections (close port, disconnect)

Any given combination of these elements is possible. Furthermore, you can define objects in a hierarchical way. So you could first define objects for the TCP and UDP protocols, then the objects for e.g. FTP (= TCP + ports 20 and 21), HTTP (= TCP + port 80) and DNS (= TCP, UDP + port 53). All these single objects could be summarized subsequently to a new object.

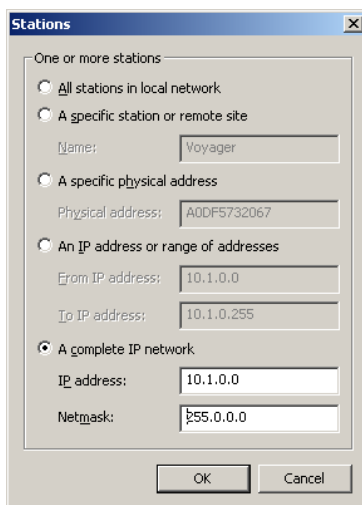
Rule table

The rule table connects objects to filter rules. The rule table contains the protocol to be filtered (you have defined it in the object table), the source objects, the destination objects and the filter action to be executed. The protocol, as well as the source and destination objects, can be composed of combined objects, and can contain direct descriptions (e.g. %P6 for TCP),

which are separated by "+" or by spaces. A direct description is marked by "%". Possible descriptions are:

Source and destination objects

Description	Object ID
local network	%L
Host name	%H
MAC address	%E
IP address	%A
Net mask	%M
Protocol (TCP/UDP/ICMP etc.)	%P
Service (Port)	%S



The same kind of description can produce comma separated lists like host lists/address lists (%A10.0.0.1, 10.0.0.2), or by hyphen-separated ranges like

port lists (%S20-25). The presentation of a "0" or a space marks the any-object:

Description	Object ID
All computers	%A0.0.0.0
All services	%S0
All protocols	%P0

Host names can only be used when the *LANCOM* is able to resolve the names into IP addresses. Therefore, *LANCOM* must have learned the names via DHCP or NetBIOS, or the classification has to be noted statically in the DNS or IP routing table. An entry in the IP routing table is able to denote a whole network by a host name.



A configuration via console (Telnet or terminal program) is only possible when inverted commas (inch sign: ") enclose the combined parameters (port, destination, source).

Preset protocol objects

ILANconfig provides a number of preset objects for simple filter generation:

- HTTP / HTTPS
- FTP
- MAIL/NEWS
- TELNET
- TFTP
- NETBIOS
- PPTP
- IPSEC
- DNS



Action objects

Any combination from the following table can be taken for an action if an entry for the packet exists in one of the two databases:

Action	Description	Object ID
Accept	The packet will be accepted	%a
Reject	The packet will be rejected with an error message	%r
Drop	The packet will be discarded silently	%d
Connect-Filter	The filter is active when no logical connection to the packet destination exists	%c
Internet-Filter	The filter is active when the packet is received or will be transmitted via the default route	%i
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

Action	Description	Object ID
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

These actions can be combined any way you want. Whereas, if you choose contrary actions (e.g. accept + drop), the more secured action will be taken. (I.e. "drop" in this case.) If no further action is declared for the "connect" or "internet" filter, any combination of these filters is implicitly converted to a "reject" action.

When the "close port" action is executed, an entry in the block list will be generated, which takes care that all sent packets to the workstation would be dropped.

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, are rejected. For the "close port" object a time-out can be indicated in seconds, minutes or hours, which is noted directly behind the object ID. This date builds itself together from the designator for the time unit (h, m, s for hour, minute and second) as well as the actual time. Thus e.g. %pm10 closes the port for 10 minutes. If no time unit is provided, then implicitly "minutes" apply (and thus %p10 being equivalent to %pm10).

If the "Deny host" action is executed, then the sender of the packet is registered into a block list. Starting from this moment, all packets received from the closed computer will be rejected. Also the "Deny host" object can be provided with a time-out, which is formed similarly to the "CLOSE port" option.

Each of these actions can be linked together with a limit, whose excess leads to the trigger of the action. Also, several limits for a filter thereby can build action chains. The following actions are available:

Limit	Description	Object ID
Data (abs)	Absolute number of kilobytes on the connection after those the action is executed	%lcd
Data (rel)	Number of kilobytes/second, minute, hour on the connection after those the action is executed	%lcds %lcdm %lcdh
Packet (abs)	Absolute number of packets on the connection after those the action is executed	%lcp
Packet (rel)): Number of packets/second, minute, hour on the connection after those 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 those 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 those 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 without limits is indicated, then implicitly a packet limit is assumed, which is exceeded immediately with the first packet.

Characteristics of action and trigger objects

Actions and limitations are treated like protocols, addresses and services as objects, and can be combined arbitrarily. For a better clearness of the objects, they are filed in their own object list.

- Limit objects are generally introduced by %l, followed by:
 - Reference
 - Connection referred (c)
 - Global (g)
 - Kind
 - Data rate (d)
 - Number of packets (p)
 - Packet rate (b)
 - Value of the limit
 - Further parameters (e.g. period, quantity)

Thus the limit described with %l`cds8` is exceeded, if within one second more than 8 kbps became to transfer over the connection. In this moment the actions connected with the limit are released. All actions following after a limitation are linked with the limit. A new limit in the respective description of object starts a new internal action list.

If you want to limit e.g. the data rate, which is permissible for a connection, on 8 kbps, and lock out the aggressor committing a flooding attempt, and send at the same time an e-mail to the administrator, the description of the object for the action reads as follows:

```
%a %lcds8%d %lgbs100%h10%m
```

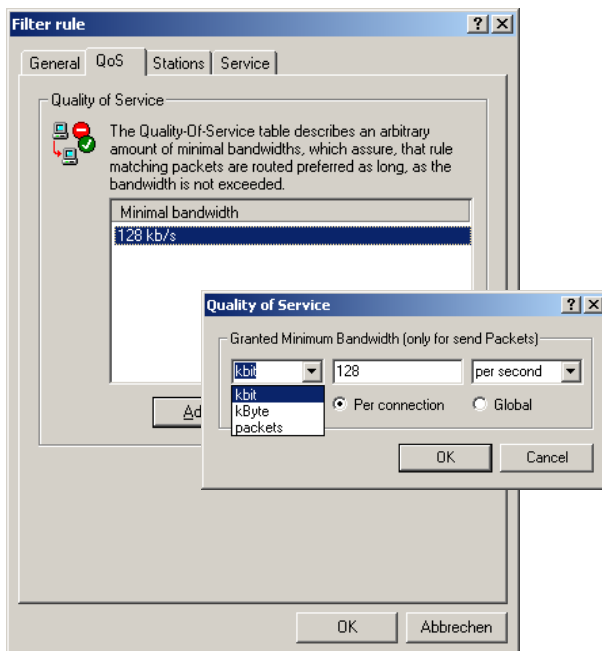
This description permits the traffic (%a) to begin. A simple %a at the beginning of the description is equivalent to a %l`p0`%a (= accept, if the limit were exceeded of zero packets, i.e. with the first packet). If over the current connection in one second now 8 kbit (%l`cds8`) was transferred, then all further packets up to the expiration of the second are silently discarded (%d), whereby a Traffic Shaping results automatically. However, if 100 packets for the server (destination address of the connection) arrive (%lgbs100) in one second, then the remote host (source address) is locked for 10 minutes (%h10), and an e-mail is sent to the administrator (%m)

The action objects can be provided - like the address and service objects of the port filter Firewall - with a name, and can be combined arbitrarily recursively, whereby the maximum recursion depth is limited to 16

recursions. In addition, they can be registered directly into the action field of the rule table. When building the actual filter table, the action objects become reduced then exactly the same as address and service objects on the smallest necessary number, i.e. multiple definitions of an action are eliminated, and contradictory actions turn into the "safest". Thus becomes e.g. out of %a (accept) and %d (drop) only %d and out of %r (reject) and %d becomes %r.

Quality of Service objects

Another limit object is the "Quality of Service" object, or QoS object, which permits to define - either globally or per connection - a minimum throughput and/or a minimum bandwidth. All delimitations can be used, that are possible with normal limit objects also, i.e. connection-oriented or global minima, absolute or time-dependent (relative) minima, packet or data rate related minima. The same conventions as with the limit objects apply.



QoS objects are introduced by the token %q and differ from limit objects only by the fact that they possess first an implicit "Accept" action, i.e. after

exceeding the threshold the following packets, further packets are accepted. The router dispatches preferentially all packets, which go through a QoS filter object (corresponding to a set "Low Delay" flag in the TOS field of the IP header), as long as the number of the transferred packets or data lies underneath the indicated threshold. If the threshold is crossed, then the actions indicated by the QoS object are triggered. So a minimum and maximum bandwidth for a service can be given by the combination of a QoS and limit object. Thus the following description results in e.g. from a minimum range of 32 kbps per connection and a total maximum of 256 kbps for all connections:

```
%a %qcds32%a %lgds256%d
```

Here the explicit declaration of the accept action as a main action, as well as a triggered action, can be omitted, and the description is accordingly shortened:

```
%qcds32 %lgds256%d
```

If the minimum and maximum range of a channel should be equal, then the drop action can be indicated also directly in the QoS object (directly in shortened way of writing):

```
%qcds32%d
```

Here a minimum range of 32 kbps is reserved, and at the same time all packets to be transferred beyond this bandwidth will be rejected. This formulation is thus equivalently to

```
%a %qcds32%a %lgds32%d
```

With the exceeding of the threshold also log actions (E-Mail, Syslog etc.) can be executed, similar to the limit objects.

