

**Reference Manual**  
**LANCOM LCOS 3.50**

© 2004 LANCOM Systems GmbH, Wuersele (Germany)

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

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

#### Trademarks

Windows<sup>®</sup>, Windows NT<sup>®</sup> and Microsoft<sup>®</sup> are registered trademarks of Microsoft, Corp.

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

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

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

LANCOM Systems GmbH  
Adenauertrasse 20 / B2  
D-52146 Würsele  
Germany

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

Würsele, August 2004

# Contents

<b>1 Preface</b>	<b>10</b>
<b>2 System design</b>	<b>13</b>
<b>3 Configuration and management</b>	<b>15</b>
3.1 Configuration tools and approaches	15
3.2 Configuration software	16
3.2.1 Configuration using LANconfig	16
3.2.2 Configuration with WEBconfig	18
3.2.3 Configuration using Telnet	19
3.2.4 Configuration using SNMP	20
3.3 Remote configuration via Dial-Up Network	20
3.3.1 This is what you need for ISDN remote configuration	21
3.3.2 The first remote connection using Dial-Up Networking	21
3.3.3 The first remote connection using a PPP client and Telnet	21
3.4 LANmonitor—know what's happening	23
3.4.1 Extended display options	24
3.4.2 Monitor Internet connection	24
3.5 Trace information—for advanced users	26
3.5.1 How to start a trace	26
3.5.2 Overview of the keys	27
3.5.3 Overview of the parameters	27
3.5.4 Combination commands	28
3.5.5 Examples	29
3.6 Working with configuration files	29
3.7 New firmware with LANCOM FirmSafe	30
3.7.1 This is how LANCOM FirmSafe works	30
3.7.2 How to load new software	31
3.8 Command line interface	32
3.8.1 Command line reference	33
3.9 Scheduled Events	34
<b>4 Management</b>	<b>37</b>
4.1 N:N mapping	37

4.1.1	Application examples	38
4.1.2	Configuration	42
4.1.3		45
<b>5</b>	<b>Diagnosis</b>	<b>46</b>
5.1	LANmonitor—know what's happening	46
5.1.1	Extended display options	46
5.1.2	Monitor Internet connection	47
5.2	Trace information—for advanced users	48
5.2.1	How to start a trace	48
5.2.2	Overview of the keys	49
5.2.3	Overview of the parameters	49
5.2.4	Combination commands	50
5.2.5	Examples	51
<b>6</b>	<b>Security</b>	<b>52</b>
6.1	Protection for the configuration	52
6.1.1	Password protection	52
6.1.2	Login barring	54
6.1.3	Restriction of the access rights on the configuration	55
6.2	Protecting the ISDN connection	58
6.2.1	Identification control	58
6.2.2	Callback	60
6.3	The security checklist	61
<b>7</b>	<b>Routing and WAN connections</b>	<b>64</b>
7.1	General information on WAN connections	64
7.1.1	Bridges for standard protocols	64
7.1.2	What happens in the case of a request from the LAN?	64
7.2	IP routing	66
7.2.1	The IP routing table	66
7.2.2	Local routing	68
7.2.3	Dynamic routing with IP RIP	69
7.2.4	SYN/ACK speedup	73
7.3	The hiding place—IP masquerading (NAT, PAT)	74
7.3.1	Simple masquerading	74
7.3.2	Inverse masquerading	78
7.3.3	Unmasked Internet access for server in the DMZ	79

7.4	N:N mapping	80
7.4.1	Application examples	81
7.4.2	Configuration	85
7.5	Configuration of remote stations	89
7.5.1	Name list	89
7.5.2	Layer list	90
7.6	Establishing connection with PPP	91
7.6.1	The protocol	92
7.6.2	Everything o.k.? Checking the line with LCP	94
7.6.3	Assignment of IP addresses via PPP	94
7.6.4	Settings in the PPP list	96
7.7	Extended connection for flat rates—Keep-alive	97
7.8	Callback functions	98
7.8.1	Callback for Microsoft CBCP	98
7.8.2	Fast callback using the LANCOM process	99
7.8.3	Callback with RFC 1570 (PPP LCP extensions)	100
7.8.4	Overview of configuration of callback function	100
7.9	Channel bundling with MLPPP	101
<b>8</b>	<b>Firewall</b>	<b>104</b>
8.1	Threat analysis	104
8.1.1	The dangers	104
8.1.2	The ways of the perpetrators	105
8.1.3	The methods	105
8.1.4	The victims	106
8.2	What is a Firewall?	107
8.2.1	Tasks of a Firewall	107
8.2.2	Different types of Firewalls	108
8.3	The LANCOM Firewall	114
8.3.1	How the LANCOM Firewall inspects data packets	115
8.3.2	Special protocols	119
8.3.3	General settings of the Firewall	121
8.3.4	Parameters of Firewall rules	125
8.3.5	Alerting functions of the Firewall	131
8.3.6	Strategies for Firewall settings	134
8.3.7	Hints for setting the Firewall	137
8.3.8	Configuration of Firewall rules	141
8.3.9	Firewall diagnosis	151

8.3.10 Firewall limitations	159
8.4 Protection against break-in attempts: Intrusion Detection	160
8.4.1 Examples for break-in attempts	160
8.4.2 Configuration of the IDS	161
8.5 Protection against "Denial of Service" attacks	162
8.5.1 Examples of Denial of Service attacks	162
8.5.2 Configuration of DoS blocking	165
8.5.3 Configuration of ping blocking and Stealth mode	166
<b>9 Quality of Service</b>	<b>168</b>
9.1 Why QoS?	168
9.2 Which data packets to prefer?	168
9.2.1 Guaranteed minimum bandwidths	171
9.2.2 Limited maximum bandwidths	172
9.3 The queue concept	172
9.3.1 Queues in transmission direction	172
9.3.2 Queues for receiving direction	175
9.4 Reducing the packet length	176
9.5 QoS parameters for Voice over IP applications	178
9.6 QoS in sending or receiving direction	182
9.7 QoS configuration	183
9.7.1 Evaluating ToS and DiffServ fields	183
9.7.2 Defining minimum and maximum bandwidths	185
9.7.3 Adjusting transfer rates for interfaces	187
9.7.4 Sending and receiving direction	189
9.7.5 Reducing the packet length	189
<b>10 Virtual LANs (VLANs)</b>	<b>192</b>
10.1 What is a Virtual LAN?	192
10.2 This is how a VLAN works	192
10.2.1 Frame tagging	193
10.2.2 Conversion within the LAN interconnection	194
10.2.3 Application examples	195
10.3 Configuration of VLANs	198
10.3.1 The network table	198
10.3.2 The port table	199
10.3.3 Configuration with LANconfig	200

10.3.4	Configuration with WEBconfig or Telnet	201
<b>11</b>	<b>Wireless LAN – WLAN</b>	<b>203</b>
11.1	What is a Wireless LAN?	203
11.1.1	Standardized radio transmission by IEEE	203
11.1.2	Operation modes of Wireless LANs and base stations	206
11.2	Developments in WLAN security	213
11.2.1	Some basic concepts	214
11.2.2	WEP	215
11.2.3	WEPplus	219
11.2.4	EAP and 802.1x	220
11.2.5	TKIP and WPA	223
11.2.6	AES and 802.11i	230
11.2.7	Summary	231
11.3	Protecting the wireless network	232
11.4	Configuration of WLAN parameters	233
11.4.1	WLAN security	234
11.4.2	General WLAN settings	243
11.4.3	The physical WLAN interfaces	244
11.4.4	The logical WLAN interfaces	250
11.4.5	Additional WLAN functions	254
11.5	Establishing outdoor wireless networks	256
11.5.1	Geometrical layout of the transmission path	256
11.5.2	Antenna power	258
11.5.3	Emitted power and maximum distance	261
11.5.4	Transmission power reduction	264
<b>12</b>	<b>Office communications with LANCAPI</b>	<b>265</b>
12.1	What are the advantages of LANCAPI?	265
12.2	The client and server principle	265
12.2.1	Configuring the LANCAPI server	265
12.2.2	Installing the LANCAPI client	268
12.2.3	Configuration of the LANCAPI clients	269
12.3	How to use the LANCAPI	270
12.4	The LANCOM CAPI Faxmodem	270

<b>13 Server services for the LAN</b>	<b>272</b>
13.1 Automatic IP address administration with DHCP	272
13.1.1 The DHCP server	272
13.1.2 DHCP—'on', 'off' or 'auto'?	273
13.1.3 How are the addresses assigned?	274
13.2 DNS	277
13.2.1 What does a DNS server do?	277
13.2.2 DNS forwarding	279
13.2.3 Setting up the DNS server	280
13.2.4 URL blocking	283
13.2.5 Dynamic DNS	284
13.3 Call charge management	285
13.3.1 Charge-based ISDN connection limits	285
13.3.2 Time dependent ISDN connection limit	286
13.3.3 Settings in the charge module	287
13.4 The SYSLOG module	287
13.4.1 Setting up the SYSLOG module	288
13.4.2 Example configuration with LANconfig	288
<b>14 Virtual Private Networks—VPN</b>	<b>291</b>
14.1 What does VPN offer?	291
14.1.1 Private IP addresses on the Internet?	293
14.1.2 Secure communications via the Internet?	294
14.2 LANCOM VPN: an overview	295
14.2.1 VPN example application	295
14.2.2 Advantages of LANCOM VPN	296
14.2.3 LANCOM VPN functions	297
14.3 VPN connections in detail	298
14.3.1 LAN-LAN coupling	298
14.3.2 Dial-in connections (Remote Access Service)	299
14.4 What is LANCOM Dynamic VPN?	300
14.4.1 A look at IP addressing	300
14.4.2 This is how LANCOM Dynamic VPN works	301
14.5 Configuration of VPN connections	306
14.5.1 VPN tunnel: Connections between VPN gateways	307
14.5.2 Set up VPN connections with the Setup Wizard	308
14.5.3 Inspect VPN rules	309
14.5.4 Manually setting up VPN connections	309



14.5.5	Prepare VPN network relationships	311
14.5.6	Configuration with LANconfig	314
14.5.7	Configuration with WEBconfig	318
14.5.8	Diagnosis of VPN connections	322
14.6	Specific examples of connections	322
14.6.1	Static/static	323
14.6.2	Dynamic/static	323
14.6.3	Static/dynamic (with LANCOM Dynamic VPN)	324
14.6.4	Dynamic/dynamic (with LANCOM Dynamic VPN)	325
14.7	How does VPN work?	326
14.7.1	IPSec—The basis for LANCOM VPN	327
14.7.2	Alternatives to IPSec	328
14.8	The standards behind IPSec	329
14.8.1	IPSec modules and their tasks	329
14.8.2	Security Associations – numbered tunnels	329
14.8.3	Encryption of the packets – the ESP protocol	330
14.8.4	Authentication – the AH protocol	332
14.8.5	Key management – IKE	335
<b>15</b>	<b>Appendix: Overview of functions for LANCOM models and LCOS versions</b>	<b>337</b>
<b>16</b>	<b>Index</b>	<b>338</b>

# 1 Preface

## User's manual and reference manual

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

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

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

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

## LCOS, the operating system of LANCOM devices

All LANCOM routers and LANCOM Wireless Access Points use the same operating system: LCOS. The operating system developed by LANCOM itself is not attackable from the outside, and thus offers high security. The consistent use of LCOS ensures a comfortable and constant operation of all LANCOM prod-

ucts. The extensive feature set is available throughout all LANCOM products (provided respective support by hardware), and continuously receives further enhancements by free, regular software updates.

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

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

### Validity

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

The functions and settings described in this reference manual are not supported by all models and/or all firmware versions. A table can be found in the appendix denoting the individual functions, from which firmware version they are supported in the respective devices ('Appendix: Overview of functions for LANCOM models and LCOS versions' →page 337).

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

### Security settings

For a carefree use of your device, we recommend to carry out all security settings (e.g. Firewall, encryption, access protection, charge lock), which are not already activated at the time of purchase of your device. The LANconfig wizard 'Check Security Settings' will support you accomplishing this. Further information regarding this topic can be found in chapter 'Security' →page 52.

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

### This documentation was compiled ...

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

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

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



Our online services ([www.lancom.de](http://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

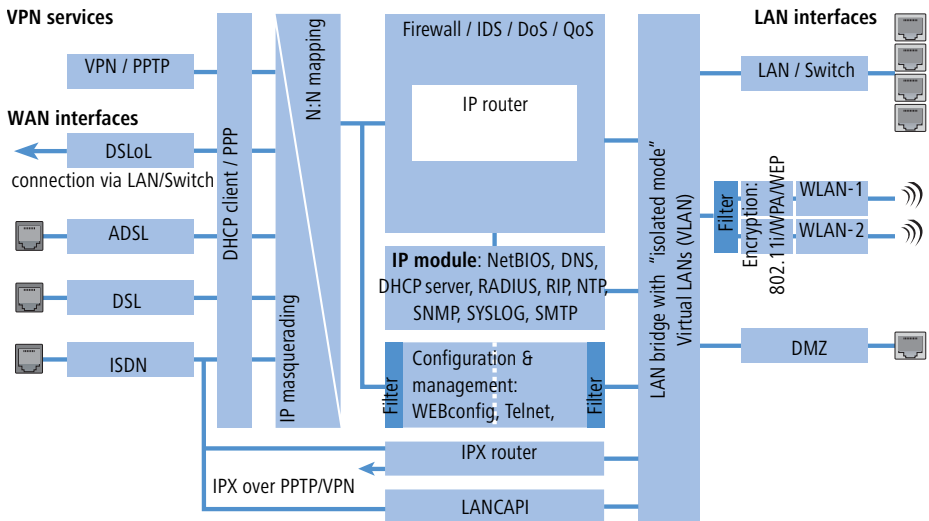
<b>Bold</b>	Menu commands, command buttons, or text boxes
Code	Inputs and outputs for the display mode
<Value>	Placeholder for a specific value

## 2 System design

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

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

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



Notes regarding the respective modules and interfaces:

- ▶ The IP router takes care of routing data on IP connections between the interfaces from LAN and WAN.
- ▶ The firewall (with the services "Intrusion Detection", "Denial of Service" and "Quality of Service") encloses the IP router like a shield. All connections via the IP router automatically flow through the firewall as well.
- ▶ LANCOM devices provide either a separate LAN interface or an integrated switch with multiple LAN interfaces as interfaces to the LAN.

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

## 3 Configuration and management

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

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

### 3.1 Configuration tools and approaches

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

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

- ▶ Through the connected network (LAN as well as WAN—inband)
- ▶ Through the configuration interface (config interface) on the rear of the router (also known as outband)
- ▶ Remote configuration via ISDN access

#### **What is the difference between these three possibilities?**

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

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

## 3.2 Configuration software

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

- ▶ **LANconfig** – nearly all parameters of the LANCOM can be set quickly and with ease using this menu-based application. Outband, inband and remote configuration are supported, even for multiple devices simultaneously.
- ▶ **WEBconfig** – this software is permanently installed in the router. All that is required on the workstation used for the configuration is a web browser. WEBconfig is thus independent of operating systems. Inband and remote configuration are supported.
- ▶ **SNMP** – device-independent programs for the management of IP networks are generally based on the SNMP protocol. It is possible to access the LANCOM inband and via remote configuration using SNMP.
- ▶ **Terminal program, Telnet** – an LANCOM can be configured with a terminal program via the config interface (e.g. HyperTerminal) or within an IP network (e.g. Telnet).
- ▶ **TFTP** – the file transfer protocol TFTP can to a limited extent also be used within IP networks (inband and remote configuration).



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

### 3.2.1 Configuration using LANconfig

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

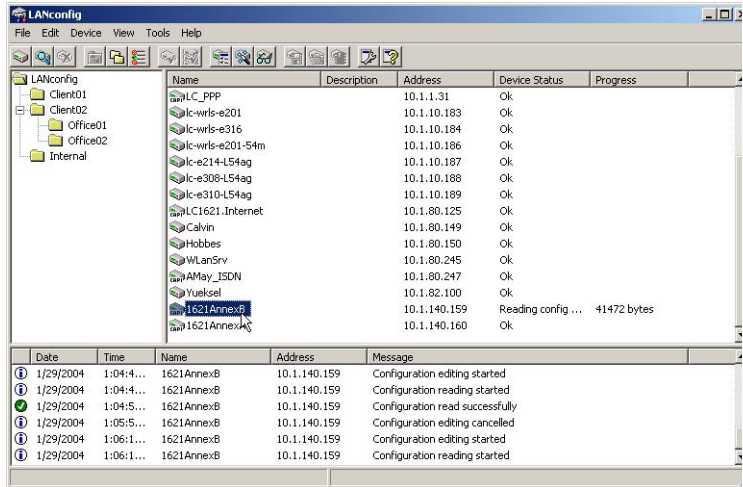
#### Find new devices



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



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



### The expanded range of functions for professionals

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

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

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



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


### The integrated Help function

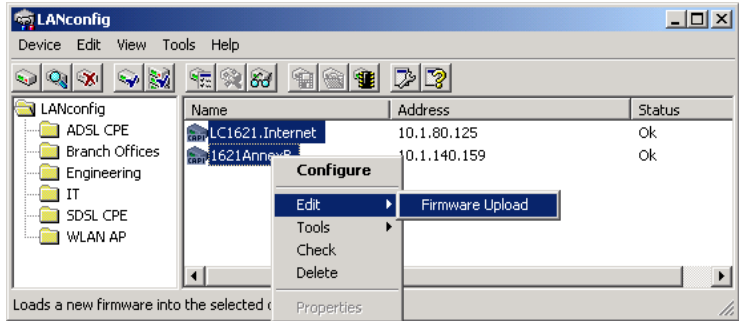
The remainder of the program's operation is self-explanatory or you can use the online help. You can click on the 'Help' button top right in any window or right-click on an unclear term at any time to call up context-sensitive help.

## Management of multiple devices

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

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

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



### 3.2.2 Configuration with WEBconfig

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

#### Functions with any web browser

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

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

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

### Secure with HTTPS

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

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



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

### 3.2.3 Configuration using Telnet

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

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

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

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

#### Change the language of the display.

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

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

### TFTP

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

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

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

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



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

### 3.2.4 Configuration using SNMP

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

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

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

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

## 3.3 Remote configuration via Dial-Up Network



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

Configuring routers at remote sites is particularly easy using the remote configuration method via a Dial-Up Network from Windows. The device is accessible by the administrator immediately without any settings being made after it is switched on and connected to the WAN interface. This means that you save a lot of time and costs when connecting other networks to your network because you do not have to travel to the other network or instruct the staff on-site on configuring the router.

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

### 3.3.1 This is what you need for ISDN remote configuration

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

### 3.3.2 The first remote connection using Dial-Up Networking

- ① In the LANconfig program select **Device / New**, enable 'Dial-Up connection' as the connection type and enter the calling number of the WAN interface to which the LANCOM is connected. If you wish, you can also enter the time period after which an idle connection is to be disconnected automatically.
- ② LANconfig now automatically generates a new entry in the Dial-Up Network. Select a device that supports PPP (e.g. the NDIS-WAN driver included with the LANCAPI) for the connection and press **OK** to confirm.
- ③ Then the LANconfig program will display a new device with the name 'Unknown' and the dial-up call number as the address in the device list.



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

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

### 3.3.3 The first remote connection using a PPP client and Telnet

- ① Establish a connection to the LANCOM with your PPP client using the following details:
  - ▷ User name 'ADMIN'
  - ▷ The password selected in LANCOM
  - ▷ An IP address for the connection, only if required

- ② Open a Telnet session to the LANCOM. Use the following IP address for this purpose:
  - ▷ '172.17.17.18', if you have not defined an IP address for the PPP client. The LANCOM automatically uses this address if no other address has been defined. The PC making the call will respond to the IP '172.17.17.17'.
  - ▷ Raise the IP address of the PC by one, if you have defined an address. Example: You have set the IP '10.0.200.123' for the PPP client, the LANCOM then responds to '10.0.200.124'. Exception: If the digits '254' are at the end of the IP address, the router responds to 'x.x.x.1'.
- ③ You can configure the LANCOM remotely just like all other devices.

### **The default layer for remote field installations**

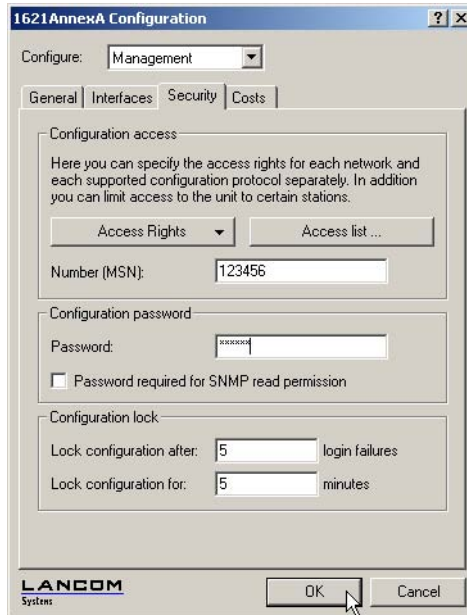
The PPP connection of any other remote site to the router, of course, will only succeed if the device answers every call with the corresponding PPP settings. This is the case using the factory default settings because the default protocol (default layer) is set to PPP.

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

### **The administrator access for ISDN remote management**

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

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



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

Alternatively, enter the following command:

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



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

```
passwd
```

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

### 3.4 LANmonitor—know what's happening

The LANmonitor includes a monitoring tool with which you can view the most important information on the status of your routers on your monitor at any

time under Windows operating systems—of all of the LANCOM routers in the network.

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

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

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



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

### 3.4.1 Extended display options

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

- ▶ Error messages
- ▶ Diagnostic messages
- ▶ System information



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

### 3.4.2 Monitor Internet connection

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

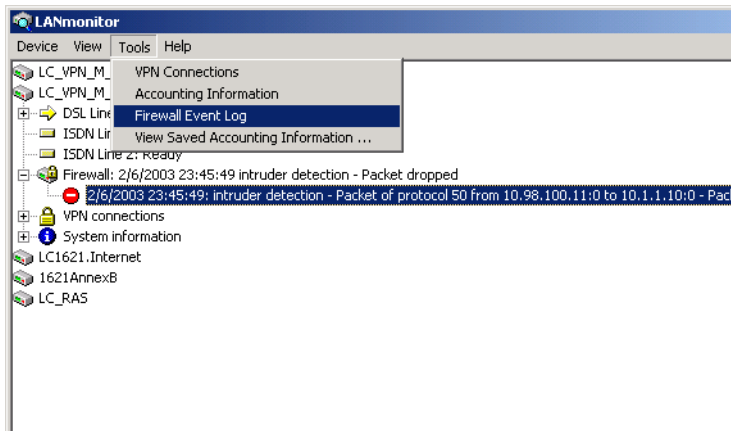
- ① To start LANmonitor, go to **Start ▶ Programs ▶ LANCOM ▶ LANmonitor**. Use **Device ▶ New** to set up a new device and in the following window, enter the IP address of the router that you would like to



monitor. If the configuration of the device is protected by password, enter the password too.

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

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



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

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

- ③ To break the connection manually, click on the active channel with the right mouse button. You may be required to enter a configuration password.
- ④ If you would like a log of the LANmonitor output in file form, select **Device ► Properties** and go to the 'Logging' tab. Enable logging and

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

## 3.5 Trace information—for advanced users

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



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

### 3.5.1 How to start a trace

Trace output can be started in a Telnet session, for example. The command to call up a trace follows this syntax:

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

The trace command, the code, the parameters and the combination commands are all separated from each other by spaces. And what is the meaning of these codes and parameters?

### 3.5.2 Overview of the keys

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

### 3.5.3 Overview of the parameters



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

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

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

### 3.5.4 Combination commands

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

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

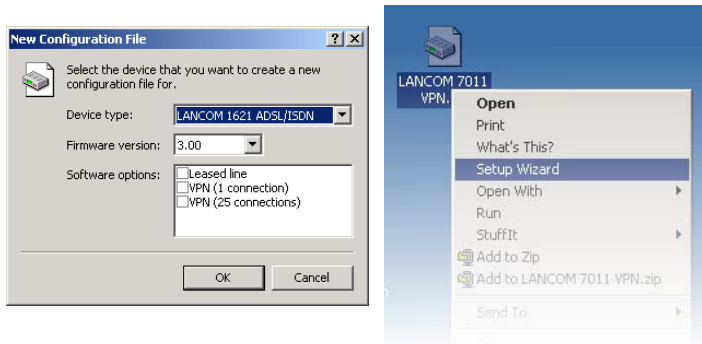
### 3.5.5 Examples

This code...	... in combination with the trace causes the following:
trace	displays all protocols that can generate outputs during the configuration, and the status of each output (ON or OFF)
trace + all	switches on all trace outputs
trace + protocol display	switches on the output for all connection protocols together with the status and error messages
trace + all - icmp	switches on all trace outputs with the exception of the ICMP protocol
trace ppp	displays the status of the PPP
trace # ipx-rt display	toggles between the trace outputs for the IPX router and the display outputs
trace - time	switches off the system time output before the actual trace output

### 3.6 Working with configuration files

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

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



#### Backup copies of configuration

With this function you can create backup copies of the configuration of your LANCOM. Should your LANCOM (e.g. due to a defect) lose its configuration data, you simply reload the backup copy.

## Convenient series configuration

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

## Running function

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

## 3.7 New firmware with LANCOM FirmSafe

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

### 3.7.1 This is how LANCOM FirmSafe works

LANCOM FirmSafe makes the installation of the new software safe: The used firmware is not simply overwritten but saved additionally in the device as a second firmware.

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

- ▶ 'Immediate': The first option is to load the new firmware and activate it immediately. The following situations can result:
  - ▷ The new firmware is loaded successfully and works as desired. Then all is well.

- ▶ The device no longer responds after loading the new firmware. If an error occurs during the upload, the device automatically reactivates the previous firmware version and reboots the device.
- ▶ 'Login': To avoid problems with faulty uploads there is the second option with which the firmware is uploaded and also immediately booted.
  - ▶ In contrast to the first option, the device will wait for five minutes until it has successfully logged on. Only if this login attempt is successful does the new firmware remain active permanently.
  - ▶ If the device no longer responds and it is therefore impossible to log in, it automatically loads the previous firmware version and reboots the device with it.
- ▶ 'Manual': With the third option you can define a time period during which you want to test the new firmware yourself. The device will start with the new firmware and wait for the preset period until the loaded firmware is manually activated and therefore becomes permanently effective.

### 3.7.2 How to load new software

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

- ▶ LANconfig
- ▶ WEBconfig
- ▶ Terminal program
- ▶ TFTP



All settings will remain unchanged by a firmware upload. All the same you should save the configuration first for safety's sake (with **Edit ▶ Save Configuration to File** if using LANconfig, for example).

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

#### LANconfig



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

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

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

### WEBconfig

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

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

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

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

### TFTP

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

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

## 3.8 Command line interface

The LANCOM command line interface is always structured as follows:



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

### 3.8.1 Command line reference

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

Command	Description
cd <directory>	Change the current directory. Certain abbreviations exists, e.g. "cd ../.." can be abbreviated to "cd ..." etc.
del <name> rm <name>	Delete the table entry with the index <name>
dir [<directory>] 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' →page 26
writeconfig	Accept a new configuration in "readconfig" syntax. All subsequent lines are interpreted as configuration values until two blank lines in a row are encountered
writeflash	load new firmware via TFTP

- ▶ All commands and directory/item names may be abbreviated as long as no ambiguity exists. For example, it is valid to shorten the "sysinfo" command to "sys" or a "cd Management" to "c ma". Not allowed would be "cd /s", since that could mean either "cd /Setup" or "cd /Status".
- ▶ Names with blanks in them must be enclosed in double quotes.
- ▶ Additionally, there is a command-specific help function available by calling functions with a question mark as the argument, i.e. entering "ping ?" displays the options for the built-in PING command.
- ▶ A complete listing of available commands for a particular device is available by entering '?' from the command line.

## 3.9 Scheduled Events

### Regular Execution of Commands

This feature is intended to allow the device to execute predefined commands in a telnet-like environment, at times defined by the user. The functionality is equivalent to the UNIX **cron** service. Subject of execution can be any LANCOM command line command. Therefore, the full feature set of all LANCOM devices can be controlled by this facility.

Application examples include:

- ▶ scheduled connections
- ▶ time-dependant firewall rules

- ▶ regular firmware or configuration updates

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

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

Entry	Description
Index	Unambiguously identifies this entry in the table
Base	The <code>Base</code> field rules whether the time check is done against the device's operation time or the real time. Rules based on real time are only executed if the device has acquired the current time, e.g. via NTP. For real-time based rules, all four columns have a meaning, while operation-time based rules only take the minute/hour fields into account.
Minute Hour DayOfWeek Day Month	The entries <code>Minute</code> to <code>Month</code> form a mask that lets the user define at which times a command will be executed. Entries in the mask field may be blank to mark that the respective component shall not be part of the compare operation; otherwise, a field may contain a list of comma-separated items that may either be a single number or a number range, given as minimum and maximum concatenated with a hyphen. For the <code>DayOfWeek</code> field, the usual cron interpretation applies: 0 Sunday 1 Monday 2 Tuesday 3 Wednesday 4 Thursday 5 Friday 6 Saturday
Command	The command itself may be a list of command line commands, separated by semicolons.

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

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



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

## 4 Management

### 4.1 N:N mapping

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

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

In the first application the so-called N:1 NAT, also known as IP masquerading ('The hiding place—IP masquerading (NAT, PAT)' →page 74) is used. All addresses ("N") of the local network are mapped to only one ("1") public address. This clear assignment of data streams to the respective internal PCs is generally made available by the ports of the TCP and UDP protocols. That's why this is also called NAT/PAT (Network Address Translation/Port Address Translation).

Due to the dynamic assignment of ports, N:1 masquerading enables only those connections, which have been initiated by the internal network. Exception: an internal IP address is statically exposed on a certain port, e.g. to make a LAN server accessible from the outside. This process is called "inverse masquerading" ('Inverse masquerading' →page 78).

A N:N mapping is used for network couplings with identical address ranges. This transforms unambiguously multiple addresses ("N") of the local network to multiple ("N") addresses of another network. Thereby, an address conflict can be resolved.

Rules for this address translation are defined in a static table in the LANCOM. Thereby new addresses are assigned to single stations, parts of the network, or the entire LAN, by which the stations can contact other networks then.

Some protocols (FTP, H.323) exchange parameters during their protocol negotiation, which can have influence on the address translation for the N:N mapping. For a correct functioning of the address translation, the connection information of these protocols are tracked appropriately by functions of the firewall in a dynamic table, and are additionally considered to the entries of the static table.



The address translation is made "outbound", i.e. the source address is translated for outgoing data packets and the destination address for incoming data packets, as long as the addresses are located within

the defined translation range. An “inbound” address mapping, whereby the source address is translated (instead of the destination address), needs to be realized by an appropriate “outbound” address translation on the remote side.

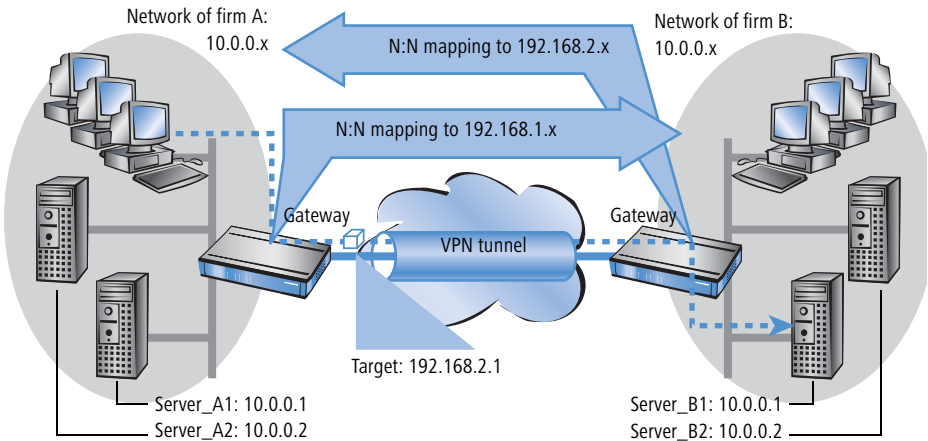
### 4.1.1 Application examples

The following typical applications are described in this section:

- ▶ Coupling of private networks utilizing the same address range
- ▶ Central remote monitoring by service providers

#### Network coupling

An often appearing scenario is the coupling of two company networks which internally use the same address range (e. g. 10.0.0.x). This is often the case, when one company should get access to one (or more) server(s) of the other one:

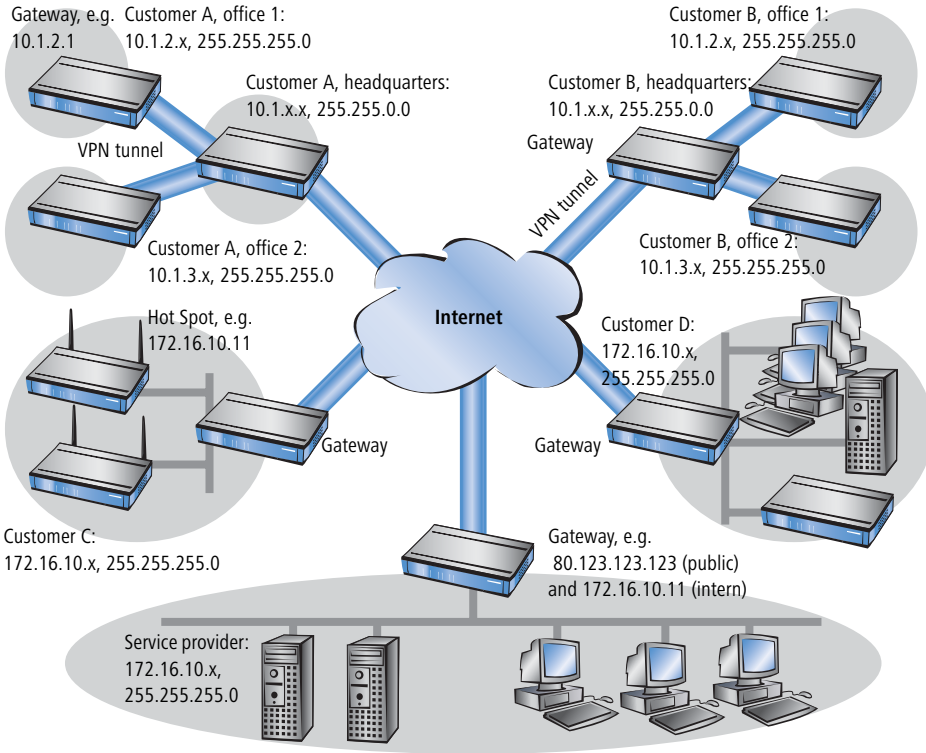


In this example network servers of company A and B should have access over a VPN tunnel to the respective other network. All stations of the LAN should have access to the server of the remote network. For the time being, there is no access possible to the other network, because both networks use the same address range. If one station of the network of company A wants to access server 1 of company B, the addressee (with an address from the 10.0.0.x network) will be searched within the own local network, and the inquiry even does not reach the gateway.

With the help of N:N mapping, all addresses of the LAN can be translated to a new address range for the coupling with the other network. The network of company A e. g. will be translated to 192.168.1.x, the network of company B to 192.168.2.x. Under these new addresses the two LANs are now reachable for the respective other network. The station from the network of company A is now addressing server 1 of company B under the address 192.168.2.1. The addressee does not reside anymore within the own network, the inquiry is now passed on to the gateway, and the routing to the other network is working as desired.

### **Remote monitoring and remote control of networks**

Remote maintenance and control of networks become more and more importance because of the possibilities given by VPN. With the use of the nearly ubiquitous broadband Internet connections, the administrator of such management scenarios is no longer dependent of the different data communication technologies or expensive leased lines.



In this example, a service provider monitors the networks of different clients out of a central control. For this purpose, the SNMP-capable devices should send the respective traps of important events automatically to the SNMP trap addressee (e. g. LANmonitor) of the network of the service provider. So the LAN administrator of the service provider has an up-to-date view of the state of the devices at any time.

The individual networks can be structured very differently: Clients A and B integrate their branches with own networks via VPN connections to their LAN, client C operates a network with several public WLAN base stations as hot spots, and client D has got an additional router for ISDN dial-up accesses in his LAN.





The networks of client A and B use different address ranges in the respective head office and the connected branches. A standard network coupling via VPN is therefore possible between these networks.

In order to avoid the effort to building up its own VPN tunnel to each individual subnetwork of the clients A and B, the service provider makes only one VPN connection to the head office, and uses the existing VPN lines between head office and branches for communication with the branches.

Traps from the networks report to the service provider whether e. g. a VPN tunnel has been build up or cut, if an user has been tried to log in three times with a wrong password, if an user has been applied for a hot spot, or if somewhere a LAN cable has been pulled out of a switch.



A complete list of all SNMP traps supported by LANCOM can be found in the appendix of this reference manual ('SNMP traps' →page 287).

Routing of these different networks reaches very fast its limiting factors, if two or more clients use same address ranges. Additionally, if some clients use the same address range as the service provider as well, further address conflicts are added. In this example, one of the hot spots of client C has got the same address as the gateway of the service provider.

There are two different variants to resolve these address conflicts:

- ▶ In the decentralized variant, alternative IP addresses for communicating with the SNMP addressee are assigned to each of the monitored devices by means of an 1:1 mapping. This address is in technical language also known as "loopback address", the method accordingly as "loopback method".

Loopback:  
decentralized  
1:1 mapping



The loopback addresses are valid only for communication with certain remote stations on the connections belonging to them. Thus a LANCOM is not generally accessible via this IP address.

- ▶ Even more appealing is the solution of a central mapping: instead of configuring each single gateway in the branch networks, the administrator configures solely one central address translation in the gateway of the head office. On this occasion, also all subnetworks located "behind" the head office are supplied with the needed new IP addresses.

Alternative:  
central  
N:N mapping

In this example, the administrator of the service provider selects 10.2.x.x as central address translation for the network of client B, so that both networks

with actual same address range looks like two different networks for the gateway of the service provider.

The administrator selects the address ranges 192.168.2.x and 192.168.3.x for client C and D, so that the addresses of these networks do differ from the own network of the service provider.

In order to enable the gateway of the provider to monitor the networks of clients C and D, the administrator sets up an address translation to 192.168.1.x also for the own network.

## 4.1.2 Configuration

### Setting up address translation

Configuration of N:N mapping succeeds with only few information. Since a LAN can be coupled with several other networks via N:N, different destinations can have also different address translations for a source IP range. The NAT table can contain 64 entries at maximum, including the following information:

- ▶ **Index:** Unambiguous index of the entry.
- ▶ **Source address:** IP address of the workstation or network that should get an alternative IP address.
- ▶ **Source mask:** Netmask of source range.
- ▶ **Remote station:** Name of the remote station over that the remote network is reachable.
- ▶ **New network address:** IP address or address range that should be used for the translation.

For the new network address, the same netmask will be used as the source address already uses. For assignment of source and mapping addresses the following hints apply:

- ▶ Source and mapping can be assigned arbitrarily for the translation of single addresses. Thus, for example, it is possible to assign the mapping address 192.168.1.88 to a LAN server with the IP address 10.1.1.99.
- ▶ For translation of entire address ranges, the station-related part of the IP address will be taken directly, only appended to the network-related part of the mapping address. Therefore, in an assignment of 10.0.0.0/255.255.255.0 to **192.168.1.0**, a server of the LAN with IP address 10.1.1.99 will get assigned the mapping address 192.168.1.**99**.



The address range for translation must be at minimum as large as the source address range.



Please notice that the N:N mapping functions are only effective when the firewall has been activated. ('Firewall/QoS enabled' →page 121)!

### Additional configuration hints

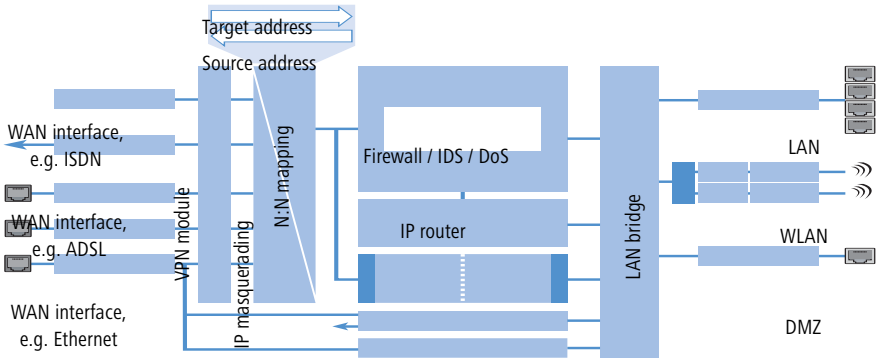
By setting up address translation in the NAT table, the networks and workstations become only visible under another address at first in the higher network compound. But for a seamless routing of data between the networks some further settings are still necessary:

- ▶ Entries in the routing tables for packets with new addresses to find the way to their destination.
- ▶ DNS forwarding entries, in order that inquiries about certain devices in the respective other networks can be resolved into mapped IP addresses ('DNS forwarding' →page 279).
- ▶ The firewall rules of the gateways must be adjusted such that (if necessary) authorized stations resp. networks from the outside are permitted to set up connections.
- ▶ VPN rules for loopback addresses in order to transmit the newly assigned IP addresses through an according VPN tunnel.



The IP address translation takes place in the LANCOM between firewall and IP router on one hand, and the VPN module on the other hand. All rules related to the own network use therefore the "unmap-

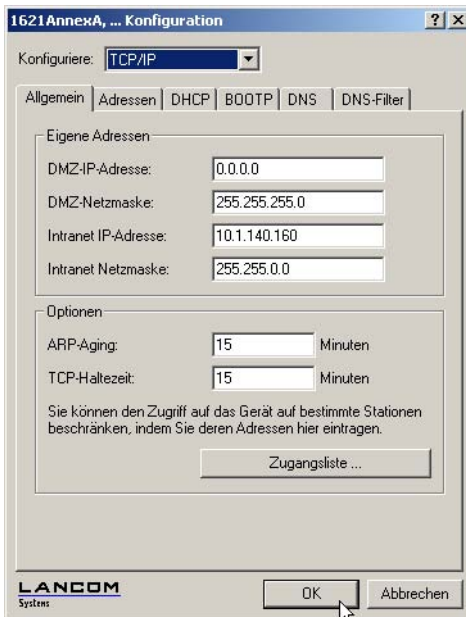
ped” original addresses. The entries of the remote network use the “mapped” addresses of the remote side, valid on the VPN connection.



### Configuration with different tools

LANconfig

With LANconfig you adjust the address translation for the configuration range 'IP router' on register card 'N:N-Mapping':



WEBconfig, Telnnet

Under WEBconfig and Telnnet you find the NAT table for configuration of N:N mapping at the following positions of the menu tree:

Configuration tool	Run
WEBconfig	Expert configuration / Setup / IP router / NAT table
Terminal/Telnnet	Setup / IP router module / NAT table

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

Expert Configuration

Setup

IP-router-module

**NAT-table**

Idx.

Src-Address

Src-Mask

Dst-Station

Mapped-Network

### 4.1.3

## 5 Diagnosis

### 5.1 LANmonitor—know what's happening

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

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

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

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



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

#### 5.1.1 Extended display options

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

- ▶ Error messages
- ▶ Diagnostic messages
- ▶ System information



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

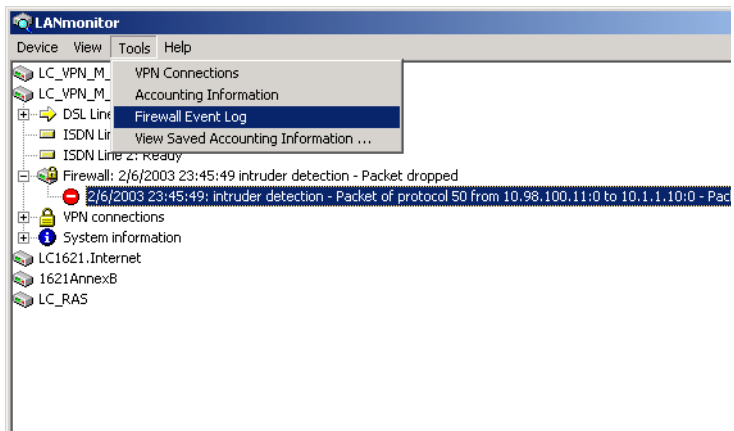
## 5.1.2 Monitor Internet connection

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

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

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

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



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

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

- ③ To break the connection manually, click on the active channel with the right mouse button. You may be required to enter a configuration password.
- ④ If you would like a log of the LANmonitor output in file form, select **Device ▶ Properties** and go to the 'Logging' tab. Enable logging and specify whether LANmonitor should create a log file daily, monthly, or on an ongoing basis.

## 5.2 Trace information—for advanced users

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



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

### 5.2.1 How to start a trace

Trace output can be started in a Telnet session, for example. The command to call up a trace follows this syntax:

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

The trace command, the code, the parameters and the combination commands are all separated from each other by spaces. And what is the meaning of these codes and parameters?



## 5.2.2 Overview of the keys

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

## 5.2.3 Overview of the parameters



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

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

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

## 5.2.4 Combination commands

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

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

## 5.2.5 Examples

This code...	... in combination with the trace causes the following:
trace	displays all protocols that can generate outputs during the configuration, and the status of each output (ON or OFF)
trace + all	switches on all trace outputs
trace + protocol display	switches on the output for all connection protocols together with the status and error messages
trace + all - icmp	switches on all trace outputs with the exception of the ICMP protocol
trace ppp	displays the status of the PPP
trace # ipx-rt display	toggles between the trace outputs for the IPX router and the display outputs
trace - time	switches off the system time output before the actual trace output

## 6 Security

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

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

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



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

- ▷ 'Firewall' →page 104
- ▷ 'The hiding place—IP masquerading (NAT, PAT)' →page 74
- ▷ 'Virtual LANs (VLANs)' →page 192

### 6.1 Protection for the configuration

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

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

#### 6.1.1 Password protection

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



As long as a password hasn't been set, anyone can change the configuration of the device. For example, your Internet account information could be stolen, or the device could be reconfigured in a way that the protection-mechanisms 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 '8"?#-\*+\_-;,!' 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 wiz-

ard **Security Settings**. In a terminal or Telnet session you set or change the password with the command `passwd`.

Configuration tool	Run
LANconfig	Management ▶ Security ▶ Configuration password
WEBconfig	Security settings
Terminal/Telnet	<code>passwd</code>

### Protecting the SNMP access

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

Configuration tool	Run
LANconfig	Management ▶ Security ▶ Password required for SNMP read permission
WEBconfig	Expert Configuration ▶ Setup ▶ SNMP-module ▶ Password-required-for-SNMP-read-access
Terminal/Telnet	<code>setup/SNMP module/password-required</code>

### 6.1.2 Login barring

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

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

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

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

- ▶ Lock configuration after (Login-errors)

- ▶ Lock configuration for (Lock-minutes)

Configuration tool	Run
LANconfig	Management ▶ Security
WEBconfig	Expert Configuration ▶ Setup ▶ Config-module
Terminal/Telnet	Setup/Config module

### 6.1.3 Restriction of the access rights on the configuration

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

- ▶ ISDN administrative account
- ▶ Network
  - ▷ LAN
  - ▷ WAN

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

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

#### Restrictions on the ISDN administrative account



This paragraph applies only to models with ISDN interface.

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

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

Enter alternatively the following instruction:

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



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



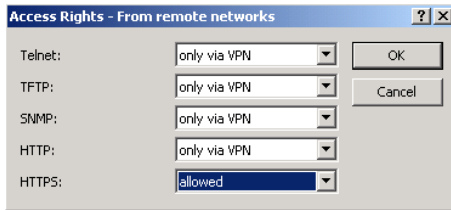
If you want to completely switch off the ISDN remote management, leave the field with Admin MSN empty.

### Limit the network configuration access

The access to the internal functions can be controlled separately for accesses from the local or from distant networks - for all configuration services sep-



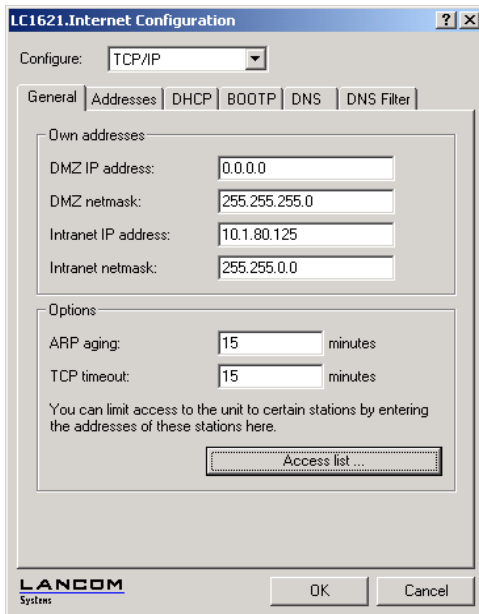
ately. The configuration access can generally be permitted or forbidden, a pure read access or - if your model is equipped with VPN - also can be permitted only over VPN.



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

### Restriction of the network configuration access to certain IP addresses

With a special filter list the access to the internal functions of the devices can be limited to certain IP addresses:



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

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

## 6.2 Protecting the ISDN connection

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

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

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

### 6.2.1 Identification control

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

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

Configuration Tool	Run
LANconfig	Communication ▶ Call accepting
WEBconfig	Expert Configuration ▶ Setup ▶ WAN-module ▶ Protect
Terminal/Telnet	setup/WAN-module/protect

You have a choice of the following:

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

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

### Verification of name and password

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

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

The PPP list can be found as follows:

Configuration tool	Run
LANconfig	Communication ▶ Protocols ▶ PPP list
WEBconfig	Expert Configuration ▶ Setup ▶ WAN-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).

## 6.2.2 Callback

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

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

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

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

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

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



Additional information on callback can be found in section 'Callback functions' →page 98.

## 6.3 The security checklist

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

### ▶ **Have you assigned a password for the configuration?**

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

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

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

### ▶ **Have you assigned a password to the SNMP configuration?**

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

### ▶ **Have you allowed remote access?**

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

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

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

▶ **Have you activated the Firewall?**

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

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

For maximum security and control you prevent at first any data transfer through the Firewall. Only those connections, which are explicitly desired have to be allowed by a dedicated Firewall rule then. Thus 'Trojans' and certain Email viruses lose their communication way back. The Firewall rules are summarized in LANconfig under 'Firewall/QoS' on the register card 'Rules'. A guidance can be found under 'Set-up of an explicit "Deny All" strategy' →page 138.

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

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

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

Access to the internal functions of the devices can be restricted using a special filter list. Internal functions in this case are configuration sessions via LANconfig, WEBconfig, Telnet or TFTP. This table is empty by default and so access to the router can therefore be obtained by TCP/IP using Telnet or TFTP from computers with any IP address. The filter is activated when the first IP address with its associated network mask is entered and from that point on only those IP addresses contained in this initial entry

will be permitted to use the internal functions. The circle of authorized users can be expanded by inputting further entries. The filter entries can describe both individual computers and whole networks. The access list can be found in LANconfig in the 'TCP/IP' configuration section on the 'General' tab.

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

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

## 7 Routing and WAN connections

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

### 7.1 General information on WAN connections

WAN connections are used for the following applications.

- ▶ Internet access
- ▶ LAN to LAN coupling
- ▶ Remote access

#### 7.1.1 Bridges for standard protocols

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

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

#### Close cooperation with router modules

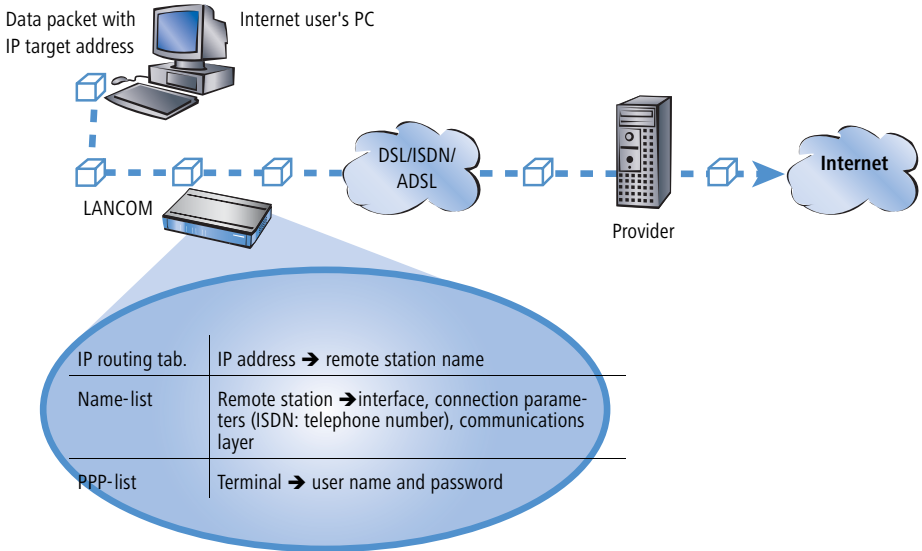
Characteristic of WAN connections is the close cooperation with the router modules in the LANCOM. The router modules (IP and IPX) take care of connecting LAN and WAN. They make use of the WAN modules to fulfil requests from PCs within the LAN for external resources.

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

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



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



- ① **Selecting the correct route**  
 A data packet from a computer initially finds the path to the Internet through the IP address of the receiver. The computer sends the packet with this address over the LAN to the router. The router determines the remote station in its IP routing table via which the target IP address can be reached, e.g. 'Provider\_A'.
- ② **Connection data for the remote station**  
 Using these names, the router checks the names list and finds the necessary connection data for provider A. Included in these connection data are, for instance, the WAN interface (DSL, ISDN) through which the provider is connected to, protocol information, or the necessary number for an ISDN call connection. The router also obtains the user name and password required for login from the PPP list.
- ③ **Establishing the WAN connection**  
 The router can then establish a connection to provider via a WAN interface. It authenticates itself with a user name and password.

#### ④ **Transmission of data packets**

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

## 7.2 IP routing

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

### 7.2.1 The IP routing table

The IP routing table is used to tell the router which remote station (which other router or computer) it should send the data for particular IP addresses or IP address ranges to. This type of entry is also known as a "route" since it is used to describe the path of the data packet. This procedure is also called "static routing" since you make these entries yourself and they remain unchanged until you either change or delete them yourself. Naturally, "dynamic routing" also exists. The routers use the routes in this way to exchange data between themselves and continually update it automatically. The static routing table can hold up to 256 entries, the dynamic table can hold 128. The IP router looks at both tables when the IP RIP is activated.

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

## Configuration of the routing table

Configuration tool	Run
LANconfig	IP router ▶ Routing ▶ Routing table
WEBconfig	Expert Configuration ▶ Setup ▶ IP-router-module ▶ IP-routing-table
Terminal/Telnet	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)' →page 74.

## 7.2.2 Local routing

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

### How can you assist the workstation computer now?

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

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

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

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

### 7.2.3 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 LANCAPI).
  - ▷ Y connections for the S<sub>0</sub> port have been explicitly excluded in the interface table.
  - ▷ The existing connection is using all B channels (channel bundling).
  - ▷ The existing connection is a leased-line connection. Only a few ISDN providers enable a dial-up connection to be established on the second B channel in addition to a permanent connection on the first B channel.

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

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

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

### What do the entries mean?

IP address and network mask identify the destination network, the distance shows the number of routers between the transmitter and receiver, the last

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

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

- ▶ The route is incorporated if it is not yet listed in the table (as long as there is enough space in the table).
- ▶ The route exists in the table with a time of '5' or '6'. The new route is then used if it indicates the same or a better distance.
- ▶ The route exists in the table with a time of '7' to '10' and thus has the distance '16'. The new route will always be used.
- ▶ The route exists in the table. The new route comes from the same router which notified this route, but has a worse distance than the previous entry. If a device notifies the degradation of its own static routing table in this way (e.g. releasing a connection increases the distance from 1 to 2, see below), the router will believe this and include the poorer entry in its dynamic table.



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

### The interaction of static and dynamic tables

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

### Routers without IP RIP support

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

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

### Scaling with IP RIP

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

### Configuration of IP-RIP function

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

- ▶ In the field 'RIP support' (or 'RIP type') the following selection is possible:
  - ▷ 'off': IP-RIP is not used (default).
  - ▷ 'RIP-1': RIP-1 and RIP-2 packets are received but only RIP-1 packets are sent.
  - ▷ 'RIP-1 compatible': RIP-1 and RIP-2 packets are received. RIP-2 packets are sent as an IP broadcast.
  - ▷ 'RIP-2': Similar to 'RIP-1 compatible', except that all RIP packets are sent to the IP multicast address 224.0.0.9.
- ▶ The entry under 'RIP-1 mask' (or 'R1 mask') can be set to the following values:
  - ▷ 'class' (default): The network mask used in the RIP packet is derived directly from the IP address class, i. e. the following network masks are used for the network classes:

Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0



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



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

#### 7.2.4 SYN/ACK speedup

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

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

The SYN/ACK speedup is activated at the factory.

#### Switching off in case of problems

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

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

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

## 7.3 The hiding place—IP masquerading (NAT, PAT)

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

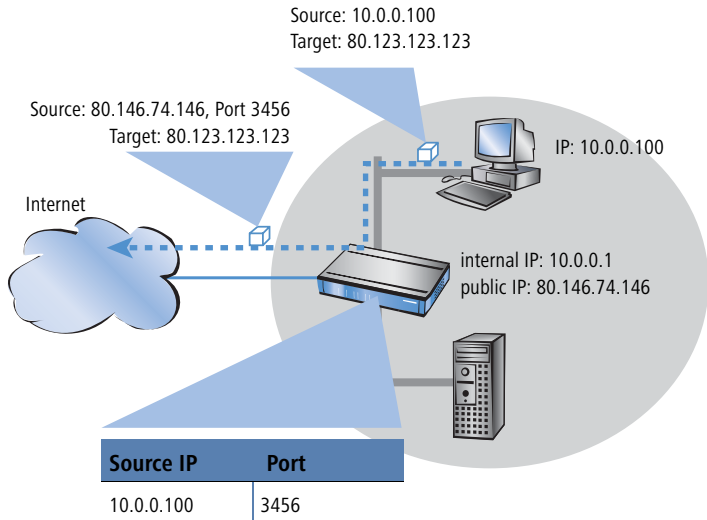
### 7.3.1 Simple masquerading

IP masquerading provides a hiding place for every computer while connected with the Internet. Only the router module of the LANCOM and its IP address are visible on the Internet. The IP address can be fixed or assigned dynamically by the provider. The computers in the LAN then use the router as a gateway so that they themselves cannot be detected. Thereby, the router separates Internet and Intranet.

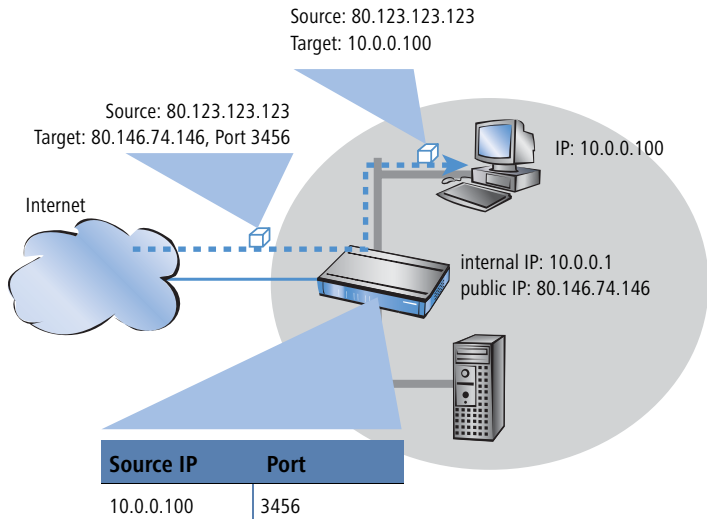
#### How does IP masquerading work?

Masquerading makes use of a characteristic of TCP/IP data transmission, which is to use port numbers for destination and source as well as the source and destination addresses. When the router receives a data packet for transfer it now notes the IP address and the sender's port in an internal table. It then gives the packet its unique IP address and a new port number, which could be

any number. It also enters this new port on the table and forwards the packet with the new information.



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



### Which protocols can be transmitted using IP masquerading?

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

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

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

### Configuration of IP masquerading

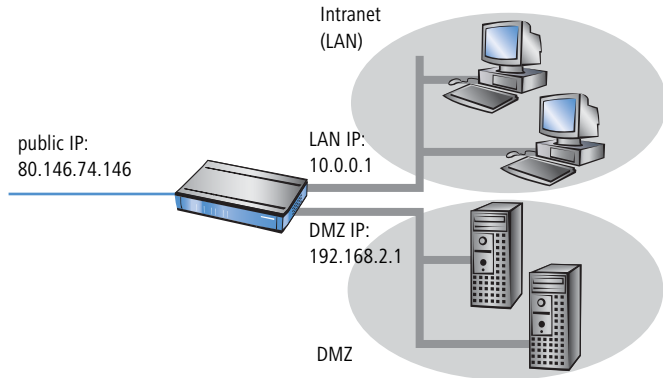
The use of IP masquerading is set individually for each route in the routing table. The routing table can be reached as follows:

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

### Multiple addresses for the router

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

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



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

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

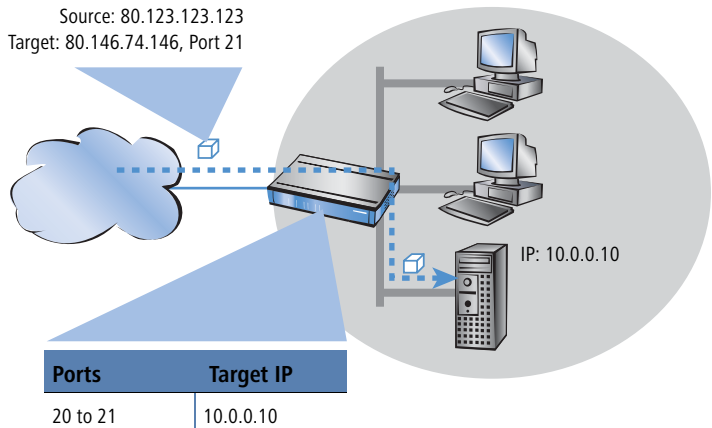
The **DMZ** and **Intranet** address assignment of the LANCOM can be entered at the following places:

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

### 7.3.2 Inverse masquerading

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

If, on the other hand, a computer sends a packet from the Internet to, for example, an FTP server on the LAN ('exposed host'), from the point of view of this computer the router appears to be the FTP server. The router reads the IP address of the FTP server in the LAN from the entry in the service table. The packet is forwarded to this computer. All packets that come from the FTP server in the LAN (answers from the server) are hidden behind the IP address of the router.



The only small difference is that:

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

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

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

## Configuration of the inverse masquerading

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

### Stateful Inspection and inverse masquerading

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

### 7.3.3 Unmasked Internet access for server in the DMZ

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

- ▶ The masquerading module must support and 'understand' the particular server service of the 'exposed host'. For instance, several VoIP servers use proprietary, non-standard ports for extended signalling. Thus such server could be used on unmasked connections solely.
- ▶ From a security point of view, it must be considered that the 'exposed host' resides within the LAN. When the host is under control of an attacker, it could be misused as a starting point for further attacks against machines in the local network.



In order to prevent attacks from a cracked server to the local network, some LANCOM provide a dedicated DMZ interface (LANCOM 7011 VPN) or are able to separate their LAN ports on Ethernet level by hardware (LANCOM 821 ADSL/ISDN and LANCOM 1621 ADSL/ISDN with the Switch set to 'Private Mode').

### Two local networks - operating servers in a DMZ

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

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

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

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

### Separation of Intranet and DMZ



Although Intranet and DMZ may be already separated on a Ethernet level by distinct interfaces, an appropriate Firewall rules must be set up in any case so that the DMZ is being separated from the LAN on the IP level as well.

Thereby, the server service shall be available from the Internet and from the Intranet, but any IP traffic from the DMZ towards the Intranet must be prohibited. For the above example, this reads as follows:

- ▶ With a 'Allow All' strategy (default): Deny access from 123.45.67.2 to "All stations in local network"
- ▶ With a 'Deny All' strategy (see 'Set-up of an explicit "Deny All" strategy' →page 138): Allow access from "All stations in local network" to 123.45.67.2

## 7.4 N:N mapping

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

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



In the first application the so-called N:1 NAT, also known as IP masquerading ('The hiding place—IP masquerading (NAT, PAT)' →page 74) is used. All addresses ("N") of the local network are mapped to only one ("1") public address. This clear assignment of data streams to the respective internal PCs is generally made available by the ports of the TCP and UDP protocols. That's why this is also called NAT/PAT (Network Address Translation/Port Address Translation).

Due to the dynamic assignment of ports, N:1 masquerading enables only those connections, which have been initiated by the internal network. Exception: an internal IP address is statically exposed on a certain port, e.g. to make a LAN server accessible from the outside. This process is called "inverse masquerading" ('Inverse masquerading' →page 78).

A N:N mapping is used for network couplings with identical address ranges. This transforms unambiguously multiple addresses ("N") of the local network to multiple ("N") addresses of another network. Thereby, an address conflict can be resolved.

Rules for this address translation are defined in a static table in the LANCOM. Thereby new addresses are assigned to single stations, parts of the network, or the entire LAN, by which the stations can contact other networks then.

Some protocols (FTP, H.323) exchange parameters during their protocol negotiation, which can have influence on the address translation for the N:N mapping. For a correct functioning of the address translation, the connection information of these protocols are tracked appropriately by functions of the firewall in a dynamic table, and are additionally considered to the entries of the static table.



The address translation is made "outbound", i.e. the source address is translated for outgoing data packets and the destination address for incoming data packets, as long as the addresses are located within the defined translation range. An "inbound" address mapping, whereby the source address is translated (instead of the destination address), needs to be realized by an appropriate "outbound" address translation on the remote side.

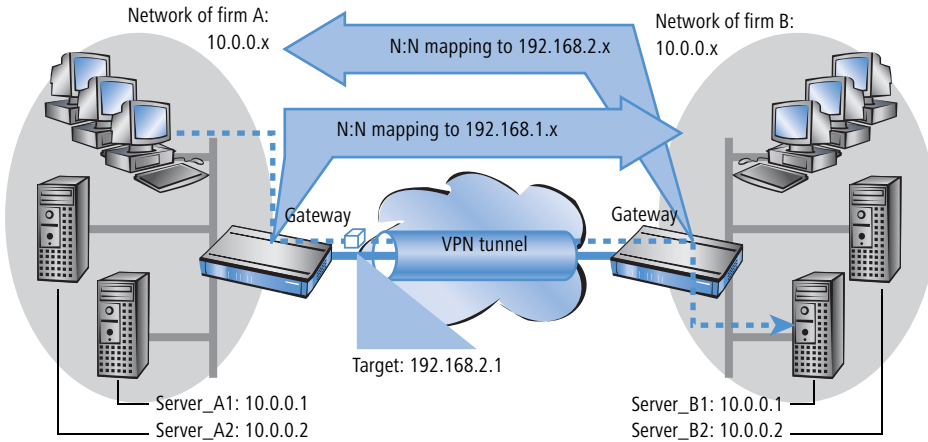
### 7.4.1 Application examples

The following typical applications are described in this section:

- ▶ Coupling of private networks utilizing the same address range
- ▶ Central remote monitoring by service providers

## Network coupling

An often appearing scenario is the coupling of two company networks which internally use the same address range (e. g. 10.0.0.x). This is often the case, when one company should get access to one (or more) server(s) of the other one:

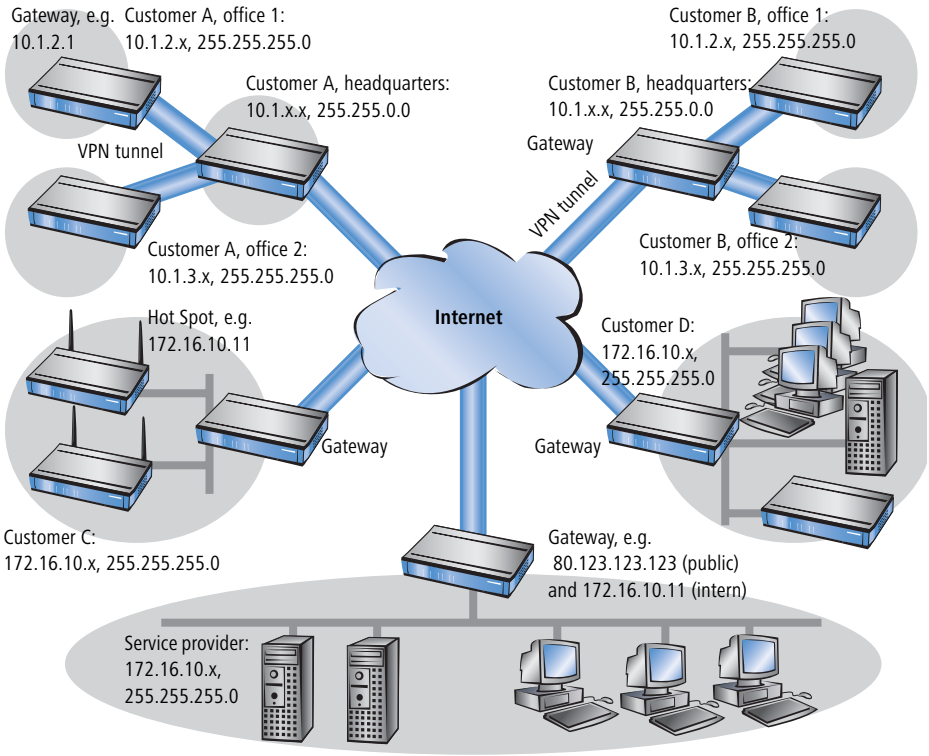


In this example network servers of company A and B should have access over a VPN tunnel to the respective other network. All stations of the LAN should have access to the server of the remote network. For the time being, there is no access possible to the other network, because both networks use the same address range. If one station of the network of company A wants to access server 1 of company B, the addressee (with an address from the 10.0.0.x network) will be searched within the own local network, and the inquiry even does not reach the gateway.

With the help of N:N mapping, all addresses of the LAN can be translated to a new address range for the coupling with the other network. The network of company A e. g. will be translated to 192.168.1.x, the network of company B to 192.168.2.x. Under these new addresses the two LANs are now reachable for the respective other network. The station from the network of company A is now addressing server 1 of company B under the address 192.168.2.1. The addressee does not reside any more within the own network, the inquiry is now passed on to the gateway, and the routing to the other network is working as desired.

### Remote monitoring and remote control of networks

Remote maintenance and control of networks become more and more importance because of the possibilities given by VPN. With the use of the nearly ubiquitous broadband Internet connections, the administrator of such management scenarios is no longer dependent of the different data communication technologies or expensive leased lines.



Routing and WAN connections

In this example, a service provider monitors the networks of different clients out of a central control. For this purpose, the SNMP-capable devices should send the respective traps of important events automatically to the SNMP trap addressee (e. g. LANmonitor) of the network of the service provider. So the LAN administrator of the service provider has an up-to-date view of the state of the devices at any time.

The individual networks can be structured very differently: Clients A and B integrate their branches with own networks via VPN connections to their LAN,

client C operates a network with several public WLAN base stations as hot spots, and client D has got an additional router for ISDN dial-up accesses in his LAN.



The networks of client A and B use different address ranges in the respective head office and the connected branches. A standard network coupling via VPN is therefore possible between these networks.

In order to avoid the effort to building up its own VPN tunnel to each individual subnetwork of the clients A and B, the service provider makes only one VPN connection to the head office, and uses the existing VPN lines between head office and branches for communication with the branches.

Traps from the networks report to the service provider whether e. g. a VPN tunnel has been build up or cut, if an user has been tried to log in three times with a wrong password, if an user has been applied for a hot spot, or if somewhere a LAN cable has been pulled out of a switch.



A complete list of all SNMP traps supported by LANCOM can be found in the appendix of this reference manual ('SNMP traps' →page 287).

Routing of these different networks reaches very fast its limiting factors, if two or more clients use same address ranges. Additionally, if some clients use the same address range as the service provider as well, further address conflicts are added. In this example, one of the hot spots of client C has got the same address as the gateway of the service provider.

There are two different variants to resolve these address conflicts:

- ▶ In the decentralized variant, alternative IP addresses for communicating with the SNMP addressee are assigned to each of the monitored devices by means of an 1:1 mapping. This address is in technical language also known as "loopback address", the method accordingly as "loopback method".



The loopback addresses are valid only for communication with certain remote stations on the connections belonging to them. Thus a LANCOM is not generally accessible via this IP address.

- ▶ Even more appealing is the solution of a central mapping: instead of configuring each single gateway in the branch networks, the administrator configures solely one central address translation in the gateway of the

Loopback:  
decentralized  
1:1 mapping

Alternative:  
central  
N:N mapping

head office. On this occasion, also all subnetworks located “behind” the head office are supplied with the needed new IP addresses.

In this example, the administrator of the service provider selects 10.2.x.x as central address translation for the network of client B, so that both networks with actual same address range looks like two different networks for the gateway of the service provider.

The administrator selects the address ranges 192.168.2.x and 192.168.3.x for client C and D, so that the addresses of these networks do differ from the own network of the service provider.

In order to enable the gateway of the provider to monitor the networks of clients C and D, the administrator sets up an address translation to 192.168.1.x also for the own network.

## 7.4.2 Configuration

### Setting up address translation

Configuration of N:N mapping succeeds with only few information. Since a LAN can be coupled with several other networks via N:N, different destinations can have also different address translations for a source IP range. The NAT table can contain 64 entries at maximum, including the following information:

- ▶ **Index:** Unambiguous index of the entry.
- ▶ **Source address:** IP address of the workstation or network that should get an alternative IP address.
- ▶ **Source mask:** Netmask of source range.
- ▶ **Remote station:** Name of the remote station over that the remote network is reachable.
- ▶ **New network address:** IP address or address range that should be used for the translation.

For the new network address, the same netmask will be used as the source address already uses. For assignment of source and mapping addresses the following hints apply:

- ▶ Source and mapping can be assigned arbitrarily for the translation of single addresses. Thus, for example, it is possible to assign the mapping address 192.168.1.88 to a LAN server with the IP address 10.1.1.99.
- ▶ For translation of entire address ranges, the station-related part of the IP address will be taken directly, only appended to the network-related part

of the mapping address. Therefore, in an assignment of 10.0.0.0/255.255.255.0 to **192.168.1.0**, a server of the LAN with IP address 10.1.1.99 will get assigned the mapping address 192.168.**1.99**.



The address range for translation must be at minimum as large as the source address range.



Please notice that the N:N mapping functions are only effective when the firewall has been activated. ('Firewall/QoS enabled' →page 121)!

### Additional configuration hints

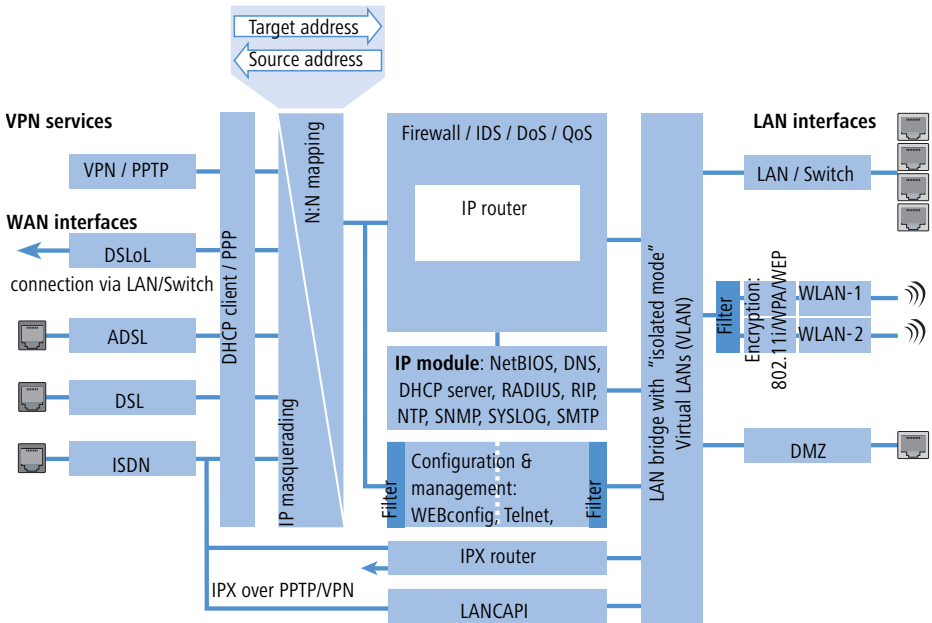
By setting up address translation in the NAT table, the networks and workstations become only visible under another address at first in the higher network compound. But for a seamless routing of data between the networks some further settings are still necessary:

- ▶ Entries in the routing tables for packets with new addresses to find the way to their destination.
- ▶ DNS forwarding entries, in order that inquiries about certain devices in the respective other networks can be resolved into mapped IP addresses ('DNS forwarding' →page 279).
- ▶ The firewall rules of the gateways must be adjusted such that (if necessary) authorized stations resp. networks from the outside are permitted to set up connections.
- ▶ VPN rules for loopback addresses in order to transmit the newly assigned IP addresses through an according VPN tunnel.



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

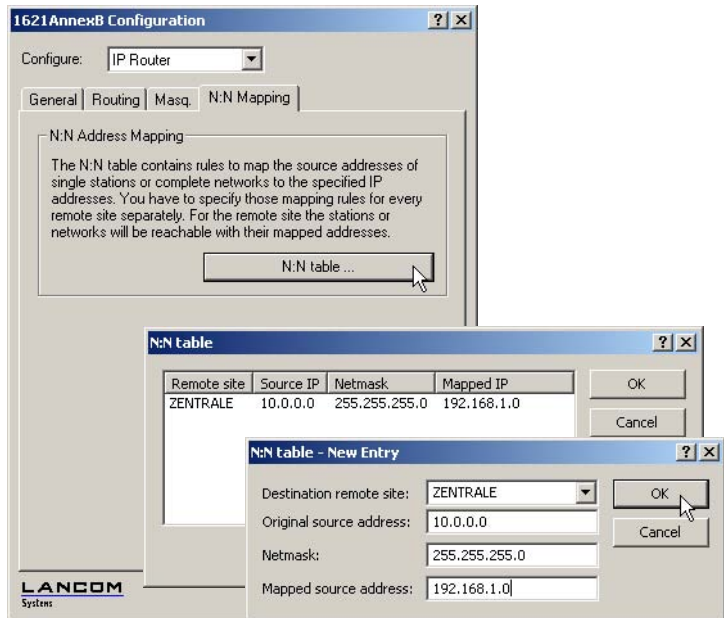
use the "mapped" addresses of the remote side, valid on the VPN connection.



## Configuration with different tools

LANconfig

With LANconfig you adjust the address translation for the configuration range 'IP router' on register card 'N:N-Mapping':



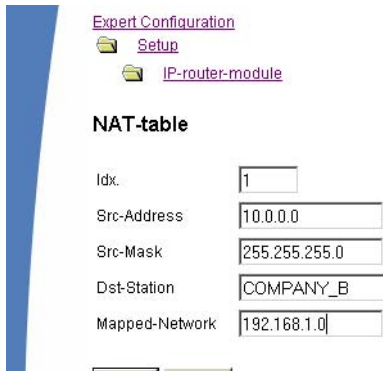
WEBconfig, Telnet

Under WEBconfig and Telnet you find the NAT table for configuration of N:N mapping at the following positions of the menu tree:

Configuration tool	Run
WEBconfig	Expert configuration / Setup / IP router / NAT table
Terminal/Telnet	Setup / IP router module / NAT table



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



## 7.5 Configuration of remote stations

Remote stations are configured in two tables:

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



The configuration of the authentication (protocol, user name, password) is not covered in this section. Information on authentication is contained in the section 'Establishing connection with PPP' →page 91.

### 7.5.1 Name list

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

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

## 7.5.2 Layer list

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

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

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



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

Parameter	Meaning	
Layer name	The layer is selected in the name list under this name.	
Encapsulation	Additional encapsulations can be set for data packets.	
	'Transparent'	No additional encapsulations.
	'Ethernet'	Encapsulation in the form of ethernet frames.
	'LLC-MUX'	Multiplexing via ATM with LLC/SNAP encapsulation according to RFC 2684. Several protocols can be transmitted over the same VC (Virtual Channel).
'VC-MUX'	Multiplexing with ATM by establishing additional VCs according to RFC 2684.	

Parameter	Meaning	
Layer-3	The following options are available for the switching layer or network layer:	
	'Transparent'	No additional header is inserted.
	'PPP'	The connection is established according to the PPP protocol (in the synchronous mode, i.e. bit-oriented). The configuration data are taken from the PPP table.
	'AsyncPPP'	Like 'PPP', only the asynchronous mode is used. This means that PPP functions character-oriented.
	'... with script'	All options can be run with their own script if desired. The script is specified in the script list.
	'DHCP'	Assignment of the network parameters via DHCP.
Layer-2	In this field the upper section of the security layer (Data Link Layer) is configured. The following options are available:	
	'Transparent'	No additional header is inserted.
	'PPPoE'	Encapsulation of the PPP protocol information in ethernet frames.
	'PPPoE'	The PPP negotiation runs via Ethernet. The PPP packets are encapsulated in Ethernet frames for this purpose. This process is frequently used for DSL connections.
Options	Here you can activate the compression of the data to be transmitted and the bundling of channels. The selected option only becomes active when it is supported by both the ports used and the selected Layer-2 and Layer-3 protocols. For further information see section 'Channel bundling with MLPPP' →page 101.	
Layer-1	In this field the lower section of the security layer (Data Link Layer) is configured. The following options are available:	
	'AAL-5'	ATM adaptation layer
	'ETH-10'	Transparent Ethernet as per IEEE 802.3.
	'HDLC'	Securing and synchronization of the data transfer as per HDLC (in the 7 or 8-bit mode).
	'V.110'	Transmission as per V.110 with a maximum of 38,400 bps.
	Modem	Modem transmission (requires Fax Modem option)

## 7.6 Establishing connection with PPP

LANCOM routers also support the point-to-point protocol (PPP). PPP is a generic term for a whole series of WAN protocols which enable the interaction

of routers made by different manufacturers since this protocol is supported by practically all manufacturers.

Due to the increasing importance of this protocol family and the fact that PPP is not associated with any specific operating mode of the routers, we will be introducing the functions of the devices associated with the PPP here in a separate section.

## 7.6.1 The protocol

### What is PPP?

The point-to-point protocol was developed specifically for network connections via serial channels and has asserted itself as the standard for connections between routers. It implements the following functions:

- ▶ Password protection according to PAP, CHAP or MS CHAP
- ▶ Callback functions
- ▶ Negotiation of the network protocol to be used over the connection established (IP or IPX, for example). Included in this are any parameters necessary for these protocols, for example IP addresses. This process is carried out using IPCP (IP Control Protocol).
- ▶ Verification of the connection through the LCP (Link Control Protocol)
- ▶ Combining several ISDN channels (MultiLink PPP)

PPP is the standard used by router connections for communication between devices or the WAN connection software of different manufacturers. Connection parameters are negotiated and a common denominator is agreed using standardized control protocols (e.g. LCP, IPCP, CCP) which are contained in PPP, in order to ensure successful data transfer where possible.

### What is PPP used for?

It is best to use the point-to-point protocol in the following applications:

- ▶ for reasons of compatibility when communicating with external routers, for example
- ▶ remote access from remote workstations with ISDN cards
- ▶ Internet access (when sending addresses)

The PPP which is implemented by LANCOM can be used synchronously or asynchronously not only via a transparent HDLC connection, but also via an X.75 connection.

### The phases of PPP negotiation

Establishment of a connection using PPP always begins with a negotiation of the parameters to be used for the connection. This negotiation is carried out in four phases which should be understood for the sake of configuration and troubleshooting.

▶ Establish phase

Once a connection has been made at the data communication level, negotiation of the connection parameters begins through the LCP.

This ascertains whether the remote site is also ready to use PPP, and the packet sizes and authentication protocol (PAP, CHAP, MS-CHAP or none) are determined. The LCP then switches to the opened state.

▶ Authenticate phase

Passwords will then be exchanged, if necessary. The password will only be sent once if PAP is being used for the authentication process. An encrypted password will be sent periodically at adjustable intervals if CHAP or MS CHAP is being used.

Perhaps a callback is also negotiated in this phase via CBCP (Callback Control Protocol).

▶ Network phase

LANCOM, supports the protocols IPCP and IPXCP.

After the password has been successfully transmitted, the IPCP and/or IPXCP network layer can be established.

IP and/or IPS packets can be transferred from the router modules to the opened line if the negotiation of parameters is successful for at least one of the network layers.

▶ Terminate phase

In the final phase the line is cleared, when the logical connections for all protocols are cleared.

### PPP negotiation in the LANCOM

The progress of a PPP negotiation is logged in the devices' PPP statistics and the protocol packets listed in detail there can be used for checking purposes in the event of an error.

The PPP trace outputs offer a further method of analysis. You can use the command

```
trace + ppp
```

to begin output of the PPP protocol frames exchanged during a terminal session. You can perform a detailed analysis once the connection has been broken if this terminal session has been logged in a log file.

## 7.6.2 Everything o.k.? Checking the line with LCP

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

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

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



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



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

## 7.6.3 Assignment of IP addresses via PPP

In order to connect computers using TCP/IP as the network protocol, all participating computers require a valid and unique IP address. If a remote station does not have its own IP address (such as the individual workstation of a

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

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



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

### Examples

#### ▶ Remote access

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

In addition to the IP address, the addresses of the DNS and NBNS servers (Domain Name Server and NetBIOS Name Server) including the backup server from the entries in the TCP/IP module are transmitted to the remote station during this configuration.

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

#### ▶ Internet access

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

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

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

## 7.6.4 Settings in the PPP list

You can specify a custom definition of the PPP negotiation for each of the remote sites that contact your net.

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

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

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



In this column of the PPP list...	...enter the following values:
Time	Time between two checks of the connection with LCP (see the following section). This is specified in multiples of 10 seconds (i.e. 2 for 20 seconds, for instance). The value is simultaneously the time between two verifications of the connection to CHAP. Enter this time in minutes. The time must be set to '0' for remote sites using a Windows operating system.
Retr.	Number of retries for the check attempt. You can eliminate the effect of short-term line interference by selecting multiple retries. The connection will only be dropped if all attempts are unsuccessful. The time interval between two retries is 1/10 of the time interval between two checks. Simultaneously the number of the "Configure requests" that the router maximum sends before it assumes a line error and clears the connection itself.
Conf, Fail, Term	These parameters are used to affect the way in which PPP is implemented. The parameters are defined in RFC 1661 and are not described in greater detail here. You will find troubleshooting instructions in this RFC in connection with the router's PPP statistics if you are unable to establish any PPP connections. The default settings should generally suffice. These parameters can only be modified via LANconfig, SNMP or TFTP!

## 7.7 Extended connection for flat rates—Keep-alive

The term flat rate is used to refer to all-inclusive connection rates that are not billed according to connection times, but instead as a flat fee for fixed periods. With flat rates, there is no longer any reason to disconnect. On the contrary: New e-mails should be reported directly to the PC, the home workplace is to be continuously connected to the company network and users want to be able to reach friends and colleagues via Internet messenger services (ICQ etc.) without interruption. This means it is desirable to continuously maintain connections.

With the LANCOM the Keep-alive function ensures that connections are always established when the remote station has disconnected them.

### Configuration of Keep-alive function

The keep alive procedure is configured in the name list.

If the holding time is set to 0 seconds, a connection is not actively disconnected by the LANCOM. The automatic disconnection of connections over which no data has been transmitted for a longer time is deactivated with a

holding time of 0 seconds then. However, connections interrupted by the remote site are not automatically re-established with this setting.

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

## 7.8 Callback functions

The LANCOM supports automatic callback via its ISDN port.

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

### 7.8.1 Callback for Microsoft CBCP

With Microsoft CBCP, the callback number can be determined in various ways.

- ▶ The party called does not call back.
- ▶ The party called allows the caller to specify the callback number itself.
- ▶ The party called knows the callback numbers and **only** calls these back.

Via CBCP, it is possible to establish connection to the LANCOM from a PC with Windows operating system and also to be called back by this PC. Three possible settings are selected in the name list via the callback entry as well as the calling number entry.

**Name list (ISDN) - New Entry**

Name: MAIN

Phonenumber:

Short hold time: 20 seconds

Short hold time (bundle): 20 seconds

Layer name: PPPHDLC

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

OK Cancel

### 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

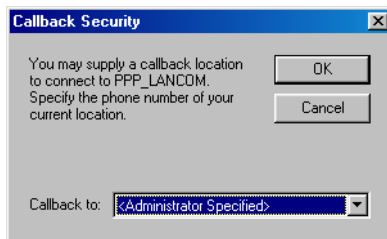
For this setting the callback entry must be set to 'Call back the remote site after name verification' (or must have the value 'Name' in WEBconfig or in the console). In the name list **no** telephone number may be specified.

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.

## 7.8.2 Fast callback using the LANCOM process

This fast, LANCOM-specific process is ideal if two LANCOM are to communicate with one another via callback.

- ▶ The caller who may wish to be called back can activate the function 'Wait for callback from remote site' in the name list (or 'Looser' when configuring via WEBconfig, terminal program or Telnet).

- ▶ 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.

### 7.8.3 Callback with RFC 1570 (PPP LCP extensions)

The callback as per 1570 is the standard method for calling back routers of other manufacturers. This protocol extension describes five possibilities for requesting a callback. All versions are recognized by LANCOM. All versions will be processed in the same way, however:

The LANCOM drops the connection after authenticating the remote station and then calls back the station a few seconds later.

#### Configuration

For callback as per PPP you select the option 'Call back the remote site' in LANconfig or 'Auto' with configuration via WEBconfig, terminal program or Telnet.



For callback as per PPP the number list for answering calls in the LANCOM must be up to date.

### 7.8.4 Overview of configuration of callback function

The following options are available in the name list under WEBconfig and terminal program/telnet for the callback function:

With this entry ...	... you set up the callback in this manner:
'Off'	No callback occurs.
'Auto' (not for Windows operating systems, see below)	The remote station will be called back if so specified in the name list. At first, the call is denied and as soon as the channel is clear again, it is called back (duration is approx. 8 seconds). If the remote station is not found in the numerical list, it is first accepted as the DEFAULT remote station, and the callback is negotiated during the protocol negotiation. A charge of one unit is incurred for this.

With this entry ...	... you set up the callback in this manner:
'Name'	Before a callback occurs, a protocol negotiation is always carried out even when the remote station was found in the numerical list (e.g. for computers with Windows having direct dialing on the device). Here only minor charges result.
'LANCOM'	When the remote station is found in the numerical list, a quick callback is carried out, i.e., the LANCOM sends a special signal to the remote station and calls back immediately when the channel is clear again. After approx. 2 seconds, the connection is established. If the remote station does not take back the call immediately after the signal, then after two seconds the situation reverts back to normal callback procedures (duration is once again approx. 8 seconds). This process is only available for DSS1 connections.
'Looser'	Use the 'Looser' option when a callback is expected from the remote station. This setting carries out two functions simultaneously. On the one hand, it ensures that a custom connection setup is taken back when there is an incoming call from the called remote station, and on the other hand, the function is activated with this setting to be able to react to the rapid callback procedure. In other words, in order to be able to use rapid callback, the caller must be in the 'Looser' mode while the party being called must discontinue callback with 'LANCOM'.



The setting 'Name' offers the greatest security when an entry is made into the number list as well as the PPP list. The setting 'LANCOM' offers the fastest callback method between two LANCOM routers.



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

## 7.9 Channel bundling with MLPPP

When establishing an ISDN connection to a remote station with PPP capability, you can transmit data more quickly. Data can be compressed and/or several B channels can be used for data transmission (channel bundling).

Connecting with cable bundling is distinguished from "normal" connections in that not only one, but rather several B channels are used parallel for data transmission.

MLPPP (**M**ultilink **PPP**) is used for channel bundling. This procedure is of course only available when PPP is used as the B-channel protocol. MLPPP is used e.g. for Internet access via Internet provider, which also operate remote stations with MLPPP capability from your direct dialing nodes.

## Two methods of channel bundling

### ▶ Static channel bundling

If a connection is established with static channel bundling, the LANCOM tries to establish the second B channel immediately after setting up the first B channel. If this does not work because, for example, this channel is already taken by another device or a different connection within the LANCOM, the connection attempt is automatically and regularly repeated until the second channel is available for it.

### ▶ Dynamic channel bundling

In the case of a connection with dynamic channel bundling, the LANCOM first only establishes one B channel and begins transmitting data. If, during this connection, it determines that the throughput rate lies above a certain threshold value, it tries to add the second channel.

If the second channel is established and the data throughput rate drops below the threshold value, the LANCOM waits for the set B2 timeout period and then automatically closes the channel again. In this way, the per minute charges are fully utilized so long as rate information is communicated during the connection. Therefore, the LANCOM only uses the second B channel if and as long as it really needs it.

## Here's how to configure your system to combine channels

The configuration of channel bundling for a connection is made up of three settings.

- ① Select a communication layer for the remote station from the layer list that has bundling activated in the Layer-2 options. Select from the following Layer-2 options:
  - ▶ **compr.** according to the LZS data compression procedure (Stac) reduces the amount of data if the data hasn't already been compressed. This procedure is also supported by routers of other manufacturers and by ISDN adapters under Windows operating systems.
  - ▶ **bundle** uses two B channels per connection.
  - ▶ **bnd+compr** uses both (compression and channel bundling) and provides the maximum possible data transmission performance.
- ② Now create a new entry in the name list. When doing so, watch the holding times for the connection. Please observe the following rules:

- ▶ Depending on the type of application, the B1 hold time should be increased to such a level so that the connection is not dropped prematurely because of packets not being transmitted for a short time. Experience has shown that values between 60 and 180 seconds are a good basis which can be adapted as required during operation.
  - ▶ The B2 holding time determines whether static or dynamic channel bundling will be used (see above). A B2 holding time of '0' or '9999' ensures that the bundling will be static; values in between permit dynamic channel bundling. The B2 holding time defines how long the data throughput may lie below the threshold for dynamic channel bundling without the second B channel automatically being disconnected.
- ③ Use the entry for the Y connection in the Router interface list to determine what should happen if a second connection to a different remote station is requested during an existing connection using channel bundling.