Special protocols

One important point during the connection tracking is the treatment of protocols that dynamically negotiate ports or addresses, over which further communication passes.

Examples of these kinds of protocols are FTP, H.323 or also many UDP-based protocols.

Here it is necessary that additionally to the first connection, further connections would be opened.

UDP connections

UDP is actually a stateless protocol, nevertheless one can speak with 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 at 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                               Server
Request
12345 -----> 53
Response
12345 <----- 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                               Server
Request
12345 -----> 69
Response
12345 <----- 54321
Ack/Data
12345 -----> 54321
Data/Ack
12345 <----- 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 as described under 'Set-up of an explicit "Deny All" strategy' on page 59, 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 be discarded silently.

With ICMP error messages, the IP header and the first 8 bytes of the IP packet (on behalf UDP or TCP headers) stand 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".

Concatenated rules

There are configurations, which cannot be covered with a single "first match" rule. For example, an alerting with 90% excess of a transfer volume could not be followed by a blockage starting from reaching 100% of the permitted transfer volume then. As a further example should be described in this context a general limitation connected with different partial limitations of individual users. Such a rule set could be formulated as follows:

- To all users applies a global limit of 1 Mbps
 - Group A of users may use 64 kbps of it
 - Group B of users may use 128 kbps of it
 - Group C of users is unrestrictedly within the global limit

If one installs now for all groups of users a filter, which contains the group-specific limit and also the global limit, then you will not obtain the desired success. You receive 3 groups, which possess in itself a maximum throughput of 1 Mbps, but they were otherwise completely independent from each other and thus - strictly speaking - the global limit would be increased indirectly to 3 Mb.

Also a splitting of the global limit on the individual groups would not lead to success, which would notice the group C of users immediately, since she would never get the "promised" bandwidth assigned.

The only possible solution of this problem is the concatenation of several rules, which are successively processed. For this, each rule possesses a "continue" - and/or "link" flag, which indicates that this rule is linked with a further one. This linkage consists of the fact that in the filter table the next filter, which matches likewise on the current packet, can be required for the determination of the actions to be executed. This happens in a way that these limits together with their actions are simply added to the first entry created by the filter in the connection state database. The linked filter can be linked with further rules again, so that a filter chain results up to the most general of the connected rules. The example above can be defined now e.g. for FTP as follows:

Name	Prot	Src	Dst	Action	Linked
USERGROUP_A	TCP	%a10.1.1.0 %m255.255.255.0	anyhost %s20	%a %lcds64 %d	yes
USERGROUP_B	TCP	%a10.1.2.0 %m255.255.255.0	anyhost %s20	%a %lcds128 %d	yes
USERGROUP_C	TCP	%a10.1.3.0 %m255.255.255.0	anyhost %s20	%a	yes
FTP_GLOBAL_LIMIT	TCP	%a10.1.0.0 %m255.255.252.0	anyhost %s20	%a %lgds1024 %d	no
DENY_ALL	TCP	anyhost	anyhost %s20	%r	no

In this example the user groups are separated from each other by different subnets. If there is a packet from user group A, then an entry in the connection state database is created, and the specified limit is associated with it. Because this filter rule has set the continue flag ('linked'), the search is continued until the next matching rule is found. This is the FTP-GLOBAL

rule, which defines a global limit that is additionally associated with the first entry then. The same applies to all packets originating from the other user groups. Due to the fact that the three user groups make up a smaller address range than that specified by the FTP-GLOBAL rule, an additional rule has to be created, which blocks all FTP accesses for the remaining addresses.

Finally, the resulting rule set list is as follows:

Name	Prot	Src	Dst	Action	Linked
FTP-BLOCK	TCP	%a10.1.0.0 %m255.255.255.0	anyhost %s20	%r	no
USERGROUP_A	TCP	%a10.1.1.0 %m255.255.255.0	anyhost %s20	%a %lcds64 %d	yes
USERGROUP_B	TCP	%a10.1.2.0 %m255.255.255.0	anyhost %s20	%a %lcds128 %d	yes
USERGROUP_C	TCP	%a10.1.3.0 %m255.255.255.0	anyhost %s20	%a	yes
FTP_GLOBAL_LIMIT	TCP	%a10.1.0.0 %m255.255.252.0	anyhost %s20	%a %lgds1024 %d	no
DENY_ALL	TCP	anyhost	anyhost %s20	%r	np



Please notice that no filter entry will be created in case of input faults, and that no error message will be created then. If you configure filter manually, please ensure to double-check whether the desired filters were created indeed (see 'The filter list' on page 64).

2.2.3

Alerting functions

This paragraph lists 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 e-mail account can be set at the following places:

Configuration tool	Run
<i>LANconfig</i>	Log & Trace / SMTP Account / SNMP / SYSLOG
<i>WEBconfig</i>	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.

Notifications by SYSLOG

If the Firewall drops an appropriate packet, a SYSLOG notification is made (see 'Setting up the SYSLOG module' on page 107) 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 mes-
sage;
```

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 minute
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' on page 14), 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
Trap was generated from a LANCOM 6021

```

```

SNMP: Agent IP address = 10.0.0.43
SNMP: Generic trap = enterpriseSpecific (6)
SNMP: Specific trap = 26 (0x1A)
SNMP: Time stamp = 1442 (0x5A2)
LANCOM Firewall trap

```

```

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
System descriptor

```

```

SNMP: OID = 1.3.6.1.2.1.1.5.0 2. System-Name
SNMP: String Value = LANCOM Business 6021
Device string

```

```

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

Time stamp

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

Source 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

Destination address

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

Protocol (6 = TCP)

SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.6.1 6.

SNMP: Integer Value = 4353 (0x1101)

Source port

SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.7.1 7.

SNMP: Integer Value = 80 (0x50)

Destination port (80 = HTTP)

SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.8.1 8.

SNMP: String Value = BLOCKHTTP

Name of filter rule

SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.9.1 9.

SNMP: Integer Value = 1 (0x1)

Limit (1 = absolute number of packets)

SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.10.1 10.

SNMP: Integer Value = 0 (0x0)

Trigger (0 = beginning with the first packet)

SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.11.1 11. Action

SNMP: Integer Value = 3758114816 (0xE0004800)

Action: (0xE0004800 = Drop, block source address, SYSLOG, SNMP-trap, e-mail)

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.

2.2.4

Tips for setting the Firewall

The *LANCOM* Firewall is an extremely flexible and powerful tool. In order to help you to create your individual Firewall rules, you'll find in the following some hints for your specific application.

The default setting 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 the 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 (see "Unmasked Internet access for server in the DMZ" on page 78), access to this service from the outside has to be permitted at first.



Set-up of an explicit "Deny All" strategy

For a 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 email viruses, which set up actively an outgoing connection on certain ports.

Some typical applications are shown in the following.



Tip: All filters described here can be installed very comfortably with the Firewall assistant, and if necessary be further refined with e.g. LANconfig.

- Example configuration "Basic Internet"

Rule name	Source	Destination	Action	Service (target port)
DENY_ALL	All stations	All stations	reject	ANY
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	Local network	IP address of LANOM (or: Local network)	transmit	DNS

- If you want to permit VPN dial-in on a *LANCOM* as VPN gateway, then you do not need an explicit Firewall rule, since the Firewall is only needed for passing data transfer.
- In case that a VPN is not terminated by the *LANCOM* (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

- If you permit ISDN dial-in 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' on page 127):

Rule	Source	Destination	Action	Service (target port)
ALLOW_DIAL_IN	remote site name	Local network	transmit	ANY

For a network coupling you permit additionally communication between the involved networks:

Rule	Source	Destination	Action	Service (target port)
ALLOW_LAN1_TO_LAN2	LAN1	LAN2	transmit	ANY
ALLOW_LAN2_TO_LAN1	LAN2	LAN1	transmit	ANY



- Additionally for VPN network coupling: After you have entered the networks to be coupled, modify the DENY-ALL rule, as well as the two rules for the LAN- LAN coupling in such a way, that the rules do not have an effect on IPSec. ("Do not create VPN security policies "on the "VPN"-register cards of the rules).
- 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 recommended to allow ICMP protocols (e.g. ping):

Rule	Source	Destination	Action	Service (target port)
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 makes an automatic sort of the Firewall rules when setting-up the filter list. In this way, the rules are sorted into the filter list on the basis of their level of detail. First all specific rules are considered, and afterwards



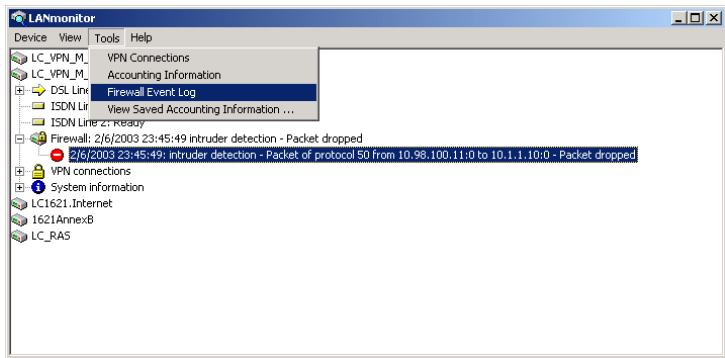
the general ones (e.g. Deny-All). Examine the filter list with complex sets of rules, as described in the following section.

2.2.5

Firewall diagnosis

All events, conditions and connections of the Firewall can be logged and supervised in detail.

The most comfortable inspection results with the display of the logging table (see below) by the LANmonitor. For this, the signaling for "SNMP (LANmonitor)" must be activated for the to be regarded Firewall, DOS or IDS event.



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 logging 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. This 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 by the output of the table into clear text)
Src-address	Source address of the filtered packet
Dst-address	Destination address of the filtered packet
Prot.	Protocol (TCP, UDP etc.) of the filtered packet
Src-p	Source port of the filtered packet (only with port-related protocols)
Dst-p	Destination port of the filtered packet (only with port-related protocols)
Filter-Rule	Name of the rule, which has produced 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 indicated in the IP routing trace (see 'to start a trace ' on page 20). Furthermore some LANCOM models have a Firewall LED, which signals each filtered packet.

The filter list

The filter list helps you to check the filters produced by the 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 the filters manually, you should in each case examine on the basis of the filter list whether the desired filters were produced.



On Telnet level, the content of the filter list can be listed 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
  VPN-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
  VPN-Flags: none
  Limit per conn.: after transmitting or receiving of 0 packets
  actions after exceeding the limit:
    reject if on default route

LC1621.Internet:/
>
```