WEBconfig	Expert Configuration ▶ Setup ▶ WAN-module ▶ Router-interface-list
Terminal/Telnet	cd /setup/WAN-module set router-interface-list [...]

- ▶ Y connection **On**: The router interrupts the bundled connection to establish a connection to the other remote station. When the second channel is free again, the originally bundled connection automatically 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.

## 8 Firewall

For most companies and many private users a work without the Internet is no longer conceivable. E-mail and web are indispensable for communication and information search. But each connection of the workstations from the own, local network to the Internet represents however a potential danger: Unauthorized users can try to see your data via this Internet connection, to modify it or to manipulate your PCs.

Therefore this chapter covers an important topic: the firewall as defensive measure against unauthorized access. Besides a brief introduction to the topic of Internet security, we show you which protection a LANCOM is able to offer you by right configuration and how to make the needed specific settings.

### 8.1 Threat analysis

To plan and to realize suitable measures to guarantee security, it is advisable to know first all possible sources of danger:

- ▶ Which imminent dangers exist for the own LAN resp. the own data?
- ▶ Which are the ways intruders take for the access to your network?



We denote the intrusion into protected networks in the following as “attack” according to the general usage, and the intruder thus as “attacker”.

#### 8.1.1 The dangers

The dangers in the Internet arise in principle from completely different motives. On the one hand the perpetrators try to enrich themselves personally or to damage the victims systematically. By the ever increasing know-how of the perpetrators, the “hacking” became already a kind of sports, in which young people often measure who takes at first the hurdles of Internet security. Regardless of the individual motivation, the intention of the perpetrators mostly leads to the following aims:

- ▶ Inspect confidential information such as trade secrets, access information, passwords for bank accounts etc.
- ▶ Use of LAN workstations for purposes of the attackers, e. g. for the distribution of own contents, attacks to third workstations etc.
- ▶ Modify data of LAN workstations, e. g. to obtain even further ways for access.



- ▶ Destroy data on the workstations of the LAN.
- ▶ Paralyse workstations of the LAN or the connection to the Internet.



We restrict ourselves in this section to the attacks of local networks (LAN) resp. to workstations and servers in such LANs.

### 8.1.2 The ways of the perpetrators

In order to undertake their objectives, the perpetrators need at first a way to access your PCs and data. In principle, the following ways are open as long as they are neither blocked nor protected:

- ▶ Via the central Internet connection, e. g. via routers.
- ▶ Via decentral connections to the Internet, e. g. modems of single PCs or mobile phones on notebooks.
- ▶ Via wireless networks operating as a supplement to wired networks.



In this chapter we only deal with the ways via the central Internet connection, via the router.



For hints on the protection of wireless networks, please refer to the respective chapters of this reference manual resp. of the appropriate device documentation.

### 8.1.3 The methods

Normally strangers have of course no access to your local area network or to the workstations belonging to it. Without the appropriate access data or passwords nobody can thus access the protected area. If spying out of these access data is not possible, the attackers will try another way to achieve their goals.

A fundamental starting point is to smuggle data on one of the allowed ways for data exchange into the network, which opens from the inside the access for the attacker. Small programs can be transferred on a computer by appendices in e-mails or active contents on web pages, e.g., in order to lead afterwards to a crash. The program uses the crash to install a new administrator on the computer, which can then be used from distance for further actions in the LAN.

If the access via e-mail or www is not possible, the attacker can also look out for certain services of servers in the LAN, which are useful for his purposes. Because services of the servers are identified over certain ports of the TCP/IP

protocol, the search for open ports is also called "port scanning". On the occasion, the attacker starts an inquiry for particular services with a certain program, either generally from the Internet, or, only on certain networks and unprotected workstations, which in turn will give the according answer.

A third possibility is to access an existing data connection and use it as a free-rider. The attacker observes here the Internet connection of the victim and analyses the connections. Then he uses e. g. an active FTP connection to smuggle his own data packets into the protected LAN.

A variant of this method is the "man-in-the-middle" attack. The attacker observes here first the communication of two workstations, and gets then in between.

#### 8.1.4 The victims

The question about the degree of exposure for an attack influences to a considerable degree the expenditure one wants to or must meet for defending. In order to assess whether your network would be particularly interesting for an attacker as a potential victim, you can consult the following criteria:

- ▶ Particularly endangered are networks of common known enterprises or institutions, where valuable information is suspected. Such information would be e.g. the results of research departments, which are gladly seen by industrial spies. Or, on the other hand, bank servers, on which big money is distributed.
- ▶ Secondly, also networks of smaller organisations are endangered, which perhaps are only interesting to special groups. On the workstations of tax consultants, lawyers or doctors do slumber certainly some information quite interesting for third persons.
- ▶ Last but not least also workstations and networks are victims of attackers, which obviously offers no use for the attackers. Just the "script kiddies" testing out their possibilities by youthful ambition are sometimes just searching for defenceless victims in order to practise for higher tasks.

The attack against an unprotected, apparently not interesting workstation of a private person can also serve the purpose to prepare a basis for further attacks against the real destination in a second step. The workstation of "no interest" becomes source of attacks in a second step, and he attacker can disguise his identity.

All things considered, we can resume that the statistical probability for an attack to the network of a global player of the industry may be higher than to a midget network of the home office. But probably it is only a matter of time

that a defenceless workstation installed in the Internet will - perhaps even accidentally - become the victim of attacks.

## 8.2 What is a Firewall?

The term "Firewall" is interpreted very differently. We want to define at this point the meaning of "Firewall" within the boundaries of this reference manual:

A Firewall is a compilation of components, which monitors at a central place the data exchange between two networks. Mostly the Firewall monitors the data exchange between an internal, local network (LAN), and an external network like the Internet.

The Firewall can consist of hard and/or software components:

- ▶ In pure hardware systems the Firewall software often runs on a proprietary operating system.
- ▶ The Firewall software can also run on a conventional workstation, which is dedicated to this task under Linux, Unix or Windows.
- ▶ As a third and frequently used alternative, the Firewall software runs directly within the router, which connects the LAN to the Internet.

In the following sections we only look at the Firewall in a router.



The functions "Intrusion Detection" and "DoS protection" are part of the content of a Firewall in some applications. The LANCOM contains these functions also, but they are realised as separate modules beside the Firewall.

Further information can be found in the section 'Protection against break-in attempts: Intrusion Detection' →page 160 and 'Protection against "Denial of Service" attacks' →page 162.

### 8.2.1 Tasks of a Firewall

#### Checking data packets

How does the Firewall supervises the data traffic? The Firewall works in principle like a door keeper for data packets: Each packet will be checked, whether it may pass the door of the network (Firewall) in the desired direction or not. For such a checking different criteria are used, in common language of Firewalls called "rules" or "guidelines". Depending on the kind of information,

which are used for creation of the rules and which are checked during the operation of the Firewall, one distinguishes different types of Firewalls.

Above all, the aspect of the “central” positioning is very important: Only when the entire data traffic between “inside” and “outside” goes through the Firewall, it can fulfil its task reliably under any circumstances. Each alternative way can reduce or even turn off the security of the Firewall. This central position of the Firewall simplifies by the way also the maintenance: One Firewall as common passage between two networks is certainly easier to maintain than a “Personal Firewall” on each of the workstations belonging to the LAN.



In principle, Firewalls operate at the interconnection between two or more networks. For the following explanation, we only look as example at the passage between a local network of a company and the Internet. These explanations can be transferred however in a general manner also to other network constellations, e.g. for the protection of a subnetwork of the personnel department of a company against the remaining network users.

### Logging and alerting

An important function of the Firewall is beside the checking of data packets and the right reaction to the results of this checking also the logging of all actions triggered by the Firewall. By analyzing these protocols, the administrator can draw conclusions from the occurred attacks and on the basis of this information he can, if necessary, go on to improve the configuration of the Firewall.

But sometimes, logging alone comes too late. Often, an immediate intervention of the administrator can prevent a major danger. That is why Firewalls have mostly an alerting function, by which the Firewall notifies the administrator e.g. by e-mail.

## 8.2.2 Different types of Firewalls

During the last years, the operating principles of Firewalls have more and more evolved. Under the generic term “Firewall”, a whole range of different technical concepts is offered to protect the LAN. Here we introduce the most important ones.

## Packet filters

One speaks about a packet filter-based Firewall, if the router only checks the details in the header of the data packets and decides on the basis of this information, whether the packet may pass or not. The following details belong to the analyzed information:

- ▶ IP address of source and destination
- ▶ Transfer protocol (TCP, UDP or ICMP)
- ▶ Port numbers of source and destination
- ▶ MAC address

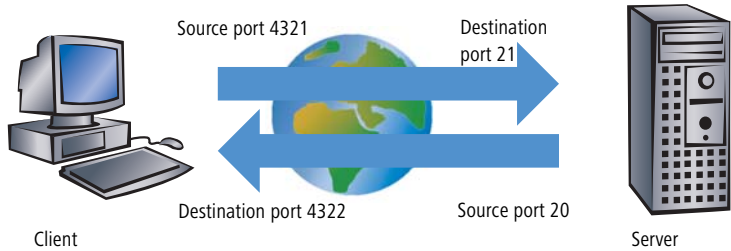
The rules defined in a packet filter-orientated Firewall determine e.g., whether the packets may pass on by a special IP address range into the local network, or whether packets should be filtered for special services (i.e. with special port numbers). By these measures, the communication with certain workstations, entire networks or via special services can be reduced or even prevented. Besides, the rules are combinable, so that e.g. only workstations with special IP addresses get access to the Internet via the TCP port 80, while this services remains blocked for all other workstations.

The configuration of packet filtering Firewalls is quite simple, and the list with the permitted or forbidden packets can be extended very easily. Because also the performance requirements of a packet filter can be address with quite little means, the packet filters are often directly implemented in routers, which operate as interface between the networks anyway.

An unfavourable effect on the packet filters is, that the list of rules becomes uncomfortable after a while. Besides, for some services the connection ports are negotiated dynamically. To enable communication then, the administrator has to leave open all possibly used ports, which is contrary to the basic orientation of most security concepts.

One example for a process, which is quite problematical for simple packet filters, is the establishing of a FTP connection from a workstation of the own LAN to a FTP server in the Internet. By the generally used active FTP, the client (of the protected LAN) sends an inquiry from a port of the upper range (>1023) to port 21 of the server. The client informs the server, over which port

it is expecting the connection. The server will establish as a result from its port 20 a connection to the desired port of the client.



To enable this process, the administrator of the packet filter must open all ports for incoming connections, because he does not know in advance for which port the client will inquire the FTP connection. An alternative is to use passive FTP. Thereby, the client establishes the connection itself to the server over a particular port, which was told to the server before. This process is, however, not supported by all clients/servers.

If we furthermore compare the Firewall with a porter, this door keeper only checks, whether he knows or not the courier with the packet at the door. If the courier is known and came ever into the building before, he has the permission to go in without hindrance and without being checked also for all following orders up to the workplace of the addressee.

### Stateful Packet Inspection

Stateful Packet Inspection (SPI), or briefly Stateful Inspection, enhances the packet filter approach by checking further connection state information. Beside the more static table with the permitted ports and address ranges, a dynamic table will be kept up in this variant, in which information about the connection state of the individual connections is held. This dynamic table enables to first block all endangered ports, and to selectively open only if required a port for a permitted connection (adjusted by source and destination address). The opening of ports is always made from the protected network to the unprotected one, that means mostly from LAN to WAN (Internet). Data

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

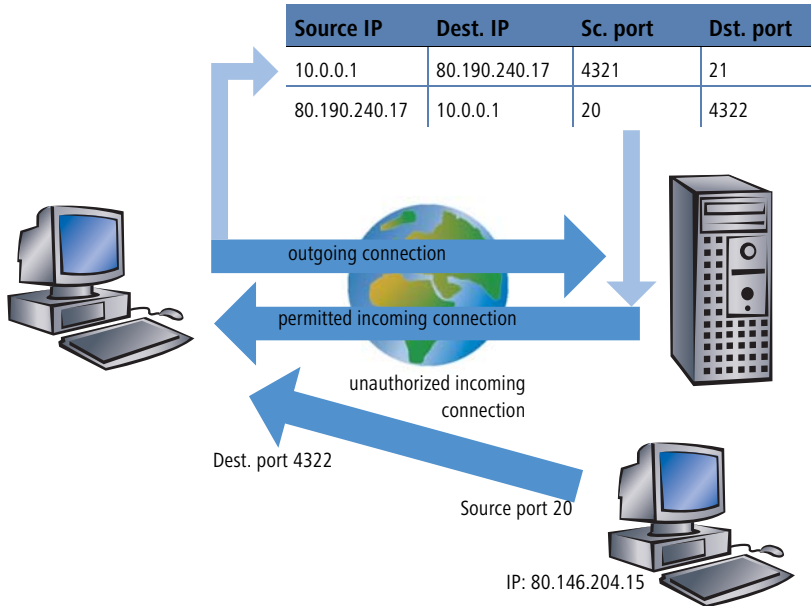
### **Stateful Inspection: direction-dependent checking**

The filter sets of a Stateful Inspection Firewall are - contrary to classical port filter Firewalls - dependent on their direction. Connections can only be established from source to their destination point. The other direction would require an explicit filter entry as well. Once a connection has been established, only the data packets belonging to this connection will be transmitted - in both directions, of course. So you can block in a reliable way all traffic not belonging to a known session, not coming from the local network.


Additionally, the Stateful Inspection is able to track from the connection set up, whether additional channels are negotiated for data exchange or not. Some protocols like e.g. FTP (for data transfer), T.120, H.225, H.245 and H.323 (for netmeeting or IP telephony), PPTP (for VPN tunnels) or IRC (for chatting) signalize when establishing the connection from the LAN to the Internet by a particular used source port whether they are negotiating further ports with the remote station. The Stateful Inspection dynamically adds also these additional ports into the connection state list, of course limited to the particular source and destination addresses only.

Let's have once again a look at the FTP download example. When starting the FTP session, the client establishes a connection from source port '4321' to the destination port '21' of the server. The Stateful Inspection allows this first set up, as long as FTP is allowed from local workstations to the outside. In the dynamic connection state table, the Firewall enters source and destination and the respective port. Simultaneously, the Stateful Inspection can inspect the control information, sent to port 21 of the server. These control signals indicate that the client requires a connection of the server from its port 20 to port 4322 of the client. The Firewall also enters these values into the dynamic

table, because the connection to the LAN has been initiated from the client. Afterwards, the server can send so the desired data to the client.



But if another workstation from the Internet tries to use the just opened port 4322 of the LAN to file itself data from its port 20 on the protected client, the Firewall will stop this try, because the IP address of the attacker does not fit to the permitted connection!

 After the successful data transfer, the entries disappear automatically from the dynamic table and the ports will be closed again.

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

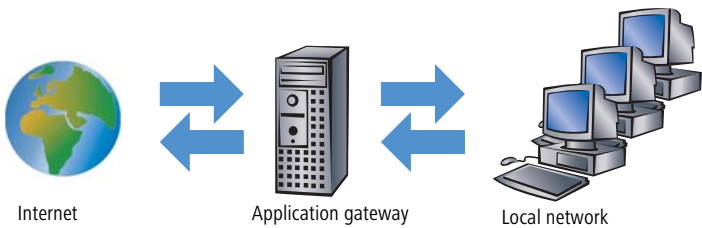
This porter is making a definite better job. When somebody in this company orders a courier, he must also inform the porter that he is expecting a courier, when he will be arriving and what information should be found on the delivery note. Only when this information matches the logbook entries of the porter, the courier may pass. If the courier brings not only one packet, but rather two,



only the one with the correct delivery note will pass. Likewise, a second courier demanding access to the employee will be rejected, too.

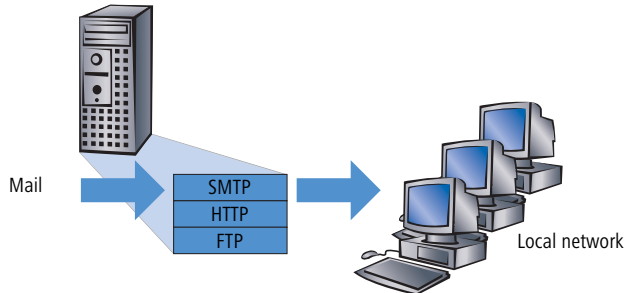
### Application Gateway

By checking of contents on application level, Application Gateways increase the address checking of the packet filters and the connection monitoring of the Stateful Packet Inspection. The Application Gateway runs mostly on a separate workstation, because of the high demands to the hardware performance. This workstation is between the local network and the Internet. Seen from both directions, this workstation is the only possibility to exchange data with the respective other network. There doesn't exist any direct connection between these two networks, but just to the Application Gateway.



The Application Gateway is thus a kind of proxy for each of the two networks. Another term for this constellation is the "dualhomed gateway", because this workstation is so to speak at home in two networks.

For each application to be allowed through this gateway, an own service will be set up, e.g. SMTP for mail, HTTP for surfing the Internet or FTP for data downloads.



This service accepts data received by either one of the two sides and depicts it to the respective other side. What seems to be at first sight a needless mirroring of existing data, is on closer examination the far-reaching concept of

Application Gateways: It never exists a direct connection e.g. between a client of the local network and a server of the Internet. The LAN workstations only see the proxy, the workstations of the Internet likewise. This physical separation of LAN and WAN, makes it quite difficult for attackers to intrude into the protected network.

Applied to the porter example, the packet will be left at the gate, the courier is not allowed to enter the company premises. The porter takes the packet, will open it after checking address and delivery note and will control also the content. When the packet has taken these hurdles successfully, then the company internal courier will bring it himself to the addressee of the company. He became proxy of the courier on company premises. The other way around, all employees, wanting to send a packet, have to inform the porter, which has to collect the packet at the workstation place and which will hand over the packet to the ordered courier at the gate.



Functions of Application Gateways are not supported by the LANCOM, mainly because of the high hardware demands.

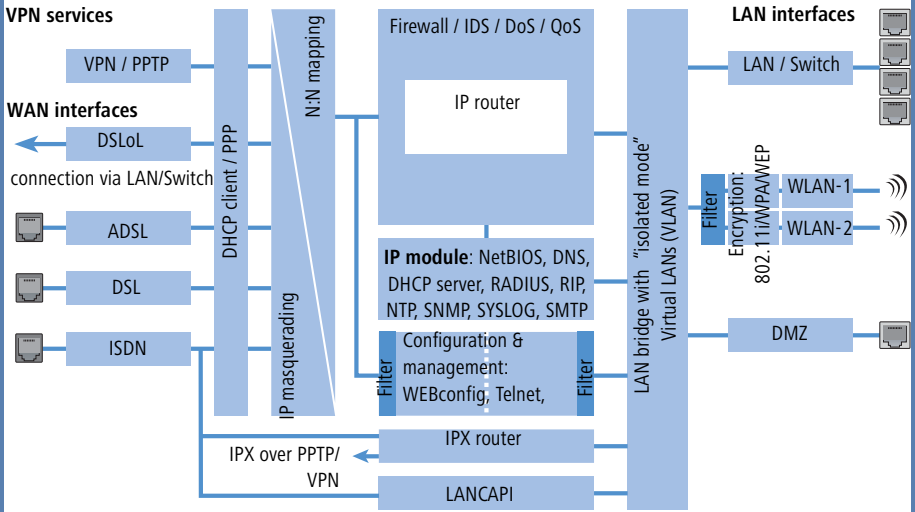
### 8.3 The LANCOM Firewall

After general explanations concerning the dangers of the Internet and the tasks and types of Firewalls, this chapter describes special functions of the LANCOM Firewall and concrete configurations.

### 8.3.1 How the LANCOM Firewall inspects data packets

The Firewall filters only those data packets out of the entire data stream running through the IP router of the LANCOM, for which a special treatment has been defined.

## The Firewall only checks routed data packets!



The Firewall only checks data packets routed by the IP router of the LANCOM. In general, these are the data packets, which are exchanged between one of the WAN interfaces and the internal networks (LAN, WLAN, DMZ).

For example, the communication between LAN and WLAN is normally not carried out by the router, as long as the LAN bridge allows a direct exchange. Thus the Firewall rules do not apply here. The same applies to the so-called "internal services" of the LANCOM like Telnet, TFTP, SNMP and the web server for the configuration with WEBconfig. The data packets of these services do not run through the router, and therefore aren't influenced by the Firewall.



Due to the positioning behind the masquerading module (seen from the WAN), the Firewall operates with the "real" internal IP addresses of the LAN stations, and not with the outside known Internet address of the LANCOM.

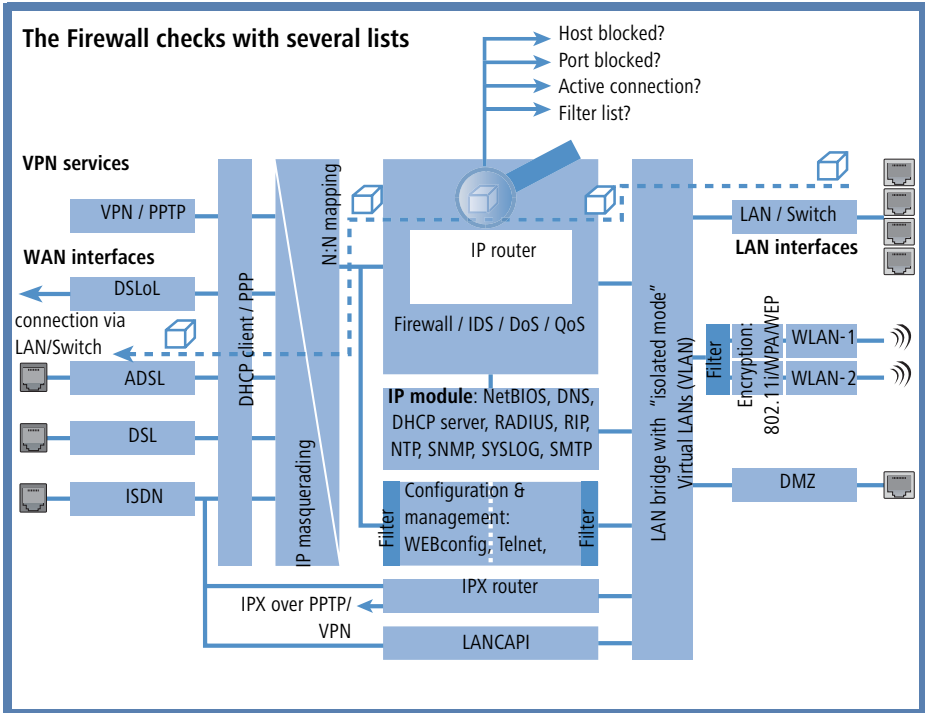
The LANCOM Firewall uses several lists for checking data packets, which are automatically generated from Firewall rules, resulting Firewall actions or by active data connections:

- ▶ Host block list
- ▶ Port block list
- ▶ Connection list
- ▶ Filter list

When a data packet should be routed via the IP router, the Firewall uses the lists as follows:

- ① The first check is, whether the packet was coming from a workstation belonging to the **host block list**. If the sender is blocked, the packet will be discarded.
- ② If the sender is not blocked in this list, the **port block list** will be checked, if the used port/protocol combination on the destination PC is closed. In this case the packet will be discarded.
- ③ If sender and destination are not blocked in the first two lists, then it will be checked whether a connection entry exists for this packet in the **connection list**. If such an entry exists, then the packet will be handled as noted in this list.
- ④ If no entry has been found for the packet, then the **filter list** will be searched, whether a suitable entry exists and the action indicated in this

list will be carried out. If the action intends to accept the packet, then an entry is made in the connection list, as well as for any further actions.



If no explicit Firewall rule exists for a data packet, the packet will be accepted ('Allow-All'). That grants a backward-compatibility for existing installations. For maximum protection by the Stateful Inspection, please note the section 'Set-up of an explicit "Deny All" strategy' →page 138.

The four lists obtain their information as follows:

- ▶ In the **host block list** are all those stations listed, which are blocked for a certain time because of a Firewall action. The list is dynamic, new entries can be added continuously with appropriate actions of the Firewall. Entries automatically disappear after exceeding the timeout.
- ▶ In the **port block list** those protocols and services are filed, which are blocked for a certain time because of a Firewall action. This list is likewise

a dynamic one, new entries can be added continuously with the appropriate Firewall actions. Entries automatically disappear after exceeding the timeout.

- ▶ For each established connection an entry is made in the **connection list**, if the checked packet has been accepted by the filter list. In the connection list is noted from which source to which destination, over which protocol and which port a connection is actually allowed. The list contains in addition, how long an entry will stay in the list and which Firewall rule is responsible for the entry. This list is very dynamic and permanently “moving”.
- ▶ The **filter list** is made of the Firewall rules. The containing filters are static and only changed when Firewall rules are added, edited or deleted.

Thus all lists, which are consulted by the Firewall to check data packets, finally base on the Firewall rules ('Parameters of Firewall rules' →page 125).

### 8.3.2 Special protocols

One important point during the connection tracking is the treatment of protocols that dynamically negotiate ports and/or addresses, over which further communication is done. Examples of these kinds of protocols are FTP, H.323 or also many UDP-based protocols. Thereby it is necessary that further connections must be opened, additionally to the first connection. See also 'Different types of Firewalls' →page 108.

#### UDP connections

UDP is actually a stateless protocol, nevertheless one can speak regarding UDP-based protocols also of a (only short term) connection, since UDP mostly carries Request/Response based protocols, with which a client directs its requests to a well known port of a server (e.g. 53 for DNS), which in turn sends its responds to the source port selected by the client:

Client port	Connection	Server port
12345	Request →	53
12345	Response ←	53

However, if the server wants to send larger sets of data (e.g. TFTP) and would not like or can not differentiate on the well known port between requests and acknowledges, then it sends the response packets to the source port of the sender of the original request, but uses as its own source port a free port, on which it reacts now only to those packets, which belong to the data communication:

Client port	Connection	Server port
12345	Request →	69
12345	Response ←	54321
12345	Ack/Data →	54321
12345	Data/Ack ←	54321

While the data communication takes place now over the ports 12345 and 54321, the server on the well-known port (69) can accept further requests. If the LANCOM pursues a "Deny All" strategy, the answer packets of an entry of the port filter Firewall, which permits only a connection to port 69 of the server, would simply be discarded. In order to prevent this, when creating the entry in the connection state database, the destination port of the connection is kept free at first, and set only with the arrival of the first answer packet, whereby both possible cases of an UDP connection are covered.

### TCP connections

TCP connections cannot be tracked only by examination of the ports. With some protocols (e.g. FTP, PPTP or H.323) examinations of the utilizable data are necessary to open all later negotiated connections, and to accept only those packets belonging really to the connections. This corresponds to a simplified version of IP masquerading, but without addresses or ports to be remapped here. It is sufficient to pursue the negotiation to open appropriate ports, and link them with the main connection, so that these ports are closed likewise with the closing of the main connection, and traffic on the secondary connection keeping open also the main connection.



### ICMP connections

For ICMP two cases must be differentiated: The ICMP request/reply connections, like to be used with "ping", and the ICMP error messages, which can be received as an answer to any IP packet.

ICMP request/reply connections can be clearly assigned to the identifier used by the initiator, i.e. in the status database an entry will be provided with the sending of an ICMP request, which lets through only ICMP replies with the correct identifier. All other ICMP replies will get discarded silently.

In ICMP error messages, the IP header and the first 8 bytes of the IP packet (on behalf UDP or TCP headers) can be found within the ICMP packet. With the help of this information, the receipt of an ICMP error message triggers automatically the search for the accessory entry in the status database. The packet passes only if such an entry exists, otherwise it is discarded silently. Additionally, potentially dangerous ICMP error messages (redirect route) are filtered out.

### Connections of other protocols

For all other protocols no related connections can be followed up, i.e. with them only a connection between involved hosts can occur in the status database. These can be initiated also only from one side, unless, in the port filter Firewall exists a dedicated entry for the "opposite direction".

## 8.3.3 General settings of the Firewall

Apart from individual Firewall rules, which ensure the entries in the filter, connection and block lists, some settings apply generally to the Firewall:

- ▶ Firewall/QoS enabled
- ▶ Default VPN rules (→page 122)
- ▶ Administrator email (→page 122)
- ▶ Fragments (→page 122)
- ▶ Re-establishing of the session (→page 123)
- ▶ Ping blocking (→page 123)
- ▶ Stealth mode(→page 124)
- ▶ Mask authentication port (→page 124)

### Firewall/QoS enabled

This option switches on or off the entire Firewall, including Quality of Service functions.



Please notice that the N:N mapping functions ('N:N mapping' →page 80) are only active when the Firewall has been switched on!

### Default VPN rules

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

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

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



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

### Administrator email

One of the actions a Firewall can trigger is alerting of an network administrator via email. The "administrator email" is the email account, to which the alerting mails are sent to.

### Fragments

Some attacks from the Internet try to outsmart the Firewall by fragmented packets (packets split into several small units). One of the main features of a Stateful Inspection like in the LANCOM is the ability to re-assemble fragmented packets in order to check afterwards the entire IP packet.

You can centrally adjust the desired behaviour of the Firewall. The following options are available:

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

- ▶ **Route:** Fragmented packets are passed on without any further checking by the Firewall, as long as permitted by valid filter settings.
- ▶ **Re-assemble:** Fragmented packets are buffered and re-assembled to complete IP packets. The re-assembled packets will then be checked and treated according to the valid filter settings.

### Session recovery

The Firewall enters all actual permitted connections into the connection list. Entries disappear automatically from the connection list after a certain time (timeout), when no data has been transmitted over this connection any more re-triggering the timeout.

Sometimes connections are ended according to the general TCP aging settings, before data packets requested by an inquiry have been received by the remote station. In this case perhaps an entry for a permitted connection still exists in the connection list, but the connection itself is no more existing.

The parameter "Session recovery" determines the behaviour of the Firewall for packets that indicate a former connection:

- ▶ **Always denied:** The Firewall re-establishes the session under no circumstances and discards the packet.
- ▶ **Denied for default route:** The Firewall re-establishes the session only if the packet wasn't received via the default route (e.g. Internet).
- ▶ **Denied for WAN:** The Firewall re-establishes the session only if the packet wasn't received over one of the WAN interfaces.
- ▶ **Always allowed:** The Firewall re-establishes the connection in principle if the packet belongs to a former connection of the connection list.

### Ping blocking

One - not undisputed - method to increase security is hiding the router. Based loosely on the method: "Who doesn't see me neither tries to attack me...". Many attacks begin with the searching for workstations and/or open ports by actual harmless inquiries, e. g. with the help of the "ping" command or with a portscan. Each answer to these inquiries, even the answer "I'm not here" indicates to the attacker that he has found a potential destination. Because anybody who answers must be existing, too. In order to prevent this conclusion, the LANCOM is able to suppress the answers to these inquiries.

In order to achieve this, the LANCOM can be instructed not to answer ICMP echo requests any more. At the same time TTL-exceeded messages of a "trace

route" are also suppressed, so that the LANCOM cannot be found, neither by "ping" nor by "trace route".

Possible settings are:

- ▶ **Off:** ICMP answers are not blocked.
- ▶ **Always:** ICMP answers are always blocked.
- ▶ **WAN only:** ICMP answers are blocked on all WAN connections.
- ▶ **Default route only:** ICMP answers are blocked on default route (usually Internet).

### TCP Stealth mode

Apart from ICMP messages, also the behaviour in case of TCP and UDP connections gives information on the existence or non-existence of the addressed workstation. Depending on the surrounding network it can be useful to simply reject TCP and UDP packets instead of answering with a TCP RESET resp. an ICMP message (port unreachable), if no listener for the respective port exists. The desired behaviour can be adjusted in the LANCOM.



If ports without listener are hidden, this generates a problem on masked connections, since the "authenticate" - resp. "ident" service does no longer function properly (resp. do no longer correctly reject). The appropriate port can so be treated separately ('Mask authentication port' →page 124).

Possible settings are:

- ▶ **Off:** All ports are closed and TCP packets are answered with a TCP reset.
- ▶ **Always:** All ports are hidden and TCP packets are silently discarded.
- ▶ **WAN only:** On the WAN side all ports are hidden and on the LAN side closed.
- ▶ **Default route only:** Ports are hidden on the default route (usually Internet) and closed on all other routes.

### Mask authentication port

When TCP or UDP ports are hidden, inquiries of mail servers to authenticate users can no more be answered correctly. Inquiries of the servers run into a timeout, and delivery of mails will be considerably delayed.

Also when the TCP Stealth mode is activated, the Firewall detects the intention of a station in the LAN to establish a connection to a mail server. As a result,

the needed port will be opened for a short time (20 seconds) solely for the authentication inquiry.

This behaviour of the Firewall in TCP Stealth mode can be suppressed specifically with the parameter "Always mask authentication port, too".



The activation of the option "Mask authentication port" can lead to considerable delays for the dispatch and receipt of e. g. e-mails or news!

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

The problem thereby is however that a setting, which hides all ports, but rejects the ident port is unreasonable - alone by the fact that rejecting the ident port would make the LANCOM visible.

The LANCOM offers now the possibility to reject ident inquiries only by mail and news servers, and to discard those of all other PCs. For this, the ident inquiries of the respective servers are rejected for a short time (20 seconds) when a mail (SMTP, POP3 IMAP2) or a news server (NNTP) is calling up.

When the timeout is exceeded, the port will be hidden again.

### 8.3.4 Parameters of Firewall rules

In this section we describe the components of Firewall rules and the available options to set up the different parameters.



Information regarding definition of Firewall rules with the different kinds of configuration tools (LANconfig, WEBconfig or Telnet) can be found in chapter 'Configuration of Firewall rules' →page 141.

#### Components of a Firewall rule

A Firewall rule is at first defined by its name and some further options:

- ▶ **On/Off switch:** Is the rule active for the Firewall?
- ▶ **Priority:** Which is the priority of the rule? (→page 126)
- ▶ **Observe further rules:** Should further Firewall rules be observed when this rule applies to a data packet? (→page 126)

- ▶ **Create VPN rule:** Is this Firewall rule also used to create a VPN rule? (→page 127)

### Priority

When setting up the filter list of the Firewall rules, the LANCOM will automatically sort the entries. Thereby the “grade of detail” will be considered: All specified rules are observed at first, after that the general ones (e. g. Deny All).

If after the automatic sorting the desired behaviour of the Firewall does not turn out, it is possible to change the priority manually. The higher the priority of the Firewall rule, the earlier it will be placed in the according filter list.



For complex rule types please check the filter list as described in section ‘Firewall diagnosis’ →page 151.

### Observe further rules

There are requirements to a Firewall, which cannot be covered by a single rule. If the Firewall is used to limit the Internet traffic of different departments (in own IP subnetworks), individual rules cannot e.g. illustrate the common upper limit at the same time. If to everyone of e.g. three departments should be granted a bandwidth of maximal 512 kbps, but the entire data rate of the three departments should not exceed a limit of 1024 kbps, then a multi-level checking of the data packets must be installed:

- ▶ In a first step it will be checked, if the actual data rate of the individual department does not exceed the limit of 512 kbps.
- ▶ In a second step it will be checked, if the data rate of all departments together does not exceed the overall limit of 1024 kbps.

Normally the list of the Firewall rules is applied sequentially to a received data packet. If a rule applies, the appropriate action will be carried out. The checking by the Firewall is terminated then, and no further rules will be applied to the packet.

In order to reach a two-stage or multi-level checking of a data packet, the “Observe further rules option” will be activated for the rules. If a Firewall rule with activated observation of further rules applies to a data packet, the appropriate action will be carried out at first, but then the checking in the Firewall will continue. If one of the further rules applies also to this data packet, the action being defined in this rule will also be carried out. If also for this following rule the observe further rules option is activated, the checking will be continued until

- ▶ either a rule applies to the packet, for which observe further rules is not activated.
- ▶ or the list of the Firewall rules has been completely worked through without applying a further rule to the packet.

To realize this aforementioned scenario it is necessary to install for each sub-network a Firewall rule that rejects from a data rate of 512 kbps up additional packets of the protocols FTP and HTTP. For these rules the observe further rules option will be activated. Defined in an additional rule for all stations of the LAN, all packets will be rejected which exceed the 1024 kbps limit.

### VPN rules

As described in section 'Default VPN rules' →page 122, a VPN rule can receive its information about source and destination network from Firewall rules.

By activating the option "This rule is used to create VPN rules" for a Firewall rule, you determine that a VPN rule will be derived from this Firewall rule.



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

Apart from this basic information, a Firewall rule answers the question when and/or on what it should apply to and which actions should be executed:

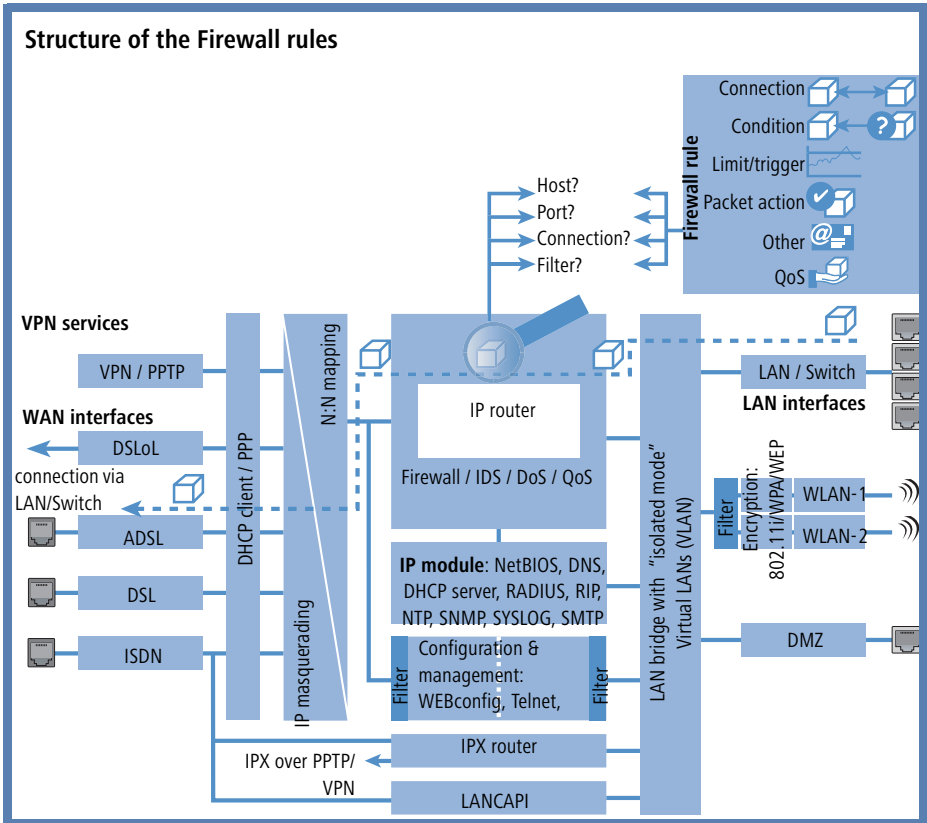
- ▶ **Stations / Service:** To which stations/networks and services/protocols does the rule refer to? (→page 128)
- ▶ **Conditions:** Is the effectiveness of the rule reduced by other conditions? (→page 129)
- ▶ **Trigger:** On exceeding of which threshold shall the rule being triggered? (→page 130)
- ▶ **Action:** What should happen to the data packets when the condition applies and the limit is reached? (→page 130)
- ▶ **Further measures:** Should further measures be initiated apart from the packet action? (→page 130)
- ▶ **Quality of Service (QoS):** Are data packets of certain applications or with the corresponding markings transferred preferentially by assurance of special Quality of Services? (→page 131)



Condition, limit, packet action and other measures form together a so-called "action set". Each Firewall rule can contain a number of

action sets. If the same trigger is used for several action sets, the sequence of action sets can be adjusted.

In section 'How the LANCOM Firewall inspects data packets' →page 115 we have already described that in the end the lists for checking data packets are created from Firewall rules. Thus the extension of the block diagram looks like as follows:



**Connection**



The connection of a Firewall rule defines to which data packets the rule should refer to. A connection is defined by its source, its destination and the used services. The following details can be used to specify the source or destination:

- ▶ All stations



- ▶ The entire local network (LAN)
- ▶ Certain remote stations (described by the name of the name list)
- ▶ Certain stations of the LAN described by the host name)
- ▶ Certain MAC<sup>1</sup> addresses
- ▶ Ranges of IP addresses
- ▶ Complete IP networks

You can only operate with host names, when your LANCOM is able to transform the names into IP addresses. For that purpose the LANCOM must have learned the names via DHCP or NetBIOS, or the assignment must be entered statically in the DNS or IP routing table. An entry in the IP routing table can therefore assign a name to a whole network.



If the source or the destination for a Firewall rule has not been determined at greater detail, the rule applies generally to data packets "from all stations" resp. "to all stations".

The service is determined by the combination of an IP protocol with respective source and/or destination port. For frequently used services (www, mail, etc.) the appropriate combinations are already predefined in the LANCOM, others can be compiled additionally as required.



### Condition

The effectiveness of a Firewall rule is also reduced with additional conditions. The following conditions are available:

- ▶ Only packets with certain ToS and/or DiffServ markings.
- ▶ Only, if the connection does not yet exist.
- ▶ Only for default route (Internet).
- ▶ Only for VPN routes.

---

1. MAC is the abbreviation for **Media Access Control** and it is the crucial factor for communication inside of a LAN. Every network device has its own MAC address. MAC addresses are worldwide unique, similar to serial numbers. MAC addresses allow distinguishing between the PCs in order to give or withdraw them dedicated rights on an IP level. MAC addresses can be found on most networking devices in a hexadecimal form (e.g. 00:A0:57:01:02:03).



### Limit / Trigger

The limit or trigger describes a quantified threshold value that must be exceeded on the defined connection before the filter action gets executed for a data packet. A limit is composed by the following parameters:

- ▶ Unit (kbit, kbyte or packets)
- ▶ Amount, that means data rate or number.
- ▶ Reference value (per second, per minute, per hour or absolute)

Additionally, you can adjust for the limit whether it refers to a logical connection or to all connections together, which exist between the defined destination and source stations via the corresponding services. Thus it is controlled whether the filter takes effect, if e.g. all HTTP connections of the users in the LAN exceed the limit in sum, or whether it is sufficient that only one of the parallel established HTTP connections exceeds the threshold value.

For absolute values it is additionally possible to specify whether the counter belonging to it will be reset to zero when the limit has been reached.



In any case, data will be transferred if a limit has not been reached yet! With a trigger value of zero a rule becomes immediately active, as soon as data packets arrive for transmission on the specified connection.



### Packet action

The Firewall has three possibilities to treat a filtered packet:

- ▶ **Transmit:** The packet will be transferred normally.
- ▶ **Drop:** The packet will be discarded silently.
- ▶ **Reject:** The packet will be rejected, the addressee receives an appropriate message via ICMP.



### Further measures

The Firewall does not only serve to discard or accept the filtered data packets, but it can also take additional measures when a data packet has been registered by the filter. The measures here are divided into the fields "protocolling/notification" and "prevent further attacks":

- ▶ **Send a Syslog message:** Sends a message via the SYSLOG module to a SYSLOG client, as defined in configuration field "Log & Trace".
- ▶ **Send an email message:** Sends an email message to the administrator, using the account specified in the configuration field "Log & Trace".

- ▶ **SNMP/LANmonitor:** Sends a SNMP trap, that will be analyzed e. g. by LANmonitor.



Each of these three message measures leads automatically to an entry in the Firewall event table.

- ▶ **Disconnect:** Cuts the connection, over which the filtered packet has been received.



On the occasion, the physical connection will be cut off (e. g. the Internet connection), not only the logical connection between the two involved PCs!

- ▶ **Lock source address:** Blocks the IP address from that the filtered packet has been received for a given time.
- ▶ **Lock target port:** Blocks the destination port to that the filtered packet has been sent for a given time.



### Quality of Service (QoS)

Apart from the restrictions for the transfer of data packets, the Firewall can also concede a “special treatment” to certain applications. QoS settings use features of the Firewall to specifically identify data packets of certain connections or services.



For further information about QoS and the appropriate configuration please see chapter ‘Quality of Service’ →page 168.

### 8.3.5 Alerting functions of the Firewall

This paragraph describes the Firewall alerts in detail that are sent on security-relevant events. The following message types are available:

- ▶ Email notification
- ▶ SYSLOG report
- ▶ SNMP trap

Alerts are triggered either separately by the intrusion detection system, by the denial of service protection or by arbitrary trigger conditions specified in the

Firewall. The specific parameters for the different alerting types such as the relevant email account can be set at the following places:

Configuration tool	Run
LANconfig	Log & Trace SMTP Account SNMP SYSLOG
WEBconfig	Expert Configuration Setup SMTP SNMP Module SYSLOG Module
Terminal/Telnet	/Setup/SMTP resp. SNMP Module or SYSLOG Module

An example:

Let us assume a filter named 'BLOCKHTTP', which blocks all access to a HTTP server 192.168.200.10. In case some station would try to access the server nevertheless, the filter would block any traffic from and to this station, and inform the administrator via SYSLOG also.

### SYSLOG notifications

If the Firewall drops an appropriate packet, a SYSLOG notification is created (see 'Setting up the SYSLOG module' →page 288) as follows:

```
PACKET_ALERT: Dst: 192.168.200.10:80 {}, Src:
10.0.0.37:4353 {} (TCP): port filter
```

Ports are printed only for port-based protocols. Station names are printed, if the LANCOM can resolve them directly (without external DNS request).

If the SYSLOG flag is set for a filter entry (%S action), then this notification becomes more detailed. Then the filter name, the exceeded limit and the filter action carried out are printed also. For the example above this should read as:

```
PACKET_ALERT: Dst: 192.168.200.10:80 {}, Src:
10.0.0.37:4353 {} (TCP): port filter
```

```
PACKET_INFO:
```

```
matched filter: BLOCKHTTP
```

```
exceeded limit: more than 0 packets transmitted or received
on a connection
```

```
actions: drop; block source address for 1 minutes; send
syslog message;
```

### Notification by email

If the email system of the LANCOM is activated, then you can use the comfortable notification by email:

```

FROM: LANCOM_Firewall@MyCompany.com
TO: Administrator@MyCompany.com
SUBJECT: packet filtered
Date: 9/24/2002 15:06:46

The packet below
Src: 10.0.0.37:4353 {cs2} Dst: 192.168.200.10:80
{ntserver} (TCP)
45 00 00 2c ed 50 40 00 80 06 7a a3 0a 00 00 25 | E...P@.
..z...%
c0 a8 c8 0a 11 01 00 50 00 77 5e d4 00 00 00 00 | .....P
.w^.....
60 02 20 00 74 b2 00 00 02 04 05 b4 | ` .t... ....
matched this filter rule: BLOCKHTTP
and exceeded this limit: more than 0 packets transmitted
or received on a connection

because of this the actions below were performed:
drop
block source address for 1 minutes
send syslog message
send SNMP trap
send email to administrator

```

### Notification by SNMP trap

If as notification method dispatching SNMP traps was activated (see also 'Configuration using SNMP' →page 20), then the first line of the logging table is sent away as enterprise specific trap 26. This trap contains additionally the system descriptor and the system name from the MIB-2.

For the example the following trap is thus produced:

```

SNMP: SNMPv1; community = public; SNMPv1 Trap; Length = 443
(0x1BB)
SNMP: Message type = SNMPv1
SNMP: Version = 1 (0x0)
SNMP: Community = public
SNMP: PDU type = SNMPv1 Trap
SNMP: Enterprise = 1.3.6.1.4.1.2356.400.1.6021
SNMP: Agent IP address = 10.0.0.43

```

	SNMP: Generic trap = enterpriseSpecific (6)
	SNMP: Specific trap = 26 (0x1A)
	SNMP: Time stamp = 1442 (0x5A2)
System descriptor	SNMP: OID = 1.3.6.1.2.1.1.1.0 1. SNMP: String Value = LANCOM Business 6021 2.80.0001 / 23.09.2002 8699.000.036
Device string	SNMP: OID = 1.3.6.1.2.1.1.5.0 2. System-Name SNMP: String Value = LANCOM Business 6021
Time stamp	SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.2.1 3. SNMP: String Value = 9/23/2002 17:56:57
Source address	SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.3.1 3. SNMP: IP Address = 10.0.0.37
Destination address	SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.4.1 4. SNMP: IP Address = 192.168.200.10
Protocol (6 = TCP)	SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.5.1 5. SNMP: Integer Value = 6 (0x6) TCP
Source port	SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.6.1 6. SNMP: Integer Value = 4353 (0x1101)
Destination port (80 = HTTP)	SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.7.1 7. SNMP: Integer Value = 80 (0x50)
Name of the filter rule	SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.8.1 8. SNMP: String Value = BLOCKHTTP



This trap and all different in the LANCOM generated traps are sent to all manually configured trap receivers, just like to each registered LANmonitor, which can evaluate this and possibly all other traps.

### 8.3.6 Strategies for Firewall settings

Firewalls are the interface between networks, and they restrict to a smaller or larger extent an unhindered data exchange. Thus Firewalls have opposite objectives than networks, although they are a part of them: networks should connect workstations, Firewalls should prevent the connection.

This contradiction shows the dilemma of the responsible administrators who have developed subsequently different strategies to solve this problem.

### **Allow All**

The Allow All strategy favours unhindered communication of the employees compared over security. Any communication is allowed at first, the LAN is still open for attackers. The LAN becomes gradually more secured by configuration of the administrator, by settings of more and more new rules, which restrict or prevent parts of communication.

### **Deny All**

The Deny All strategy proceeds at first according to the method "Block all!". The Firewall blocks completely the communication between the protected network and the rest of the world. In a second step, the administrator opens address ranges or ports, which are necessary e.g. for daily communication with the Internet.

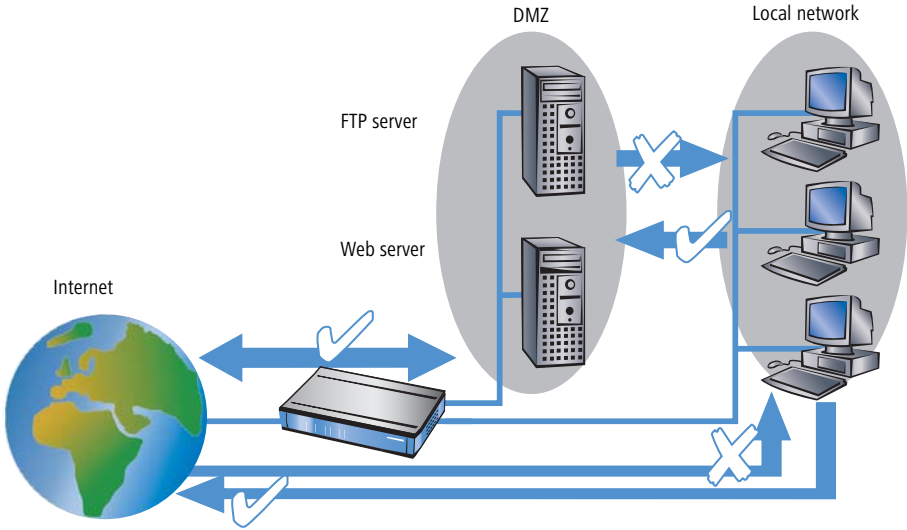
This approach ensures superior security for the LAN security compared to the Allow All strategy, but may lead especially in its initial stages to difficulties for the users. After activation of the Deny All strategy, some things just may behave differently than before, some stations may not be reached any more etc.

### **Firewall with DMZ**

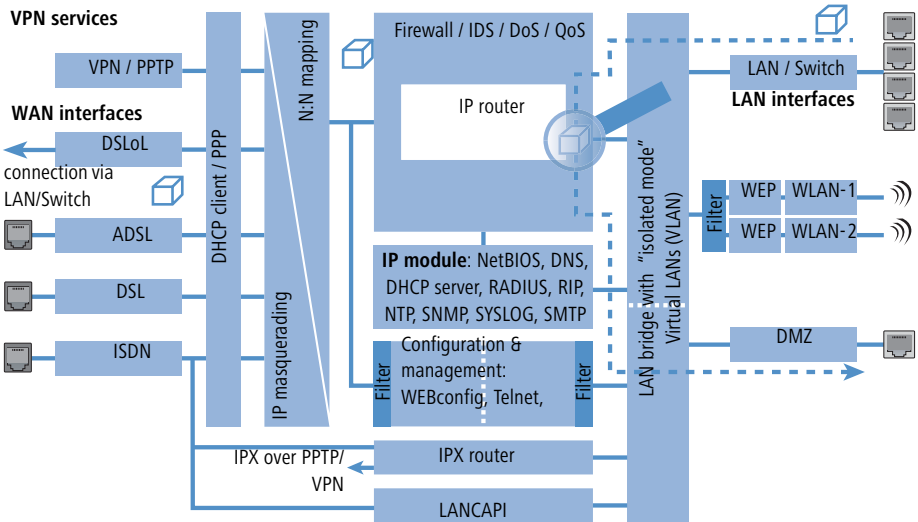
The demilitarized zone (DMZ) is a special range of the local network, which is shielded by a Firewall both against the Internet and against the normal LAN. All stations or servers that should be accessible from the unsecured network (Internet) should be placed into this network. These include for example own FTP and web servers.

The Firewall protects at first the DMZ against attacks from the Internet. Additionally, the Firewall protects also the LAN against the DMZ. To do so, the Firewall is configured in this way that only the following accesses are possible:

- ▶ Stations from the Internet can access to the servers in the DMZ, but no access from the Internet to the LAN is possible.
- ▶ The stations of the LAN can access the Internet, as well as servers in the DMZ.
- ▶ Servers of the DMZ have no access to the stations of the LAN. That guarantees that no "cracked" server of the DMZ becomes a security risk for the LAN.



Some LANCOM models support this structure by a separate LAN interface only used for the DMZ. Looking at the path of data through the LANCOM, then the function of the Firewall for shielding the LAN against the DMZ becomes visible.





A direct data exchange between LAN and DMZ via LAN bridge is not possible if a dedicated DMZ port is used. The path from LAN to DMZ and vice versa is therefore only possible through the router, and thus also only through the Firewall! This shields the LAN against inquiries from the DMZ, similar to the LAN against inquiries from the Internet.



The shielding of the DMZ against the Internet on one side and the LAN on the other is solved in many network structures with two separate Firewalls. When using a LANCOM with DMZ port, only one device for this setup is needed, which e.g. results in a clearly simplified configuration.

### 8.3.7 Hints for setting the Firewall

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

#### The default settings of the Firewall

On delivery there is exactly one entry in the Firewall rule table: "WINS". This rule prevents unwanted connection set-ups on the default route (gen. to the Internet) by the NetBIOS protocol. Windows networks send inquiries in regular intervals into the network to find out if known stations are still available. This leads in case of a time-based account of a network coupling to unwanted connection set-ups.



The LANCOM can prevent this by the integrated NetBIOS proxy also for network couplings, by pretending an answer for the concerned resource, until a real access takes place.

#### Security by NAT and Stateful Inspection

If no further Firewall rule will be entered, the local area network is protected by the interaction of Network Address Translation and Stateful Inspection: Only connections from the local area network produce an entry in the NAT table, whereupon the LANCOM opens a communication port. The Stateful Inspection supervises communication via this port: Only packets, which belong exactly to this connection may communicate via this port. For accesses from the outside to the local network results thus an implicit "Deny All" strategy.



If you operate a web server in your LAN, that has been permitted access to this service from the outside (see 'The hiding place—IP masquerading (NAT, PAT)' →page 74), stations from the Internet can establish from the outside connections to this server. The inverse masquerading has priority over the Firewall in this case, as long as no explicit "Deny All" rule has been set.

### Set-up of an explicit "Deny All" strategy

For maximum protection and optimum control of the data traffic it is recommended to prevent first any data transfer by the Firewall. Then only the necessary functions and communication paths are allowed selectively. This offers e.g. protection against so-called "Trojans" and/or e-mail viruses, which set up actively an outgoing connection on certain ports.

#### Deny All: The most important Firewall rule!

The Deny All rule is by far the most important rule to protect local networks. By this rule the Firewall operates according to the principle: "All actions, which are not explicitly allowed, remain forbidden!" Only by this strategy the administrator can be sure not to have "forgotten" an access method, because only those accesses exist, which have been opened explicitly by himself.

We recommend to set up the Deny All rule before connecting the LAN via a LANCOM to the Internet. Then you can analyse in the logging table (to start e. g. via LANmonitor), which connection attempts have been blocked by the Firewall. With the help of this information the Firewall and the "Allow rules" can be gradually extended.

Some typical applications are shown in the following.



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

## ▶ Example configuration "Basic Internet"

Rule name	Source	Destination	Action	Service (target port)
ALLOW_HTTP	Local network	All stations	transmit	HTTP, HTTPS
ALLOW_FTP	Local network	All stations	transmit	FTP
ALLOW_EMAIL	Local network	All stations	transmit	MAIL, NEWS
ALLOW_DNS_FORWARDING	IP address of LANOM (or: Local network)	transmit	transmit	DNS
DENY_ALL	All stations	reject	reject	ANY

- ▶ If you want to permit a VPN dial-in to a LANCOM acting as VPN gateway, then you need a Firewall rule allowing incoming communication from the client to the local network:

Rule	Source	Destination	Action	Service
ALLOW_VPN_DIAL_IN	remote site name	Local network	transmit	ANY

- ▶ In case a VPN is not terminated by the LANCOM itself (e.g. a VPN Client in the local area network, or LANCOM as Firewall in front of an additional VPN gateway), you'd have to allow IPSec and/or PPTP (for the "IPSec over PPTP" of the LANCOM VPN Client) ports additionally:

Rule	Source	Destination	Action	Service (target port)
ALLOW_VPN	VPN Client	VPN Server	transmit	IPSEC, PPTP

- ▶ For ISDN or V.110 dial-in (e.g. by HSCSD mobile phone) you have to allow the particular remote site (see also 'Configuration of remote stations' →page 89):

Rule	Source	Destination	Action	Service
ALLOW_DIAL_IN	remote site name	Local network	transmit	ANY

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

Rule	Source	Destination	Action	Service
ALLOW_LAN1_TO_LAN2	LAN1	LAN2	transmit	ANY
ALLOW_LAN2_TO_LAN1	LAN2	LAN1	transmit	ANY

- ▶ If you operate e.g. an own web server, you selectively allow access to the server:

Rule	Source	Destination	Action	Service (target port)
ALLOW_WEBSERVER	ANY	Webserver	transmit	HTTP, HTTPS

- ▶ For diagnostic purposes it is helpful to allow ICMP protocols (e.g. ping):

Rule	Source	Destination	Action	Service
ALLOW_PING	Local network	ANY	transmit	ICMP

These rules can now be refined as needed - e.g. by the indication of minimum and maximum bandwidths for the server access, or by a finer restriction on certain services, stations or remote sites.

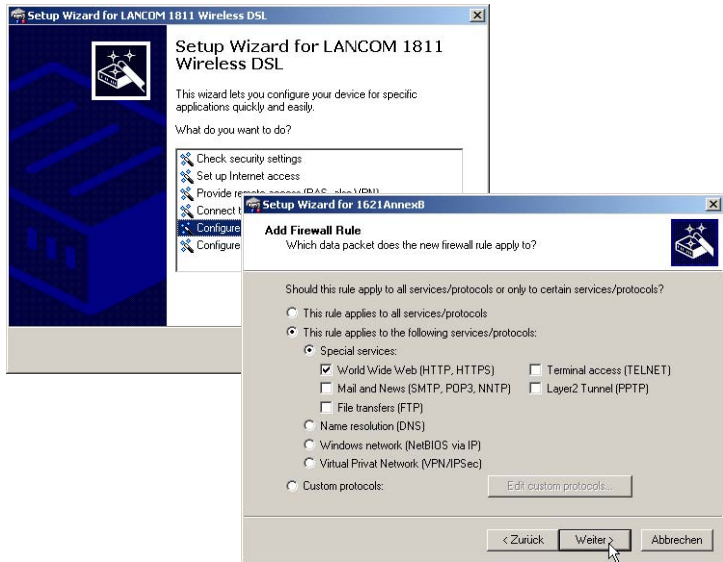


The LANCOM automatically sorts Firewall rules when creating the filter list. Thereby, the rules are sorted into the filter list on the basis of their level of detail. First all specific rules are considered, afterwards the general ones (e.g. Deny All). Examine the filter list in case of complex rule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

## 8.3.8 Configuration of Firewall rules

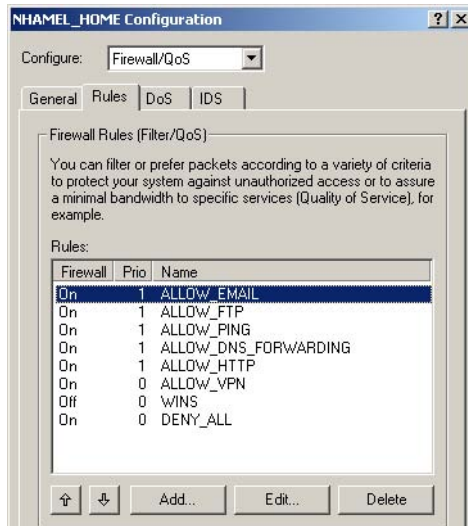
### Firewall wizard

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



## LANconfig

The filters can be installed very comfortably with LANconfig. Starting from the general register card "Firewall / QoS / Rules", you reach after "Add" or "Edit" the dialogue to define the Firewall rules:

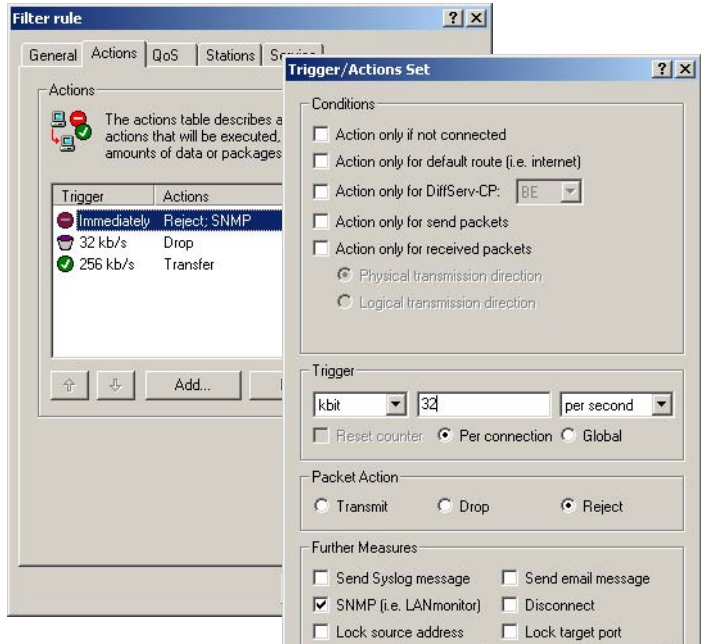


Within the dialogue for the definition of filter rules, the following options can be found on different index cards:

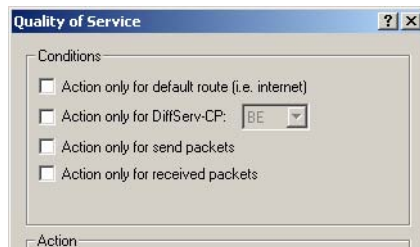
- ▶ **General:** Here the name of the Firewall rule is specified, as well as if further rules should be considered after this rule matched, and whether a VPN rule should be derived from this rule.



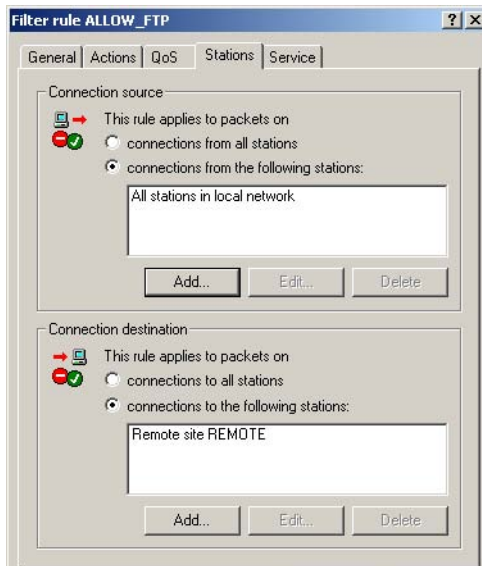
- ▶ The option 'Observe further rules ...' can be used to create complex functions ensuring e.g. certain bandwidths with QoS ('Connection' →page 128)
- ▶ The option 'This rule is used to create VPN rules' enables to utilize the information about source and destination networks of this rule also to define VPN networks ('Default VPN rules' →page 122).
- ▶ **Actions:** Here the Firewall actions are defined, consisting of condition, trigger, packet action and further measures.



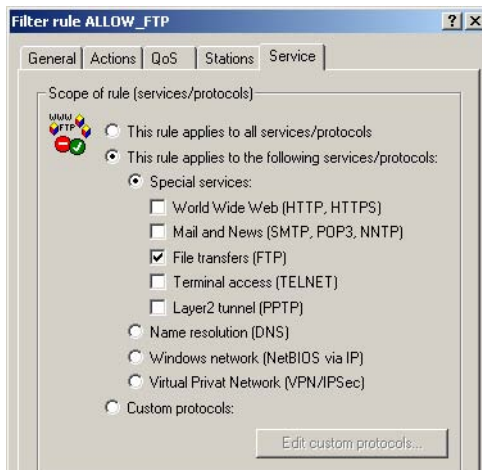
- ▶ **QoS:** Here you can assign minimum bandwidths for data packets specified by according Firewall rules (see also 'Defining minimum and maximum bandwidths' →page 185).



- ▶ **Stations:** Here the stations – as sender or addressee of the packets – are specified, for which the filter rule shall match.



- ▶ **Services:** Here the IP protocols, source and destination ports are specified for which the filter rule shall apply. For example, it can be specified here that only access to web pages and emails shall be permissible.





### WEBconfig, Telnet

Under WEBconfig or Telnet the Firewall rules are configured in the following menus and lists:

Configuration tool	Run
WEBconfig	Expert Configuration / Setup / IP Router Module/ Firewall: Rule Table, Object Table, Actions Table
Terminal/Telnet	Setup / IP Router Module/ Firewall / Rule Table, Object Table, Actions Table

There is a special syntax in LCOS for the description of the Firewall rules. This syntax allows to describe also complex relations for checking and treatment of data packets within the Firewall just with a few characters.

Rules are defined in the rule table. Pre-defined objects can be saved in two additional tables in order to prevent entering frequently used objects each time again in LCOS syntax:

- ▶ The action table contains Firewall actions
- ▶ The object table contains stations and services



Objects from these tables can be used for rule definition, but this is not a must. They simply facilitate the use of frequently used objects.

Rule table

The rule table combines different information to a Firewall rule. The rule contains the protocol to be filtered, the source, the destination as well as the Firewall action to be executed. For each Firewall rule there is an additional on/off-switch, a priority, the option for a linkage with other rules and an activation of the rule for VPN connections. General information concerning these parameters can be found in section 'Parameters of Firewall rules' →page 125.


The definition of the Firewall rules can be composed of entries of the object table for protocols, services, stations (→page 146), and of entries of the

action table for Firewall actions (→page 147). It can also contain direct descriptions in the appropriate LCOS syntax (e. g. %P6 for TCP).

The screenshot shows a web-based configuration interface for a firewall. At the top, there are navigation links: [Expert Configuration](#), [Setup](#), [IP-router-module](#), and [Firewall](#). Below these is the **Rule-table** configuration section. The fields are as follows:

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

At the bottom of the window, there is a status bar with "Done" on the left and "Internet" on the right.

 For direct entering of rule parameters in LCOS syntax, the same guidelines apply as described in the following sections for protocols, source and destination, as well as for Firewall actions.

#### Object table

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

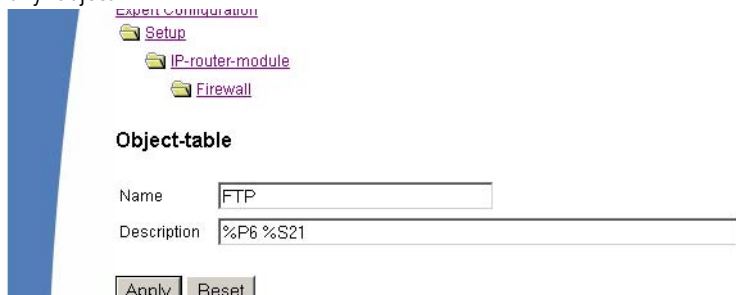
- ▶ Single PCs (MAC or IP address, host name)
- ▶ Entire networks
- ▶ Protocols
- ▶ Services (ports or port ranges, e. g. HTTP, Mail&News, FTP, ...)


Any combination of these elements is possible. Furthermore, objects can be defined hierarchically. So one can first define objects for TCP and UDP protocols, then objects for e.g. FTP (= TCP + ports 20 and 21), HTTP (= TCP + port 80) and DNS (= TCP, UDP + port 53). All these single objects can be assembled subsequently into a new object, which contains all previously defined single objects then.

Stations and services can be described according to the following rules in the object table:

Description	Object ID	Examples and notes
Local network	%L	
Remote stations	%H	Name must be in DSL /ISDN /PPTP or VPN name list
Host name	%D	Note advice for host names (→page 129)
MAC address	%E	00:A0:57:01:02:03
IP address	%A	%A10.0.0.1, 10.0.0.2; %A0 (all addresses)
Netmask	%M	%M255.255.255.0
Protocol (TCP/UDP/ICMP etc.)	%P	%P6 (for TCP)
Service (port)	%S	%S20-25 (for ports 20 to 25)

Equal identifier can generate comma-separated lists as for example host lists/ address lists (%A10.0.0.1, 10.0.0.2), or hyphen-separated ranges like port ranges (%S20-25). The occurrence of a "0" or an empty string represents the 'any' object.



 When configuring via console (Telnet or terminal program), the combined parameters (port, destination, source) must be embraced with inverted commas (character ").

Action table

As described above, a Firewall action consists of condition, limit, packet action and further measures. In the action table Firewall actions are composed as any combination of the following elements:

## ▶ Conditions

Condition	Description	Object ID
Connect filter	The filter is active when no physical connection to the packet destination exists.	@c
DiffServ filter	The filter is active when the packet contains the indicated Differentiated Services Code Point (DSCP) ('Evaluating ToS and DiffServ fields' →page 183.	@d (plus DSCP)
Internet filter	The filter is active when the packet is received or will be transmitted via default route.	@i
VPN filter	The filter is active when the packet is received or will be transmitted via VPN connection.	@v

If no further actions are specified in a "connect" or "Internet" filter, then implicitly a combination of these filters with the "reject" action is assumed.

## ▶ Limits/Trigger

Each Firewall action can be tied together with a limit, whose excess leads to the triggering of the action. Also, several limits for a filter thereby can build action chains.

Limit objects are generally introduced by %L, followed by:

- ▷ Reference: per connection (c) or globally (g)
- ▷ Kind: Data rate (d), number of packets (p) or packet rate (b)
- ▷ Value of the limit
- ▷ Further parameters (e. g. period and quantity)

The following limitations are available:

Limit	Description	Object ID
Data (abs)	Absolute number of kilobytes on the connection after which the action is executed.	%lcd
Data (rel)	Number of kilobytes/second, minute, hour on the connection after which the action is executed.	%lcds %lcdm %lcdh
Packet (abs)	Absolute number of packets on the connection after which the action is executed.	%lcp

Limit	Description	Object ID
Packet (rel)	Number of packets/second, minute, hour on the connection after which the action is executed.	%lcps %lcpm %lcph
Global data (abs)	Global data (abs): Absolute number of kilobytes received from the destination station or sent to it, after which the action is executed.	%lgd
Global data (rel)	Number of kilobytes/second, minute or hour received from the destination station or sent to it, after which the action is executed.	%lgds %lgdm %lgdh
Global packet (abs)	Absolute number of packets received from the destination station or sent to it, after which the action is executed.	%lgp
Global packet (rel)	Number of packets/second, minute or hour received from the destination station or sent to it, after which the action is executed.	%lgps %lgpm %lgph
Receive option	Limit restriction to the direction of reception (this affects in the context with above limitations). In the ID object column, examples are indicated.	%lgdsr %lcdsr
Transmit option	Limit restriction to the sending direction (this affects in the context with above limitations). In the ID object column, examples are indicated.	%lgdst %lcdst



If an action is given without any associated limit, then implicitly a packet limit is assumed that is immediately exceeded with the first packet.

▶ Packet action

Packet action	Description	Object ID
Accept	The packet will be accepted.	%a
Reject	The packet will be rejected with the corresponding error message.	%r
Drop	The packet will be discarded silently.	%d

These packet actions can be combined arbitrarily. If you choose absurd or ambiguous actions (e. g.: Accept + Drop), then the more secured action will be taken (here: "Drop").

## ▶ Further measures

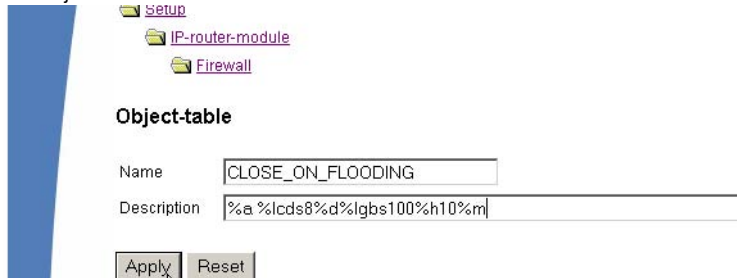
Measure	Description	Object ID
Syslog	Gives a detailed notification via SYSLOG.	%s
Mail	Sends an email to the administrator.	%m
SNMP	Sends a SNMP trap.	%n
Close port	Closes the destination port for a given time.	%p
Deny host	Locks out the sender address for a given time.	%h
Disconnect	Disconnects the connection to the remote site from which the packet was received or sent.	%t
Zero limit	Resets the limit counter to 0 again upon exceeding of the trigger threshold.	%z
Fragmentation	Forces a fragmentation of all packets not matching to the rule.	%f

If the "close port" action is executed, an entry in a block list is made, by which all packets, which are sent at the respective computer and port, get rejected. For the "close port" object a timeout can be given in seconds, minutes or hours, which is inserted directly behind the object ID. This time value is composed of the designator of the time unit (h, m, s for hour, minute and second), and the actual time. Thus e.g. %pm10 closes a port for 10 minutes. If no time unit is provided, then implicitly "minutes" apply (and thus %p10 is equivalent to %pm10).

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

If you want to limit e.g. the permissible data rate for a connection to 8 kbps and to lock out the aggressor committing a flooding attempt, and furthermore

send at the same time an email to the administrator, then the description of the object for the action reads as follows:



- ▶ This description permits traffic (%a) at the beginning. A simple %a at the beginning of the description is equivalent to a %lp0%a (= accept, if the limit was exceeded on zero packets, i.e. with the first packet).
- ▶ If over the current connection now 8 kbit (%lcds8) is transferred in one second, then all further packets - up to the expiration of the second - will be silently discarded (%d), thus automatically creating a Traffic Shaping.
- ▶ If 100 packets for the server (destination address of the connection) arrive (%lgbs100) in one second, then the remote host (source address) is locked for 10 minutes (%h10), and an email is sent to the administrator (%m).

Similar to the address and service objects of the object table, action objects can be provided with a name, and can arbitrarily be combined recursively, whereby the maximum recursion depth is limited to 16. In addition, they can be entered directly into the action field of the rule table.

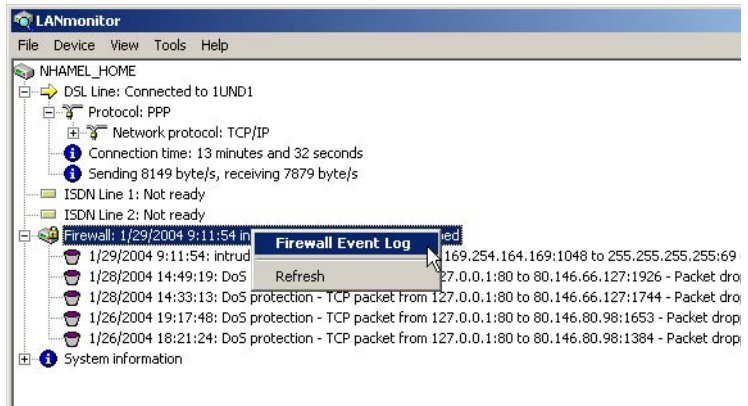
When building the actual filter table, action objects get minimized similarly to the address and service objects to the smallest necessary number, i.e. multiple definitions of an action get eliminated, and contradictory actions are turned into the "safest". Thus e.g. %a (accept) and %d (drop) becomes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

### 8.3.9 Firewall diagnosis

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

The most comfortable inspection is accomplished by displaying the logging table (see below) with LANmonitor. LANmonitor displays under 'Firewall' the

last five events, that were triggered either by a Firewall rule, the DoS, or the IDS system with activated 'SNMP/LANmonitor' option.



A new window with the complete logging table opens by clicking the right mouse button in the **Firewall Event Log** context menu. (→page 152).

All lists and tables described in this section can be found under the following menu options:

Configuration tool	Run
WEBconfig	Expert Configuration Status IP-Router-Statistics
Terminal/Telnet	/Status/IP-Router-Statistics

### The Firewall table

If an event occurred that had to be logged in either way, i.e. a log action was specified with the receipt of a packet, or a report by e-mail, Syslog or SNMP was generated, then this event is held in the logging table.



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

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

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

[Expert Configuration](#)

[Status](#)

[IP-router-statistics](#)

### Log-table

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

The table contains the following values:

Element	Element meaning
Idx.	Current index (so that the table can be polled also via SNMP)
System time	System time in UTC codification (will be transformed on displaying of the table into clear text)
Src address	Source address of the filtered packet
Dst address	Destination address of the filtered packet
Prot.	Protocol (TCP, UDP etc.) of the filtered packet

Element	Element meaning
Src-p	Source port of the filtered packet (only with port-related protocols)
Dst-p	Destination port of the filtered packet (only with port-related protocols)
Filter-Rule	Name of the rule, which has raised the entry.
Limit	Bit field, which describes the crossed limit, which has filtered the packet. The following values are defined at present: 0x01 Absolute number 0x02 Number per second 0x04 Number per minute 0x08 Number per hour 0x10 Global limit 0x20 Byte limit (if not set, it concerns a packet-related limit) 0x40 Limit applies only in receiving direction 0x80 limit applies only in transmission direction
Threshold	Exceeded limit value of the trigger limit
Action	Bit field, which specifies all implemented actions. At present the following values are defined: 0x00000001 Accept 0x00000100 Reject 0x00000200 Connect filter 0x00000400 Internet- (Default route-) filter 0x00000800 Drop 0x00001000 Disconnect 0x00004000 Block source address 0x00020000 Block destination address and port 0x20000000 Send SYSLOG notification 0x40000000 Send SNMP trap 0x80000000 Send email



All Firewall actions are likewise displayed within the IP router trace ('How to start a trace' → page 48). Furthermore, some LANCOM models have a Firewall LED, which signals each filtered packet.

### The filter list

The filter list allows to examine filters generated by rules defined in the action, object and rule table.



Please note that manually entered filter rules do not generate a fault indication and also no error message. If you configure filters manually, you should in each case examine on the basis of the filter list whether the desired filters were generated or not.

On Telnet level, the content of the filter list can be displayed with the command `show filter`:

```

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

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

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

LC1621.Internet:/
>

```

Under WEBconfig the filter list has the following structure:

- [Expert Configuration](#)
- [Status](#)
- [IP-router-statistics](#)

#### Filter-list

Idx.	Prot.	Src-MAC	Src-address	Src-netmask	S-st.	S-end	Dst-MAC	Dst-address	Dst-netmask
0001	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0
0002	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0
0003	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0
0004	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0
0005	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0
0006	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0
0007	1	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0

The individual fields in the filter list have the following meaning:



Entry	Description
Idx.	Current index
Prot	Protocol to be filtered, e.g. 6 for TCP or 17 for UDP.
Src MAC	Ethernet source address of the packet to be filtered or 000000000000, if the filter should apply to all packets.

Entry	Description
Src address	Source IP address or 0.0.0.0, if the filter should apply to all packets.
Source mask	Source network mask, which determinates the source network together with the source IP address, or 0.0.0.0, if the filter should apply to packets from all networks.
Q start	Start source port of the packets to be filtered.
Q end	End source port of the packets to be filtered. Makes up the port range together with the start source port, in which the filter takes effect. If start and end port are 0, then the filter is valid for all source ports.
Dst MAC	Ethernet destination address of the packet to be filtered or 000000000000, if the filter should apply to all packets.
Dst address	Destination address or 0.0.0.0, if the filter should apply to all packets.
Dst mask	Destination network mask, which determinates the destination network together with the destination IP address, or 0.0.0.0, if the filter should apply to packets to all networks.
Z start	Start destination port of the packets to be filtered.
Z end	Destination port of the packets to be filtered. Makes up the port range together with the start destination port, in which the filter takes effect. If start and end port are 0, so the filter is valid for all destination ports.
Action	Into this column, the "main action" is unveiled as a text, which will be executed when the first limit has been exceeded. The first limit can be also an implicit limit, e.g. if only one limit for the restriction of the throughput was configured. Then an implicit limit - linked with an "accept" action - is inserted. In this case, "accept" is unveiled as main action. You can see the complete actions under the command show filter.
Linked	Indicates whether it concerns a "first Match" rule (linked = no). Only with linked rules in the case of applying of this rule, also further rules are evaluated.
Prio	Priority of the rule having generated the entry.






### The connection list

The connection table files source address, destination address, protocol, source port, destination port, etc. of a connection, as well as possible actions. This table is sorted according to source address, destination address, protocol, source port and destination port of the packet, which caused the entry in the table.

Under WEBconfig the filter list has the following structure:

- [Expert Configuration](#)
-  [Status](#)
-  [IP-router-statistics](#)

### Connection-list

	Src-address	Dst-address	Prot.	Src-port	Dst-port	Timeout	Flags	Filter-rule	Src-route	D
	<a href="#">192.168.2.60</a>	80.190.240.17	6	3617	80	295	00020008	ALLOW_HTTP		1
	<a href="#">192.168.2.60</a>	80.190.240.17	6	3618	80	296	00020008	ALLOW_HTTP		1
	<a href="#">192.168.2.60</a>	212.227.15.181	6	3610	110	1	00020038	ALLOW_EMAIL		1
	<a href="#">192.168.2.60</a>	212.227.15.181	6	3612	110	2	00020038	ALLOW_EMAIL		1
	<a href="#">192.168.2.60</a>	212.227.15.181	6	3614	110	3	00020038	ALLOW_EMAIL		1

The table contains the following elements:

Element	Element meaning
Src addr.	Source address of the connection
Dst addr.	Destination address of the connection
Protocol	Used protocol (TCP/UDP etc.). The protocol is decimally indicated.
Src port	Source port of the connection. The port is only indicated with port-related protocols (TCP/UDP) or protocols, which own a comparable field (ICMP/ GRE).
Dst port	Destination port of the connection (with UDP connections, this one is occupied only with the first answer).
Timeout	Each entry ages out with the time of this table, thus the table does not overflow with "died" connections.
Flags	In the flags the condition of the connection and further (internal) information are stored in a bit field.(→page 158) As conditions the following values are possible: <b>new, establish, open, closing, closed, rejected</b> (corresponding to the TCP flags: SYN, SYN ACK, ACK, FIN, FIN ACK and RST). UDP connections know the conditions <b>new, open</b> and <b>closing</b> (the last one only, if the UDP connection is linked with a condition-afflicted control path. This is e.g. the case with protocol H.323.).
Src route	Name of the remote station, over which the first packet has been received.
Dst route	Name of the remote station, where the first packet will be sent to.
Filter rule	Name of the rule, which has generated the entry (determines also the actions to be executed), when a suitable packet is received.

## Meaning of the flags of the connection list

Flag	Flag meaning
00000001	TCP: SYN sent
00000002	TCP: SYN/ACK received
00000004	TCP: waiting for ACK of the server
00000008	all: open connection
00000010	TCP: FIN received
00000020	TCP: FIN sent
00000040	TCP: RST sent or received
00000080	TCP: session will be re-established
00000100	FTP: passive FTP connection will be established
00000400	H.323: belonging to T.120 connection
00000800	connection via loopback interface
00001000	checking concatenated rules
00002000	rule is catenated
00010000	destination is on "local route"
00020000	destination is on default route
00040000	destination is on VPN route
00080000	physical connection is not established
00100000	source is on default route
00200000	source is on VPN route
00800000	no route for destination
01000000	contains global actions with condition

## Port block list

Address, protocol and port of a destination station are filed in the port block list, if blocking of the destination port on the destination station was selected as a filter's packet action. This table is likewise a sorted semi-dynamic table.

Sorting is done according to address, protocol and port. The table contains the following elements:

Element	Element meaning
Address	Address of the station, to which the blocking should apply.
Protocol	Used protocol (TCP/UDP etc.) The protocol is decimally indicated.
Port	Port to close at the station. If the respective protocol is not port related, then the entire protocol for this station becomes closed.
Timeout	Duration of the blocking in minutes.
Filter rule	Name of the rule, which has produced the entry (determines also the actions to be executed), when a suitable packet is received.

### Host block list

The address of a station is filed in the host block list, if blocking of the sender was selected in a filter's packet action. This table is a sender address sorted semi-dynamic table and contains the following elements:

Element	Element meaning
Address	Address of the station, to which the blocking should apply.
Timeout	Duration of the blocking in minutes.
Filter rule	Name of the rule, which has generated the entry (determines also the actions to be executed), when a suitable packet is received.

### 8.3.10 Firewall limitations

Apart from understanding the functioning of Firewalls, it is also very important to discern their limitations and to extend them if necessary. The Firewall does not protect against malicious contents coming through the permitted ways into your local network. It is true that certain effects of some viruses and worms are stopped, because communication is blocked via the required ports, but no Firewall alone is a comprehensive protection against viruses.

Also monitoring of sensitive data in the Internet is not be prevented by a Firewall. If data once reaches the unsecured net beyond the Firewall, then it is exposed to well-known dangers. Despite using a Firewall, any confidential information such as contracts, passwords, development information etc. should be transmitted only over protected connections, i.e. by using suitable data encryption and VPN connections.

## 8.4 Protection against break-in attempts: Intrusion Detection

A Firewall has the task to examine data traffic across borders between networks, and to reject those packets, which do not have a permission for transmission. Beside attempts to access directly a computer in the protected network, there are also attacks against the Firewall itself, or attempts to outwit a Firewall with falsified data packets.

Such break-in attempts are recognized, repelled and logged by the Intrusion Detection system (IDS). Thereby it can be selected between logging within the device, email notification, SNMP traps or SYSLOG alarms. IDS checks the data traffic for certain properties and detects in this way also new attacks proceeding with conspicuous patterns.

### 8.4.1 Examples for break-in attempts

Typical break-in attempts are falsified sender addresses ("IP Spoofing") and port scans, as well as the abuse of special protocols such as e.g. FTP in order to open a port on the attacked computer and the Firewall in front of it.

#### IP Spoofing

With IP Spoofing the sender of a packet poses itself as another computer. This happens either in order to trick the Firewall, which trusts packets from the own network more than packets from untrusted networks, or in order to hide the author of an attack (e.g. Smurf).

The LANCOM Firewall protects itself against spoofing by route examination, i.e. it examines, whether a packet was allowed to be received over a certain interface at all, from which it was received.

#### Portscan Detection

The Intrusion Detection system tries to recognize Portscans, to report and to react suitably on the attack. This happens similarly to the recognition of a 'SYN Flooding' attack (see 'SYN Flooding' →page 162): The "half-open" connections are counted also here, whereby a TCP RESET, which is sent by the scanned computer, leaves a "half-open" connection open again.

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

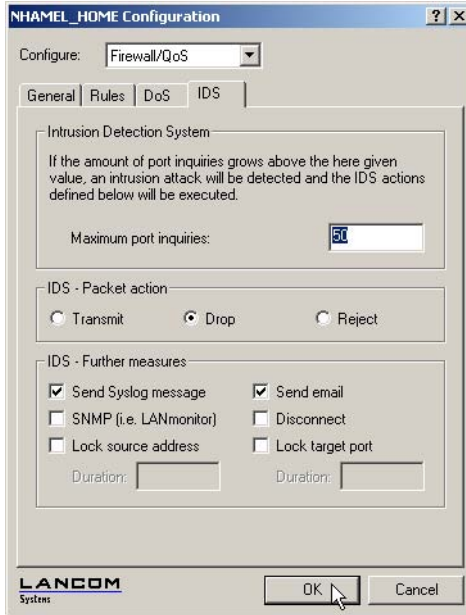
Likewise, the receipt of empty UDP packets is interpreted as an attempted port scan.



## 8.4.2 Configuration of the IDS

LANconfig

Parameters of the Intrusion Detection System are set in LANconfig in the configuration tool 'Firewall/QoS' on index card 'IDS':



Apart from the maximum number of port inquiries, fragment action and the possible registration mechanisms, also these reactions are possible:

- ▶ The connection will be cut off.
- ▶ The sender address will be blocked for an adjustable period of time.
- ▶ The destination port of the scan will be blocked for an adjustable period of time.

WEBconfig, Telnet

The behaviour of the Intrusion Detection Systems can be configured here under WEBconfig or Telnet:

Configuration tool	Run
WEBconfig	Expert Configuration: Setup/IP Router Module/Firewall
Terminal/Telnet	Setup/IP Router Module/Firewall

## 8.5 Protection against “Denial of Service” attacks

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

### 8.5.1 Examples of Denial of Service attacks

Denial of service attacks do profit from fundamental weaknesses of TCP/IP protocols, as well as from incorrect implementations of TCP/IP protocol stacks. Attacks, which profit from fundamental weaknesses are e.g. SYN Flood and Smurf. Attacks aiming at incorrect implementations are all attacks, which operate with incorrectly fragmented packets (e.g. Teardrop), or which work with falsified sender addresses (e. g. Land). In the following some of these attacks are described, their effects and possible countermeasures.

#### SYN Flooding

SYN Flooding means that the aggressor sends in short distances TCP packets with set SYN flag and with constantly changing source ports on open ports of its victim. The attacked computer establishes as a result a TCP connection, replies to the aggressor a packet with set SYN and ACK flags and waits now in vain for the confirmation of the connection establishment. Hundreds of "half-open" TCP connections are staying thereby, and just consume resources (e.g. memory) of the attacked computer. This procedure can go that far that the victim can accept no more TCP connection or crashes due to the lack of memory.

An appropriate countermeasure of a Firewall is to supervise the number of "half-open" TCP connections, which exists between two stations and to limit it. That means, if further TCP connections between these workstations were established, these connections would be blocked by the Firewall.

#### Smurf

The Smurf attack works in two stages and paralyzes two networks at once. In the first step a Ping (ICMP echo Request) packet with a falsified sender address is sent to the broadcast address of the first network, whereupon all workstations in this network answer with an ICMP echo Reply to the falsified sender address, which is located in the second network. If the rate of incoming echo requests is high enough, as well as the number of answering workstations, then the entire incoming traffic of the second network is blocked

during the attack and, moreover, the owner of the falsified address cannot receive normal data any more during the attack. If the falsified sender address is the broadcast address of the second network, also all workstations are blocked in this network, too.

In this case the DoS recognition of the LANCOM blocks passing packets, which are addressed to the local broadcast address.

## **LAND**

The land attack is a TCP packet that is sent with set SYN flag and falsified sender address to the victim workstation. The bottom line is that the falsified sender address is equal to the address of the victim. With an unfortunate implementation of TCP, the victim interprets the sent SYN-ACK again as SYN, and a new SYN-ACK is sent. This leads to a continuous loop, which lets the workstation freeze.

In a more up to date variant, the loopback address "127.0.0.1" is taken as sender address, but not the address of the attacked workstation. Sense of this deception is to outwit personal firewalls, which react in fact to the classical variant (sender address = destination address), but which pass through the new form without hindrance. This variant is also recognized and blocked by a LANCOM.

## **Ping of Death**

The Ping of Death belongs to those attacks, which use errors when fragmented packets are reassembled. This functions as follows:

In the IP header there is a field "fragment offset" that indicates in which place the received fragment is to be assembled into the resulting IP packet. This field is 13 bits long and gives the offset in 8 byte steps, and can form an offset from 0 to 65528. With a MTU on the Ethernet of 1500 bytes, an IP packet can be made up to  $65528 + 1500 - 20 = 67008$  bytes. This can lead to an overrun of internal counters or to buffer overruns, and thus it can provoke the possibility to the aggressor of implementing own code on the victim workstation.

In this case, the Firewall offers two possibilities:

Either, the Firewall reassembles the entire incoming packet and examines its integrity, or solely the fragment which goes beyond the maximum packet size is rejected. In the first case, the Firewall itself can become the victim when its implementation was incorrect. In the second case "half" reassembled packets accumulate at the victim, which are only rejected after a certain time, whereby

a new Denial of Service attack can result thereby if the memory of the victim is exhausted.

### Teardrop

The Teardrop attack works with overlapping fragments. After the first fragment another one is sent, which overlaps completely within the first one, i.e. the end of the second fragment is located before the end of the first. If - due to the indolence of the IP stack programmer - it is simply counted "new end" - "old end" when determining the number of bytes to copy for the reassembly, then a negative value results, resp. a very large positive value, by which during the copy operation parts of the memory of the victim are overwritten and thereupon the workstation crashes.

The Firewall has again two possibilities:

Either the Firewall reassembles and rejects if necessary the entire packet, or it holds only minimum offset and maximum end of the packet and rejects all fragments, whose offset or end fall into this range. In the first case the implementation within the Firewall must be correct, so that the Firewall does not become the victim itself. In the other case "half" reassembled packets accumulate again at the victim.