The filter list has the following structure (incl. the default NetBIOS filter):

LC1621.Internet

LANCOM
Systems

(LANCOM 1621 ADSL/SDN 2.80.0004 / 18.11.2002)

[Experten-Konfiguration](#)

[Status](#)

[IP-Router-Statistik](#)

Filter-Liste

Idx.	Prot.	Quell-MAC	Quell-Adresse	Quell-Netz-Maske	Q-von	Q-bis	Ziel-MAC	Ziel-Adresse	Ziel-Netz-Maske	Z-von	Z-bis	Aktion	verknuepft	VPN-Flags
0001	17	000000000000	0.0.0.0	0.0.0.0	137	139	000000000000	0.0.0.0	0.0.0.0	0	0	inet: reject nein	keine	
0002	6	000000000000	0.0.0.0	0.0.0.0	137	139	000000000000	0.0.0.0	0.0.0.0	0	0	inet: reject nein	keine	

Diese Tabelle beobachten

Auffrisch-Periode (s):

21.11.2002 14:47

[Vorherige Seite](#) [Startseite](#) [LANCOM Systems Startseite](#)

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
Quell-MAC	Ethernet source address of the packet to be filtered or 000000000000, if the filter should apply to all packets
Quell-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
Dest-MAC	Ethernet destination address of the packet to be filtered or 000000000000, if the filter should apply to all packets
Dest-address	Destination address or 0.0.0.0, if the filter should apply to all packets
Dest-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	<p>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.</p> <p>You can see the complete actions under the command <code>show filter</code></p>
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
VPN-Flags	The VPN flags defined in the rule list (VPN-Only, ignore)

The connection list

In the connection table source address, destination address, protocol, source port, destination port, etc. of a connection are filed, 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. The table contains the following elements:

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	<p>In the flags the condition of the connection and further (internal) information are stored in a bit field</p> <p>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)</p> <p>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.)</p>
Rule	Name of the rule, which produced the entry

Port block list

If as action the blockage of the destination port on the destination station was selected, the address, protocol and port of the destination station are filed in the port block list. This table is likewise a sorted semi-dynamic table.

The assortment happens after address, protocol and port. The table contains the following elements:

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 produced the entry

Host block list

If as action of a filter the blockage of the sender was selected, then the address of the station is filed in the host block list. This table is a sender address sorted semi-dynamic table and contains the following elements:

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 produced the entry

2.3

Protection against break-in attempts: Intrusion Detection

Break-in attempts into the local network or on the central Firewall are recognized, repelled and logged by the Intrusion Detection system (IDS) of the *LANCOM*. Thereby it can be selected between logging within the device, email notification, SNMP trap or SYSLOG alarms.

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.

The behaviour of the *LANCOM* Intrusion Detection System can be configured here:

Configuration tool	Run
<i>LANconfig</i>	Firewall/QoS / IDS
<i>WEBconfig</i>	Expert Configuration / Setup / IP-Router-Module / Firewall
Terminal/Telnet	/Setup/IP-Router-Module/Firewall

IP-Spoofing

With IP Spoofing the sender of a packet reports 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 of the *LANCOM* 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' on page 70): 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.

2.4

Protection against "Denial of Service" attacks

Attacks from the Internet can be break-in attempts as well as attacks with the aim of blocking the accessibility and functionality of individual services. Therefore a *LANCOM* is equipped with appropriate protective mechanisms, which recognize well-known hacker attacks and which guarantee the functionality.

2.4.1 Blocking of DoS attacks

To reduce drastically 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 in the *LANCOM* explicitly the connection state, source addresses and correctness of fragments are examined. This happens for incoming and for outgoing packets, since an attack can be started also from the local area network.

In order not to open a gate for DoS attacks by incorrect configuration of the Firewall, this part is configured centrally. Configurable is:

- The maximum number from half-open connections to a host (against SYN Flooding)
- Whether fragments are to be rejected, or to be reassembled and examined by the *LANCOM*
- How the administrator is to be informed in case of DoS attacks (Syslog/Email):

Configuration tool	Run
<i>LANconfig</i>	Firewall/QoS / DoS
<i>WEBconfig</i>	Expert Configuration / Setup / IP Router Module / Firewall
Terminal/Telnet	/Setup/IP-Router-Module/Firewall

Always actively however are the following protection mechanisms:

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

2.4.2 Denial of Service attacks in detail

Denial of service attacks do profit from principle weaknesses of TCP/IP protocols as well as incorrect implementations of TCP/IP protocol stacks. Attacks, which profit from principle weaknesses, are e.g. SYN Flood and Smurf. Attacks aiming to incorrect implementations are all attacks, which operate with incorrectly fragmented packets (e.g. Teardrop), or which work

with falsified sender addresses. In the following are some of these attacks 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 the incoming echo requests as well as the number of answering workstations is high enough, 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 during the attack. If the falsified sender address is the broadcast address of the second network, even all workstations are blocked in this network.

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 the 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.

Ping of Death

The Ping of Death belongs to the 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 built into the 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 produced 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/Frag router

Bonk is a variant of the Teardrop attack, which targets not to crash the attacked computer, but to trick simple port filter Firewalls, which accept also fragmented packets and to penetrate thus into the network to be protected. During this attack, by skillful choice of the off set fragment, the UDP or TCP Header of the first fragment is overwritten. Thereby simple port filter Firewalls accept the first packet and the appropriate fragments by overwriting a first packet's header by the second fragment, suddenly a permitable packet is created, which rather should be blocked actually 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 suggested by the one or the other solution above.

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



2.5

Making "Invisible"

One - not undisputed - method to increase security is hiding the Router; freely according to the method: "who does not see me, will not also try me to attack...".

The relevant settings (explanation see below) can be made at the following places:

Configuration tool	Run
<i>LANconfig</i>	Firewall/QoS / General
<i>WEBconfig</i>	Expert Configuration / Setup / IP-Router-Module / Firewall
Terminal/Telnet	/Setup/IP-Router-Module/Firewall

2.5.1

Ping blocking

In order to achieve this, the *LANCOM* can be instructed not to answer ICMP echo Requests anymore. 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
ICMP answers are blocked on all WAN connections
- Default route
ICMP answers are blocked on Default route (usually Internet)

2.5.2

TCP Stealth mode

Apart from ICMP messages, also the behavior in case of TCP and UDP connections gives information on the existence or non-existence of the addressed workstation.

Depending on surrounding network it can be useful to simply reject TCP and UDP packets, instead of answering with a TCP RESET resp. an ICMP message (port unreachable), if no Listener for the respective port exists. The desired behavior can be adjusted in the *LANCOM*.

If ports without Listener are hidden, this generates a problem on masked connections, since the "authenticate" - resp. "ident" service does no longer function properly (resp. do no longer correctly reject).

A mail or a news server, which requests additional information from the user with the help of this service, runs first into a disturbing timeout, before beginning to deliver the mails. This service needs thus its own switch to hide and/or to keep it "conformal".

The problem thereby: A setting, which hides all ports but rejects the ident port, is unreasonable. The *LANCOM* would become visible, solely because the ident port was rejected. To solve this problem, the *LANCOM* offers to deny ident inquiries only from the mail and news servers and to simply reject inquiries of all other workstations. For that purpose, the respective mail (SMTP, POP3 IMAP2) or news (NNTP) servers receive rejected ident inquiries

for a short time (20 seconds) only when polling. If the time ran off, the port is hidden again.

Possible settings are:

- off
all ports are closed and TCP packets with a TCP RESET are answered
- allways
all ports are hidden and TCP packets are silently discarded
- WAN
on the WAN side all ports are hidden and on the LAN side closed
- Default route
Ports are hidden on the Default route (usually Internet) and closed on all other routes

Settings to the special treatment of ident inquiries (only with "stealth"):

- closed
Inquiries to the authenticate and/or ident port are answered with a TCP Reset, if they came from a shortly before queried mail or news server. Otherwise, they will be rejected.
- stealth
Packets to the authenticate and/or ident port are always silently discarded

2.6 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.