### Bonk/Fragrouter

Bonk is a variant of the Teardrop attack, which targets not at crashing the attacked computer, but to trick simple port filter Firewalls, which accept also fragmented packets and thus to penetrate into the network being protected. During this attack, the UDP or TCP Header of the first fragment is overwritten by skillful choice of the fragment offset. Thereby, simple port filter Firewalls accept the first packet and the appropriate fragments while overwriting the first packet's header by the second fragment. Thus suddenly a permissible packet is created, which rather actually should be blocked by the Firewall.

Concerning this occurrence, the Firewall can itself either reassemble or filter only the wrong fragment (and all following), leading to the problems already indicated by either one of the other solutions above.

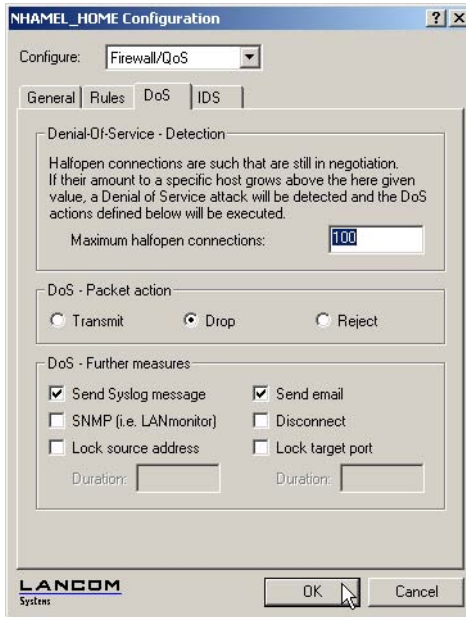


By default installation all items are configured as "secure", i.e. maximal 100 permissible half-open connections by different workstations (see SYN Flooding), at most 50 half-open connections of a single computer (see Portscan) of fragmented packets to be reassembled.

## 8.5.2 Configuration of DoS blocking

LANconfig

Parameters against DoS attacks are set in the LANconfig in the configuration tool 'Firewall/QoS' on the register card 'DoS':



In order to drastically reduce the susceptibility of the network for DoS attacks in advance, packets from distant networks may be only accepted, if either a connection has been initiated from the internal network, or the incoming packets have been accepted by an explicit filter entry (source: distant network, destination: local area network). This measure already blocks a multitude of attacks.

For all permitted accesses explicitly connection state, source addresses and correctness of fragments are tracked in a LANCOM. This happens for incoming and for outgoing packets, since an attack could be started also from within the local area network.

This part is configured centrally in order not to open a gate for DoS attacks by incorrect configuration of the Firewall. Apart from specifying the maximum number of half-open connections, fragment action and possible notification mechanisms, also these more extensive possibilities of reaction exist:

- ▶ The connection will be cut off.
- ▶ The sender address will be blocked for an adjustable period of time.
- ▶ The destination port of the scan will be blocked for an adjustable period of time.

WEBconfig, Telnet

The behaviour of the DoS detection and blocking can be configured here under WEBconfig or Telnet:

Configuration tool	Run
WEBconfig	Expert Configuration: Setup/IP Router Module/Firewall
Terminal/Telnet	Setup/IP Router Module/Firewall

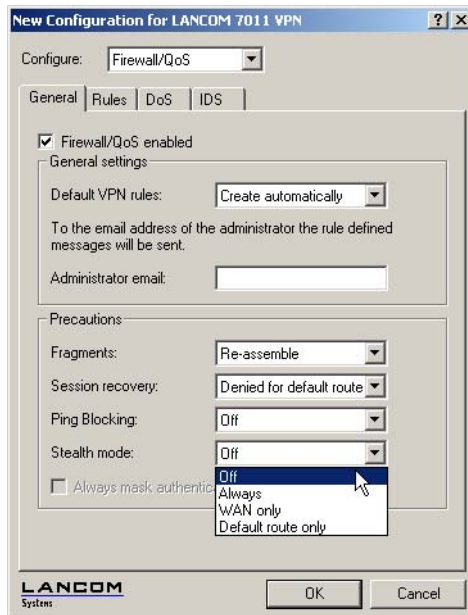
However, always active are the following protection mechanisms:

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

### 8.5.3 Configuration of ping blocking and Stealth mode

LANconfig

Parameters for ping blocking and Stealth mode can be set with LANconfig under 'Firewall/QoS' on register card 'General':



WEBconfig, Telnet      With WEBconfig or Telnet the suppression of responses can be configured here:

Configuration tool	Run
WEBconfig	Expert Configuration: Setup/IP Router Module/Firewall
Terminal/Telnet	Setup/IP Router Module/Firewall

## 9 Quality of Service

This chapter dedicates itself to quality: Under the generic term Quality of Service (short: QoS) those LCOS functions are summarized, which are concerned with the guarantee of certain service availabilities.

### 9.1 Why QoS?

The main objective of Quality of Service is to transfer certain data packets either particularly safe or as immediately as possible:

- ▶ It may happen during a data transfer that data packets are not delivered to the addressee. But for some applications it is very important that all sent packets really do arrive. An e-mail, for example, divided into several small data packets, can only be assembled together again, when all parts have arrived completely. Whether one or another packet arrives with little time delay does not make any difference. These applications often count on the connection-orientated Transmission Control Protocol (TCP). This protocol ensures that data will be transferred correctly and chronologically via the net. It automatically adjusts the sending rate downwards if the confirmation of sent data packets is outstanding for longer times, and also takes care of repeated transmission in case of packet losses.
- ▶ In other applications, e.g. telephony via the Internet (Voice-over-IP, VoIP), it is - differently to the case above - very important that the data packets arrive at the addressee with only little time delay. But it really doesn't matter if once a data packet gets lost in this case. The participant at the other end of the connection will understand the caller, even if small parts of the speech got lost. This application aims at the fastest sending of data packets as possible. The connectionless User Datagram Protocol (UDP) is often used for this kind of application. Also this protocol has very little administrative overhead. But chronological delivery of packets is not guaranteed, data packets are simply sent out. Because no confirmation receipt exists, lost packets never get delivered again.

### 9.2 Which data packets to prefer?

The necessity of a QoS concept results only from the fact that the available bandwidth is not always sufficient for transferring all pending data packets reliably and on time. Load peaks result easily from running simultaneously large FTP downloads, while exchanging e-mails and using IP telephones over the data line. In order to meet also in these situations the demands of the



desired data transfer, certain data packets must be treated preferentially. It is necessary for this, that at first a LANCOM recognizes which data packets should be preferred at all.

There are two possibilities to signal the need for a preferential treatment of data packets in the LANCOM:

- ▶ The application, as e.g. the software of certain IP telephones, is itself able to mark the data packets appropriately. This marking, the “tag”, is set within the header of the IP packets. The two different variants of this marking “ToS” and “DiffServ” can simply described assume the following states:
  - ▷ ToS “Low Delay”
  - ▷ ToS “High Reliability”
  - ▷ DiffServ “Expedited Forwarding”
  - ▷ DiffServ “Assured Forwarding”



The IP header bits of the ToS resp. DiffServ field are copied in case of a VPN route also into the enclosing IP header of the IPSec VPN packet. Thus QoS is available also for VPN routes over the Internet, as long as your provider treats according packets preferentially also in the WAN.

- ▶ When the application itself has no possibility to mark the data packets appropriately, the LANCOM can ensure the correct treatment. For this, it uses the existing functions of the firewall, which can classify e.g. data packets according to subnets or services (applications). Due to these functions it is e. g. possible to treat individually data packets of a FTP connection or those of a certain department (in a separate subnet).  
For treatment of data packets classified by the firewall the following two possibilities can be chosen:
  - ▷ Guaranteed minimum bandwidth

## ▶ Limited maximum bandwidth

**What is DiffServ?**

DiffServ stands for “Differentiated Services” and is a quite recent model to signal the priority of data packets. DiffServ is based on the known Type-of-Service(ToS) field and uses the same byte within the IP header.

ToS is using the first three bits to describe the priorities (precedence) 0 to 7, as well as four further bits (the ToS bits) to optimize the data stream (e.g. “Low Delay” and “High Reliability”). This model is rather inflexible, and this is why it has been used quite rarely in the past.

The DiffServ model uses the first 6 bits to make distinctions of different classes. Up to 64 gradings are thus possible (Differentiated Services Code Point, DSCP) which enable a finer prioritisation of the data stream:

- ▶ To ensure downward compatibility with ToS implementations, the previous precedence levels can be depicted with the “Class Selectors” (CS0 to CS7). Thereby, the level “CS0” denotes so-called “Best Effort” (BE) and stands for usual transfer of data packets without special treatment.
- ▶ The “Assured Forwarding” classes are used for a secured transfer of data packets. The first digit of the AF class describes each the priority of the transfer (1 to 4), the second digit the “drop probability” (1 to 3). Packets with AFxx marking are transferred in a secured way, and thus not dropped.
- ▶ Finally, the class “Expedited Forwarding” marks those packets, that shall be transferred preferentially, before all other packets.

Code point	DSCP bits	Dec.
CS0 (BE)	000000	0
CS1	001000	8
CS2	010000	16
CS3	011000	24
CS4	100000	32
CS5	101000	40
CS6	110000	48
CS7	111000	56

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

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

## 9.2.1 Guaranteed minimum bandwidths

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

### Full dynamic bandwidth management for sending

Concerning the sending direction, the bandwidth management takes place dynamically. This means that e.g. a guaranteed minimum bandwidth is only available, as long as the corresponding data transfer really exists.

An example:

For the transmission of VoIP data of an appropriate VoIP gateway, a bandwidth of 256 Kbps is to be guaranteed always. Thereby, each individual VoIP connection consumes 32 Kbps.

As long as nobody telephones, the entire bandwidth is at the disposal to other services. Per adjacent VoIP connection 32 Kbps less is available to other applications, until 8 VoIP connections are active. As soon as a VoIP connection is terminated, the corresponding bandwidth is available again to all other applications.



For correct functioning of this mechanism, the sum of the configured minimum bandwidth must not exceed the effectively available transmission bandwidth.

### Dynamic bandwidth management also for reception

For receiving bandwidth control, packets can be buffered and only belatedly confirmed. Thus TCP/IP connections regulate themselves automatically on a smaller bandwidth.

Each WAN interface is assigned a maximum reception bandwidth. This bandwidth will be accordingly degraded by every QoS rule that guarantees a minimum bandwidth of reception on this interface.

- ▶ If the QoS rule has been defined connection-related, the reserved bandwidth will be unblocked immediately after releasing the connection and the maximum available bandwidth will increase accordingly on the WAN interface.
- ▶ If the QoS rule has been defined globally, then the reserved bandwidth will be unblocked only after the ending of the last connection.

## 9.2.2 Limited maximum bandwidths

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

An example:

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

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

### Combination possible

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

## 9.3 The queue concept

### 9.3.1 Queues in transmission direction

Quality of Service requirements are realized in LCOS by using different queues for the data packets. For the transmission side, the following queues are utilized:

#### ▶ Urgent queue I

This queue is always processed at first before all others. The following data packets are handled here:

- ▷ Packets with ToS "Low Delay"
- ▷ Packets with DiffServ "Expedited Forwarding"
- ▷ All packets that have been assigned a certain minimum bandwidth, as long as the guaranteed minimum bandwidth is not exceeded.
- ▷ TCP control packets can be likewise dispatched by this queue preferentially (see 'SYN/ACK speedup' →page 73).

#### ▶ Urgent queue II

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

As long as the interval for the minimum bandwidth is not exceeded (i.e. up to the end of the current second), all packets in this queue are treated without further special priority. All packets of this queue, of the "secured queue" and the "standard queue" share now the existing bandwidth. The packets are taken in order from the queues when sending in exactly the same sequence, in which they have been placed into these queues. If the interval runs off, all blocks, which are at this time still in the "Urgent queue II" up to the exceeding of the in each case assigned minimum bandwidth, are placed again into the "Urgent queue I". The rest remains in the "Urgent queue II".

With this procedure it is guaranteed that prioritized connections do not crush the remaining data traffic.

▶ Secured queue

This queue does not have a separate priority. However, packets in this queue are never dropped (transmission guaranteed).

▷ Packets with ToS "High Reliability"

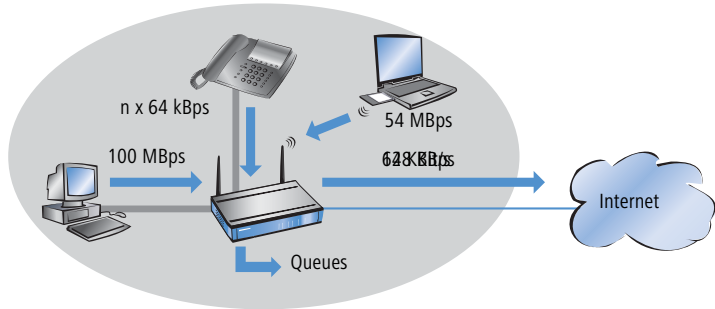
▷ Packets with DiffServ "Assured Forwarding"

▶ Standard queue

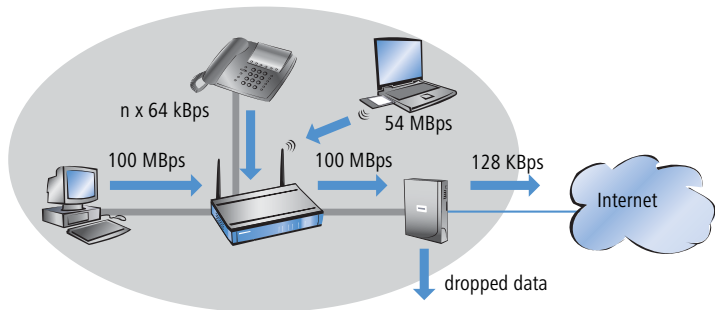
The standard queue contains all not classified data traffic. Packets in this queue are dropped at first when packets cannot be delivered fast enough.

The queue concept can, however, only work out when a "traffic congestion" of data packets has been accumulated at the interface from LAN to the WAN. Such a congestion is created when the interface within the LANCOM can submit fewer data to the WAN than data are delivered in peak periods from the LAN. This is e.g. the case, if the interface to the WAN is an integrated ADSL interface with comparatively low transmission speed ("upstream"). The integrated ADSL modem automatically reports back to the LANCOM how many

data packets it is still able to receive, and thus brakes the data stream already within the router. As a result, the queues will automatically fill up.



Different is the case, if an Ethernet interface represents the connection to the WAN. From the LANCOM's point of view, the connection to the Internet via an external broadband modem looks like an Ethernet segment. On the distance from the LANCOM to the DSL modem, data will be transferred with full LAN speed of 10 or 100 Mbps. Because of an equal input and output speed, no natural congestion will be produced then. Furthermore, the Ethernet between the LANCOM and the broadband modem does not report anything about the capacity of the connection. The consequence: a congestion will only be happen within the broadband modem. But because no queues are deployed therein, surplus data will be lost. Thus a prioritisation of "preferred" data is not possible!



To solve this problem, the transfer rate of the LANCOM's WAN interface will be reduced artificially. This interface will thereby be adjusted to the transfer rate that is available for the actual data transport towards the WAN. For a

standard DSL connection, the DSL interface is thus adjusted in the LANCOM to the appropriate upstream rate (e.g. 128 kbps).

Data rates indicated by providers are mostly likely net rates. The gross data rate, which is available for the interface is a little bit higher than the net data rate guaranteed by the provider. If you know the gross data rate of your provider, you can enter this value for the interface and slightly increase in this way the data throughput. However, with entering the net data rate you play safe in any case!

### 9.3.2 Queues for receiving direction

Apart from the data transfer rate in transmission direction, the same consideration applies also to the receiving direction. Due to its 10 or 100 Mbps Ethernet interface, the LANCOM's WAN interface is fed by clearly fewer data from the broadband modem than would actually be receiveable. All data packets received on the WAN interface are transferred to the LAN with equal rights.

In order to be able to prioritise incoming data as well, thus an artificial "brake" must be added also in this direction. Like already incorporated for the upstream direction, the data transfer rate of the interface is therefore adapted to the provider's offer in the downstream direction. For a standard DSL connection thus e.g. a downstream rate of 768 kbps applies. Again, the gross data rate can be entered here, if known.

Reducing the receiving bandwidth makes possible to treat received data packets suitably. Preferred data packets will be directly passed on to the LAN up to the guaranteed minimum bandwidth, all remaining data packets are running into congestion. This congestion produces generally a delayed confirmation of the packets. For a TCP connection, the sending server will react to this delay by reducing its sending frequency and adapting itself to the available bandwidth.

The following queues operate on the receiving side:

▶ **Deferred Acknowledge Queue**

Each WAN interface contains additionally a QoS reception queue, which takes up those packets that should be „slowed down“. The storage period of each individual packet depends on its length and on the actual permitted reception bandwidth on the receiving side. Packets with a minimum reception bandwidth assigned by a QoS rule are passing through without any further delay, as long as the minimum bandwidth is not exceeded.

▶ Standard reception queue

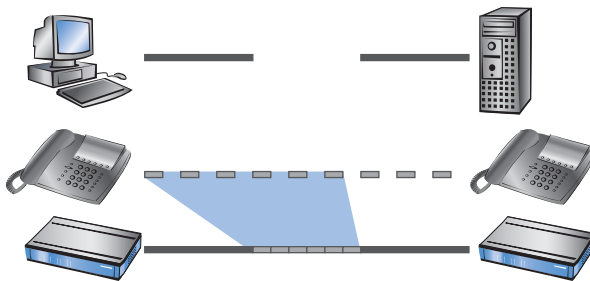
All packets that do not need special treatment because of an active QoS rule on the receiving side end up here. Packets of this queue are directly passed on resp. confirmed without consideration of maximum bandwidths.

## 9.4 Reducing the packet length

The preferential treatment of data packets belonging to important applications can be endangered - depending on the situation - by very long data packets of other applications. This is the case e.g. when IP telephony and a FTP data transfer are simultaneously active on the WAN connection.



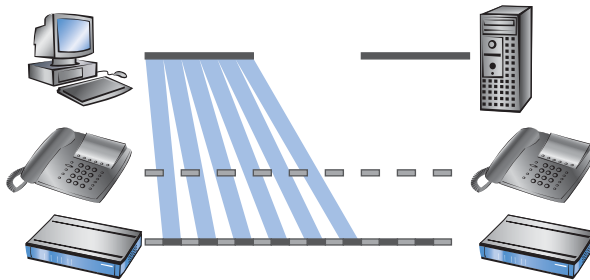
The FTP transfer uses quite large data packets of 1500 byte, whereas, the Voice over IP connection sends packets of e.g. 24 byte net in relatively short intervals. If FTP packets are in the sending queue of the LANCOM just at the moment when a VoIP packet is to be transferred, then the VoIP packet can only be sent after the line is free again. Depending on the transfer rate of the connection, this may cause a noticeable delay of the speech transmission.



This annoying behaviour can be compensated if all data packets, which are not belonging to the connection preferred by QoS, do not exceed a certain packet length. While doing so, the data packets of the FTP connection will be divided into such small sections that the time-critical VoIP connection is able to deliver the packets without noticeable delay within the required time slots.



A resulting delay has no disadvantageous effect to the TCP-secured FTP transfer.



Two different procedures exist to influence the packet length:

- ▶ The LANCOM can inform the peers of a data connection that they should only send data packets up to a certain length. Thereby, an appropriate PMTU (Path Maximum Transmission Unit) is enforced on the sending side. This procedure is called "PMTU reduction".

The PMTU reduction can be used for sending as well as for receiving direction. For the sending direction, the data source of the own LAN is adjusted with the PMTU reduction to a smaller packet size, for the receiving direction the data source of the WAN, e.g. web or FTP servers in the Internet.

Provided that the data connection already exists when the VoIP connection is started, the senders regulate packet lengths very quickly to the permitted value. When setting up new data connections while a VoIP connection is already established, the maximum permitted packet length is negotiated directly during the connection phase.



The reduced packet length on the data connection still remains also after terminating the VoIP connection, as long as the sender checks the PMTU value again.

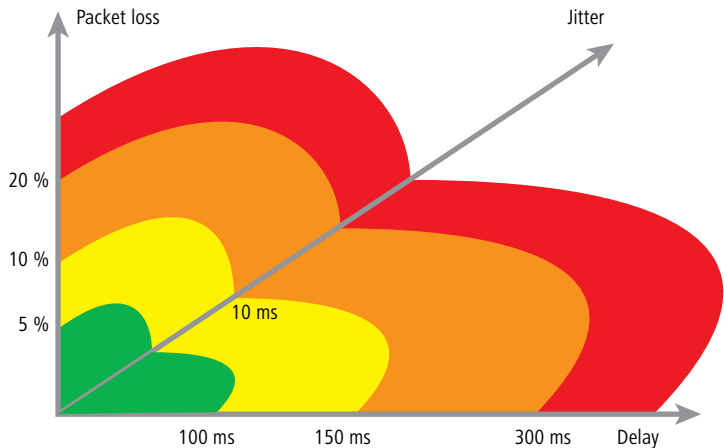
- ▶ The LANCOM is able to split packets to be sent above an adjustable maximum size (e.g. 256 byte) into smaller units itself. But such a procedure called "fragmentation" is not supported by all servers of the Internet, because dealing with fragmented packets is considered as a security risk, and therefore is turned off by many servers. That's why disturbances can occur e.g. while downloading or while transmitting web pages.

Thus, this procedure is recommended only for connections without involving unknown servers, e.g. for a direct connection of branches to their head

office via VPN connection, over which the Internet traffic is not running simultaneously.

## 9.5 QoS parameters for Voice over IP applications

An important task when configuring VoIP systems is to guarantee a sufficient voice quality. Two factors considerably influence the voice quality of a VoIP connection: The voice delay on its way from sender to addressee, as well as the loss of data packets, which do not arrive or do not arrive in time at the addressee. The "International Telecommunications Union" (ITU) has examined in extensive tests, what human beings perceive as sufficient voice quality, and has published as the result in the ITU G.114 recommendation.



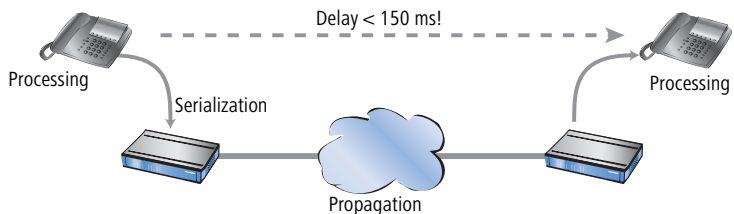
In case of a delay of not more than 100 ms, and a packet loss of less than 5%, the quality is felt like a "normal" telephone connection. In case of more than 150 ms delay and less than 10% packet loss, the telephone user perceives still a very good quality. Up to 300 ms and 20%, some listeners feel this quality like still suitable, beyond that the connection is considered as no more suitable for voice transmission.

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

Accordingly, a VoIP connection should be configured such that the criteria for good speech quality are met: Packet loss up to 10%, delay up to 150 ms and jitter up to 10ms.

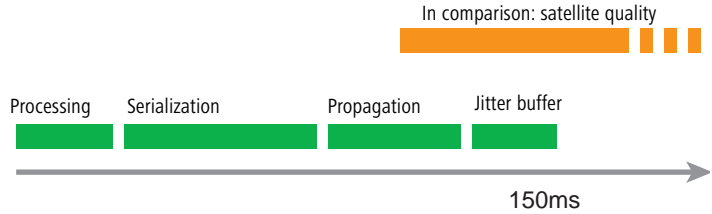
- ▶ Jitter can be removed in the receiving station by an appropriate buffer. In this buffer (jitter buffer) the packets are stored intermediately, and passed on at a constant rate to the addressee. By this intermediate buffering, the delay variations due to individual transmission times of the individual packets can be removed.
- ▶ The delay is influenced by several components:
  - ▷ Time of processing (packeting, coding and compression by the sender and the addressee), duration of handing over the packet from application to the interface (serialization), and the time for transmitting via the WAN distance (propagation) contribute to the fixed part of delay.
  - ▷ The variable part is determined by the jitter resp. by the setting of the jitter buffer.

These two parts together compose a delay, which should ideally not exceed 150 ms.



- ▶ Apart from the general loss by network transmission, the packet loss is significantly influenced by the jitter buffer. If packets arrive with a larger delay than it can be balanced by the jitter buffer, the packets will be discarded and will increase the packet loss. The larger the jitter buffer, the smaller is the loss. Conversely, the entire delay will increase with the jitter buffer size. That means for configuration, that the jitter buffer should be selected as small as the quality can be considered still as sufficient.

In detail, delay is determined especially by the codec used, the resulting packet size and the available bandwidth:



- ▶ The time for processing is determined by the used codec. For a sampling time of 20 ms, exactly each 20 ms a new packet is generated. Times for compression can mostly be neglected.
- ▶ The time for handing over the packet to the interface is defined by the quotient of packet size and available bandwidth:

	Packet size in bytes						
	1	64	128	256	512	1024	1500
56 Kbps	0,14	9	18	36	73	146	215
64 Kbps	0,13	8	16	32	64	128	187
128 Kbps	0,06	4	8	16	32	64	93
256 Kbps	0,03	2	4	8	16	32	47
512 Kbps	0,016	1	2	4	8	16	23
768 Kbps	0,010	0,6	1,3	2,6	5	11	16
1536 Kbps	0,005	0,3	0,6	1,3	3	5	8

A 512 byte packet of an FTP connection occupies the line at 128 Kbps upstream for at least 32 ms.

Besides, the packets of the VoIP connection are often much larger than the pure net payload. The additional headers of the IP and Ethernet packets, as well eventual IPsec headers have to be added as well. The net load results from the product of net data rate and sampling time of the used codec. For all codecs, each 40 bytes UDP header and at least 20 bytes for

the IPSec header must be added (RTP and IPSec headers can be larger, depending on the configuration).

Codec	Net data rate	Sampling	Packets per sec.	payload	IP packet	IPsec packet	Bandwidth
G.723.1	6,3 Kbit/s	30 ms	33,3	24 byte	64 byte	84 byte	22,3 Kbps
G.711	64 Kbit/s	20 ms	50	160 byte	200 byte	276 byte	110.4 Kbps

Since packets encrypted with DES, 3DES, or AES, are only able to grow in block sizes of 64 bytes, the IPSec packet for G.711 consists of 160 bytes payload + 96 bytes up to the next block limit + 20 bytes IPsec header = 276 bytes.

A similar “quote of loss” can also occur for the G.723 codec, if e.g. the RTP header is longer than 12 bytes. Then, the IP packet will grow up to the next block limit of 128 bytes; plus 20 bytes for the IPsec header creates packets of an overall length of 128 bytes, which means more than the sixfold net load!

The required bandwidth for transmission results finally from the quotient of packet size and sampling time.

- ▶ The time for transmission via Internet depends on the distance (about 1 ms per 200 km), and on the thereby passed routers (about 1 ms per hop). This time can be approximated by the half average ping time to the remote station.
- ▶ The jitter buffer can be adjusted directly at many IP telephones, e.g. as fixed number of packets, which should be used for buffering. The telephones load then up to 50% of the adjusted packets and begin afterwards to replay. The jitter buffer correspond therefore to half of the entered packets multiplied with the sampling time of the codec.
- ▶ Conclusion: The total delay is composed as follows for the according bandwidth, a ping time of 100 ms to the remote station and a jitter buffer of 4 packets for both codecs in this example:

Codec	Processing	Serializa-tion	Propaga-tion	Jitter buffer	Sum
G.723.1	30 ms	32 ms	50 ms	60 ms	172 ms
G.711	20 ms	32 ms	50 ms	40 ms	142 ms

The transfer time of the packets to the interface (serialization) assumes a PMTU of 512 bytes on a 128 Kbps connection. Therefore, for slower interfaces or other codecs it is eventually necessary to adjust jitter buffers and/or PMTU values.



Please notice that the bandwidths are required in the sending and receiving direction, as well as just for one single connection.

## 9.6 QoS in sending or receiving direction

For controlling data transfer by means of QoS one can select whether the according rule applies to the sending or to the receiving direction. But which direction refers to sending and receiving for a given a data transfer depends on the particular point of view. The following two variants apply:

- ▶ The direction corresponds to the logical connection setup
- ▶ The direction corresponds to the physical data transfer over the appropriate interface

The differences are unveiled by looking at a FTP transfer. A client of the LAN is connected to the Internet through a LANCOM.

- ▶ During an active FTP session, the client sends by the PORT command the information to the server, on which port the DATA connection is expected. As the result, the server establishes the connection to the client and sends the data in the same direction. In this case, the logical connection as well as the real data stream over the interface go from the server to the client, and the LANCOM takes both as the receiving direction.
- ▶ Different is the case of a passive FTP session. Here the client itself establishes the connection to the server. The logical connection setup thus is from client to server, but the data transmission over the physical interface flows in the reverse direction from server to client.

With standard settings, a LANCOM assumes the sending or receiving direction depending on the logical connection setup. Because such a point of view may not be easy to follow in certain application scenarios, the point of view can alternatively be changed to the flow of the physical data stream.



The differentiation between sending and receiving direction applies only to the installation of maximum bandwidths. For a guaranteed minimum bandwidth, as well as for fragmentation and PMTU reduc-

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

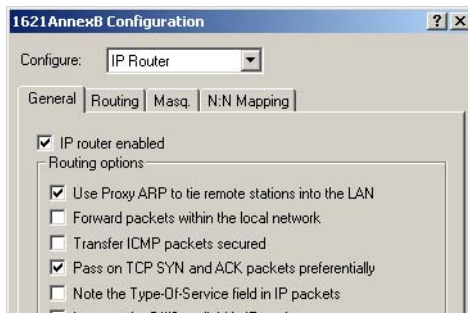
## 9.7 QoS configuration

### 9.7.1 Evaluating ToS and DiffServ fields

#### ToS or DiffServ?

LANconfig

For configuration with LANconfig, select the configuration field 'IP router'. Adjust on index card 'General' whether the 'Type of service field' or alternatively the 'DiffServ field' is to be observed for prioritisation of data packets. When both options are turned off, the ToS/DiffServ field will be ignored.



WEBconfig, Telnet

For configuration with WEBconfig or Telnet, your decision for the evaluation of the ToS or DiffServ fields are entered at the following places:

Configuration tool	Run
WEBconfig	Setup/IP router module/Routing method
Telnet	Setup/IP router module/Routing method

Feature settings for routing method values are the following:

- ▶ **Standard:** The ToS/DiffServ field is ignored.
- ▶ **TOS:** The ToS/DiffServ field is considered as ToS field, the bits "Low delay" and "High reliability" will be evaluated.

- ▶ **DiffServ:** The ToS/DiffServ field is interpreted as DiffServ field and evaluated as follows:

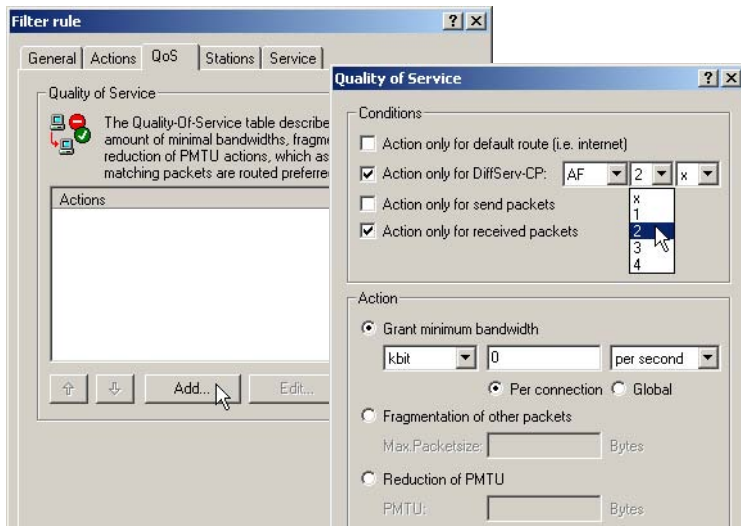
DSCP code points	Kind of transmission
CSx (including CS0 = BE)	normal transmission
AFxx	secured transmission
EF	preferred transmission

### DiffServ in Firewall rules

The code points from the DiffServ field can be evaluated by Firewall rules for further control of QoS parameters such as minimum bandwidth or PMTU reduction.

LANconfig

The parameters for evaluating the DiffServ fields are adjusted when defining the QoS rule in LANconfig:



According to your selection of the DSCP type (BE, CS, AF, EF) the valid values can be adjusted in additional drop down lists. Alternatively, the DSCP decimal value can be entered directly. A table listing valid values can be found under 'What is DiffServ?' →page 170.



WEBconfig, Telnet

For configuration with WEBconfig or Telnet, the parameters are entered at the following places into a new Firewall rule:

Configuration tool	Run
WEBconfig	Setup/IP router module/Firewall/Rule list
Telnet	Setup/IP router module/Firewall/Rule list

The Firewall rule is extended by condition “@d” and the DSCP (Differentiated Services Code Point). The code point can either be indicated with its name (CS0 - CS7, AF11 to AF 43, EF or BE) or its decimal resp. hexadecimal depiction. “Expedited Forwarding” can therefore be indicated as “@dEF”, “@d46” or “@d0x2e”. Furthermore, collective names (CSx resp. AFxx) are possible.

Examples:

- ▶ **%Lcds0 @dAFxx %A**: Accept (secured transmission) on DiffServ “AF”, limit “0”
- ▶ **%Qcds32 @dEF**: Minimum bandwidth for DiffServ “EF” of 32 kbps
- ▶ **%Fprw256 @dEF**: PMTU reduction for reception for DiffServ “EF” to 256 bytes

These examples reserve a desired bandwidth for Voice over IP phone calls. The first element “%Lcds0 @dAFxx %A” accepts DSCP “AFxx” marked packets of signalling calls. Voice data marked with “EF” is transferred preferentially by the entry “%Qcds32 @dEF”, and a bandwidth of 32 Kbps is guaranteed thereby as well. In parallel, the PMTU is reduced to 256 byte by “%Fprw256 @dEF”, which enables ensuring the required bandwidth in receiving direction at all.



Further information about defining Firewall rules can be found in chapter ‘Firewall’ →page 104.

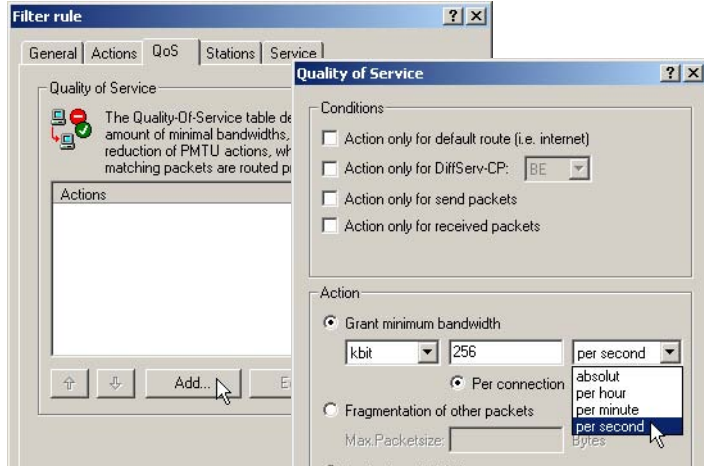
## 9.7.2 Defining minimum and maximum bandwidths

LANconfig

A minimum bandwidth for certain applications is defined in LANconfig by a Firewall rule according to the following conditions:

- ▶ The rule does not need an action, because QoS rules always implicitly assume “transfer” as action.

- ▶ The guaranteed bandwidth is defined on index card 'QoS'.



- ▶ The option 'Action only for default route' limits the rule to those packets, which are sent or received via default route.
- ▶ The option 'Action only for VPN route' limits the rule to those packets, which are sent or received via VPN tunnel.
- ▶ The option 'Per connection' resp. 'Globally' specifies, whether the minimum bandwidth set here is valid for each single connection corresponding to this rule ('per connection'), or, if this should be the upper limit for the sum of all connections together ('globally').
- ▶ Like for other Firewall rules, index cards 'Stations' and 'Services' determine for which stations in the LAN / WAN and for which protocols this rule applies.

WEBconfig, Telnet

For configuration with WEBconfig or Telnet, the minimum resp. maximum bandwidths are entered into a new Firewall rule at the following places:

Configuration tool	Run
WEBconfig	Setup/IP router module/Firewall/Rule list
Telnet	Setup/IP router module/Firewall/Rule list

A required minimum bandwidth is introduced by "%Q". Here it is implicitly assumed that the respective rule is an "Accept" action, and that the packets will thus be transmitted.

A maximum bandwidth is simply defined by a limit rule, which discards by a "Drop" action all packets, which exceed the defined bandwidth.

Examples:

- ▶ **%Qcds32**: Minimum bandwidth of 32 kbps for each connection
- ▶ **%Lgds256 %d**: Maximum bandwidth of 256 kbps for all connections (globally)



Further information about defining Firewall rules can be found in chapter 'Firewall' →page 104.

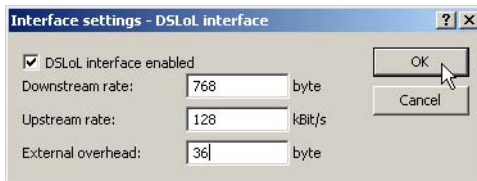
### 9.7.3 Adjusting transfer rates for interfaces



Devices with built-in ADSL/SDSL modem resp. with an ISDN adapter make these settings independently for the respective interface. For a LANCOM model with Ethernet **and** ISDN interface, these settings have to be made solely for the Ethernet interface.

LANconfig

Data rate restrictions for Ethernet, DSL and DSLoL interfaces are entered in LANconfig under configuration field 'Management' on index card 'Interfaces' within the settings for the different WAN interfaces:



- ▶ An Ethernet WAN (DSL/cable) and DSLoL interface can be switched off completely in this dialogue.
- ▶ As upstream and downstream rate the gross data rates are entered, which are usually a little bit higher than the net data rates indicated by the provider as the guaranteed data rate (see also 'The queue concept' →page 172).
- ▶ The "external overhead" considers information added to the packets during the data transfer. Concerning applications with small data packets

(e.g. Voice over IP), this extra overhead is quite noticeable. Examples for the external overhead:

Transfer	External overhead	Note
PPPoEoA	36 bytes	additional headers, loss by not completely used ATM cells
PPTP	24 bytes	additional headers, loss by not completely used ATM cells
IPoA (LLC)	22 bytes	additional headers, loss by not completely used ATM cells
IPoA (VC-MUX)	18 bytes	additional headers, loss by not completely used ATM cells
Cable modem	0	direct transfer of Ethernet packets

WEBconfig, Telnet

Under WEBconfig or Telnet the restrictions of data transfer rates for Ethernet, DSL and DSLoL interfaces are entered at the following places:

Configuration tool	Run
WEBconfig	Setup/Interfaces/DSL Interfaces
Telnet	Setup/Interfaces/DSL Interfaces

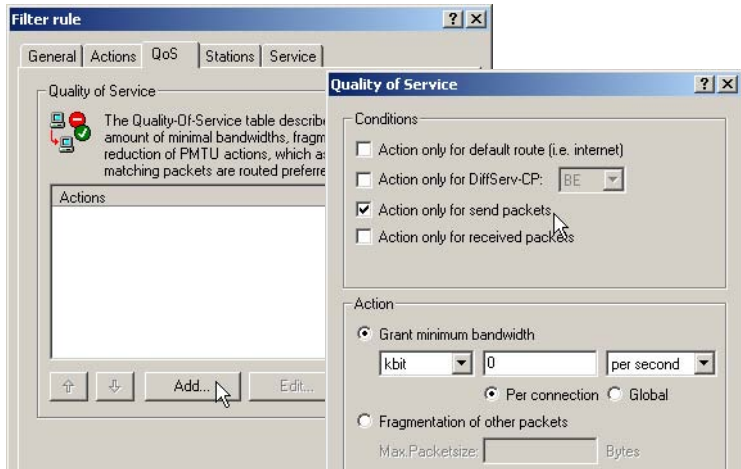


Only upstream and downstream rates are indicated by Kbps, external overhead in bytes/packet.

### 9.7.4 Sending and receiving direction

LANconfig

The interpretation of the data transfer direction can be adjusted in LANconfig when defining the QoS rule:



WEBconfig, Telnet

For configuration with WEBconfig or Telnet, the interpretation of the data transfer direction is specified at the following places in a new Firewall rule by parameters "R" for receive, "T" for transmit (send) and "W" for reference to the WAN interface:

Configuration tool	Run
WEBconfig	Setup/IP router module/Firewall/Rule list
Telnet	Setup/IP router module/Firewall/Rule list

A restriction of data transfer to 16 Kbps in sending direction applying to the physical WAN interface is e.g. made by the following Firewall rule:

▶ %Lcdstw16%d

### 9.7.5 Reducing the packet length

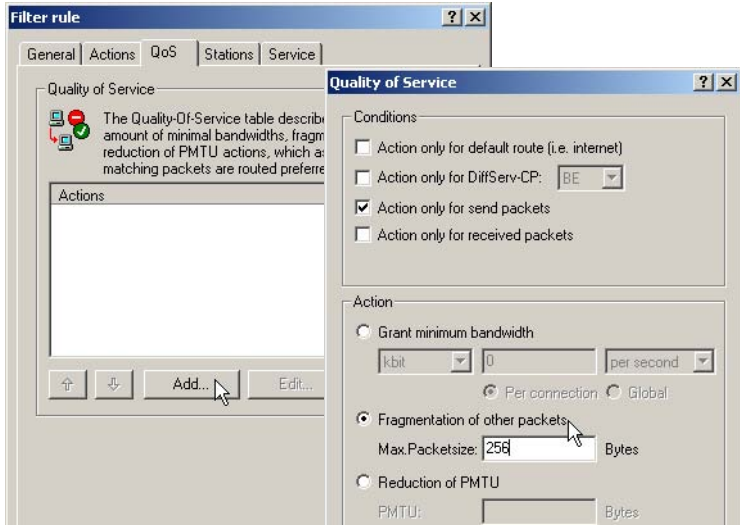
The length reduction of the data packets is defined by a Firewall rule according to the following conditions:

▶ The reduction refers to **all** packets, which will be sent to the interface and which do **not** correspond to the rule.

- ▶ Not packets of certain protocols are reduced, rather than all packets globally on that interface.

LANconfig

The length reduction of the data packets is set in LANconfig when defining the QoS rule:



WEBconfig, Telnet

For configuration with WEBconfig or Telnet, the reduction is entered at the following places in a new Firewall rule by parameter "P" for PMTU reduction (Path MTU, MTU = Maximum Transmission Unit) and "F" for the fragment size:

Configuration tool	Run
WEBconfig	Setup/IP router module/Firewall/Rule list
Telnet	Setup/IP router module/Firewall/Rule list

**i** PMTU reduction and fragmentation refer always to the physical connection. Indicating parameter "W" for WAN sending direction is not required here and hence will be ignored if existing.

The following example shows a setting for Voice over IP telephony:

Rule	Source	Destination	Action	Protocol
VOIP	IP addresses of IP telephones in the LAN, all ports	IP addresses of IP telephones in the LAN, all ports	%Qcds32 %Prt256	UDP

This rule defines the minimum bandwidth for sending and receiving to 32 Kbps, forces and reduces the PMTU while sending and receiving to packets of 256 byte size. For the TCP connection, the maximum segment size of the local workstation is determined to 216, so that the server will send packets of maximum 256 byte (reduction of the PMTU in sending and receiving direction).

## 10 Virtual LANs (VLANs)

### 10.1 What is a Virtual LAN?

The increasing availability of inexpensive layer 2 switches enables the setup of LANs much larger than in the past. Until now, smaller parts of a network had been combined with hubs. These individual segments (collision domains) had been united via routers to larger sections. Since a router represents always a border between two LANs, several LANs with own IP address ranges arose by this structure.

By using switches, it is possible to combine much more stations to one large LAN. By the specific control of data on the individual ports, the available bandwidth can be utilized much better than by using hubs, and the configuration and maintenance of routers within the network can be omitted.

But also a network structure based on switches has disadvantages:

- ▶ Broadcasts are sent like hubs over the entire LAN, even if the respective data packets are only important for a certain segment of the LAN. A sufficient number of network stations can thus lead to a clear reduction of the available bandwidth in the LAN.
- ▶ The entire data traffic on the physical LAN is “public”. Even if single segments are using different IP address ranges, each station of the LAN is theoretically able to tap data traffic from all logical networks on the Ethernet segment. The protection of individual LAN segments with firewalls or routers increases again the requirements to network administration.

One possibility to resolve these problems are virtual LANs (VLANs), as described in IEEE 802.1p/q. By this concept, several virtual LANs are defined on a physical LAN, which do not obstruct each other, and which also do not receive or tap data traffic of the respective other VLANs on the physical Ethernet segment.

### 10.2 This is how a VLAN works

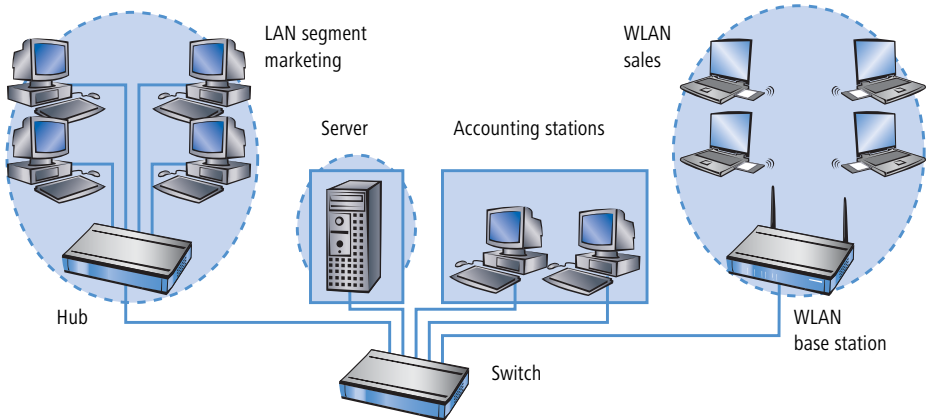
By defining VLANs on a LAN the following goals should be achieved:

- ▶ Data traffic of certain logical units should be shielded against other network users.
- ▶ Broadcast traffic should also be reduced to logical units, not bearing a burden on the entire LAN.



- ▶ Data traffic of certain logical units should be transmitted with a specific priority compared to other network users.

An example to clarify: A switch is connected to a hub within a LAN, which connects four stations from the marketing department to the network. One server and two stations of the accounting department are directly connected to the switch. The last section is the base station of a wireless network, where four WLAN clients reside from the sales department.



The stations from marketing and sales should be able to communicate with each other. Additionally, they should be able to access the server. The accounting department needs also access to the server, but should otherwise be shielded against the other stations.

### 10.2.1 Frame tagging

In order to shield or, if necessary, to prioritise data traffic of a virtual LAN against the other network users, data packets must have an additional feature (a “tag”). That’s why the respective process is also called “frame tagging”.

Frame tagging must be realized such that the following requirements are fulfilled:

- ▶ Data packets with and without frame tagging must be able to exist in parallel on a physical LAN.
- ▶ Stations and switches in a LAN, which do not support VLAN technology, must ignore the data packets with frame tagging and/or treat them as “normal” data packets.

The tagging is realized by an additional field within the MAC frame. This field contains two important information for the virtual LAN:

- ▶ **VLAN ID:** A unique number describes the virtual LAN. This ID defines the belonging of data packets a logical (virtual) LAN. With this 12 bit value it is possible to define up to 4094 different VLANs (VLAN IDs "0" and "4095" are reserved resp. inadmissible).



VLAN ID "1" is used by many devices as the Default VLAN ID. Concerning unconfigured devices, all ports belong to this Default VLAN. However, this assignment can also be changed by configuration. ('The port table' →page 199).

- ▶ **Priority:** The priority of a VLAN-tagged data packet is indicated by a 3 bit value. "0" represents the lowest priority, "7" the highest one. Data packets without VLAN tag are treated with priority "0".

This additional field makes the MAC frames longer than actually allowed. These "overlong" packets can only be recognized and evaluated by VLAN-capable stations and switches. Frame tagging incidentally leads to the desired behaviour for network users without VLAN support:

- ▶ Switches without VLAN support simply pass on these data packets and ignore the additional fields within the MAC frame.
- ▶ Stations without VLAN support are not able to recognize the protocol type due to the inserted VLAN tag and discard the packets silently.



Older switches in the LAN are perhaps not able to pass on correctly the overlong frames between the individual ports and will reject the tagged packets.

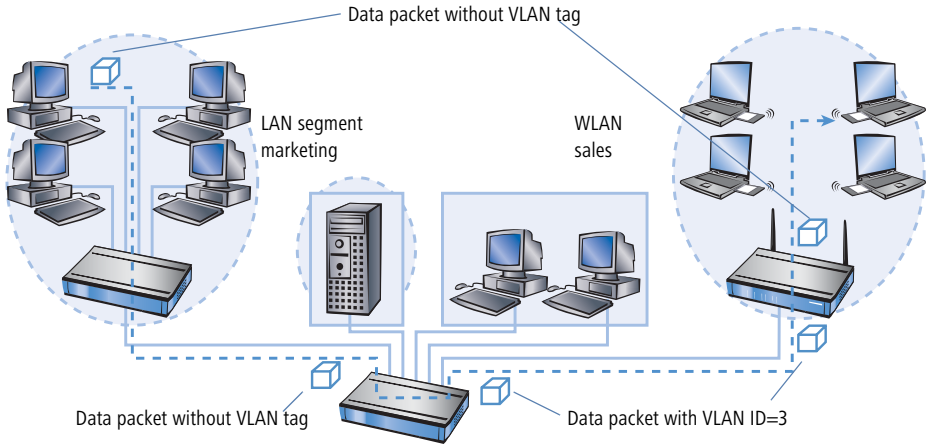
## 10.2.2 Conversion within the LAN interconnection

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

Data traffic between network users always runs over different interfaces of the distributors in the LAN. These distributors (switches, base stations) have got the task to insert VLAN tags according to the desired application into the data packets, to evaluate them and, if necessary, to remove them again. Because logical units are each connected to different interfaces of the distributors, the

rules for generating and processing of the VLAN tags are assigned to the single interfaces.

Coming back again to the first example:



A workstation from the marketing sends a data packet to a workstation of the sales department. The marketing hub passes the packet simply on to the switch. The switch receives the packet at its port no. 1, and recognizes that this port belongs to a VLAN with the VLAN ID "3". It inserts an additional field into the MAC frame with the appropriate VLAN tag, and issues the packet only on ports (2 and 5), which also belong to VLAN 3. The base station of the sales department will receive the packet on its LAN interface. By its settings, the base station can recognize that the WLAN interface belongs also to VLAN 3. It will remove the VLAN tag from the MAC frame, and issues the packet again on the wireless interface. The WLAN client can handle the packet then, which has a "usual" length again, like each other data packet without VLAN tagging.

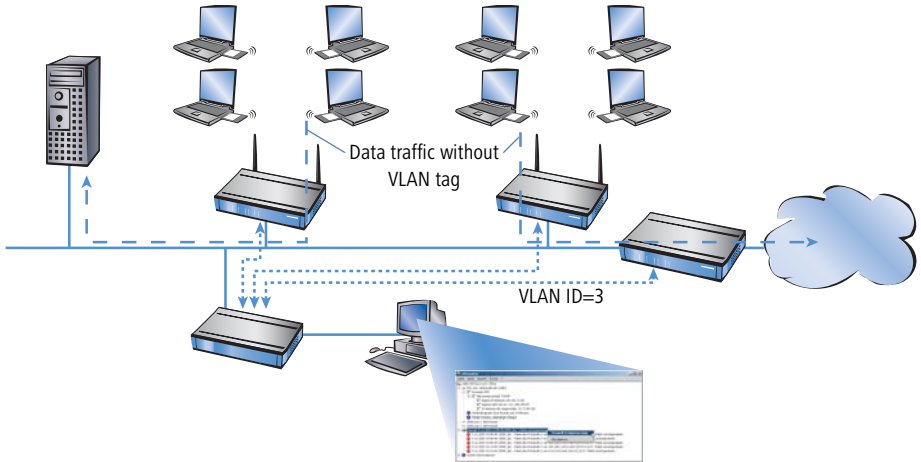
### 10.2.3 Application examples

Main application of virtual LANs is to install different logical networks on a physical Ethernet segment, whose data traffic is protected against the other logical networks.

The following sections present examples for the operation of virtual LANs on behalf of this background.

### Management and user traffic on a LAN

Several hot spots are installed on an university campus, so that students equipped with notebooks and WLAN cards have access to the Internet and to the server of the library. The hot spots are connected to the university LAN. Via this LAN the administrators also access the base stations to carry out several management tasks via SNMP.

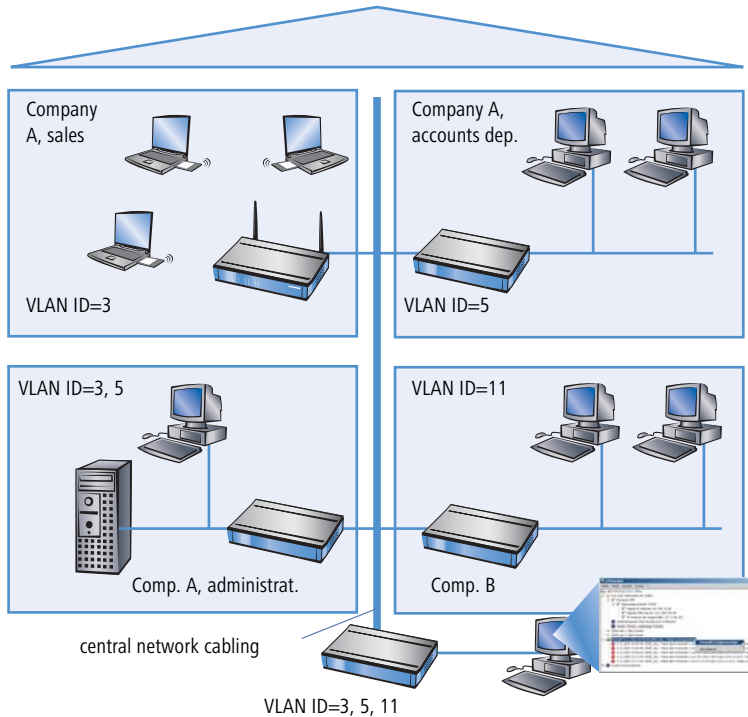


By setting up a virtual LAN between the base stations and the administrator's switch, management data is shielded against all "public" traffic on the LAN.

### Different organisations on one LAN

The flexibility of the modern world of work raises new challenges for administrators concerning planning and maintenance of network structures. The occupation of the rooms by leaseholders changes permanently in public office buildings, and also inside of a company, teams are often newly assembled. In both cases, the individual units must have an independent, protected LAN.

But this task is very burdensome to realize by hardware changes, or even not at all, because e.g. only one single central cabling exists in the office building.



Virtual LANs enable to perform this task in a very smart way. Also when departments or companies change at a later time inside of the building, the network structure can be easily adjusted.

All network users in this example use the central Ethernet, which is, like the connected devices, supervised by a service provider. Company A has three departments on two floors. The sales department can communicate with the administration department via VLAN ID 3, the accounts department with the administration via VLAN ID 5. The networks of accounts department and sales do not see each other. Company B is also shielded by VLAN ID 11 against all other networks, only the service provider can access all devices for maintenance purposes.

## 10.3 Configuration of VLANs



VLAN technology functions are presently only supported by LANCOM Wireless devices.

The configuration of LANCOM Wireless devices within the VLAN realm has to perform two important tasks:

- ▶ Defining virtual LANs and assigning them a name, a VLAN ID and the affected interfaces.
- ▶ Defining for the interfaces how to proceed with data packets with or without VLAN tags.

### 10.3.1 The network table

In the network table are those virtual LANs defined, in which the LANCOM should participate. The table contains 32 entries at maximum with the following information:

- ▶ **Name:** The VLAN name serves only as a description during configuration. This name is used at no other place.
- ▶ **VLAN ID:** This number marks the VLAN unambiguously. Possible values range from 1 to 4094.
- ▶ **Port list:** All LANCOM interfaces belonging to the VLAN are entered into this list. As ports can be entered:
  - ▷ “LAN-n” for all Ethernet ports of the device.
  - ▷ “WLAN-n” for point-to-station WLAN ports.
  - ▷ “P2P-n” for point-to-point WLAN ports.

Given a device with a LAN interface and a WLAN port, e.g. ports “LAN-1” and “WLAN-1” can be entered. In case of port ranges, the individual ports must be separated by a tilde: “P2P-1~P2P-4”.



The available ports can be found in the port table (→page 199).

Example for a network table:

Name	VLAN ID	Port list
Default	1	LAN-1, WLAN-1, WLAN-2
Sales	2	LAN-1, WLAN-1
Marketing	3	LAN-1, WLAN-2

### 10.3.2 The port table

The port table configures the individual ports of the device for use by the VLAN. The table has got an entry for each port of the device with the following values:

- ▶ **Port:** Name of the port, not editable.
- ▶ **Use tagging:** This option indicates, whether data packets should be tagged on this port. The tagging refers only to data packets **sent** over this port.
- ▶ **Allow untagged frames:** This option indicates, whether untagged data packets are passed on, which have been **received** on this port.
- ▶ **Allow all VLANs:** This option indicates, if tagged data packets with any VLAN IDs should be accepted even if the port itself is not belonging to the same VLAN ID.
- ▶ **Default ID:** This VLAN ID has two functions:
  - ▷ Untagged packets received on this port are provided with this VLAN ID.
  - ▷ If tagging for sent packets is switched on, this VLAN ID will **not** be assigned to the packets. If a packet with this VLAN ID is received, it will be passed on **without** this ID, although tagging has been switched on.

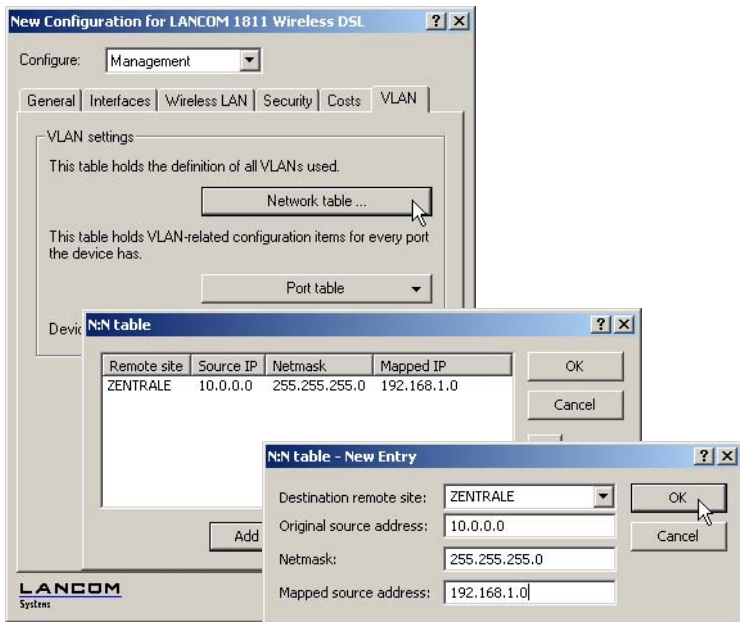
Example for a port table:

Port	Use tagging	Allow untagged frames	Allow all VLANs	Default ID
LAN-1	On	On	On	1
WLAN-1	Off	On	Off	1
WLAN-2	Off	On	Off	1
P2P-1	Off	On	Off	1

Port	Use tagging	Allow untagged frames	Allow all VLANs	Default ID
P2P-2	Off	On	Off	1
P2P-3	Off	On	Off	1
P2P-4	Off	On	Off	1
P2P-5	Off	On	Off	1
P2P-6	Off	On	Off	1

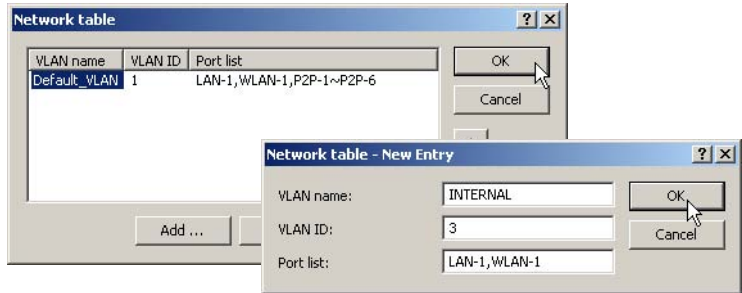
### 10.3.3 Configuration with LANconfig

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

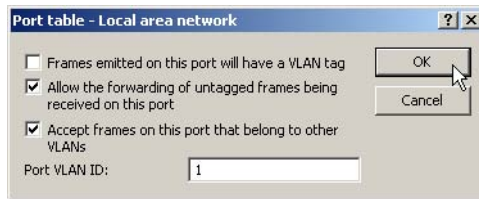




The definition of the used virtual networks can be accessed via the button **VLAN table** :



The button **Port table** opens a drop down list where a VLAN port can be selected for editing:

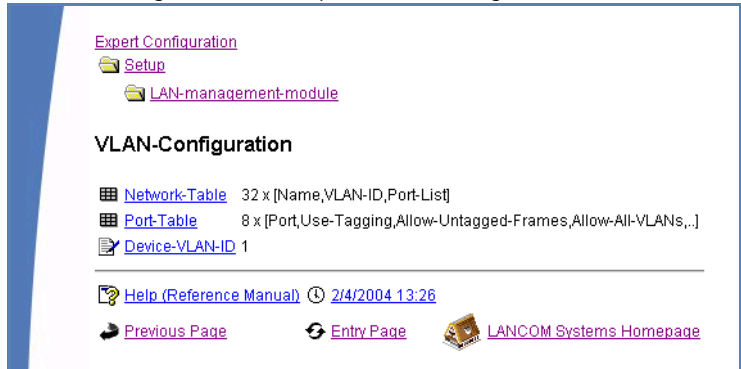


### 10.3.4 Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet the tables for configuring the VLANs can be found via the following paths:

Configuration tool	Menu/table
WEBconfig	Expert Configuration ▶ Setup ▶ LAN Management module ▶ VLAN Configuration
Terminal/Telnet	cd /Setup/LAN Management module/VLAN Configuration

The VLAN configuration shows up under WEBconfig as follows:



The screenshot displays the 'Expert Configuration' section of the LANCOM WEBconfig interface. It shows a navigation tree with 'Setup' and 'LAN-management-module' expanded. The 'VLAN-Configuration' section is active, listing three configuration items: 'Network-Table' (32 x [Name,VLAN-ID,Port-List]), 'Port-Table' (8 x [Port,Use-Tagging,Allow-Untagged-Frames,Allow-All-VLANs,..]), and 'Device-VLAN-ID' (1). Below the list, there are links for 'Help (Reference Manual)' with a timestamp of '2/4/2004 13:26', 'Previous Page', 'Entry Page', and 'LANCOM Systems Homepage' with a small icon.

Expert Configuration


- Setup
  - LAN-management-module

### VLAN-Configuration

- Network-Table 32 x [Name,VLAN-ID,Port-List]
- Port-Table 8 x [Port,Use-Tagging,Allow-Untagged-Frames,Allow-All-VLANs,..]
- Device-VLAN-ID 1

---

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

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

# 11 Wireless LAN – WLAN

## 11.1 What is a Wireless LAN?



The following sections are a general description of the LCOS operating system functions in wireless networks. The precise functions supported by your device are described in its manual.

In this chapter we will show you briefly the technology of wireless networks. In addition, we give you an overview of the various applications, functions and abilities of your base station.

A Wireless LAN connects single terminals (e.g. PCs or notebooks) to a local network (also LAN – **L**ocal **A**rea **N**etwork). In contrast to a conventional LAN, communication takes place via radio links rather than via network cables. This is the reason why a Wireless LAN is also called a **W**ireless **L**ocal **A**rea **N**etwork (WLAN).

All functions of a cable-bound network are also available in a Wireless LAN: access to files, servers, printers etc. is as possible as the connection of individual stations to an internal mail system or to the Internet access.

The advantages of Wireless LANs are obvious: notebooks and PCs can be set up just where they are needed. Due to Wireless LANs, problems with missing connections or structural alterations belong to the past.

### 11.1.1 Standardized radio transmission by IEEE

IEEE 802.11

LANCOM network products comply with the IEEE 802.11 standards. These standard's family represents an extension to the already existing IEEE standards for LANs, of which IEEE 802.3 for Ethernet is the most popular one. Within the IEEE 802.11 family, different standards exist for the radio transmission in different frequency ranges and with different speeds. LANCOM base stations and AirLancer client adapters support according to their respective type different standards:

- ▶ IEEE 802.11a with up to 54 Mbps transfer rate in the 5 GHz band
- ▶ IEEE 802.11b with up to 11 Mbps transfer rate in the 2,4 GHz band
- ▶ IEEE 802.11g with up to 54 Mbps transfer rate in the 2,4 GHz band

**IEEE 802.11a: 54 Mbps**

IEEE 802.11a describes the operation of Wireless LANs in the 5 GHz frequency band (5,15 GHz to 5,75 GHz), with up to 54 Mbps maximum transfer rate. The real throughput depends however on the distance and/or on the quality of the connection. With increasing distance and diminishing connecting quality, the transmission rate lowers to 48 Mbps, afterwards to 36 Mbps etc., up to a minimum of 6 Mbps. The distance of transmission ranges from up to 125 m in open expanses, in buildings typically up to 25 m. The IEEE 802.11a standard uses OFDM (Orthogonal Frequency Division Multiplexing) as modulation scheme.

OFDM

In the 5 GHz frequency band, the OFDM modulation scheme is used for IEEE 802.11a. OFDM is a modulation scheme, which utilizes multiple independent carrier frequencies for the signal transmission, and which modulates these multiple carriers each with a reduced data transfer rate. Thus the OFDM modulation scheme is very insensitive in particular to echoes and other impairments and enables high data transfer rates.

Turbo mode

In 'turbo mode', LANCOM Wireless base stations are able to use simultaneously two radio channels and can so increase the transfer rate up to maximum 108 Mbps. The turbo mode can be used in conjunction with the IEEE 802.11a standard between LANCOM base stations and AirLancer wireless network cards. The increase of the transfer rate must be switched on in the base station, but can also reduce the transmitting power and the range of the radio connection.

**IEEE 802.11b: 11 Mbps**

IEEE 802.11b describes the operation of local Wireless LANs in the ISM frequency band (Industrial, Scientific, Medical: 2.4 up to 2.483 GHz). The maximum transfer rate is up to 11 Mbps. The real throughput depends however on the distance and/or on the quality of the connection. With increasing distance and diminishing connecting quality the transmission rate lowers to 5,5 Mbps, afterwards to 2 and finally to 1 Mbps. The range of the transmission distances is between up to 150 m in open expanses and in buildings typically up to 30 m. Due to different frequency bands in use, IEEE 802.11b is not compatible to IEEE 802.11a.

DSSS

For shielding against interferences by other transmitters, which have possibly the same frequency band, the DSSS procedure (Direct Sequence Spread Spectrum) is used for IEEE 802.11b in the 2,4 GHz frequency band. A transmitter normally uses only a very narrow range of the available frequency band for

transmission. If exactly this range is used by another transmitter, interferences in transmission would be the result. With the DSSS procedure the transmitter uses a broader spread of the possible frequencies and becomes more insensitive to narrow-band disturbances then. This procedure is also used in military range for increasing tap-proof security.

### **IEEE 802.11g: 54 Mbps**

The IEEE 802.11g standard works likewise with up to 54 Mbps data transmission rate in the 2,4 GHz ISM-frequency band. Contrary to IEEE 802.11b, the OFDM modulation is used for IEEE 802.11g, like already introduced for IEEE 802.11a. IEEE 802.11g contains a special compatibility mode that ensures a downward compatibility to the popular IEEE 802.11b standard. However, in this compatibility mode you encounter reduced transmission speeds. Due to the different frequency bands, IEEE 802.11g can not be compatible to IEEE 802.11a. The transmission distances of IEEE 802.11g products are comparable with those of IEEE 802.11b products.

Turbo mode

The 'Turbo Mode' increases the transfer rates to a maximum of 108 Mbps with the 802.11g standard, too.

### **Transfer rates**

The indicated transfer rates are always to be interpreted as gross data rates, i.e. the entire protocol overhead - as for example the complex protocols to secure the radio transmission - is included in the indicated transfer rates. The net data transfer rate can be thus lower than the indicated gross data rates, typically over up to the half for all IEEE 802.11 standards mentioned above.

### **Ranges**

The actually obtained distances for radio transfers depend strongly on the individual environment. In particular influences of noise and obstacles have an effect on the range. Decisive is an optimal placement of the radio stations (both network adapters and base stations). For further increase of the transfer distance, we recommend the operation with additional antennas (e.g. AirLancer Extender).

### **IEEE standards**

In order to guarantee a maximum of compatibility, LANCOM Systems fully complies with the industry standards of the IEEE<sup>1</sup> described in the preceding paragraph. For this reason, your LANCOM base station operates without problems and with reliably also with devices of other manufacturers.

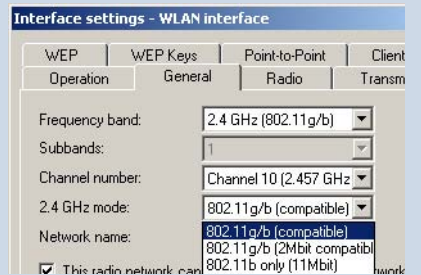
Your LANCOM base station supports - according to the model type - the standards IEEE 802.11g (downward-compatible to IEEE 802.11b), and/or IEEE 802.11a.

The operation of the integrated wireless card of your base station is only possible in one single frequency band, that is, either 2,4 GHz or 5 GHz. Thus a simultaneous operation of IEEE 802.11g and IEEE 802.11a is not possible. Since IEEE 802.11g is downward-compatible to IEEE 802.11b, an simultaneous operating of these two standards is possible, but with certain speed constraints.

### Transfer rates in compatibility mode

Please notice that the reached data transfer rates depend on the used 2,4 GHz mode. You will achieve the highest transfer rates with a base station operating in the 802.11g mode. The transfer rate will go down when starting the compatibility mode, even, if only inactivated 802.11b stations are near to your base station. When these 802.11b stations start to be activated in a wireless network with operating compatibility mode, the actual transfer rate will fall again.

That's why you should only activate the compatibility mode, when you have really operating 802.11b and 802.11g stations in your wireless network.



Please notice that not all frequencies are permitted in each country! You will find a table with the allotted frequencies and the permission regulations in the appendix.

## 11.1.2 Operation modes of Wireless LANs and base stations

Wireless LAN technology and base stations in Wireless LANs are used in the following operation modes:

- ▶ Simple direct connections between terminals without base station (ad-hoc mode)

1. Institute of Electrical and Electronic Engineers – International association, which established i.a. numerous technology standards.

- ▶ Larger Wireless LANs, connection to LANs with one or more base stations (infrastructure network)
- ▶ Connecting two LANs via a direct radio link (point-to-point mode)
- ▶ Connecting of devices with Ethernet interface via base stations (client mode)
- ▶ Extending an existing Ethernet network with WLAN (bridge mode)
- ▶ Multiple radio cells with one access point (Multi-SSID)

Application examples:

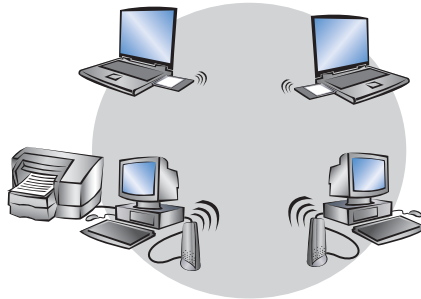
- ▶ Setting-up of an Internet access for WLAN clients
- ▶ Passing-through of VPN-encrypted connections with VPN pass-through

### The ad-hoc mode

When two terminals are equipped with compatible wireless interfaces, they both can communicate directly via radio. This simplest use is the so-called ad-hoc mode.

In ad-hoc networks you connect two or more PCs with own wireless interfaces directly together for building a Wireless LAN.

Only in IEEE  
802.11b or IEEE  
802.11g standard



This operation mode is generally called peer-to-peer network (spontaneous network). PCs can immediately get in touch and exchange data.

### The infrastructure network

By use of one or more base stations (also called access point), a Wireless LAN becomes more comfortable and more efficient. A Wireless LAN with one or more base stations is referred to as an infrastructure network in Wireless LAN terminology.

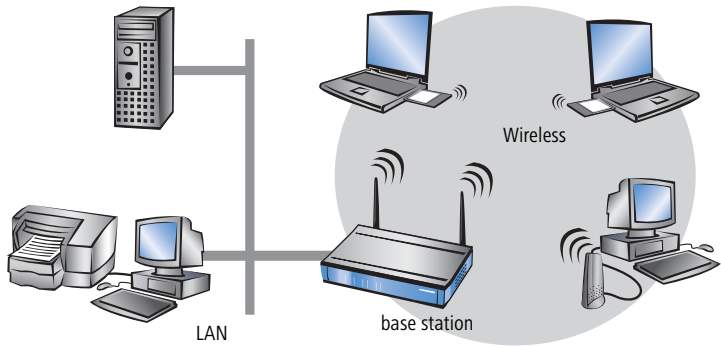
Interesting applications arise for the Wireless LAN from the LAN connection of base stations:

- ▶ Connecting the Wireless LAN to an existing LAN
- ▶ Extending the coverage of a Wireless LAN

Additionally, the use of a base station enables a central administration of the Wireless LAN.

Connection to an existing LAN

An infrastructure network is ideally suitable as an extension to existing wired LANs. For extension of a LAN in areas, where a wiring is not possible or uneconomical, the infrastructure network represents an ideal alternative.

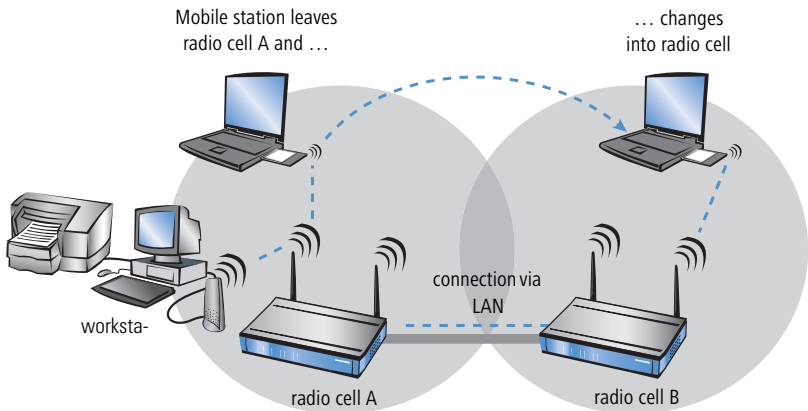


Larger extension by roaming function

The area, in which mobile stations can get in touch with a base station, is called radio cell.

If the range of a radio cell is not sufficient any longer to serve all mobile stations of a wireless network, several base stations can be brought in action. It is possible to change from a radio cell into another one without interruption of the network connection. The transmission of roaming information and data between the base stations is enabled by the wired LAN connection.





In the example above, the roaming function of the mobile station enables the access to the workstation in radio cell A also after changing into radio cell B. After the radio cell change, the base station in radio cell B passes on the data of the mobile station via LAN to the base station in radio cell A. From there, they arrive via radio at the workstation in radio cell A. In this way, the connection between both devices remains existing at any time.

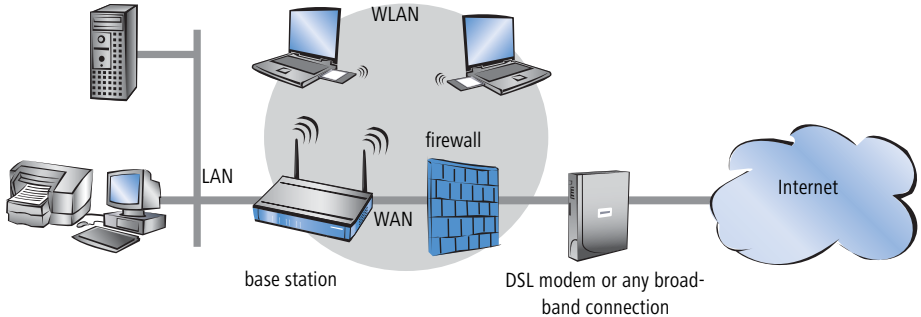
A Wireless LAN can consist of as many as desired radio cells. Thus the extension of a Wireless LAN is unlimited.

### Base station as router

The LANCOM Wireless base station possesses a WAN connector for all current broadband modems with cable-bound Ethernet connection (DSL or cable modem). In this operation mode, the base station offers all functions of a complete IP and IPX router as well. The base station serves in this connection variant as gateway to the Internet. The router checks for all received data packets whether they need to be transferred to another network or workstation. The router itself establishes the connections as required.

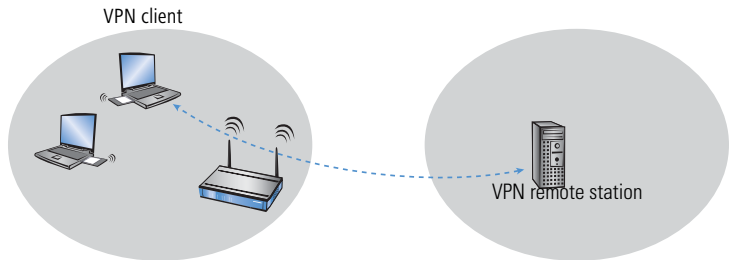
The integrated Stateful Inspection Firewall prevents effectively the penetration of undesired data traffic into the own network by permitting incoming data only as reaction to outgoing data traffic. For accessing the Internet, the IP masquerading function of the router hides all workstations of the LAN behind a single public IP address. The real identities (IP addresses) of the individual workstations remain concealed. Firewall filters of the router permit specific IP addresses, protocols and ports to be blocked. With MAC address filters it is

also possible to specifically control the access of workstations in the LAN to the IP routing function of the device.



### VPN pass-through

VPN technology (VPN=Virtual Private Network) is more and more frequently in use to protect sensitive data. The LANCOM Wireless DSL base station is able to route and mask simultaneously the encrypted data between a VPN client of the WLAN and another workstation of the cable-bound LAN. This “passing-through” of VPN encrypted data is called in technical jargon “VPN pass-through”.

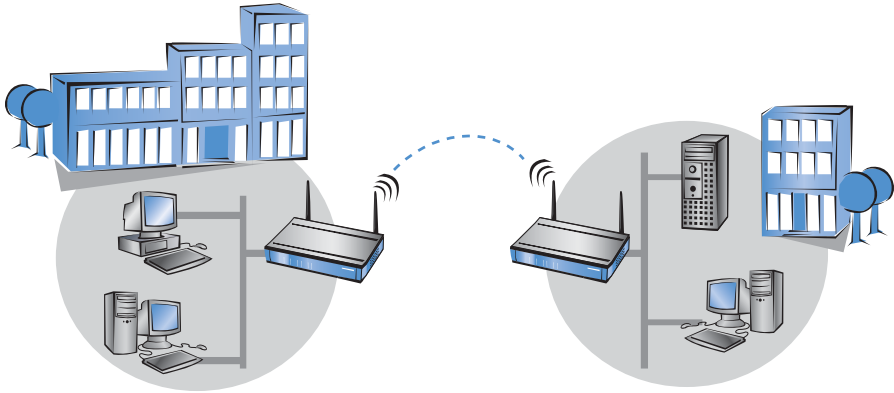


The LANCOM Wireless DSL base stations support VPN pass-through function for multiple stations within a wireless network.

### Wireless bridge between two Ethernet segments

With two base stations, two LANs can be connected via a radio link (point-to-point mode). In this so-called bridge mode, all data is transferred automatically to the remote network.

By the use of narrow beam antennas (e.g. AirLancer Extender), also larger distances can be bridged securely. An additional increase of reach can be achieved by use of further base stations, which operate in relay mode between two LAN segments.

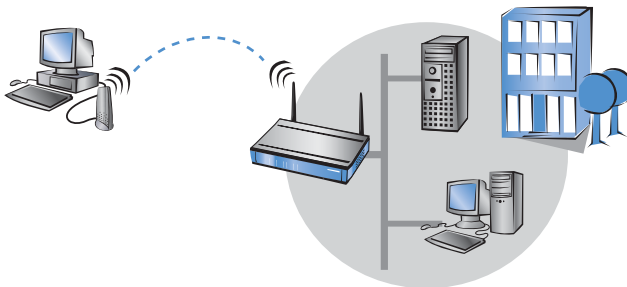


Point-to-multipoint operation

It is possible to couple up to seven remote network segments to an united network by wireless bridges in the so-called P2MP operation (point-to-multipoint) mode.

Point-to-station operation

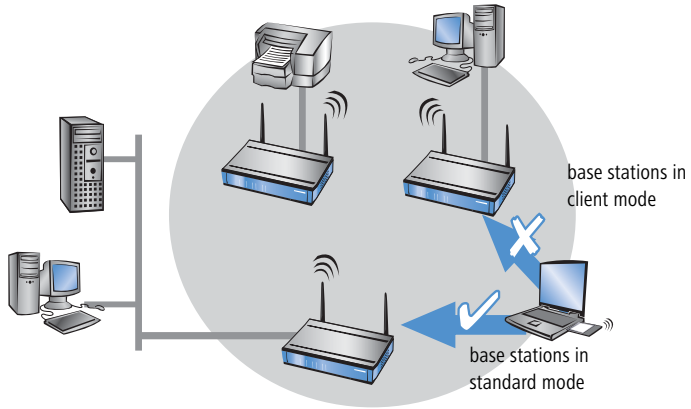
The so-called P2Station operation (point-to-station) connects a single station is to a remote LAN.



**Base station in client mode**

For binding single devices with Ethernet interfaces to a Wireless LAN, LANCOM Wireless base stations can be put into the so-called client mode, in which they behave like a conventional Wireless LAN adapter and not like a

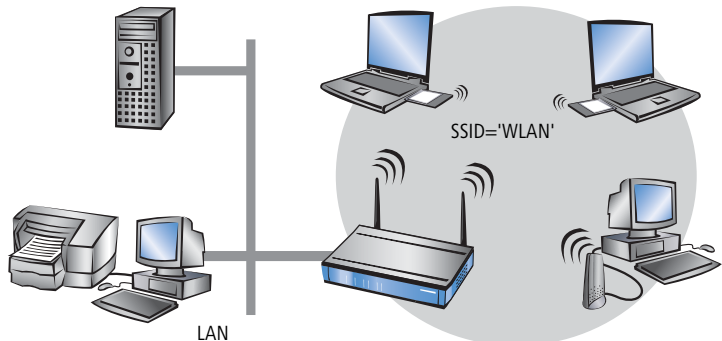
base station. Due to the client mode, it is also possible to integrate devices like PCs or printers having only one Ethernet interface into a Wireless LAN.



### Multiple radio cells with Multi-SSID

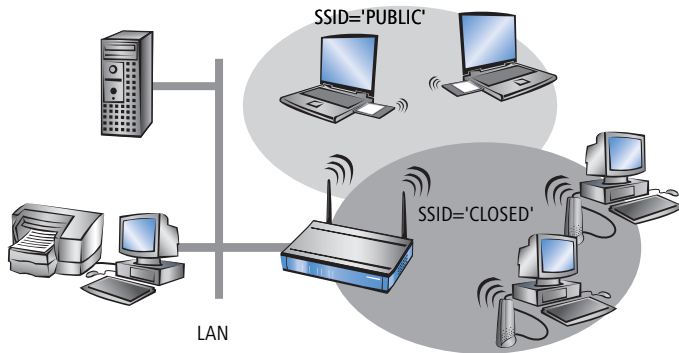
Conventionally, a wireless network card supports exactly one radio cell.

These radio cells are given a network name, known as the 'SSID' (**S**ervice **S**et **I**dentifier), that is entered into the access points and network cards during configuration. Certain settings that apply to the radio cell can be defined under the SSID during the configuration of the access point. The settings include, for example, the data transfer speed and the first WEP key, which is also used as passphrase for encryption with 802.11i and WPA. Those clients that are programmed with the SSID can make use of the radio cell and work with the parameters as defined. The access point treats all clients on an equal basis



In some applications, however, it may be desirable to divide the clients the radio cell into different groups, each of which is treated in a certain way by the access point. It may be necessary, for example, to operate a public wireless network without any encryption simultaneous to a protected, WPA- or WEP-encrypted wireless network that excludes unauthorised parties.

The Multi-SSID function of the LANCOM access points is ideally suited to scenarios like this. This function enables a physical WLAN interface of an access point to be assigned with more than one SSID. Up to eight different logical radio cells—each with its own SSID—can be supported by a single WLAN interface.



## 11.2 Developments in WLAN security

The WLAN standards WPA and 802.11i are currently redeeming the reputation of WLAN security, an issue which has recently been under attack. The processes incorporated into the original standard proved insufficient in practice. This lack led on the one hand to a series of proprietary extensions of the standard, like "CKIP" from Cisco, or "KeyGuard" from Symbol Technologies, and on the other hand to solutions which offered the required security on higher protocol layers with tools like PPTP or IPSec. All these processes are quite functional, but they introduce limitations, for instance those relative to interoperability or data transmission rates.

In the recently released standard 802.11i, the IEEE Committee has redefined the topic "WLAN and security" from the ground up. The result is a set of standardised methods that enable the construction of secure and manufacturer-independent WLANs in line with current standards.

On the way from the original WEP of the 802.11 standard to 802.11i, a whole series of concepts have arisen that have tended to increase confusion and insecurity among the users. This document should help to explain the concepts and the processes used, in chronological order of their development.

### 11.2.1 Some basic concepts

Even though one constantly hears the blanket term 'Security' when talking about computer networks, it is still important for the coming exposition to differentiate a little more closely between the requirements it actually entails. The first point in security is access security:

- ▶ Here, a protective mechanism is involved which allows access to the network only to authorised users.
- ▶ On the other hand, however, it must also be ensured that the client is connected to the precise desired access point, and not with some other access point with the same name which has been smuggled in by some nefarious third party. Such an authentication can be provided, for example, using certificates or passwords.
- ▶ Once access is provided, one would like to ensure that data packets reach the receiver without any falsification, that is, that no-one can change the packets or insert other data into the communication path. The manipulation of data packets themselves cannot be prevented, but changed packets can indeed be identified using suitable checksum processes, and then discarded.

Quite separate from access security is confidentiality, that is, unauthorised third parties must not be able to read the data traffic. To this end, the data are encrypted. This sort of encryption process is exemplified by DES, AES, RC4, or Blowfish. Along with encryption, of course, there must also be a corresponding decryption on the receiving end, generally with the same key (a so-called symmetric encryption process). The problem naturally then arises, how the sender can give the key to the receiver for the first time—a simple transmission could very easily be read by a third party, who could then easily decrypt the data traffic.

In the simplest case, this problem is left to the user, that is, one simply assumes that the user can make the key known at both ends of the connection. In this case, one speaks of pre-shared keys, or 'PSK'.

More sophisticated processes come into play when the use of pre-shared keys is impractical, for instance in an HTTP connection built over SSL—in this case, the user can't retrieve a key from a remote web server quite so easily. In this

case, so-called asymmetric encryption methods such as RSA can be used, that is, to decrypt the data, a different key is used than the one used to encrypt it. Such methods are, however, much slower than symmetric encryption methods, which leads to a two-phase solution: one side possesses an asymmetric key pair and transmits the encryption key to the other side, generally as a part of a certificate. The other side chooses an arbitrary symmetric key, and encrypts this symmetric key with the asymmetric key previously received. The owner of the asymmetric key pair can now decrypt it, but a potential eavesdropper cannot—the aim of the secure key exchange is achieved.

In the following sections, we will see these methods again, sometimes in modified form.

### 11.2.2 WEP

WEP is an abbreviation for **W**ired **E**quivalent **P**rivacy. The primary goal of WEP is the confidentiality of data. In contrast to signals which are transmitted over cables, radio waves spread out in all directions—even into the street in front of the house and other places where they really aren't desired. The problem of undesired interception is particularly obvious in wireless data transmission, even though it can also arise in larger installations with wired networks—however, access to cables is far more easily restricted than is the case with radio waves.

During the development of the WLAN security standard, the IEEE Committee did not intend to develop a "perfect" encryption method. Such high-security encryption methods are, for instance, required and also used in electronic banking—in this case, however, the applications themselves use high-quality encryption methods, and it would be unnecessary to repeat this effort at the radio transmission level. With the new security standards, only those applications which normally work without encryption in wired LANs should be provided with sufficient security against eavesdropping by unauthorised third parties.

Figure 1 shows the process of WEP encryption—decryption runs in precisely the opposite manner. WEP is therefore a symmetrical encryption method. WEP uses RC4 algorithm as its basic encryption technology, a process already well-known in other areas and considered highly secure. RC4 uses a key between 8 and 2048 bits in length, which is used to generate a pseudo-random series of bytes using a predetermined process. The data packet is then XOR'd byte by byte with this byte stream. The receiver simply repeats this process with the same key and thus with the same sequence, in order to retrieve the original

data packet—a double application of the XOR operation with the same values cancels out.

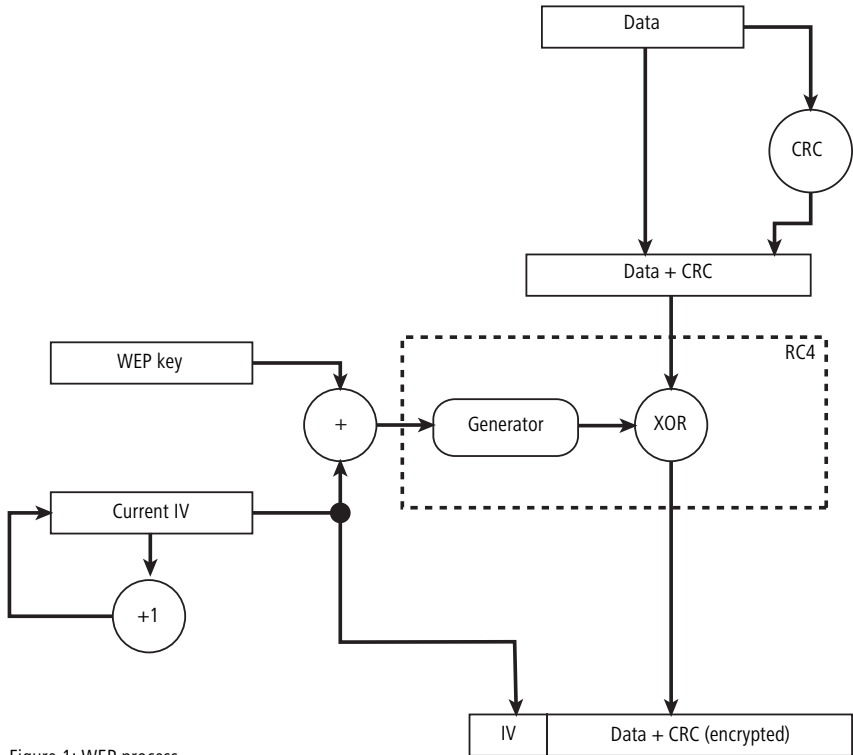


Figure 1: WEP process

The advantage of RC4 is that the operations

- ▶ generation of the byte sequence from the key
- ▶ XOR operation on the data stream

on the sending and receiving sides are identical—so the hardware need only be built into the WLAN card once, and then can be used for both transmission and receiving. Since the data in the WLAN are transmitted half-duplex only, simultaneous transmission and receiving will never occur. However, RC4 has one serious disadvantage: one may only use a particular RC4 key once for a single packet! If the same RC4 key is used for two different data packets, then a potential eavesdropper is able to take the two packets and XOR them together. This operation doesn't result in clear text, but the pseudo-random sequence, and thus the encryption, cancels out, and one has the XOR



combination of two clear text packets. If one already knows the contents of one of the two packets, then the clear text of the other is easily determined. Thus WEP does not directly use the key entered by the user for the RC4 algorithm, but rather combines it with a so-called **Initial Vector (IV)** to arrive at the actual RC4 key. This IV is automatically changed from packet to packet by the sender, generally by simple incrementation, and is transmitted along with the encrypted packet. The receiver uses the IV included in the packet in order to reconstruct the RC4 key actually used for the packet.

WEP also calculates a CRC checksum for the unencrypted packet and appends it to the packet before it is RC4-encrypted. The receiver can check this CRC checksum after decryption and determine whether the decryption was faulty—for example, due to an incorrect WEP key. In this way, WEP also happens to offer a certain degree of access security, since an intruder without knowledge of the WEP key can only generate "defective" packets, which will automatically be filtered out by the WLAN card.

This additional IV explains some of the confusion one sees about the key length in WEP—since larger key lengths sound more secure, the 24 bits of the IV sound nice when added to the actual key length, although the user can of course only configure the left-over portion. The IEEE standard originally foresaw a relatively short key length of 40 bits, which was probably oriented towards the then-existing US export restrictions on strong cryptography—this variant is usually called WEP64 in brochures. Most WLAN cards today support a variant in which the user can configure a 104-bit key, which results in a 128 bit long RC4 key—correspondingly, this is often called WEP128. More seldom are key lengths of 128 bits (WEP152) or 232 bits (WEP 256).

As explained above, RC4 can in principle work with key lengths up to 2048 bits, which would correspond to WEP keys of up to 2024 bits. In the practice, key lengths reach a simple limit at which the user can manage to enter the columns of digits without making a mistake. Since WEP is a pure PSK method, the keys must be entered identically on both sides of the connection. The IEEE standard provides no mechanism to distribute WEP keys in a WLAN automatically. Some manufacturers have, for instance, attempted to simplify entry for users by requiring entry not of the WEP key itself, but rather a passphrase (a sort of overly long password) from which the key can be calculated. However, this procedure varies from manufacturer to manufacturer so that the same passphrase for different manufacturers might lead to different WEP keys—besides, users have a tendency to choose passwords which are relatively easy to guess, so that the resulting keys are

usually weaker than 40 or 104 bits (the current IEEE standards, for instance, assume that a typical password has a strength of about 2.5 bits per character.) The IEEE standard specifies that up to four different WEP keys can exist in one WLAN. The sender encodes the number of the WEP key used in the encrypted packet along with the IV, so that the receiver can use the appropriate key. The idea behind this was that old keys in a WLAN could gradually be exchanged for new keys, in that stations which had not yet received the new key could still use an old key during a transition period.