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

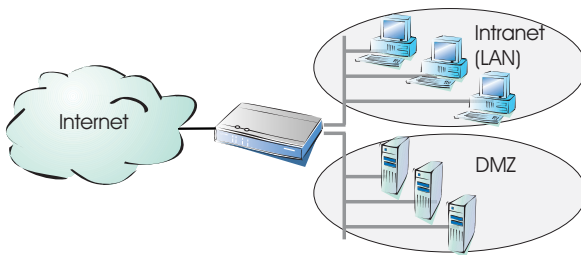
The use of IP masquerading is set individually for each route in the routing table. The routing table can be reached as follows:

Configuration tool	Run
<i>LANconfig</i>	IP router / Routing / Routing table
<i>WEBconfig</i>	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:

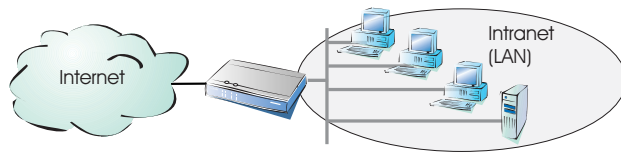
- 'IP Masquerading switched off': No masquerading.
This variant is intended for Internet access with multiple static IP addresses (to be entered under DMZ network address and DMZ netmask). Examples would be to connect servers to the Internet, or to connect two Intranet subnets via VPN.
- 'masking Intranet 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
<i>LANconfig</i>	TCP/IP / General
<i>WEBconfig</i>	Expert Configuration / Setup / TCP-IP-Module
Terminal/Telnet	/Setup/TCP-IP-Module

Simple and 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
<i>LANconfig</i>	IP router / Masq. / Service list
<i>WEBconfig</i>	Expert Configuration / Setup / IP-router-module / Masquerading / Service-table
Terminal/Telnet	/setup/IP-router-module/masquerading/ service-table

Stateful Inspection and inverse masquerading



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

2.6.1

Unmasked Internet access for server in the DMZ

While the inverse masquerading described in the preceeding 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').

EN

Two local networks - operating servers in a DMZ



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

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

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

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

Separation of Intranet and DMZ



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

- With a 'Allow All' strategy (default): Deny access from 123.45.67.2 to "All stations in local network"
- With a 'Deny All' strategy (see 'Set-up of an explicit "Deny All" strategy' on page 59): Allow access from "All stations in local network" to 123.45.67.2

2.7

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

2.7.1

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
<i>LANconfig</i>	Communication / Call accepting
<i>WEBconfig</i>	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 establishment. When a computer dials into the *LANCOM*, the communications software, for example Windows Dial-Up Network, prompts the user for the user name and password to be transferred.

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

The PPP list can be found as follows:

Configuration tool	Run
<i>LANconfig</i>	Communication / Protocols / PPP list
<i>WEBconfig</i>	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).

2.7.2

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
<i>LANconfig</i>	Communications / Remote site / Name list (ISDN)
<i>WEBconfig</i>	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 behavior 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' on page 136.



2.8

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 – **C**alling **L**ine **I**dentifier). Access to your own network is granted if the call number appears in the number list, or the caller is called back if the callback option is activated (this callback via the D channel is not supported by the Windows Dial-Up Network). If the *LANCOM* is set to provide security

using the telephone number, any calls from remote stations with unknown numbers are denied access.

- **Have you activated the Firewall?**

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

- **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.

- **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 the a dedicated Firewall rule then. Thus 'Trojans' and certain Email viruses loose their communication way back. The Firewall rules are summarized in LANconfig under 'Firewall/Qos' on the register card 'Rules'. A guidance can be found under 'Set-up of an explicit "Deny All" strategy' on page 59.

- **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.

3 Quality of Service

This chapter dedicates itself to quality: Under the generic term Quality of Service (short: QoS) these functions of the *LANCOM* are summarized, which are concerned with the guaranty of certain service availabilities. These functions - described already in the preceding chapter - are made available by the Firewall (see 'Quality of Service objects' on page 50).

That has the advantage that the QoS functions can be realized with the existing, powerful classification methods of the Firewall (e.g. restriction on sub networks, individual workstations or dedicated services). Thus QoS features can be used also for applications, which on their part do not offer QoS methods themselves. In the following sections the underlying concepts are described more exactly.

3.1 Overview



Additionally to the layer 3 IP QoS, some LANCOM offer QoS also on other network layers, such as the layer 1 ATM. Please take the description of these special features from the appropriate user's manuals of these models.

The following QoS functions below are available in a *LANCOM*. Thereby appropriate quality rules ("QoS Policies") can be provided for bandwidth management ("traffic engineering").

3.1.1 Guaranteed minimum bandwidths

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

Full dynamic bandwidth management

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. Each individual VoIP connection thereby 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 may not exceed the effectively available transmission bandwidth.

3.1.2

Limited maximum bandwidths

Hereby you limit e.g. the entire or connection-referred maximum bandwidth for server accesses.

An example:

You operate both a Web server and a local network at a shared Internet access.

To prevent that your productive network (LAN) is paralyzed by many Internet accesses to your Web server, you limit all server accesses to half of the available bandwidth. In order to guarantee furthermore that your server services are available equally to many users at the same time, you set a certain maximum bandwidth per each server connection.

Combination possible



Minimum and maximum bandwidths can be used combined together. Thus the available bandwidth can be distributed accordingly depending on your requirements e.g. on certain user groups or applications.

3.1.3

Type of Service (TOS) and/or DiffServ support

Applications are preferred, which set certain flags within the IP header.

In particular:

- TOS "Low Delay"
- DiffServ "Expedited Forwarding"
- TOS "High Reliability"



The IP header bits of the TOS resp. DiffServ field are copied in case of a VPN route also into the enclosing IP headers of the IPSec VPN packet.

Thus QoS is available also for VPN routes over the Internet, if your provider treats appropriate packets also in the WAN preferentially.

3.2

IP Quality of Service in detail

Quality of Service in the *LANCOM* is produced by the fact that different priority queues are available.

The QoS features are available only for the transmission direction, as the local network (LAN) does have usually a clearly higher bandwidth than the long-distance traffic access (WAN).

The following queues are available:

- Urgent queue I

All packets with set TOS "Low Delay" - and/or DiffServ "Expedited Forwarding" attribute are handled here. This queue is always processed before all others. Likewise, all packets, which have been assigned a certain minimum bandwidth, are processed in this queue - however, only as long, as the guaranteed minimum bandwidth is not exceeded. Furthermore, TCP control packets can be likewise dispatched by this queue preferentially (see 'SYN/ACK speedup' on page 127).

- Urgent queue II

This is for all packets, which got assigned a guaranteed minimum bandwidth, but whose connection has exceeded this minimum bandwidth.

As long as the interval for the minimum bandwidth is not exceeded (i.e. up to the end of the current second), all packets in this queue are treated without further special priority. All packets in this queue, the "secured queue" and the "standard queue" share now the existing bandwidth. The packets are taken in the order from the queues when sending in exactly the same sequence, in which they were 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 rejected (transmission guaranteed). This queue is used for packets, which set the TOS attribute "High Reliability".

- Standard queue

The standard queue contains every not separately classified data traffic. Packets in this queue are first rejected if the packets cannot be delivered fast enough ('best effort').

4 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

4.1 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.

4.1.1 The DHCP server

As a DHCP server, the *LANCOM* can administer the IP addresses in its TCP/IP network. In doing so, it passes the following parameters to the workstation computers:

- IP-address
- network mask
- broadcast address
- standard gateway

- DNS server
- NBNS server
- period of validity for the parameters assigned

The DHCP server takes the IP addresses either from a freely defined address pool or determines the addresses automatically from its own IP address (or intranet address).

In DHCP mode, a completely unconfigured device can even automatically assign IP addresses to itself and the computers in the network.

In the simplest case, all that is required is to connect the new device to a network without other DHCP servers and switch it on. The DHCP server then interacts with *LANconfig* using a wizard and handles all of the address assignments in the local network itself.

4.1.2

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'.

4.1.3

How are the addresses assigned?

IP address assignment

Before the DHCP server can assign IP addresses to the computers in the network, it first needs to know which addresses are available for assignment. Three options exist for determining the available selection of addresses:

- The IP address can be taken from the address pool selected (start address pool to end address pool). Any valid addresses in the local network can be entered here.
- If '0.0.0.0' is entered instead, the DHCP server automatically determines the particular addresses (start or end) from the IP or intranet address settings in the 'TCP-IP-module' using the following procedure:
 - If only the Intranet address or only the DMZ address is entered, the start or end of the pool is determined by means of the associated network mask.
 - If both addresses have been specified, the Intranet address has priority for determining the pool.

From the address used (Intranet or DMZ address) and the associated network mask, the DHCP server determines the first and last possible IP address in the local network as a start or end address for the address pool.

- If the router has neither an Intranet address nor an DMZ address, the device has gone into a special operating mode. It then uses the IP address '172.23.56.254' for itself and the address pool '172.23.56.x' for the assignment of IP addresses in the network.

If only one computer in the network is started up that is requesting an IP address via DHCP with its network settings, a device with an activated DHCP module will offer this computer an address assignment. A valid address is taken from the pool as an IP address. If the computer was assigned an IP address at some point in the past, it requests this same address and the DHCP server attempts to reassign it this address if it has not already been assigned to another computer.