Based on WEP, the 802.11 standard also defines a Challenge-Response procedure for authentication of clients. The access point sends a clear-text packet which contains a 128-byte long challenge, which the client encrypts and sends back with WEP. If the access point can successfully decrypt this answer (that is, the CRC is correct) and the result is the originally transmitted challenge, it can assume that the client has a correct WEP key and thus is authorised for access.

Unfortunately, this process provides a potential attacker with 128 bytes of clear text and the corresponding encrypted text, which offer scope for crypto analysis. Furthermore, many clients don't implement this variant, so that this process, called Shared Key, is seldom used—instead, processes started after the WLAN registration are used for authentication, such as 802.1x (see below).

While the WEP process theoretically sounds good up to now, in practice there are unfortunately serious flaws which significantly reduce the advantages—regardless of the WEP key length used. These weaknesses really should have been found by closer analysis at the time when WEP was being defined. Unfortunately, no cryptology experts participated in the WEP definition process, so these flaws only became obvious once the WEP process was massively implemented thanks to the market success of 802-11b WLAN cards (earlier 2MB designs often included no encryption at all—WEP is an optional function in the 802.11 standard).

The chief weakness of WEP is the IV length, which is far too short. As already mentioned, the reuse of a key in RC4 is a serious security loophole—but it occurs in WEP at least every 16 million packets, when the IV counter overflows from 0xfffff to zero. An 11MB WLAN can achieve a net data rate of around 5MB/sec; with a maximum packet length of 1500 bytes, that comes to about 400 packets per second at full throttle. After about 11 hours, the IV counter would theoretically overflow, and an eavesdropper receives the information needed to 'crack' the WEP key. In practice, the attacker will actually receive this information much sooner. Mathematical analyses of RC4 have shown that

for certain values of the RC4 key, conclusions may be drawn about the first values of the pseudo-random sequence it generates—thus about the bytes with which the beginning of the packet are encrypted. This property of RC4 can be relatively easily avoided, for instance by discarding the first bytes of the pseudo-random byte sequence and only using the "later" bytes for encryption, and this is often done nowadays when RC4 is used. But when this discovery was first made WEP in its described form was already part of the IEEE standard and indelibly incorporated into the hardware of the widely distributed WLAN cards.

Very unfortunately, these "weak" values of RC4 keys can be recognised by particular values in the first bytes of the RC4 key, and in WEP that happens in the IV in each packet—which is transmitted in clear text. Once this connection was discovered, specialised sniffer tools quickly appeared on the Internet, which watched for packets with these 'weak IVs', and thus only had to process a fraction of the total traffic. Depending on the amount of data being transferred in a WLAN, such tools can crack the encryption in a fraction of the time mentioned above. With longer WEP keys (such as 104 instead of 40 bits) this may take a little longer, but the time required for cracking grows at best linearly with the key length, not exponentially, as is usually the case.

Unfortunately the CRC checksums contained in the packets also haven't lived up to expectations. Ways were found to change encrypted packets under certain conditions even without knowledge of the WEP key in such a way that the CRC is still valid after decryption on the receiving end. So WEP therefore cannot guarantee that a packet hasn't been changed on the way from sender to receiver.

These weaknesses unfortunately degraded WEP to an encryption scheme which at best could be used to protect a home network against 'accidental eavesdroppers.' These discoveries gave rise to much controversy, gave WLAN the reputation of being unsafe technology, and forced manufacturers to action. WLAN is, however, a standardised technology, and better standards don't come into being from one day to the next—which is why there were a few intermediate steps to a secure solution, which at least blunted the worst of WEP's design flaws.

### 11.2.3 WEPplus

As explained in the previous section, the use of 'weak' IV values was the problem which weakened the WEP process most. Only a few weeks after the publication, tools like 'WEPCrack' and 'AirSnort' appeared on the Internet,

which could automatically crack an arbitrary WLAN connection within a few hours. With this, WEP was essentially worthless.

A first 'quick shot' to secure WLANs against this kind of program was the simple notion that the weak IV values are known, and that they could simply be skipped during encryption—since the IV used is after all transmitted in the packet, this procedure would be completely compatible with WLAN cards which didn't understand this extension, dubbed WEPplus. A true improvement in security would naturally only result once all partners in the WLAN were using this method.

In a network equipped with WEPplus, a potential attacker again has the chore of listening to the entire data traffic, waiting for IV repetitions—simply waiting for the few packets with weak IVs is no longer an option. This raised the bar for an attacker again, particularly if one didn't simply set the IV counter to zero when initialising a WLAN card, but rather initialised with a random value: the IV counter at an access point only starts to count when the first station logs in and starts transmitting data. If the access point and station each initialised their IV counters to zero, packets with identical IV values occur immediately after the connection is made. By initialisation to a random value, the collision can at least be delayed by an average of 223 packets, that is, half the space of possible IVs—with more than one station in a WLAN, this value is naturally reduced. WEPplus is thus technically only a slight improvement—but it did serve to calm the user base enough to make WEP acceptable again, at least for home use (as long as a new key was configured often enough.) For use in a professional environment, of course, that didn't suffice.

#### 11.2.4 EAP and 802.1x

Obviously, an 'add-on' like WEPplus can't eliminate the basic problem of too-short IVs, without changing the format of packets on the WLAN, thus rendering all existing WLAN cards incompatible. There is, however, a possibility of solving several of our problems with one central change: no longer use the formerly fixed WEP key, but to negotiate them dynamically instead. As the process to be used for this purpose, the Extensible Authentication Protocol has emerged. As the name suggests, the original purpose of EAP is authentication, that is, the regulated access to a WLAN—

the possibility of installing a valid WEP key for the next session is more or less a byproduct. Figure 2 shows the basic process of a session secured by EAP.

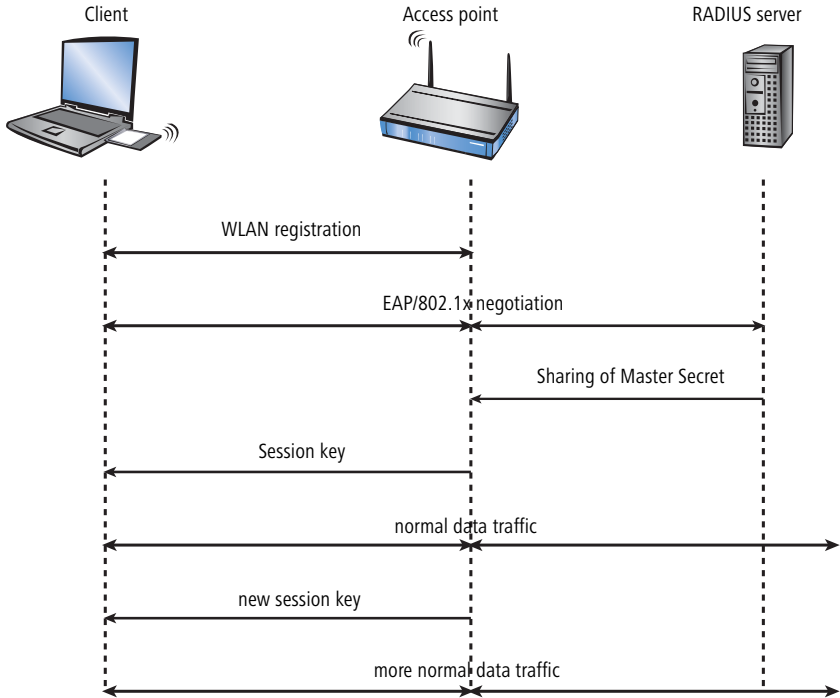


Figure 2: Schematic process of a WLAN session with EAP/802.1x

In the first phase, the client registers with the access point as usual, and enters the state in which it can now send and receive over the access point in normal WEP or WEPplus—but not with EAP, because in this state the client still doesn't have a key to secure its data traffic from eavesdropping. Instead, the client is in an 'intermediate state' from the point of view of the access point, in which only particular packets from the client are forwarded, and these are only directed to an authentication server. These packets implement EAP/802.1x as already mentioned, which can easily be distinguished from other protocols due to its Ethernet type 0x888e. The access point packages these packets in RADIUS queries and sends them on to the authentication server. The access point converts the replies coming from the RADIUS server back into EAP packets, and sends them back to the client.

The access point is thus a sort of middle man between client and server. It doesn't have to check the contents of these packets, it just has to check that no other data traffic to or from the client can occur.

This process has two advantages:

- ▶ The implementation effort in the access point is low. While the client and the server are usually PCs with high levels of resources, access points are devices which are limited both in memory and in computing power.
- ▶ New processes for authentication require no firmware upgrade on the access point.

Over this tunnel through the access point, the client and server authenticate one another, that is, the server checks the client's access privilege to the network, and the client checks that it is talking to the right network. "Wild" access points set up by hackers can be recognised in this way.

A whole series of authentication processes exist which can be used in this tunnel. A current process (and one supported by Windows XP) is for instance TLS, in which server and client exchange certificates; another is TTLS, in which only the server supplies a certificate—the client is authenticated using only a username and password.

After the authentication phase, a secure tunnel even without WEP encryption has been set up, in which the access point is connected in the next step.

For this, the RADIUS server sends the so-called 'Master Secret', a session key calculated during the negotiation, to the access point. The LAN behind it is considered secure in this scenario, so that this transmission can be performed in clear text.

With this session key, the access point now takes over the tunnel and can use it to provide the actual WEP key to the client. Depending on the capabilities of the access point hardware, this can be a true session key (that is, a WEP key which will only be used for data packets between the access point and precisely this client), or a so-called group key, which the access point will use for communication with multiple clients. Classical WEP hardware can usually handle only group keys, these being the four mentioned in the chapter on WEP.

The particular advantage of this procedure is that the access point can regularly change the WEP key over the EAP tunnel, that is, it can perform a so-called rekeying. In this way, WEP keys can be replaced by new ones long before they run the risk of being cracked due to IV collisions. A common 'use time' for such WEP keys might be 5 minutes.

Further advantages of this procedure include its simple implementation in the access point, with little extension to existing hardware. The disadvantage of the procedure is its complexity. The maintenance of the central RADIUS server and the certificates stored there is generally only possible in large installations with a separate IT department—it is less suitable for use in the home or in smaller companies. Furthermore, a minimum set of procedures has not been established which a client or a server must support. Thus scenarios are quite thinkable in which a client and a server cannot establish an EAP tunnel, because the sets of procedures they support don't match. These practical hurdles have thus limited EAP/802.1x to professional use so far—the home user must simply make do with WEPplus, or address security problems on the applications level.

### 11.2.5 TKIP and WPA

As should be clear from the last section, the WEP algorithm is flawed and insecure in principle; the measures taken so far were largely either 'quick fixes' with limited improvement, or so complicated that they were basically impractical for home use or smaller installations.

The IEEE started a Task Group after the discovery of the problems with WEP which addressed the definition of better security mechanisms, and which should eventually result in the IEEE 802.11i standard. The composition and ratification of such a standard, however, generally takes several years. In the meantime, market pressure had grown to the point where the industry could no longer wait for the finalisation of 802.11i. Under the auspices of Microsoft, therefore, the WiFi Alliance defined the Wifi Protected Access (WPA) 'standard'. The WiFi Alliance is an association of WLAN manufacturers which promotes the manufacturer-independent function of WLAN products and, for example, awards the Wifi logo.

In the definition of standards, and 802.11i is no exception, the basic mechanisms are generally known fairly quickly. The publication of the standard mostly takes such a long time because of the fine details. These details are often important only for rare applications. WPA thus took the pragmatic route of extracting the parts of the 802.11i proposal which were already clear and important for the market, and packing them into their own standard. These details include:

- ▶ TKIP and Michael as replacement for WEP
- ▶ A standardised handshake procedure between client and access point for determination/transmission of the session key.

- ▶ A simplified procedure for deriving the Master Secret mentioned in the last section, which can be performed without a RADIUS server.
- ▶ Negotiation of encryption procedure between access point and client.

### TKIP

TKIP stands for **T**emporal **K**ey Integrity **P**rotocol. As the name suggests, it involves an intermediate solution for temporary use until a truly strong encryption procedure is introduced, but which deals with the problems of WEP, never the less. One design requirement was therefore that the new encryption procedure should be implementable on existing WEP/RC4 hardware with a reasonable effort. When TKIP was defined, it was already foreseeable that it would be used well into the era of 54/108Mbit LANs, and a purely software-based encryption would be associated with too high a speed penalty on most systems. In the 'block diagram' of TKIP (Figure 3), therefore, there are many components of WEP to be seen, which generally exist in hardware in WEP cards and thus can effectively be used for TKIP.

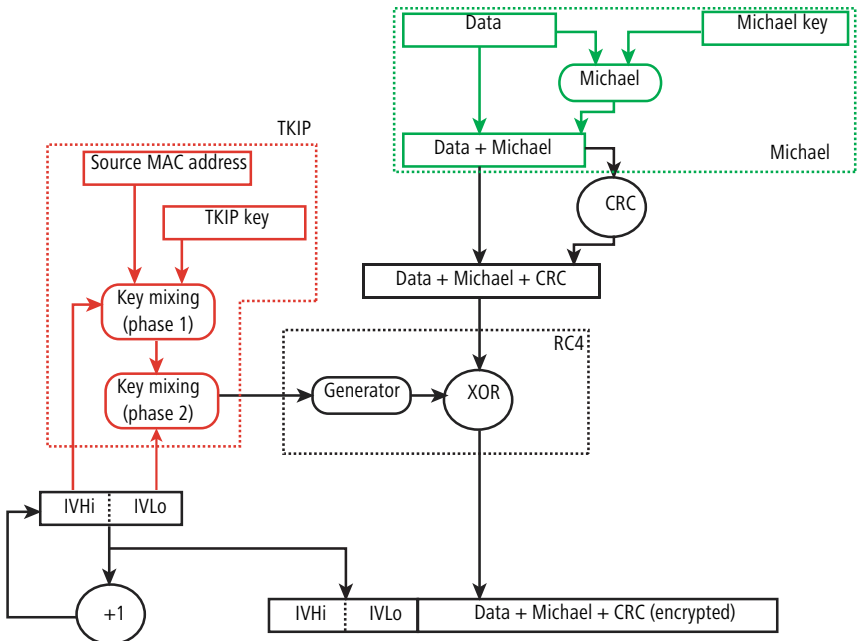


Figure 3: Procedure for TKIP/Michael

As components already familiar from WEP, one recognises the RC4 engine used for the actual encryption and decryption, as well as the CRC module. As



a new component (green), however, besides the CRC, the unencrypted package also has a so-called Michael-MIC attached. This is a hash algorithm developed especially for WLAN, which was designed so that it can be computed on older WLAN hardware with reasonable overhead. Since in contrast to the CRC a second key (the Michael key) must be agreed in this hash, it can neither be calculated nor used to falsify a data packet without detection by the receiver. This is only remains true if an attacker doesn't break the Michael hash with brute force techniques. Due to the requirement of high run-time efficiency, Michael makes a few compromises: although a 64-bit key is used, the effective strength of Michael is only about 40 bits. This was still seen as sufficient, since a potential attacker would have to break the TKIP components in the first place in order to generate data packets which would get past the CRC check of the WEP/RC4 components.

TKIP (red) takes care of the calculation of the actual key for the RC4 engine. In contrast to WEP, the actual key and the IV contained in the packet are never used directly as the RC4 key, but rather it runs through two so-called key mixing phases along with the IV—so an attacker can draw no direct conclusions about the RC4 key from the IV contained in clear text, which solves the problem of 'weak' IVs in WEP (the key mixing itself is designed so that weak RC4 keys can never occur).

Furthermore, the internally incremented IV transmitted in clear text in the packet is 48 bits long instead of 24 - so a sender can now transmit some 280 trillion packets before the 128-bit TKIP key must be changed. Even in a modern WLAN with a net 108 Mbps, which achieves a net rate of around 50 Mbps, using the same assumptions made above for WEP, this would correspond to about 2000 years.

It must still be noted that the IV is split into two parts for reasons of optimisation: a 16-bit low part and a 32-bit high part. The background for this is that the key mixing proceeds in two phases, as shown in the illustration:

- ▶ For the first (computationally intensive) phase, only the upper part is needed, so it only needs to be performed once for every 65,536 packets.
- ▶ The second, relatively simple phase of the key mixing uses the result of the first phase along with the low part of the IV (which changes with each packet) in order to create the actual RC4 key.

In contrast to WEP, it is additionally determined in TKIP that the IVs to be used from packet to packet must increase in a strictly monotone manner, so the receiver only has to perform phase 1 for every 65,536 received packets. The

decryption part of TKIP checks this sequentiality and discards packets which contain an already-used IV, which prevents replay attacks.

As a further detail, TKIP also mixes the MAC address of the sender into the first phase. This ensures that the use of identical IVs by different senders cannot lead to identical RC4 keys and thus again to attack possibilities.

As mentioned above, the Michael hash does not represent a particularly tough cryptographic hurdle: if the attacker can break the TKIP key or get encrypted packets past the CRC check via modifications similar to those for WEP, then not many barriers remain. For this reason, WPA defines countermeasures if a WLAN card detects more than two Michael errors per minute: both the client and the access point break data transfer off for one minute, afterwards renegotiating TKIP and Michael keys.

### **The key handshake**

In the discussion of 802.1x it was already noted that EAP/802.1x provides a possibility to inform the client at the outset of a session of the key valid for it. WPA now places that on a standardised basis, and considers the session-key option offered by modern access points that, in addition to the four 'global' keys, assigns each registered client with a session key that is used exclusively with data packets to or from that client.

If you take another look at the procedure shown in Figure 2, the newly defined key handshake replaces the phase in which the access point transmits the WEP key to the client after receiving the Master Secret from the RADIUS server.

The key handshake breaks down into two phases: first the pairwise key handshake, then the group key handshake (Figure 4).

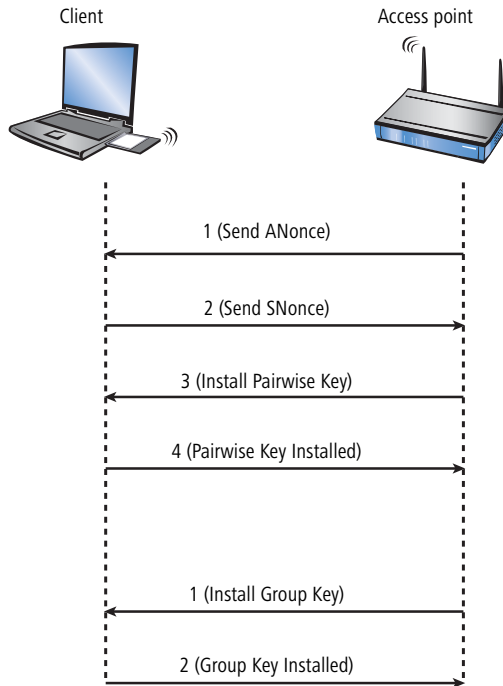


Figure 4: Key handshake in WPA

As you can see, the handshake consists of pairs of packets which each consist in turn of a 'query' of the access point and a 'confirmation' of the client. The first pair serves mostly for the client and access point to exchange the specific random values (so-called nonces) to be used for this negotiation. The Master Secret already known to both sides is now mixed with these nonces and after a predetermined hash procedure, further keys are generated, on the one hand to take care of securing further exchanges, and on the other to be used as a pairwise key for this station. Since the Master Secret isn't used directly, it can be reused later for any necessary renegotiations, since it can then be mixed with new random value and thus will deliver different keys.

In the second pair, the access point instructs the client to install the calculated TKIP session key, and as soon as the client confirms this, the access point does the same. This concludes the pairwise handshake, and as a result it is now possible to exchange data between client and access point via TKIP.

The client still can't be 'approved', however, because the access point must still transmit a further key—the group key, which it uses to transmit broadcast and multicast packets simultaneously to all stations. This must be determined unilaterally by the access point, and it is simply transmitted to the station, which confirms receipt. Since at this point a pairwise key is already installed on both sides, both of these packets are already encrypted.

After a successful group key handshake, the access point can finally release the client for normal data transfer. The access point is free to perform a rekeying again during the session using the same type of packets. In principle, the client may also request rekeying from the access point.

WPA also takes the case of older WLAN hardware into account, in which the access point does not support pairwise keys, but only group keys. The first phase of the handshake in this case proceeds exactly as before, but doesn't result in the installation of a pairwise key—the group key handshake simply proceeds in clear text, but an encryption in the EAP packets themselves prevents an attacker from simply reading the keys.

### **WPA with passphrase**

The handshake described in the previous section runs strictly under WPA, i.e. the user will never have to define any TKIP or Michael keys. In environments in which no RADIUS server is available to provide master secrets (for instance in smaller companies or home networks), WPA therefore provides the PSK method besides authentication using a RADIUS server; here, the user must enter a passphrase of 8 to 32 characters on the access point and on all stations, from which the master secret is calculated along with the SSID used using a hash procedure. The master secret is therefore constant in such a PSK network; the nonces ensure, however, that different TKIP keys still result.

In a PSK network—similar to classical WEP—both access security and confidentiality depend on the passphrase not being divulged to unauthorised people. As long as this is the case, WPA-PSK provides enormously improved security against break-ins and eavesdropping over any WEP variant. For larger installations in which such a passphrase would have to be made known to too large a user community for it to be kept secret, EAP/802.11i is used in combination with the key handshake described here.

### **Negotiation of the encryption method**

The original WEP definition only specified a fixed key length, so that only a single bit was required in the registration packets from the station and access

point to show whether encryption should be used or not. This became insufficient the moment WEP was used with key lengths other than 40 bits—the user just had to take care that not only the same value but that the same length was defined as well. WPA provides a mechanism with which client and access point can agree on the encryption and authentication procedures to be used. For this purpose, a new info element was defined which can contain the following:

- ▶ The encryption method to be used for broadcasts in this network (also the type of group key). Each client wanting to register in a WPA-WLAN must support this procedure. Here, besides TKIP, WEP is also still allowed, in order to support mixed WEP/WPA networks—in a pure WPA network, TKIP will be selected.
- ▶ A list of encryption methods which the access point provides for the pairwise key—here, WEP is explicitly disallowed.
- ▶ A list of authentication methods a client may use to show itself to the WLAN as authorised for access—possible methods are currently EAP/802.1x or PSK.

The access point broadcasts such an element with its beacons, so that clients know whether this network is suitable for them or not. When registering at the access point, the client sends another such packet, in which it gives the desired type of pairwise key as well as its authentication scheme. The access point then starts either the EAP/802.1x negotiation, or starts directly with the key handshake.

Since neither beacons nor registration packets are cryptographically secured, it is possible that a third party might interfere in this exchange and force the client and/or the access point down onto a weaker method than the one actually desired. Both the access point and the client are therefore required to exchange these info elements again during the key handshake, and if the element received doesn't match the one from the registration, they immediately break the connection.

As mentioned, the original WPA standard specifies only TKIP/Michael as an improved encryption method. With the further development of the 802.11i standard, the AES/CCM method described below was added. In a WPA network it is now possible for some clients to communicate with the access point using TKIP, while other clients use AES.

## 11.2.6 AES and 802.11i

In mid-2004, the long awaited 802.11i standard was approved by the IEEE, which should put the entire security concept of the WLAN on a new basis—which is to be expected, since errors as serious as those encountered during the introduction of WEP are unlikely to occur with 802.11i. As mentioned in the last section, WPA has already implemented a whole series of concepts from 802.11i—so in this section we will only describe the components which are new compared to WPA.

### AES

The most obvious extension is the introduction of a new encryption process, namely AES-CCM. As the name already hints, this encryption scheme is based on DES's successor AES, in contrast to WEP and TKIP, which are both based on RC4. Since only the newest generation of WLAN chips contain AES hardware, 802.11i continues to define TKIP, but with the opposite prerequisites: any 802.11i-compliant hardware must support AES, while TKIP is optional—in WPA that was exactly the other way around. Due to the widespread adoption of non-AES-compatible hardware, however, it is to be expected that every AES-capable WLAN card will still support WEP and TKIP. WLAN devices will, however, probably provide configuration options which prevent use of TKIP—many agencies in the USA consider TKIP insufficiently secure, which due to the comparatively weak Michael hash is fairly well justified.

The suffix CCM denotes the way in which AES is used in WLAN packets. The process is actually quite complicated, for which reason CCM is only sensibly implemented in hardware—software-based implementations are possible, but would result in significant speed penalties due to the processors commonly used in access points.

In contrast to TKIP, AES only requires a 128-bit key, with which both the encryption and protection against undetected changes to packets is achieved. Furthermore, CCM is fully symmetric, i.e. the same key is used in both communications directions—a compliant TKIP implementation, on the other hand, requires the use of different Michael keys in the send and receive directions, so that CCM is significantly simpler in use than TKIP.

Occasionally one finds other AES variants in older publications or drafts of the 802.11i standard, namely AES-OCB or WRAP. In these variants, AES was used in a different form, which was dropped in favor of CCM in the final standard. WRAP is nowadays meaningless.

Similar to TKIP, CCM uses a 48-bit Initial Vector in each packet—an IV repetition is impossible in practice. As in TKIP, the receiver notes the last IV used and discards packets with an IV which is equal to or less than the comparison value.

### **Pre-authentication and PMK caching**

As mentioned earlier, the delay in publishing standards is usually due to the details. In the case of 802.11i, there were two details which should particularly help with the use of WLAN for speech connection (VoIP) in enterprise networks. Especially in connection with WLAN-based wireless telephony, quick roaming (switching from one access point to another without lengthy interruptions) is of special significance. In telephone conversations, interruptions of 100 milliseconds are irritating, but the full authentication process over 802.11x, including the subsequent key negotiation with the access point, could take significantly longer.

For this reason, the so-called PMK caching was introduced as a first measure. The PMK, of course, serves as the basis for key negotiation in an 802.1x authentication for both client and access point. In VoIP environments it is possible that a user moves back and forth among a relatively small number of access points. Thus it may happen that a client switches back to an access point in which it was already registered earlier. In this case it wouldn't be sensible to repeat the entire 802.1x authentication again. For this reason, the access point can provide the PMK with a code, the so-called PMKID, which it transmits to the client. Upon a new registration, the client uses the PMKID to ask whether this PMK is still stored. If yes, the 802.1x phase can be skipped and only the exchange of six short packets is required before the connection is restored. This optimisation is unnecessary if the PMK in a WLAN is calculated from a passphrase as this applies everywhere and is known.

A second measure allows for some acceleration even in the case of first-time registration, but it requires a little care on the part of the client. The client must already detect a degrading connection to the access point during operation and select a new access point while it is still in communication with the old access point. In this case it has the opportunity to perform the 802.1x negotiation with the new access point over the old one, which again reduces the "dead time" by the time required for the 802.1x negotiation.

## **11.2.7 Summary**

After the security loopholes in WEP encryption became public knowledge, the presentation of short-term solutions such as WEPplus and the intermediate

steps like WPA, the IEEE committee has now presented the new WLAN security standard 802.11i. The TKIP procedure used by WPA is based on the older RC4 algorithm, the foundation of WEP. AES is the first important and conclusive step towards a truly secure encryption system. 802.11i/AES have confined the practical and theoretical security loopholes in previous methods to history.

The AES procedure provides security on a level that satisfies the Federal Information Standards (FIPS) 140-2 specifications that are required by many public authorities.

LANCOM equips its 54Mbps products with the Atheros chip set featuring a hardware AES accelerator. This guarantees the highest possible level of encryption without performance loss.

The user-friendly pre-shared key procedure (entry of a passphrase of 8-63 characters in length) makes 802.11i quick and easy for anybody to set up. Professional infrastructures with a larger number of users can make use of 802.1x and RADIUS servers.

In combination with further options such as Multi-SSID and VLAN tagging, it is possible to provide highly secure networks for multiple user groups and with different levels of security.

- ▶ LANCOM provides the PSK procedure with the LCOS version 3.50.
- ▶ 802.1x is foreseen for realisation in LCOS version 4.
- ▶ Multi-SSID is available as of LCOS 3.42.
- ▶ VLAN tagging is available as of LCOS version 3.32.

## 11.3 Protecting the wireless network

A wireless LAN does not, like conventional LAN, use cable as the transmitting medium for data transfer, but the air instead. As this medium is openly available to any eavesdropper, the screening of the data in a WLAN is an important topic.

Depending on how critical WLAN security is for your data, you can take the following steps to protect your wireless network:

- ① Activate the "Closed network function". This excludes all WLAN clients using "Any" as the SSID, and those that do not know your network SSID. ('Network settings' →page 251)
- ② Do not use your access point's default SSID. Only take a name for your SSID that cannot be guessed easily. The name of your company, for



example, is not a particularly secure SSID. ('Network settings' →page 251)

- ③ If you know exactly which wireless network cards are permitted to access your WLAN, you can enter the MAC addresses of these cards into the access control list, thus excluding all other cards from communications with the access point. This reduces access to the WLAN only to those clients with listed MAC addresses. ('Access Control List' →page 235)
- ④ Use encryption on the data transferred in the WLAN. Activate the strongest possible encryption available to you (802.11i with AES, WPA or WEP) and enter the appropriate keys or passphrases into the access point and the WLAN clients ('Encryption settings' →page 238 and 'WEP group keys' →page 241).
- ⑤ Regularly change the WEP key. Also change the standard key ('Encryption settings' →page 238) in the configuration. Alternatively, you can use a cron job to automatically change the key every day, for example ('Zeitautomatik für LCOS-Befehle' →page 46). The passphrases for 802.11i or WPA do not have to be changed regularly as new keys are generated for each connection anyway. This is not the only reason that the encryption with 802.11i/AES or WPA/TKIP is so much more secure than the now aged WEP method.
- ⑥ If the data is of a high security nature, you can further improve the WEP encryption by additionally authenticating the client with the 802.1x method ('IEEE 802.1x/EAP' →page 255) or activate an additional encryption of the WLAN connection as used for VPN tunnels ('IPSec over WLAN' →page 256). In special cases, a combination of these two mechanisms is possible.



Further information is available from our web site [www.lancom-systems.com](http://www.lancom-systems.com) under **Support ▶ FAQ**.

## 11.4 Configuration of WLAN parameters

Changes to the wireless network settings can be made at various points in the configuration:

- ▶ Some parameters concern the physical WLAN interface. Some LANCOM models have one WLAN interface, others have the option of using a second WLAN card as well. The settings for the physical WLAN interface

apply to all of the logical wireless networks supported by this card. These parameters include, for example, the transmitting power of the antenna and the operating mode of the WLAN card (access point or client).

- ▶ Other parameters are related solely to the logical wireless network that is supported by a physical interface. These include, for example, the SSID or the activation of encryption, either 802.11i with AES or WPA with TKIP or WEP.
- ▶ A third group of parameters affect the wireless network operation, but are not significant **only** to WLANs. These include, for example, the protocol filter in the LAN bridge.

### 11.4.1 WLAN security

In this part of the configuration, you can place limitations on the communications available to the users in the wireless network. This is done by limiting the data transfer between user groups according to individual stations or the protocol being used. Further, the key for the WLAN encryption is set here.

#### General settings

Depending on the application, it may be required that the WLAN clients connected to an access point can—or expressly cannot—communicate with other clients. You can centrally define the permissible communication for all physical and logical networks, and consider the three following cases in doing so:

- ▶ Allow data traffic: This setting allows all WLAN clients to communicate with other stations in their own and in other available wireless networks.
- ▶ Do not allow data traffic between stations that are logged on to this access point: In this case, WLAN clients can only communicate with mobile stations located in other available wireless networks, but not with the stations in their own WLAN.
- ▶ Do not allow data traffic: This last variant prevents all communications between the WLAN clients.

Communications  
between the WLAN  
clients

Roaming

In addition to controlling the communication between the clients, you can define whether the mobile stations in the wireless network can change to a neighbouring access point (roaming).

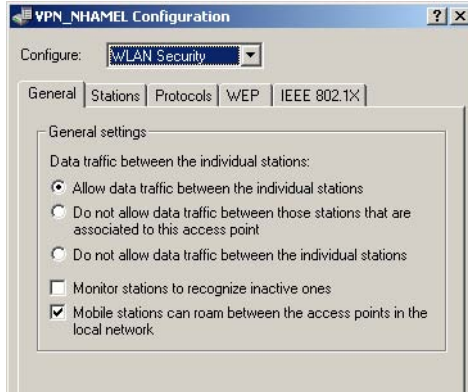
Monitor stations

In particular for public WLAN access points (public spots), the charging of usage fees requires the recognition of stations that are no longer active. Monitoring involves the access point regularly sending packets to logged-in

stations. If the stations do not answer these packets, then the charging systems recognises the station as no longer active.

Configuration with LANconfig

For configuration with LANconfig you will find the general WLAN access settings under the configuration area 'WLAN Security' on the 'General' tab.



Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you will find the general WLAN access settings under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ WLAN module ▶ Inter-stations traffic, monitor stations or IAAP protocol (for roaming)
Terminal/Telnet	cd /Setup/WLAN module/Inter-station traffic, Monitor stations or IAAP protocol (for roaming)

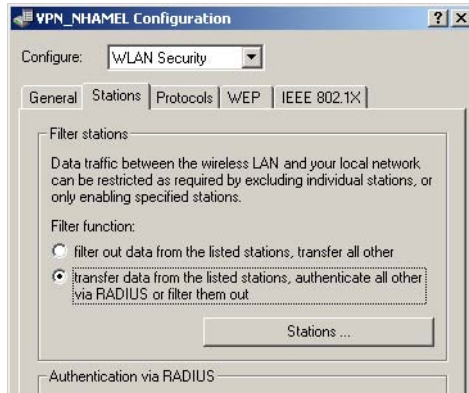
### Access Control List

With the **Access Control List (ACL)** you can permit or prevent the access to your wireless LAN by individual clients. The decision is based on the MAC address that is permanently programmed into wireless LAN adapters.

Configuration with LANconfig

For configuration with LANconfig you will find the general WLAN access settings under the configuration area 'WLAN Security' on the 'Stations' tab.

Check that the setting 'filter out data from the listed stations, transfer all other' is activated. New stations that are to participate in your wireless network are added with the button 'Stations'.



Configuration with  
WEBconfig or Telnet

Under WEBconfig or Telnet you will find the Access Control List under the following paths:

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

### Protocol filter

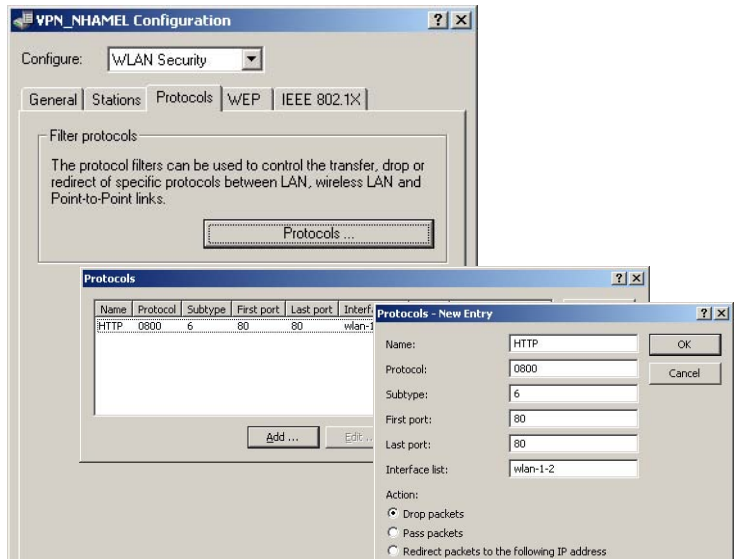
With the protocol filter you can influence the handling of certain protocols during transfer from the WLAN to the LAN.



Packets from the WLAN for certain protocols/ports can be redirected to special IP addresses in the LAN by the protocol filter. This function known as "Redirect" is described in detail in the section 'Redirect function' →page 254.

Configuration with  
LANconfig

For configuration with LANconfig you will find the protocol filter under the configuration area 'WLAN Security' on the 'Protocols' tab.



Make an entry in the protocol list for each protocol that requires special handling. Enter the following values:

- ▶ A name of your choice for the filter entry
- ▶ Protocol number, e.g. '0800' for IP. If no protocol is entered, the filter will be applied to **all** packets.
- ▶ Subprotocol, e.g. '6' for TCP. If no subprotocol is entered, the filter will be applied to **all** packets of the entered protocol.
- ▶ Port start and port end, e.g. each '80' for HTTP. If no ports are entered, then this filter will be applied to all ports of the appropriate protocol/subprotocol.



Lists of the official protocol and port numbers are available in the Internet under [www.iana.org](http://www.iana.org).

- ▶ Action for the data packets:
  - ▷ Let through
  - ▷ Reject
  - ▷ Redirect (and state the target address)
- ▶ List of interfaces that the filters apply to

- ▶ Redirect address when the 'Redirect' action is selected

Example:

Name	Protocol	Subtype	Start port	End port	Interface list	Action	Redirect IP address
ARP	0806	0	0	0	WLAN-1-2	Let through	0.0.0.0
DHCP	0800	17	67	68	WLAN-1-2	Let through	0.0.0.0
TELNET	0800	6	23	23	WLAN-1-2	Redirect	192.168.11.5
ICMP	0800	1	0	0	WLAN-1-2	Let through	0.0.0.0
HTTP	0800	6	80	80	WLAN-1-2	Redirect	192.168.11.5

ARP, DHCP, ICMP will be let through, Telnet and HTTP will be redirected to 192.168.11.5, all other packets will be rejected.



As soon as an entry is made in the protocol filter, all packets not matching the filter will be automatically rejected!

Configuration with  
WEBconfig or Telnet

Under WEBconfig or Telnet you will find the protocol filter under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ LAN management module ▶ Protocol table
Terminal/Telnet	<code>cd /Setup/LAN-Management-Module/Protocol-Table</code>

## Encryption settings

Access points of the LANCOM range support the most up-to-date methods of encryption and security for data that is transferred via WLAN.

- ▶ The IEEE standard 802.11i/WPA stands for the highest degree of security that is currently available for WLAN connections. This standard uses a new encryption procedure (AES-CCM) which, in combination with other methods, achieves levels of security equalled only by VPN connections until now. When using AES-capable hardware (such as the 54-Mbit AirLancer clients and the 54-Mbit LANCOM access points) the transmissions are much faster than with comparable VPN security.
- ▶ WEP is also supported to ensure compatibility with older hardware. WEP (**W**ired **E**quivalent **P**rivacy) is the encryption method originally

incorporated in the 802.11 standard for the encryption of data in wireless transmission. This method uses keys of 40 (WEP64), 104 (WEP128) or 128 bits (WEP152) in length. A number of security loopholes in WEP have come to light over time, and so the latest 802.11i/WPA methods should be used wherever possible.



Further information about the 802.11i and WPA standards are available under 'Developments in WLAN security' →page 213.

The tab '802.11i/WEP' in the configuration area 'WLAN Security' is used for setting the encryption parameters for each logical WLAN. Open the list with the button for **WPA or Private WEP settings**.

Type of encryption

First of all, select the type of encryption for the individual logical WLAN interfaces:

- ▶ Yes—Access only for stations with encryption (recommended): In this mode, only the WLAN clients with activated WEP and the correct key can register with the access point.
- ▶ Yes—Access also for stations without encryption allowed: In this mode, WLAN clients with activated WEP and AirLancer MC 11 clients (without WEP) can register with this access point.
- ▶ No—No encryption

Method/  
Key 1 length

Set the encryption method to be used here.

- ▶ 802.11i (WPA)-PSK – Encryption according to the 802.11i standard offers the highest security. The 128-bit AES encryption used here offers security equivalent to that of a VPN connection.
- ▶ WEP 152, WEP 128, WEP 64 – encryption according to the WEP standard with key lengths of 128, 104 or 40 bits respectively. This setting is only to be recommended when the hardware used by the WLAN client does not support the modern method.
- ▶ WEP 152-802.1x, WEP 128-802.1x, WEP 64-802.1x – encryption according to the WEP standard with key lengths of 128, 104 or 40 bits respectively, and with additional authentication via 802.1x/EAP. This setting is also only to be recommended when the hardware used by the WLAN client does not support the 802.11i standard. The 802.1x/EAP authentication offers a higher level of security than WEP encryption alone, although the necessity for a RADIUS server makes very high demands of the IT infrastructure.

## Key 1/passphrase

In line with the encryption method activated, you can enter a special WEP key for the respective logical WLAN interface or a passphrase when using WPA-PSK:

- ▶ The passphrase, or the 'password' for the WPA-PSK method, is entered as a string of at least 8 and up to 63 ASCII characters.



Please be aware that the security of this encryption method depends on the confidential treatment of this passphrase. Passphrases should not be made public to larger circles of users.

- ▶ The WEP key 1, that applies only to its respective logical WLAN interface, can be entered in different ways depending on the key length. Rules of the entry of the keys can be found in the description of the WEP group key 'Rules for entering WEP keys' →page 243.

## WPA session key type

If '802.11i (WPA)-PSK' has been entered as the encryption method, the procedure for generating a session or group key can be selected here:

- ▶ AES – the AES method will be used.
- ▶ TKIP – the TKIP method will be used.
- ▶ AES/TKIP – the AES method will be used. If the client hardware does not support the AES method, TKIP will be used.

## Authentication

If the encryption method was set as WEP encryption, two different methods for the authentication of the WLAN client are available:

- ▶ The 'Open system' method does not use any authentication. The data packets must be properly encrypted from the start to be accepted by the access point.
- ▶ With the 'Shared key' method, the first data packet is transmitted unencrypted and must be sent back by the client correctly encrypted. This method presents potential attackers with at least one data packet that is unencrypted.

## Default key

If WEP encryption is selected, the access point can select from four different WEP keys for each logical WLAN interface:

- ▶ Three WEP keys for the physical interface
- ▶ An additional WEP key particular to each logical WLAN interface

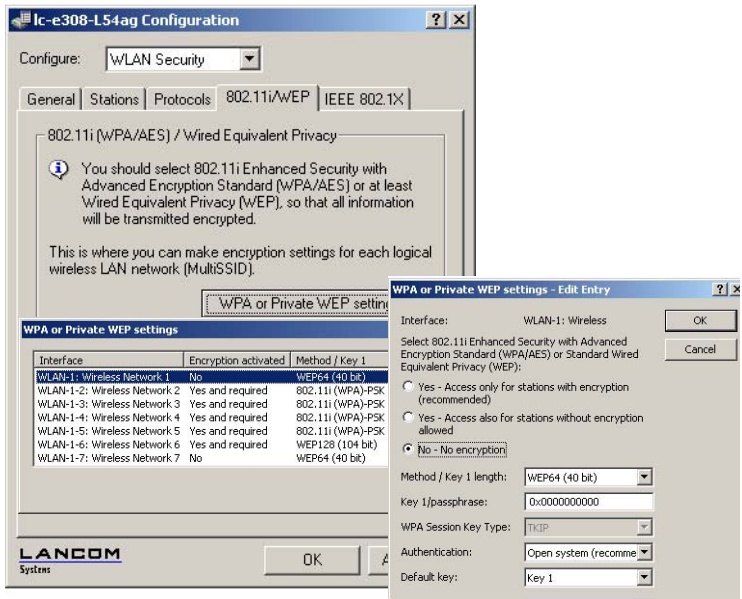
The private WEP settings are used to set the additional key for each logical WLAN interface (see 'Key 1/passphrase'). You should also select which of the four keys is currently to be used for the encryption of the data (default key). This setting can be used to change the key frequently, so increasing security.



Rules of the entry of the keys can be found in the description of the WEP group key 'Rules for entering WEP keys' →page 243.

Configuration with LANconfig

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



Configuration with WEBconfig or Telnet


Under WEBconfig or Telnet you will find the individual key settings for logical WLAN networks under the following paths:

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

### WEP group keys

**Wired Equivalent Privacy (WEP)** is an effective method for the encryption of data for wireless transmission. The WEP method uses keys of 40 (WEP64), 104 (WEP128) or 128 bits (WEP152) in length. Each WLAN interface has four WEP

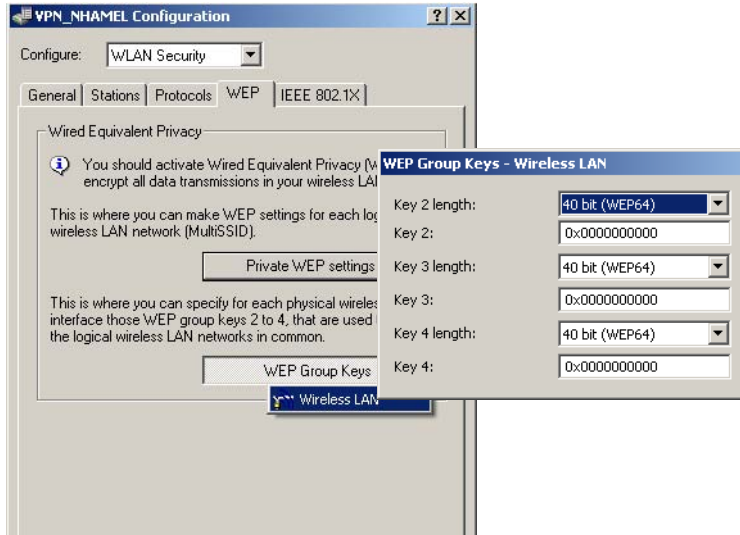
keys: a special key for each logical WLAN interface and three common group WEP keys for each physical WLAN interface.

 If 802.1x/EAP is in use and the 'dynamic key generation and transmission' is activated, the group keys from 802.1x/EAP will be used and are consequently no longer available for WEP encryption.

Rules of the entry of the keys can be found in the description of the WEP group key 'Rules for entering WEP keys' →page 243.

Configuration with  
LANconfig

The tab '802.11i/WEP' in the configuration area 'WLAN Security' is used for setting the three WEP keys 2 to 4. Open the list with the button for **WEP Group Keys**. These WEP keys apply to the physical WLAN interface and thus globally to all of the associated logical WLAN interfaces.



Configuration with  
WEBconfig or Telnet

Under WEBconfig or Telnet you will find the group keys for the physical WLAN interface under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ Interfaces ▶ WLAN-Interfaces ▶ Group-Keys
Terminal/Telnet	cd /Setup/Interfaces/WLAN-Interfaces/ Group-Keys

### Rules for entering WEP keys

WEP keys can be entered as ASCII characters or in hexadecimal form. The hexadecimal form begins with the characters '0x'. The keys have a length depending on the WEP method:

Method	ASCII	HEX
WEP 64	5 characters Example: 'aR45Z'	10 characters Example: '0x0A5C1B6D8E'
WEP 128	13 characters	26 characters
WEP 152	16 characters	32 characters

The ASCII character set includes the characters '0' to '9', 'a' to 'z', 'A' to 'Z' and the following special characters:

! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~

The HEX form uses the numbers '0' to '9' and the letters 'A' to 'F' to display each character as a character pair, which is why twice the number of characters is required to display a HEX key.

Select the length and the format (ASCII or HEX) of the key depending on the best option available in the wireless network cards that register with your WLAN. If the encryption in an access point is set to WEP 152, some clients may not be able to log into the WLAN as their hardware does not support the key length.