The DHCP server also checks whether the address selected is still available in the local network. As soon as the uniqueness of an address has been established, the requesting computer is assigned the address found.



Netmask assignment

The network mask is assigned in the same way as the address. If a network mask is entered in the DHCP module, this mask is used for the assignment. Otherwise, the network mask from the TCP/IP module is used. The order is the same as during the assignment of the addresses.

Broadcast address assignment

Normally, an address yielded from the valid IP addresses and the network mask is used for broadcast packets in the local network. In special cases, however (e.g. when using subnetworks for some of the workstation computers), it may be necessary to use a different broadcast address. In this case, the broadcast address to be used is entered in the DHCP module.

The default setting for the broadcast address should be changed by experienced network specialists only. Incorrect configuration of this section can result in the undesired establishment of connections subject to connect charges!

Standard gateway assignment

The device always assigns the requesting computer its own IP address as a gateway address.

If necessary, this assignment can be overwritten with the settings on the workstation computer.

DNS and NBNS assignment

This assignment is based on the associated entries in the 'TCP/IP-module'.

If no server is specified in the relevant fields, the router passes its own IP address as a DNS address. This address is determined as described under 'IP address assignment'. The router then uses DNS-forwarding (also see 'DNS-forwarding'), to resolve DNS or NBNS requests from the host.

Period of validity for an assignment

The addresses assigned to the computer are valid only for a limited period of time. Once this period of validity has expired, the computer can no longer use these addresses. In order for the computer to keep from constantly losing its addresses (above all its IP address), it applies for an extension ahead of time that it is generally sure to be granted. The computer loses its address only if it is switched off when the period of validity expires.

For each request, a host can ask for a specific period of validity. However, a DHCP server can also assign the host a period of validity that differs from what it requested. The DHCP module provides two settings for influencing the period of validity:

- Maximum lease time in minutes

Here you can enter the maximum period of validity that the DHCP server assigns a host.

If a host requests a validity that exceeds the maximum length, this will nevertheless be the maximum available validity!

The default setting is 6000 minutes (approx. 4 days).

- Default lease time in minutes

Here you can enter the period of validity that is assigned if the host makes no request. The default setting is 500 minutes (approx. 8 hours).

Precedence for the DHCP server—request assignment

In the default configuration, almost all the settings in the Windows network environment are selected in such a way that the necessary parameters are requested via DHCP. Check the settings by clicking **Start / Settings / Control Panel / Network**. Select the **TCP/IP** entry for your network adapter and open **Properties**.

Check the various tabs for special entries, such as for the IP address or the standard gateway. If you would like all of the values to be assigned by the DHCP server, simply delete the corresponding entries.

On the 'WINS configuration' tab, the 'Use DHCP for WINS Resolution' option must also be selected if you want to use Windows networks over IP with name resolution using NBNS servers. In this case, the DHCP server must also have an NBNS entry.

Priority for computer—overwriting an assignment

If a computer uses parameters other than those assigned to it (e.g. a different default gateway), these parameters must be set directly on the workstation computer. The computer then ignores the corresponding parameters assigned to it by the DHCP server.

Under Windows 98, this is accomplished through the properties of the Network Neighborhood.

Click **Start / Settings / Control Panel / Network**. Select the 'TCP/IP' entry for your network adapter and open **Properties**.

You can now enter the desired values by selecting the various tabs.

Checking of IP addresses in the LAN

Configuration tool	Run/Table
<i>WEBconfig</i>	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.

4.2

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.

4.2.1

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.
- 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.

4.2.2

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.

<i>LANconfig</i>	TCP/IP / Addresses / Primary DNS / Secondary DNS
<i>WEBconfig</i>	Expert Configuration / Setup / TCP-IP-module / DNS-default / DNS-backup
Terminal/Telnet	/setup/TCP-IP-module/DNS-default /setup/TCP-IP-module/DNS-backup

- If no DNS server is entered in the router, it will attempt to reach a DNS server over a PPP connection (e.g. from the Internet provider) to get the IP address assigned to the name from there. This can only succeed if the address of a DNS server is sent to the router during PPP negotiation.
- The default route is established and the DNS server searched for there if no connection exists.

This procedure does not require you to have any knowledge of the DNS server address. Entering the Intranet address of your router as the DNS server for the workstation computers is sufficient to enable you obtain the name assignment. This procedure also automatically updates the address of the DNS server. Your local network always receives the most current information even if, for example, the provider sending the address changes the name of his DNS server or you change to another provider.

4.2.3

Setting up the DNS server

The settings for the DNS server are contained in the following menu or list:

Configuration tool	Run/Table
<i>LANconfig</i>	TCP/IP / DNS
<i>WEBconfig</i>	Expert Configuration / Setup / DNS-module
Terminal/Telnet	cd /setup/DNS-module

Proceed as follows to set the DNS server:

- Switch the DNS server on.

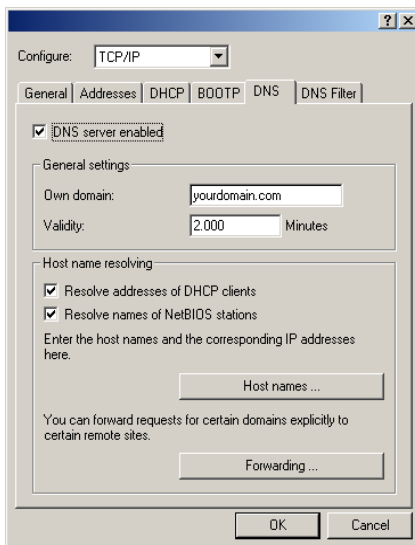
<i>WEBconfig</i>	... / Operating
Terminal/Telnet	set operating on

- b 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.

<i>WEBconfig</i>	... / Domain
Terminal/Telnet	set domain yourdomain.com

- c Specify whether information from the DHCP server and the NetBIOS module should be used.

<i>WEBconfig</i>	... / DHCP-usage ... / NetBIOS-usage
Terminal/Telnet	set DHCP-usage yes set NetBIOS-usage yes



Activated DNS server
in the TCP/IP configuration

- d 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:

<i>LANconfig</i>	TCP/IP / DNS / Host names / Add
<i>WEBconfig</i>	... / DNS-table / Add
Terminal/Telnet	<pre>cd setup/DNS-module/DNS- table set mail.yourdomain.com 10.0.0.99</pre>

For example, if would like to access the mail server at your headquarters (name: mail.yourdomain.com, IP: 10.0.0.99) via the router from a branch office, enter:



Stating the domain is optional but recommended.

When you now start your mail program, it will probably automatically look for the server 'mail.yourdomain.com'. The DNS server thereupon returns the IP address '10.0.0.99'. The mail program will then look for that IP address. With the proper entries in the IP routing table and name list, a connection is automatically established to the network in the headquarters, and finally to the mail server.

- e To resolve entire name areas of another DNS server, add a forwarding entry consisting of a name area and remote station:

<i>LANconfig</i>	TCP/IP / DNS / Forwarding / Add
<i>WEBconfig</i>	... / 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.

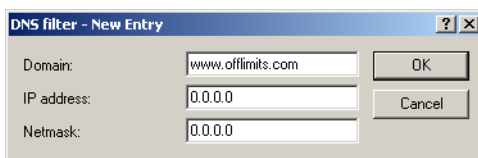
4.2.4

URL blocking

- f 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:

<i>LANconfig</i>	TCP/IP / DNS Filter / DNS filter... / Add
<i>WEBconfig</i>	... / 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>

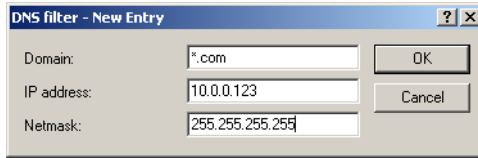


The index '001' in the console command can be selected as desired and is used only for clarity.



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:



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.



4.2.5

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://MyLANCOM.dynDNS.org>").

The advantage is obvious: If you want to accomplish e.g. remote maintenance for a remote site without ISDN available (e.g. over WEBconfig/HTTPS), or to connect with the LANCOM VPN Client to a branch office with dynamic IP address, then you just need to know the appropriate Dynamic DNS name.

How to deposit the current IP adresse 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.

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

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

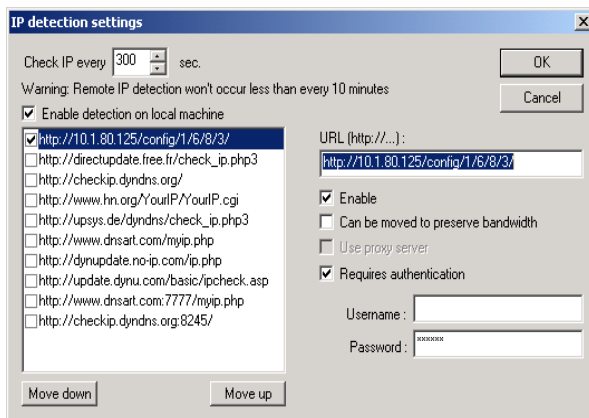


Figure: Picking the current IP address out of a LANCOM

4.3 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.

4.3.1 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 maximum of 830 charge units may be used in six days. The router will not permit the establishment of any further connections once this limit has been reached.



*The best way to use the router's call charge monitoring function is if you have "call charge information enabled **during** the connection" to the ISDN network (i.e. AOCD). If necessary, subscribe to this facility from your telecommunications carrier. Charge monitoring with the "Charge information **after** connection" feature is also possible in principle, but in this case continuous connections may not be detected!*



If you have enabled least-cost routing on the router modules, connections may be established to providers who do not transmit any charge information!

4.3.2

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 LANcapi are not affected.

4.3.3

Settings in the charge module

Configuration tool	Run/table
<i>LANconfig</i>	Management / Costs
<i>WEBconfig</i>	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.



4.4

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.

4.4.1

Setting up the SYSLOG module

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

4.4.2

Example configuration with *LANconfig*

Create SYSLOG client

- Start *LANconfig*. Under 'Management', select the 'Log & Trace' tab.
- Turn the module on and click **SYSLOG clients**.
- In the next window click **Add....**
- 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 [OK] [Cancel]

Source:

☒ System ☒ Login

☒ System time ☐ Console login

☒ Connections ☐ Accounting

☐ Administration ☐ Router

Priority:

☒ Alert ☒ Error

☒ Warning ☒ Information

☐ Debug

SYSLOG comes from the UNIX world, in which specified sources are predefined. *LANCOM* assigns its own internal sources to these predefined SYSLOG sources, the so-called "facilities".

The following table provides an overview of the significance of all news sources that can be set in the *LANCOM*. The last column of the table also shows the alignment between the internal sources of the *LANCOM* and the SYSLOG facilities.

Source	Meaning	Facility
System	system messages (boot processes, timer system etc.)	KERNEL
Login	messages regarding login and logout of a user during the PPP negotiation and errors occurring during this process	AUTH
System time	messages regarding changes to the system time	CRON
Console login	messages regarding console logins (Telnet, outband, etc.), logouts and errors occurring during this process	AUTHPRIV
Connections	messages regarding establishing and releasing connections and errors occurring during this process (display trace)	LOCAL0
Accounting	accounting information after release of a connection (user, online time, transfer volume)	LOCAL1
Administration	messages regarding configuration changes, remotely executed commands etc.	LOCAL2
Router	regular statistics on the most frequently used services (sorted by port numbers) and messages regarding filtered packets, routing errors etc.	LOCAL3

The eight priority stages defined initially in the SYSLOG are reduced to five stages in the *LANCOM*. The following table shows the relationship of alarm level, significance and SYSLOG priorities.

Priority	Meaning	SYSLOG priority
Alert	All messages requiring the attention of the administrator are collected under this heading.	PANIC, ALERT, CRIT
Error	All error messages that can occur during normal operation without requiring administrative intervention are sent to this level (e.g. connection errors).	ERROR
Warning	Error messages that do not affect normal operation of the device are sent to this level.	WARNING
Information	All messages that are purely informative in character are sent to this level (e.g. accounting information).	NOTICE, INFORM
Debug	Transfer of all debug messages. Debug messages generate a high data volume and interfere with the normal operation of the device. They should therefore be disabled during normal operation and should only be activated for troubleshooting.	DEBUG

- e 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`.

4.5 Office communications with *LANcapi*

LANcapi 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 *LANcapi* and its use for office communications tasks.

4.5.1 What are the advantages of *LANcapi*?

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

For example, faxes are sent by simulating a fax machine at the workstation. With *LANcapi*, the PC forwards the fax via the network to the router which establishes the connection to the recipient.



Please note: All LANcapi-based applications access the ISDN directly and do not run across the router of the device. The connect-charge monitoring and firewall functions are thus disabled!

4.5.2 Installing the *LANcapi* client

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

- a Place the *LANCOM Office* 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 Office* CD in the Windows Explorer.
- b Select the Install LANCOM software entry.
- c Highlight the ***LANcapi*** option. Click **Next** and follow the instructions for the installation routine.

If necessary, the system is restarted and *LANcapi* is then ready to accept all jobs from the office communications software. After successful installation, an icon for *LANcapi* will be available in the toolbar. A double-click on this icon opens a status window that permits current information on the *LANcapi* to be displayed at any time.

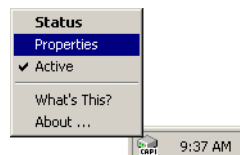
4.5.3 Configuration of the *LANcapi* clients

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.

- a Start the *LANcapi* client in the 'LANCOM' program group. Information regarding the drivers for the available service can be found on the 'General' tab.



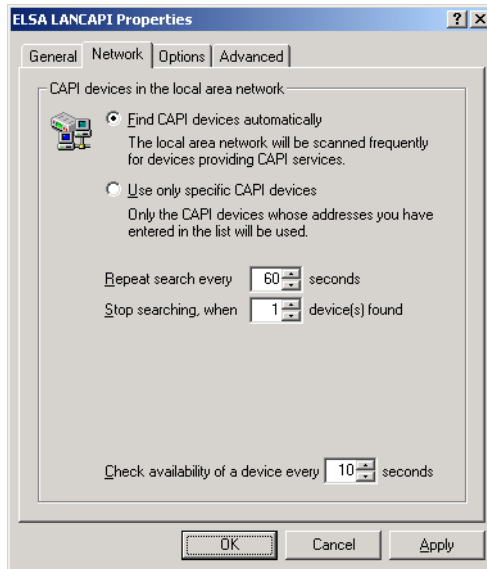
*You can also run the *LANcapi* client through the Windows taskbar. To do this, simply click with the right mouse button on the *LANcapi* symbol in the Windows taskbar next to the clock and select **Properties**.*



- b 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.



4.5.4

Configuring the *LANcapi* server

Two basic issues are important when configuring the *LANcapi* server:

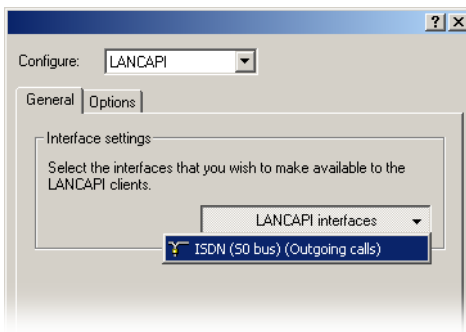
- What call numbers from the telephone network should *LANcapi* respond to?
- Which of the computers in the local network should be able to access the telephone network via *LANcapi*?

The *LANcapi* server is configured in the following menus:

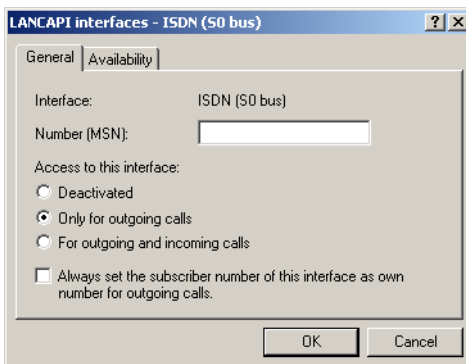
Configuration tool	Run command/menu
<i>LANconfig</i>	LANCAPI
<i>WEBconfig</i>	Expert Configuration / Setup / LANCAPI-module
Terminal/Telnet	cd /setup/LANCAPI-module

Example configuration with *LANconfig*

- Open the configuration of the router by double-clicking on the device name in the list and select the configuration area **LANCAPI**.
- Select the ISDN port you want to set.



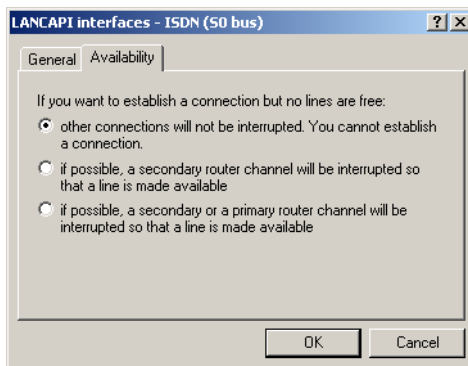
- Activate the *LANcapi* server for the outgoing and incoming calls, or allow only outgoing calls.



- d In the latter case, the *LANcapi* 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 *LANcapi*.
- e When the *LANcapi* server is activated, enter the call numbers to which the *LANcapi* should respond in the 'Number (MSN)' field. You can enter several call numbers separated by semicolons. If you do not enter a call number here, all incoming calls are reported to *LANcapi*.
- f *LANcapi* 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.
- g If you do not wish all the computers in the local network to be able to access the *LANcapi* 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 LANcapi, 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.

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



The meaning of the options offered here:

- The connection via *LANCapi* can not be performed. A fax program using the *LANCapi* will then probably attempt to send again at a later time.
- The connection via the *LANcapi* 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 *LANcapi* must wait if two router connections are established to separate remote stations (two main channels busy).
- A connection via *LANcapi* 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.

4.5.5 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'.

4.5.6 The LANCOM *CAPI Faxmodem*

The LANCOM *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 LANCOM *CAPI Faxmodem* can be installed from the CD setup. Always install the LANCOM *CAPI Faxmodem* together with the current version of *LANcapi*. After restarting, the LANCOM *CAPI Faxmodem* will be available for you, e.g. in Windows 98 under **Start / Settings / Control Panel / Modems**.

Faxing with the LANCOM CAPI Faxmodem

Most major fax programs recognize the *LANCOM 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.

5 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.

5.1 General information on WAN connections

WAN connections are used for the following applications.

- Internet access
- LAN to LAN coupling
- Remote access

5.1.1 Bridges for standard protocols

WAN connections differ from direct connections (for example, via the *LANcap*) 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).

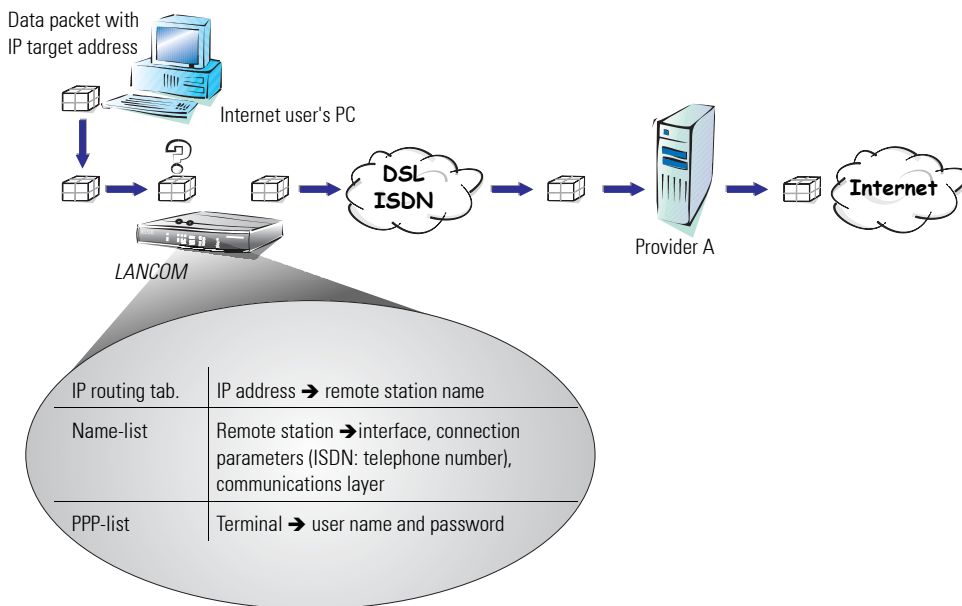
Close cooperation with router modules

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 fulfill requests from PCs within the LAN for external resources.

5.1.2 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.



a 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'.

b 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.

c 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.

d **Transmission of data packets**

As soon as the connection is established, the router can send the data packet to the Internet.

5.2

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.

5.2.1

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). “Unfavorable” routes like this will only be used if no other route to the remote station in question can be found.

Configuration of the routing table

Configuration tool	Run
<i>LANconfig</i>	IP router / Routing / Routing table
<i>WEBconfig</i>	Expert Configuration / Setup / IP-router-module / IP-routing-table
Terminal/Telnet	cd /setup/IP-router/IP-routing-table

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.

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)' on page 74.

5.2.2

Local routing

You know the following behavior of a workstation within a local network: The computer searches for a router to assist with transmitting a data packet to an IP address which is not on its own LAN. This router is normally introduced to the operating system with an entry as standard router or standard gateway. It is often only possible to enter one default router which is supposed to be able to reach all the IP addresses which are unknown to the workstation computer if there are several routers in a network. Occasionally, however, this default router cannot reach the destination network itself but does know another router which can find this destination.

How can you assist the workstation computer now?

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

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

Configuration tool	Run
<i>LANconfig</i>	IP router / General / Forward packets within the local network
<i>WEBconfig</i>	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.

5.2.3 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.

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 *LANcap*).
 - 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
<i>LANconfig</i>	IP router / General / RIP options
<i>WEBconfig</i>	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.

5.2.4

Policy-based routing

Policy-based routing describes a process in which particular data packets are given preferential treatment. This requires evaluation of a special field within the IP data packet, known as the Type of Service (TOS) field. This preferential treatment of a number of data packets can, for example, simplify the configuration of the router via the WAN when large data volumes are to be transferred simultaneously.

Policy based routing can be activated and deactivated as follows:

Configuration tool	Menu/table
<i>LANconfig</i>	IP router / General / Note the Type-Of-Service field in IP packets
<i>WEBconfig</i>	Expert Configuration / Setup / IP-router-module / Routing-method / Routing-method
Terminal/Telnet	cd /setup/IP-router-module/routing-method set routing method TOS (on) set routing method NORMAL (off)

5.2.5

SYN/ACK speedup

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

The greatest effect occurs with SYN/ACK speedup with fast connections 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
<i>LANconfig</i>	IP router / General / Pass on TCP SYN and ACK packets preferentially
<i>WEBconfig</i>	Expert Configuration / Setup / IP-router-module / Routing-method / SYN/ACK-speedup
Terminal/Telnet	<code>cd /setup/IP-router-module/routing-method set SYN/ACK-speedup OFF</code>

5.3

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' on page 130.



5.3.1

Name list

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

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

5.3.2

Layer list

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

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

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



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

Parameter	Meaning
Layer name	The layer is selected in the 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.
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.
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' on page 140.

Parameter	Meaning	
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)

5.4 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.

5.4.1 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.

5.4.2

Everything o.k.? Checking the line with LCP

The devices involved in the establishment of a connection through PPP negotiate a common behavior during data transfer. For example, they first decide whether a connection can be made at all using the security procedure, names and passwords specified.

The reliability of the line can be constantly monitored using the LCP once the connection has been established. This is achieved within the protocol by the LCP echo request and the associated LCP echo reply. The LCP echo request is a query in the form of a data packet which is transferred to the remote station along with the data. The connection is reliable and stable if a valid response to this request for information is returned (LCP echo reply). This request is repeated at defined intervals so that the connection can be continually monitored.

What happens when there is no reply? First a few retries will be initiated to exclude the possibility of any short-term line interference. The line will be dropped and an alternative route sought if all the retries remain unanswered. If, for example, the high-speed connection refuses to work, an existing ISDN port can open the way to the Internet as a backup.



During remote access of individual workstations with Windows operating systems, we recommend switching off the regular LCP requests since these operating systems do not reply to LCP echo requests.



The LCP request behavior is configured in the PPP list for each individual connection. The intervals at which LCP requests should be made are set by the entries in the 'Time' and 'Retr.' fields, along with the number of retries that should be initiated without a response before the line can be considered faulty. LCP requests can be switched off entirely by setting the time at '0' and the retries at '0'.

5.4.3

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 telecommuter), the *LANCOM* assigns it an IP address for the duration of the connection, enabling communications to take place.

This type of address assignment is carried out during PPP negotiation and implemented only for connections via WAN. In contrast, the assignment of addresses via DHCP is (normally) used within a local network.



Assignment of an IP address will only be possible if the LANCOM can identify the remote station by its call number or name when the call arrives, i.e. the authentication process has been successful.

Examples

- Remote access

Address assignment is made possible by a special entry in the IP routing table. 255.255.255.255 is specified as the network mask as the IP address to be assigned to the remote site in the 'Router-name' field. In this case, the router name is the name, with which the remote site must identify itself to the *LANCOM*.

In addition to the IP address, the addresses of the DNS and NBNS servers (Domain Name Server and NetBIOS Name Server) including the backup

server from the entries in the TCP/IP module are transmitted to the remote station during this configuration.

So that everything functions properly, the remote site must also be adjusted in such a way that it can obtain the IP address and the name server from the *LANCOM*. This can be accomplished with Windows dial-up networking through the settings in the 'TCP settings' under 'IP address' and 'DNS configuration'. This is where the options 'IP address assigned by server' and 'Specify name server addresses' are activated.

- Internet access

If Internet access for a local network is realized via the *LANCOM*, the assignment of IP addresses can occur in a reverse manner. Configurations are possible in which the *LANCOM* does not have a valid IP address in the Internet and is assigned one by the Internet provider for the duration of the connection. In addition to the IP address, the *LANCOM* also receives information via the DNS server of the provider during the PPP negotiation.

In the local network, the *LANCOM* is only known by its internal valid intranet address. All workstations in the local network can then access the same Internet account and also reach e.g. the DNS server.

Windows users are able to view the assigned addresses via *LANmonitor*. In addition to the name of the remote station, the current IP address as well as the addresses of DNS and NBNS servers can be found there. Options such as channel bundling or the duration of the connection are also displayed.

5.4.4

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
<i>LANconfig</i>	Communication / Protocols / PPP list
<i>WEBconfig</i>	Expert Configuration / Setup / WAN-module / PPP-list
Terminal/Telnet	cd /setup/WAN module set PPP-list [...]

The PPP list may have up to 64 entries and contain the following values:

In this column of the PPP list...	...enter the following values:
Remote site (device name)	Name the remote site uses to identify itself to your router.
User name	The name with which your router logs onto the remote site. The device name of your router is used if nothing is specified here.
Password	Password transferred by your router to the remote site (if demanded). An asterisk (*) in the list indicates that an entry is present.
Auth.	Security method used on the PPP connection ('PAP', 'CHAP' or 'none'). Your own router demands that the remote site observes this procedure. Not the other way round. This means that 'PAP', 'CHAP' security is not useful when connecting to Internet service providers, who may not wish to provide a password. Select 'none' as the security attribute for connections such as these.
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 <i>LANconfig</i> , <i>SNMP</i> or <i>TFTP</i> !

5.5 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 reestablished with this setting.

With a holding time of 9,999 seconds the connection is always reestablished after any disconnection. Additionally, the connection is reestablished after a reboot of the device ('auto reconnect').

5.6 Callback functions

The *LANCOM* supports automatic callback via its ISDN port.

In addition to callback via the D channel, the CBCP (**C**allback **C**ontrol **P**rotocol) specified by Microsoft and callback via PPP as per RFC 1570 (PPP LCP extensions) are also offered. There is also the option of a particularly fast callback using a process developed by LANCOM. PCs with Windows operating system can be called back only via the CBCP.

5.6.1 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: OK

Phonenumber:

Cancel

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.

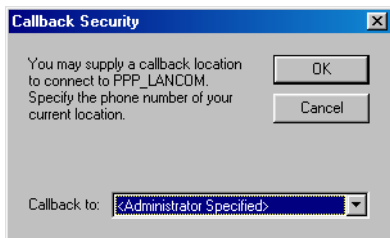
After the Authentication an input window appears on the caller's screen in Windows that requests the ISDN telephone number of the PC.

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.

5.6.2

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).
- 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.

5.6.3

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.

5.6.4

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 <i>LANCOM</i> 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.

5.7

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.

- a Select a communication layer for the remote station from the layer list that has bundling activated in the Layer-2 options. Select from the following Layer-2 options:
 - **compr.** according to the LZS data compression procedure (Stac) reduces the amount of data if the data hasn't already been compressed. This procedure is also supported by routers of other manufacturers and by ISDN adapters under Windows operating systems.
 - **bundle** uses two B channels per connection.
 - **bnd+cmpr** uses both (compression and channel bundling) and provides the maximum possible data transmission performance.
- b 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.
- c 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 takes the channel back (always in the case of static bundling, only as required when using dynamic bundling).
- Y connection **Off**: The router maintains the existing bundled connection; the establishment of the new connection must wait.



Please note that if channel bundling is used, the cost of two connections is charged. Here no additional connections via the LANcapi are possible! So you should only use channel bundling if the double transmission capacity can really be used in full.

6 Index

- **A**
 - AAL-5 130
 - Access protection 80
 - for the configuration 80
 - by name or number 80
 - by number 80
 - via TCP/IP 34
 - Address administration
 - IP address administration 91
 - Address pool 93
 - ADSL 21
 - AOCD 105
 - ATM 21
 - ATM adaptation layer 130
 - Auth. 137
 - Authentication 135
 - auto reconnect 136
 - Availability 113
- **B**
 - B-channel
 - protocol 81
 - Bonk 72
 - Brute force 33
- **C**
 - Call charge
 - information 105
 - limit 104
 - management 104, 109
 - Callback 80, 82
 - according to RFC 1570 138
 - Fast callback 82
 - for Microsoft CBCP 136
 - Callback procedure
 - fast callback 138
 - Caller ID 80
 - Calling Line Identifier Protocol 82
 - Capab. 97
 - CAPI Faxmodem 114
 - CAPI interface 109
 - Channel bundling 140
 - dynamic 140
 - static 140
 - Charge limiting 104
 - Charges
 - information 140
 - units 104, 140
 - CLIP 81, 82
 - Command line interface 26
 - Command line reference 27
 - Common ISDN Application
 - Programming Interface (CAPI) 109
 - Computer names 96
 - Conf 135
 - Configuration
 - procedure 9
 - SNMP 14
 - Configuration files 22
 - Configuration interface 9
 - Connection limit 105
 - Cost reduction 104
- **D**
 - D channel 21, 81
 - Data compression procedure
 - LZS 141
 - Data transfer 140
 - Denial of Service attack
 - Bonk/Frag Router 72
 - LAND 70
 - Ping of Death 71
 - Smurf 70
 - SYN flooding 70

- Teardrop 71
 - Denial of Service attacks 68
 - Device-name 135
 - DHCP 21, 91, 129
 - assignment
 - broadcast address 94
 - DNS and NBNS server 94
 - network mask 94
 - standard gateway 94
 - DHCP server 91, 97
 - mode 92
 - for WINS resolution 95
 - period of validity 94
 - Dial-Up Network 14
 - Dial-Up Networking 81
 - DiffServ 88
 - Distance of a route 121
 - DMZ 77, 79
 - IP address assignment 93
 - DNS 21, 96
 - DNS forwarding 98
 - DNS server 91, 94, 97
 - available information 98
 - filter mechanism 97
 - DNS-table 101, 102
 - Dynamic DNS 103
 - Domain 96, 102
 - deny access 102
 - Domain name service (DNS)
 - DNS 96
 - Dynamic channel bundling 140
 - Dynamic DNS 103
 - Dynamic Host Configuration Protocol (DHCP) 91
 - Dynamic routing 119
- **E**
 - Encapsulation 129
 - End address 93
 - ETH-10 130
 - Exclusion routes 120
 - exposed host 78
 - **F**
 - Fail 135
 - Fast callback 82
 - Fax 114
 - Fax Class 1 114
 - Fax driver 114
 - Fax transmission 115
 - Filter 74
 - Firewall 38, 74, 109
 - Firmware-upload 25
 - with LANconfig 25
 - with terminal program 26
 - with TFTP 26
 - with WEBconfig 26
 - Flash ROM memory 24
 - Flat rate 136
 - Frag Router 72
 - **G**
 - Gateway 74, 91
 - **H**
 - HDLC 130
 - High telephone costs 104
 - Host 97
 - Host name table 100
 - HTTPS 12
 - **I**
 - Identification control 80
 - Identifying the caller 80
 - IEEE 802.3 130
 - Inband 9
 - inband
 - Configuration via Inband 9
 - with Telnet 13
 - Install software 24

- Internet 74
- Internet access 134
- Intranet
 - IP address assignment 93
- Intranet address 76, 77
- Intrusion Detection 67
- Intrusion-Detection
 - IP-Spoofing 68
- Inverse masquerading 77
- IP address ranges 39
- IP broadcast 125
- IP masquerading 21, 74
 - simple masquerading 77
- IP multicast 125
- IP routing
 - standard router 121
- IP-address 19, 74, 133
- IP-routing-table 119
- IP-Spoofing 68
- ISDN
 - D channel 82
- **K**
 - Keep-Alive 136
- **L**
 - LANCOM FirmSafe 24
 - LANconfig 10, 15, 25
 - Management of multiple devices ... 11
 - LAND 70
 - LANmonitor 17
 - display options 18
 - monitor Internet connection 18
 - system information 18
 - Layer-2 129
 - Layer-3 129
 - LCP echo reply 132
 - LCP echo request 132
 - LCR 105
 - Least-cost routing 105
 - LLC-MUX 129
 - Login 24, 34
 - Login barring 33, 34
 - LZS data compression 141
 - **M**
 - Mail server 101
 - Making Invisible 72
 - Microsoft Network 95
 - Modem 130
 - Monitoring 17
 - MS-CHAP 130, 131
 - Multilink PPP (MLPPP) 130, 140
 - **N**
 - NAT 74
 - NBNS server 91, 95
 - NetBIOS 21, 97
 - NetBIOS networks 97
 - NetBIOS proxy 59
 - Network names 96
 - No charge information 105
 - **O**
 - Office communications 109
 - Online minutes 104
 - Outband 9
 - configuration via Outband 9
 - **P**
 - Packet dump 21
 - passwd 33
 - Password 17, 18, 32, 80, 81, 135
 - PAT 74
 - Period 104
 - Period of validity 92, 94
 - Ping blocking 73
 - Ping of Death 71
 - Policy-based routing 126
 - Port 77

- IP port 113
- PPP 19, 81, 129, 140
 - callback functions 136
 - checking the line with LCP 132
 - handshake 16
 - IP address assignment 133
 - LCP Extensions 138
- PPP client 14
- PPP connection 16
- PPPoE 129
- Priority control 113
- Protection
 - for the configuration 31
 - for the LAN 74
- **R**
 - Remote access 14, 133
 - Remote configuration 9
 - Remote connection 15
 - Remote-ID 135
 - Repetitions 135
 - RIP 21
 - Router-interface-list 141
 - Router-name 120
- **S**
 - Security 31, 74
 - Security checklist 83
 - Security procedures 81
 - Security settings 33
 - Serial port 9
 - Single user access 74
 - Smurf 70
 - SNMP 14
 - Stac data compression 141
 - Standard fax programs 114
 - Start address 93
 - Stateful Inspection 38
 - Static channel bundling 140
 - Static routing 119
- SYN Flooding 70
- SYN/ACK speedup 127
- SYSLOG 106
- **T**
 - TCP Stealth mode 73
 - TCP/IP 119
 - TCP/IP networks 96
 - Teardrop 71
 - Telnet 15
 - Term 135
 - Terminal program 25
 - TFTP 13
 - Throughput 140
 - Time 135
 - Time budget 105
 - Time dependent connection-limit 105
 - Time-out 140, 141
 - Trace
 - examples 22
 - keys and parameters 20
 - outputs 20
 - starting 20
 - Transmission rates 19
 - Troubleshooting 18
 - Type of Service 88, 126
- **U**
 - Upload 24
 - User name 16, 81, 135
- **V**
 - V.110 130
 - VC-MUX 129
 - VoIP 78
 - VPN
 - client 60
 - gateway 60

- **W**
 - WAN-layer 129
 - WEBconfig 10, 12, 25
 - HTTPS 12
 - Wildcards 102
- WINS Address 95
- **Y**
 - Y connection 141