## 11.4.2 General WLAN settings

### Country setting

Regulations for the operation of WLAN cards differ from country to country. The use of some radio channels is prohibited in certain countries. To limit the operation of the LANCOM access points to the parameters that are allowed in various countries, all physical WLAN interfaces can be set up for the country where they are operated.

Configuration with  
LANconfig

For the configuration with LANconfig, the country settings can be found in the configuration area 'Management' on the tab 'Wireless LAN' in the group 'General':



This group includes two other parameters in addition to the country setting:

ARP handling

▶ Mobile stations in the wireless network that are on standby do not answer the ARP requests from other network stations reliably. If 'ARP handling' is activated, the access point takes over this task and answers the ARP requests on behalf of stations that are on standby.

Broken link  
detection

▶ The 'Broken link detection' deactivates the WLAN card if the access point loses contact to the LAN.

Configuration with  
WEBconfig or Telnet

Under WEBconfig or Telnet you will find the general WLAN parameters under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert-Configuration ▶ Setup ▶ WLAN-Module
Terminal/Telnet	cd /Setup/WLAN

### 11.4.3 The physical WLAN interfaces

#### Setting up the WLAN card

Apart from the parameters common to all WLAN cards, there is a series of settings to be made that are particular to each WLAN card of the access point.

Configuration with  
LANconfig

For configuration with LANconfig you will find the settings for the WLAN card under the configuration area 'Management' on the 'Wireless LAN' tab. Open

the list of physical WLAN interfaces by clicking on the button **Physical WLAN settings**.



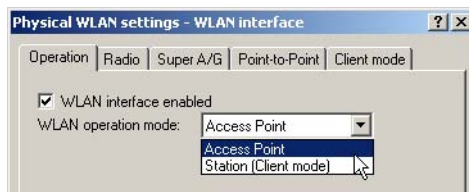
## WLAN card operation

Operation mode

LANCOM Wireless devices can be operated in two basic operation modes:

- ▶ As an access point, it forms the link between the WLAN clients and the cabled LAN.
- ▶ In Client mode the device seeks another access point and attempts to register with a wireless network. In this case the device serves to link a cabled network device to another access point over a wireless connection.

Select the operation mode from the tab 'Operation'. If the WLAN interface is not required, it can be completely deactivated.



Configuration with  
WEBconfig or Telnet

Under WEBconfig or Telnet you can set the operation mode for the physical WLAN interface under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ Interfaces ▶ WLAN-Interfaces ▶ Operation-Settings
Terminal/Telnet	<code>cd /Setup/Interfaces/WLAN-Interfaces/ Operation-Settings</code>

### Radio settings

Frequency band,  
Subband

When selecting the frequency band on the 'Radio' tab under the physical interface settings, you decide whether the WLAN card operates in the 2.4 GHz or in the 5 GHz band (also see 'Standardized radio transmission by IEEE' →page 203), and thus the available radio channels.

In the 5 GHz band, a subband can also be selected which is linked to certain radio channels and maximum transmission powers.



In some countries, the use of the DFS method for automatic channel selection is a legal requirement. Selecting the subband also defines the radio channels that can be used for the automatic channel selection.

Channel number

The radio channel selects a portion of the conceivable frequency band for data transfer.



In the 2.4-GHz band, two separate wireless networks must be at least three channels apart to avoid interference.

Compatibility mode

Two different wireless standards are based on the 2.4-GHz band: the IEEE 802.11b standard with a transfer rate of up to 11 Mbps and the IEEE 802.11g standard with up to 54 Mbps. When 2.4 GHz is selected as the frequency band, the data transfer speed can be set as well.



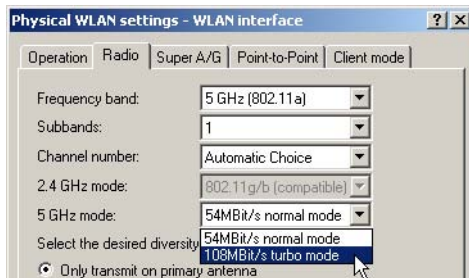
Please observe that clients supporting only the slower standards may not be able to register with the WLAN if the speeds set here are higher.

The 802.11g/b compatibility mode offers the highest possible speeds and yet also offers the 802.11b standard so that slower clients are not excluded. In

this mode, the WLAN card in the access point principally works with the faster standard and falls back on the slower mode should a client of this type log into the WLAN. In the '2Mbit compatible' mode, the access point supports older 802.11b cards with a maximum transmission speed of 2 Mbps.

Turbo mode

Using two neighbouring, vacant channels for wireless transmissions can increase the transfer speeds up to 108 Mbps. Set this option for the 2.4-GHz band by selecting the drop down list '2.4 GHz mode', for the 5-GHz band in the appropriate list '5 GHz mode' below.



Antenna gain  
Transmission power  
reduction

Where the transmission power of an antennae exceeds the levels permitted in the country of operation, the power must be attenuated accordingly.

- ▶ The field 'Antenna gain' is for the gain of the antenna minus the actual cable loss. For an AirLancer Extender O-18a antenna with a gain of 18dBi and a 4m cable with a loss of 1dB/m, the 'Antenna gain' would be entered as  $18 - 4 = 14$ . This value for true antenna gain is dynamically used to calculate and emit the maximum permissible power with regards to other parameters such as country, data rate and frequency band.
- ▶ In contrast to this, the entry in the field 'Tx power reduction' causes a static reduction in the power by the value entered, and ignores the other parameters. Also see 'Establishing outdoor wireless networks' →page 256.

Antenna gain:	<input type="text" value="3"/>	dBi
Tx power reduction:	<input type="text" value="0"/>	dB



The transmission power reduction simply reduces the emitted power. The reception sensitivity (reception antenna gain) remains unaffected. This option is useful, for example, where large distances have to be bridged by radio when using shorter cables. The reception antenna gain can be increased without exceeding the legal limits on transmission power. This leads to an improvement in the maximum

possible range and, in particular, the highest possible data transfer rates.

Access point density

The more access points there are in a given area, the more the reception areas of the antennae intersect. The setting 'Access point density' can be used to reduce the reception sensitivity of the antenna.

TX power reduction:  dB  
 Access point density:

Maximum distance

Large distances between transmitter and receiver give rise to increasing delays for the data packets. If a certain limit is exceeded, the responses to transmitted packets no longer arrive within an acceptable time limit. The entry for maximum distance increases the wait time for the responses. This distance is converted into a delay which is acceptable for wireless communications.

Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you will find the radio parameters under the following paths:

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

## Point-to-point connections

Access points are not limited to communications with mobile clients; they can also transfer data from one access point to another. On the 'Point-to-Point' tab for the physical interface settings, you can allow the additional exchange of data with other access points. You can select from:

Physical WLAN settings - WLAN interface

Operation | Radio | Super A/G | Point-to-Point | Client mode

Point-to-Point operation mode:

- Off - This access point can only communicate with mobile stations.
- On - This access point can also communicate with other access points to connect several local wireless networks.
- Exclusiv - This access point can only communicate with other access points; mobile stations can not connect to this access point (pure WLAN bridge).

Do not forward among P2P links on the same interface

Channel Selection Scheme:

Access point 1:



- ▶ Point-to-point 'Off': The access point only communicates with mobile clients
- ▶ Point-to-point 'On': The access point can communicate with other access points and with mobile clients
- ▶ Point-to-point 'Exclusive': The access point only communicates with other access points

The input fields are for the MAC addresses of the WLAN cards for the point-to-point connections (up to 7).



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

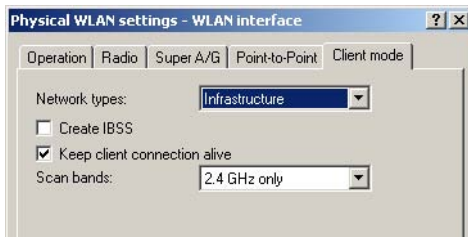
Configuration with WEBconfig or Telnet

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

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

### Client mode

If the LANCOM Wireless device is operating as a client, the tab 'Client mode' can be used for further settings that affect the behaviour as a client.



Network types

'Network types' controls whether the station can register only with infrastructure networks, or also with adhoc networks. Further information about these network types can be found under 'The ad-hoc mode' →page 207 and 'The infrastructure network' →page 207.

Create IBBS	If the station can establish an IBBS (Independent Basic Service Set), meaning an adhoc network, then the station can connect to other WLAN clients. If the connection of devices with a client station, this is mostly unwanted or not required.
Keep client connection alive	This option ensures that the client station keeps the connection to the access point alive even when the connected devices do not send any data packets. If this option is switched off, the client station will automatically log off from the wireless network if no packets are transferred over the WLAN connection within a given time.
Scan bands	This defines whether the client station scans just the 2.4 GHz, just the 5 GHz, or all of the available bands for access points.
Configuration with WEBconfig or Telnet	Under WEBconfig or Telnet you will find the settings for the client mode under the following paths:

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

#### 11.4.4 The logical WLAN interfaces

Every physical WLAN interface can support up to eight different logical wireless networks (Multi-SSID). Parameters can be defined specifically for each of these networks, without the need of additional access points.

Configuration with LANconfig	For configuration with LANconfig you will find the settings for the logical WLAN interface under the configuration area 'Management' on the 'Wireless
------------------------------	---

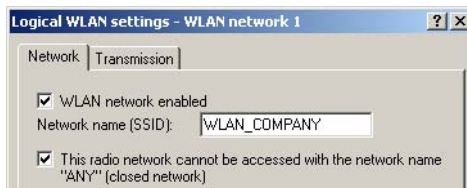
LAN' tab. Open the list of logical WLAN interfaces by clicking on the button **Logical WLAN settings** and select the required logical interface.



## Network settings

Set the SSID

Define an unambiguous SSID (network name) for each of the logical wireless networks on the 'Network' tab for the logical interfaces. Only network cards that have the same SSID can register with this wireless network.



Closed network mode

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

Activate the closed network mode if you wish to prevent WLAN clients using the SSID 'ANY' from registering with your network.

Switch logical WLAN on and off

The switch 'WLAN network enabled' enables the logical WLAN to be switched on or off separately.

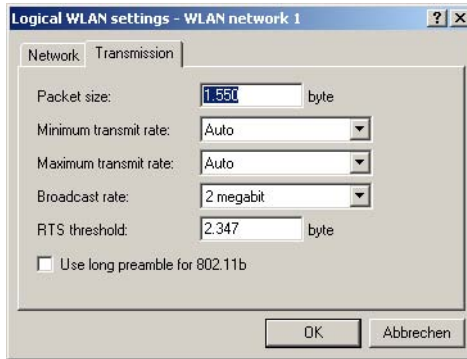
Configuration with  
WEBconfig or Telnet

Under WEBconfig or Telnet you can set the network settings for the logical WLAN interface under the following paths:

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

### Transmission settings

Details for the data transfer over the logical interface are set on the 'Transmission' tab.



Packet size

Smaller data packets cause fewer transmission errors than larger packets, although the proportion of header information in the traffic increases, leading to a drop in the effective network load. Increase the factory value only if your wireless network is largely free from interference and very few transmission errors occur. Reduce the value to reduce the occurrence of transmission errors.

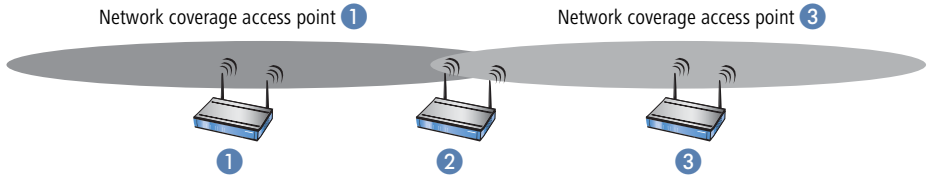
Minimum and  
maximum transmit  
rate

The access point normally negotiates the data transmission speeds with the connected WLAN clients continuously and dynamically. In doing this, the access point adjusts the transmission speeds to the reception conditions. As an alternative, you can set fixed values for the minimum and maximum transmission speeds if you wish to prevent the dynamic speed adjustment.

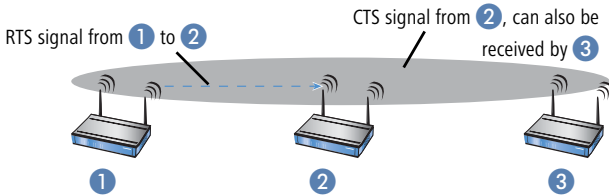
Broadcast rate

The defined broadcast rate should allow the slowest clients to connect to the WLAN even under poor reception conditions. A higher value should only be set here if all clients are able to connect "faster".

RTS threshold      The RTS threshold prevents the occurrence of the "hidden station" phenomenon.



Here, the three access points ①, ②, and ③ are positioned such that no direct wireless connection between the two outer devices is possible. If ① sends a packet to ②, ③ is not aware of this as it is outside of ①'s coverage area. ③ may also try, during the transmission from ①, to send a packet to ② as well, because ③ has no knowledge of the medium (in this case the wireless connection) being blocked. A collision results and neither of the transmissions from ① nor ③ to ② will be successful. The RTS/CTS protocol is used to prevent collisions.



To this end, ① precedes the actual transmission by sending an RTS packet to ②, that ② answers with a CTS. The CTS sent by ② is now within "listening distance" of ③, so that ③ can wait with its packet for ②. The RTS and CTS signals each contain information about the time required for the transmission that follows.

A collision between the very short RTS packets is improbable, although the use of RTS/CTS leads to an increase in overhead. The use of this procedure is only worthwhile where long data packets are being used and the risk of collision is higher. The RTS threshold is used to define the minimum packet length for the use of RTS/CTS. The best value can be found using trial and error tests on location.

Long preamble for 802.11b

Normally, the clients in 802.11b mode negotiate the length of the preamble with the access point. "Long preamble" should only be set when the clients require this setting to be fixed.

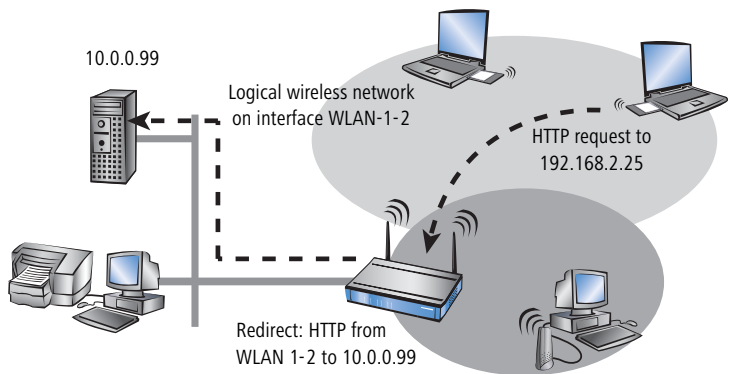
## 11.4.5 Additional WLAN functions

Apart from the different encryption methods 802.11i/AES, WPA/TKIP or WEP and the closed network, a variety of other functions exist for securing the operation of a wireless network. The Redirect function provides the convenient control over the connection of WLAN clients in changing environments. As this function has significance to other modules of the LANCOM LCOS, the configuration parameters are to be found outside of the WLAN settings.

### Redirect function

Clients within wireless networks often have one main aspect in common: a high degree of mobility. The clients are thus not always connected to the same access point, but frequently change between access points and the related LANs.

The redirect function assist the applications being used by the WLAN clients to find the correct target computer in the LAN automatically. If a WLAN client's HTTP request from a certain logical wireless network should always be directed to a certain server in the LAN, then a filter setting for the appropriate protocol with the action "redirect" will be set up for the desired logical WLAN interface.



All requests with this protocol from this logical wireless network will automatically be redirected to the target server in the LAN. The returning data packets are sent to the senders' addresses and ports according to the entries in the connection statistics, which ensures the trouble-free operation in both directions.

### IEEE 802.1x/EAP

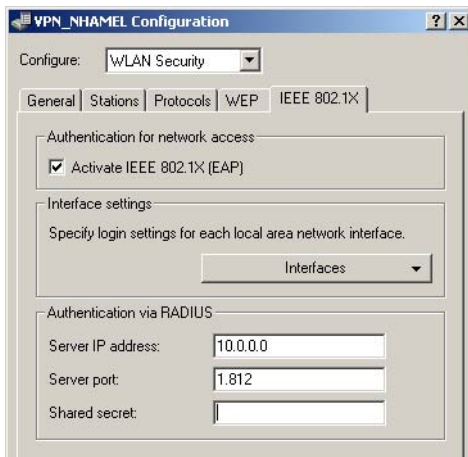
The international industry standard IEEE 802.1x and the Extensible Authentication Protocol (EAP) enable access points to carry out reliable and secure access checks. The access data can be managed centrally on a RADIUS server and can be called up by the access point on demand.

This technology also enables the secure transmission and the regular automatic changing of WEP keys. In this way, IEEE 802.1x improves the security of WEP.

The IEEE-802.1x technology is already fully integrated in Windows XP. Client software exists for other operating systems.

Configuration with LANconfig

For the configuration with LANconfig you will find the IEEE-802.1x settings in the configuration area 'WLAN Security'. This is where you decide if you want to activate IEEE-802.1x. If IEEE-802.1x is activated, a RADIUS server must be defined for the IEEE-802.1x authentication.



Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you will find the settings for IEEE-802.1x under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ User authentication module ▶ EAP config
Terminal/Telnet	cd /Setup/User-Authentication-Module/EAP-Config

Only with the LANCOM VPN Option. Not available with all LANCOM devices.

### **IPSec over WLAN**

With the help of the IPSec-over-WLAN technology in addition to the security measures described already, a wireless network for the exchange of especially sensitive data can be optimally secured. To this end, the LANCOM Wireless access point is upgraded to a VPN gateway with the LANCOM VPN Option. In addition to the encryption per 802.11i, WPA or WEP, the LANCOM Wireless now offers the possibility of encrypting wireless connections with an IPSec-based VPN.

## **11.5 Establishing outdoor wireless networks**

LANCOM access points in combination with appropriate external antennae are ideally suited to establishing point-to-point wireless connections to other access points.

There are two main questions to be answered when setting up the wireless connection:

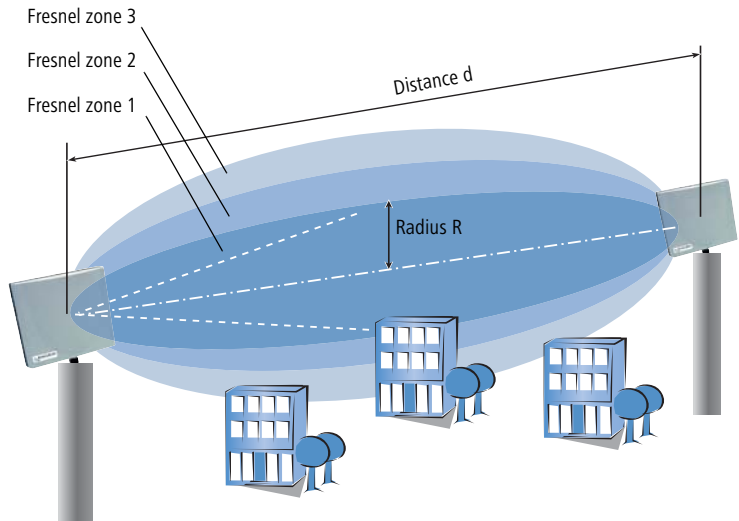
- ▶ How should the antennae be positioned to ensure a problem-free connection?
- ▶ What performance characteristics do the antennae need to ensure sufficient data rates within legal limitations?

### **11.5.1 Geometrical layout of the transmission path**

Antennae do not emit their signals linearly, but within an angle that depends on the model in question. The spherical expansion of the signal waves is characterised by constructive and destructive interference between these waves at certain distances perpendicular to the line of sight between



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



To ensure an optimal signal reception between transmitter and receiver, the Fresnel zone 1 should remain free from any obstruction. Any disturbances from elements protruding into this zone will significantly reduce the effective signal power. The object not only screens off a portion of the Fresnel zone, but the resulting reflections also lead to a significant reduction in the signal reception.

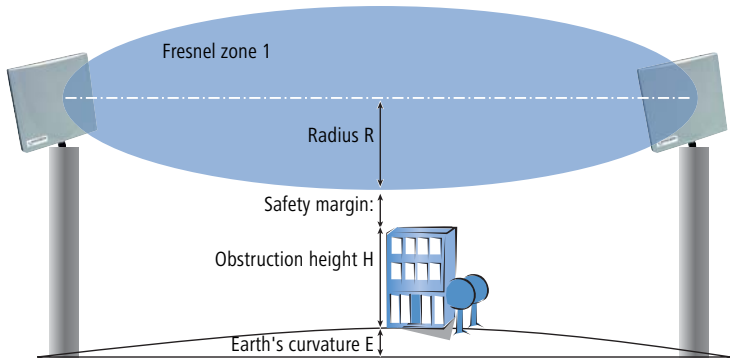
The radius (R) of Fresnel zone 1 is calculated with the following formula assuming that the signal wavelength ( $\lambda$ ) and the distance between transmitter and receiver (d) are known.

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

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

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

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



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

The height of the Earth's curvature is calculated from  $E = d^2 * 0,0147$  – even at a distance of 8 km that results in almost 1m!

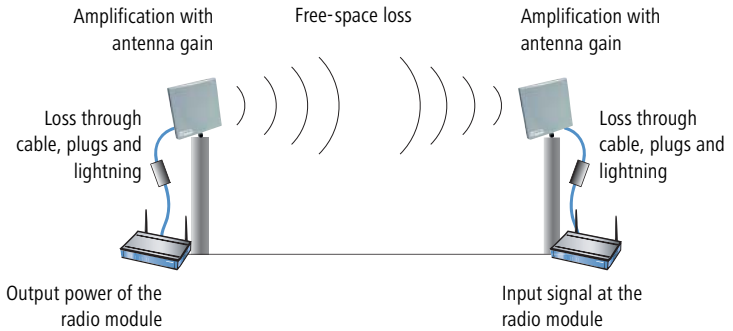
**Example:** With a distance of 8 km between the antennae, the result in the 2.4-GHz band is a mast height above the level of the highest obstruction of approx. **13 m**, in the 5-GHz band **9 m**.

### 11.5.2 Antenna power

The power of the antenna must be high enough to ensure acceptable data transfer rates. On the other hand, the country's legal limitations on transmission power should not be exceeded.

The calculation of effective power considers everything from the radio module in the transmitting access point to the radio module in the receiving access point. In between there are attenuating elements such as the cable, plug


connections, and even the air, and amplifying elements such as the external antennae.



- ① The calculation of the power over the path begins at the transmitter's radio module. The radio module in the LANCOM access points in 802.11a mode emits the following power levels depending on the channel used and the data transmission rate:

Mbps	5.150 - 5.250 GHz	5.250 - 5.350 GHz	5.470 - 5.725 GHz	5.725 - 5.850 GHz
6	17	17	17	17
9	17	17	17	17
12	17	17	17	17
18	17	17	17	17
24	17	17	17	17
36	14	14	14	14
48	13	13	13	13
54	12	12	12	12
72 (Turbo)	14	14	14	14
96 (Turbo)	13	13	13	13
108 (Turbo)	12	12	12	12

To achieve a data transmission rate of 24 Mbps the radio module emits a power of 17 dBm.


 The data transmission rate is set according to the reception power. A WLAN module has an input sensitivity equivalent to a power level of, for example, -80dBm. If the received power falls below this level, then a lower data rate can be switched in that corresponds with an improved sensitivity with a lower level of power.

② Outdoor wireless connections are usually realised with external antennae and extension cables together with lightning protection for safety. The power loss from the cable is approx. 1 dB per metre. A cable 4 m long thus reduces power by 4 dB, the lightning protection and the various plug connections also lead to the loss of a further 1 dB. Thus the power of the external antenna is:

$$17 \text{ dBm} - 4 \text{ dB} - 1 \text{ dB} = 12 \text{ dBm.}$$

③ The power received by the antenna is then amplified. An AirLancer Extender O-18a (with an emitting angle of 18°) supplies an antenna gain of 18 dBm. The total power output from the antenna is thus:

$$12 \text{ dBm} + 18 \text{ dBm} = 30 \text{ dBm.}$$

 This power emission must be within the legal limits of the country where the antenna is in operation!

④ Radio transmission through air is subject to power attenuation from the so-called "free-space loss"  $x$ , which is logarithmically related to the distance  $d$  (in km) between transmitter and receiver.

$$x = 100 + 20 * \log (d) \text{ [dB] in the 2.4-GHz band}$$

$$x = 105 + 20 * \log (d) \text{ [dB] in the 5-GHz band}$$

A 802.11a transmission over a distance of 4 km results in a free-space loss  $x$  of:

$$x = 105 \text{ dB} + 20 * \log (4) \text{ dB} = 105 \text{ dB} + 12 \text{ dB} = 117 \text{ dB.}$$

⑤ A 10 dB safety margin is added to this attenuation so that the total loss for this example can be taken as 127 dB.

⑥ This loss between the transmitting and receiving antenna is subtracted from the output power of the transmitting antenna:

$$30 \text{ dBm} - 127 \text{ dBm} = - 97 \text{ dBm.}$$

This determines the reception power at the receiving antenna.

- ⑦ The receiving end also has amplifying and attenuating elements. If the same antenna is used as at the transmitter, the antenna gain is 18 dB and the loss from cable (again 4m), lightning protection and plug connectors is 5 dB. The radio signal thus arrives at the receiver's radio module with the following power:
- $$- 97 \text{ dBm} + 18 \text{ dBi} - 5 \text{ dB} = -84 \text{ dBm.}$$
- ⑧ From the table for reception sensitivity of the radio module, the attainable data rate can be read off, in this case 24 Mbps:

Reception sensitivity 802.11a [dBm]		
Mbps	5.150 - 5.725 GHz	5.725 - 5.850 GHz
6	-90	-85
9	-89	-84
12	-88	-83
18	-87	-82
24	-85	-80
36	-81	-76
48	-76	-71
54	-73	-68
72 (Turbo)	-78	-73
96 (Turbo)	-73	-68
108 (Turbo)	-70	-65



This values are the result of a calculation that includes a 'safety margin' of 10dB. As every radio path is unique, these values can only serve as a rough guide.

### 11.5.3 Emitted power and maximum distance

For a simplified calculation of attainable distances and data rates for AirLancer Extender antennae, please refer to the following table. All tables include a 10 dB safety reserve and can be considered to be realistic.

For each antenna, the table has a column for point-to-point mode (P2P, connection between two access points) and for point-to-multipoint mode

(P2mP, connection from an access point to the registered clients, e.g. notebooks).

The last column in the table shows the transmission power reduction to be set so that the upper limits of 30 dBm (802.11a) or 20 dBm (802.11b/g) cannot be exceeded.



The specifications for 802.11a apply only for Germany, the Netherlands, Luxembourg and Great Britain. In Belgium, Austria and Switzerland, only the 802.11b/g standard is approved for outdoor use.

### AirLancer Extender O-18a (802.11a)

- ▶ Antenna gain: 18 dBi
- ▶ Assumed cable loss: 4 dB

Mbps	Maximum distance [km]	
	P2P	P2mP
6	7,94	1,78
9	7,08	1,58
12	6,31	1,41
18	5,62	1,26
24	4,47	1,00
36	2,00	0,45
48	1,00	0,22
54	0,63	0,14
72 (Turbo)	1,41	0,32
96 (Turbo)	0,71	0,16
108 (Turbo)	0,45	0,10

### AirLancer Extender O-30 (802.11b/g)

- ▶ Antenna gain: 15 dBi

- ▶ Assumed cable loss: 9 dB

Mbps	Maximum distance [km]	
	P2P	P2mP
1,0	2,82	1,58
2,0	2,51	1,41
5,5	2,24	1,26
6,0	2,24	1,26
9,0	2,24	1,26
11,0	2,00	1,12
12,0	1,78	1,00
18,0	1,41	0,79
24,0	1,00	0,56
36,0	0,71	0,40
48,0	0,35	0,20
54,0	0,18	0,10

### AirLancer Extender O-70 (802.11b/g)

- ▶ Antenna gain: 8.5 dBi
- ▶ Assumed cable loss: 6 dB

Mbps	Maximum distance [km]	
	P2P	P2mP
1,0	1,26	1,06
2,0	1,12	0,94
5,5	1,00	0,84
6,0	1,00	0,84
9,0	1,00	0,84
11,0	0,89	0,75
12,0	0,79	0,67
18,0	0,63	0,53
24,0	0,45	0,38

Mbps	Maximum distance [km]	
	P2P	P2mP
36,0	0,32	0,27
48,0	0,16	0,13
54,0	0,08	0,07

#### 11.5.4 Transmission power reduction

Every country has regulations concerning the permissible output power from WLAN antennae, often with differences according to the WLAN standard or divided according to indoor or outdoor use. The output power from external antennae may not exceed these maximum power levels. The relevant power level is the result of adding the radio module power and the antenna gain, and subtracting the loss from cable, connectors and lightning protection.

Setting the transmission power reduction is described in the section 'Radio settings' →page 246.



## 12 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.

### 12.1 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!

### 12.2 The client and server principle

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

#### 12.2.1 Configuring the LANCAPI server

Two basic issues are important when configuring the LANCAPI server:

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

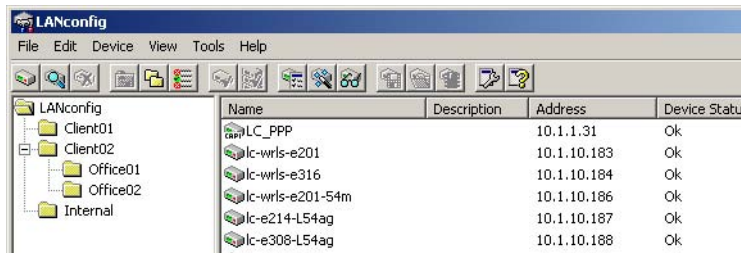
- ▶ Which of the computers in the local network should be able to access the telephone network via LANCAPI?

The LANCAPI server is configured in the following menus:

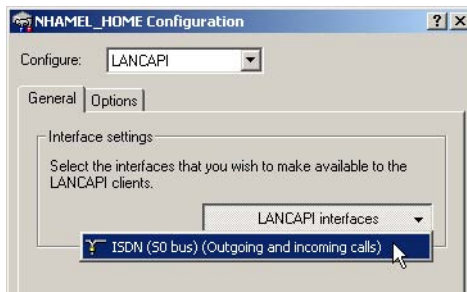
Configuration tool	Run command/menu
LANconfig	LANCAPI
WEBconfig	Expert Configuration / Setup / LANCAPI-module
Terminal/Telnet	cd /setup/LANCAPI-module

### Example configuration with LANconfig

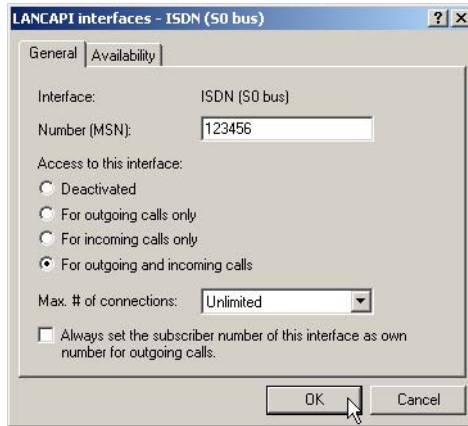
- ① Open the configuration of the router by double-clicking on the device name in the list and select the configuration area **LANCAPI**.



- ② Select the ISDN port you want to set.



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

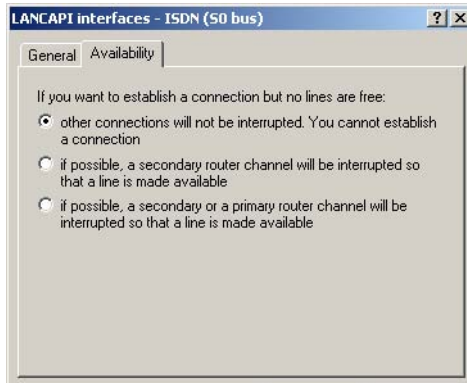


- ④ In the latter case, the LANCAPI will not respond to incoming calls—to receive faxes, for example. Permitting outgoing calls only is useful if you do not have a specific call number available for the LANCAPI.
- ⑤ When the LANCAPI server is activated, enter the call numbers to which the LANCAPI should 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.
- ⑥ 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.
- ⑦ 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.

- ⑧ 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:

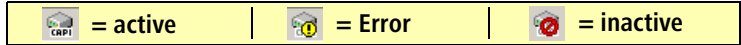
- ▷ The connection via *LANCAPI* can not be performed. A fax program using the *LANCAPI* will then probably attempt to send again at a later time.
- ▷ The connection via the LANCAPI can then be established when a main channel is free. A main channel is the first B channel used when a router connection 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.

### 12.2.2 Installing the LANCAPI client

- ① Place the LANCOM CD in your CD-ROM drive. If the setup program does not automatically start when you insert the CD, simply click 'autorun.exe' in the main directory of the LANCOM CD in the Windows Explorer.
- ② Select the Install LANCOM software entry.
- ③ Highlight the **LANCAPI** option. Click **Next** and follow the instructions for the installation routine.

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


The LANCAPI client starts automatically and shows the status in the windows task bar.

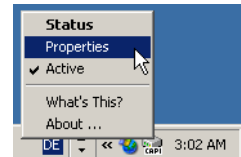


### 12.2.3 Configuration of the LANCAPI clients

The configuration of the LANCAPI clients is used to determine which LANCAPI servers will be used and how these will be checked. All parameters can remain at their default settings if you are using only one LANCOM in your LAN as an LANCAPI server.

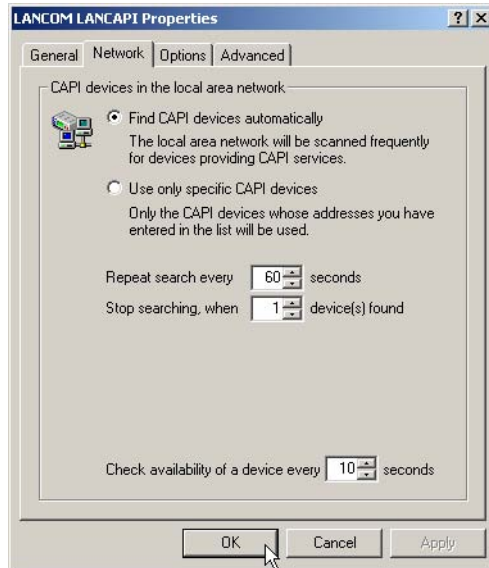
- ① Start the LANCAPI client in the 'LANCOM' program group. Information regarding the drivers for the available service can be found on the 'General' tab.

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



- ② In the LANCAPI client, change to the **Network** tab. First, select whether the PC should find its own LANCAPI server, or specify the use of a particular server.
  - ▷ For the former, determine the interval at which the client should search for a server. It will continue searching until it has found the number of servers specified in the next field. Once the required number of servers has been found, it will stop searching.
  - ▷ In the event that the client should not automatically search for servers, list the IP addresses of the servers to be used by the client. This can be useful if you are operating several LANCOM in your LAN as LANCAPI servers and you would like to specify a server for a group of PCs, for example.

- ▶ It is also possible to set the interval at which the client checks whether the found or listed servers are still active.



## 12.3 How to use the LANCAPI

Two options are available for the use of the LANCAPI:

- ▶ You may use software which interacts directly with a CAPI (in this case, the LANCAPI) port. This type of software searches for the CAPI during its installation and uses it automatically.
- ▶ Other programs such as LapLink can establish a variety of connection types, for example, using Windows Dial-Up Networking. You may select the installed communications device that you would like to use when creating a new dial-up connection. For the LANCAPI, select the entry 'ISDN WAN Line 1'.

## 12.4 The LANCOM CAPI Faxmodem

The CAPI Faxmodem provides a Windows fax driver (Fax Class 1) as an interface between the LANCAPI and applications, permitting the use of standard fax programs with an LANCOM.

## Installation

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

## Faxing with the CAPI Faxmodem

Most major fax programs recognize the CAPI Faxmodem automatically during installation and identify it as a 'Class 1' fax modem. Fax transmissions can thus be realized at speeds of up to 14,400 bps. If your fax program offers you a choice (such as WinFax and Talkworks Pro), select the option 'CLASS 1 (Software Flow Control)' when setting up the modem.



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

## 13 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

### 13.1 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.

#### 13.1.1 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.

### 13.1.2 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'.

### 13.1.3 How are the addresses assigned?

#### IP address assignment

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

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

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

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

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

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

#### Netmask assignment

The network mask is assigned in the same way as the address. If a network mask is entered in the DHCP module, this mask is used for the assignment.

Otherwise, the network mask from the TCP/IP module is used. The order is the same as during the assignment of the addresses.

### **Broadcast address assignment**

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



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

### **Standard gateway assignment**

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

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

### **DNS and NBNS assignment**

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

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

### **Period of validity for an assignment**

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

For each request, a host can ask for a specific period of validity. However, a DHCP server can also assign the host a period of validity that differs from what

it requested. The DHCP module provides two settings for influencing the period of validity:

▶ **Maximum lease time in minutes**

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

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

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

▶ **Default lease time in minutes**

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

### **Precedence for the DHCP server—request assignment**

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

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

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

### **Priority for computer—overwriting an assignment**

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

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

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

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

## Checking of IP addresses in the LAN

Configuration tool	Run/Table
WEBconfig	Expert Configuration Setup / DHCP-module Table-DHCP
Terminal/Telnet	setup/DHCP-module/table-DHCP

The DHCP table provides a list of the IP addresses in the LAN. This table contains the assigned or used IP address, the MAC address, the validity, the name of the computer (if available) and the type of address assignment.

The 'Type' field specifies how the address was assigned. This field can assume the following values:

- ▶ 'new'  
The computer has made its initial request. The DHCP server verifies the uniqueness of the address that is to be assigned to the computer.
- ▶ 'unknown'  
While verifying uniqueness, it was determined that the address has already been assigned to another computer. Unfortunately, the DHCP server has no means of obtaining additional information on this computer.
- ▶ 'static'  
A computer has informed the DHCP server that it has a fixed IP address. This address can no longer be used.
- ▶ 'dynamic'  
The DHCP server assigned the computer an address.

## 13.2 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.

### 13.2.1 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.

### 13.2.2 DNS forwarding

If it cannot serve the request from its own DNS tables, the DNS server forwards the request to other DNS servers. This process is called DNS forwarding.

Here a distinction is made between

- ▶ special DNS forwarding  
Requests for certain name areas are forwarded to certain DNS servers.
- ▶ general DNS forwarding  
All other names not specified in detail are forwarded to the “higher-level” DNS server.

#### Special DNS forwarding

With “special DNS forwarding” name areas can be defined for the resolution of which specified DNS server are addressed.

A typical application for special DNS forwarding results for a home workstation: The user wants to be able to connect to the company intranet and directly to the Internet at the same time. The requests sent into the intranet must be routed to the company DNS server, and all other requests to the DNS server of the provider.

#### General DNS forwarding

All DNS requests that cannot be resolved in another way are forwarded to a DNS server. This DNS server is determined according to the following rules:

- ▶ Initially the router checks whether a DNS server has been entered in its own settings. If it is successful there, it obtains the desired information from this server. Up to two higher-level DNS servers can be specified.

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

- ▶ 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.

### 13.2.3 Setting up the DNS server

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

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

Proceed as follows to set the DNS server:

- ① Switch the DNS server on.

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

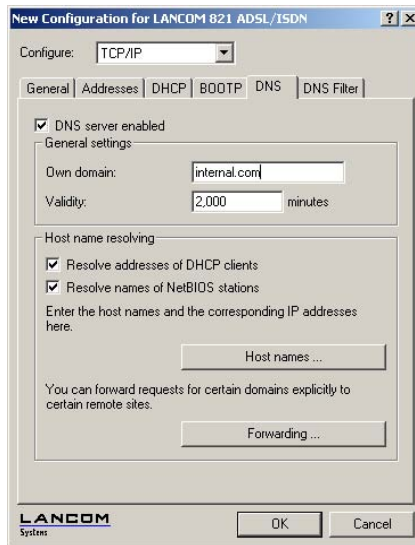


- ② Enter the domain in which the DNS server is located. The DNS server uses this domain to determine whether the requested name is located in the LAN. Entering the domain is optional.

WEBconfig	... ▶ Domain
Terminal/Telnet	set domain yourdomain.com

- ③ Specify whether information from the DHCP server and the NetBIOS module should be used.

WEBconfig	... ▶ DHCP-usage ... ▶ NetBIOS-usage
Terminal/Telnet	set DHCP-usage yes set NetBIOS-usage yes



Activated DNS server in the TCP IP configuration

- ④ The main task of the DNS server is to distinguish requests for names in the Internet from those for other remote stations. Therefore, enter all computers in the Host names table,
  - ▷ for which you know the name and IP address,
  - ▷ that are not located in your own LAN,
  - ▷ that are not on the Internet and

▷ that are accessible via the router.

With the following commands you add stations to the Host names table:

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

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



Stating the domain is optional but recommended.

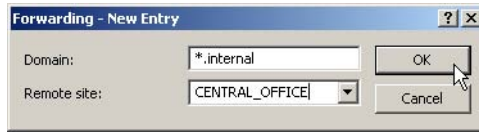
When you now start your mail program, it will probably automatically look for the server 'mail.yourdomain.com'. The DNS server thereupon returns the IP address '10.0.0.99'. The mail program will then look for that IP address. With the proper entries in the IP routing table and name list, a connection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


- ⑤ To resolve entire name areas of another DNS server, add a forwarding entry consisting of a name area and remote station:

LANconfig	TCP/IP ▶ DNS ▶ Forwarding ▶ Add
WEBconfig	... ▶ DNS destination table ▶ Add
Terminal/Telnet	<pre>cd setup/DNS-module/ DNS-destination- table set *.intern COMPANY</pre>

When entering the name areas, the wildcards '?' (for individual characters) and '\*' (for multiple characters) may be used.

To reroute all domains with the ending '.intern' to a DNS server in the LAN of the remote station 'COMPANY', create the following entry:



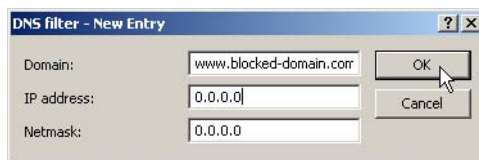
 The DNS server may either be specified by the remote site name (for automatic setting via PPP), or by an explicit IP address of the according name server.

### 13.2.4 URL blocking


① Finally, one can restrict access to certain names or domains with the filter list.

To block the domain (in this case the web server) 'www.offlimits.com' for all computers in the LAN, the following commands and entries are required:

LANconfig	TCP/IP ▶ DNS Filter ▶ DNS filter... ▶ Add
WEBconfig	... ▶ Filter-list ▶ Add
Terminal/Telnet	<pre>cd setup/DNS-module/filter-list set 001 www.blocked.com 0.0.0.0 0.0.0.0</pre>



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

 When entering the domains, the wildcards '?' (represents exactly one character) and '\*' (for any number of characters) are permitted.

To only block the access of a certain computer (e.g. with IP 10.0.0.123) to COM domains, enter the following values:

DNS filter - New Entry

Domain: \*.com

IP address: 10.0.0.23

Netmask: 255.255.255.255

OK Cancel

In the console mode the command is:

```
set 002 *.com 10.0.0.123 255.255.255.255
```



The hit list in the DNS statistics contains the 64 most frequently requested names and provides a good basis for setting up the filter list.

If your LAN uses subnetting, you can also apply filters to individual departments by carefully selecting the IP addresses and subnet masks. The IP address '0.0.0.0' stands for all computers in the network, and the subnet mask '0.0.0.0' for all networks.

### 13.2.5 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](http://www.dynDNS.org).

Thereby a LANCOM becomes available under a certain DNS-resolvable name (FQDN - 'fully qualified Domain Name', for example "http://MyLAN-COM.dynDNS.org").

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

#### How to deposit the current IP address at the Dynamic DNS server?

All Dynamic DNS provider support a set of client programs, which can determine the current assigned WAN IP address of a LANCOM via different methods, and transfer this address - in case of a change - to their respective Dynamic DNS server.

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

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

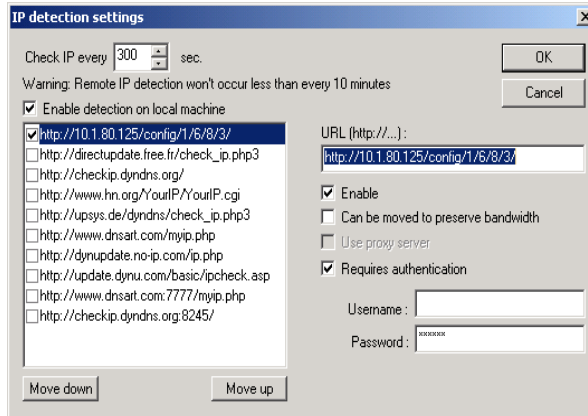


Figure: Picking the current IP address out of a LANCOM

## 13.3 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.

### 13.3.1 Charge-based ISDN connection limits

If charge information is sent to an ISDN connection, the resulting connection charges can be limited quite easily. For example, in its default state, a maxi-

imum 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!

### 13.3.2 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.

### 13.3.3 Settings in the charge module

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

In the charges module, the online time can be monitored and used to control call establishment.

- ▶ Day(s)/Period  
The duration of the monitoring period in days can be specified here.
- ▶ Budget units, Online minutes budget  
The maximum number of ISDN units or online minutes in a monitoring period



The current charge and connect-time information is retained when rebooting (e.g. when installing new firmware) is not lost until the unit is switched off. All the time references here are in minutes.

## 13.4 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.

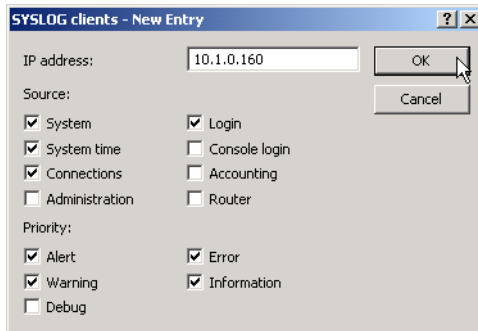
### 13.4.1 Setting up the SYSLOG module

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

### 13.4.2 Example configuration with LANconfig

#### Create SYSLOG client

- ① Start LANconfig. Under 'Management', select the 'Log & Trace' tab.
- ② Turn the module on and click **SYSLOG clients**.
- ③ In the next window click **Add....**
- ④ First enter the IP address of the SYSLOG client, and then set the sources and priorities.



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

The following table provides an overview of the significance of all news sources that can be set in the LANCOM. The last column of the table also



shows the alignment between the internal sources of the LANCOM and the SYSLOG facilities.

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

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

Priority	Meaning	SYSLOG priority
Alert	All messages requiring the attention of the administrator are collected under this heading.	PANIC, ALERT, CRIT
Error	All error messages that can occur during normal operation without requiring administrative intervention are sent to this level (e.g. connection errors).	ERROR

Priority	Meaning	SYSLOG priority
Warning	Error messages that do not affect normal operation of the device are sent to this level.	WARNING
Information	All messages that are purely informative in character are sent to this level (e.g. accounting information).	NOTICE, INFORM
Debug	Transfer of all debug messages. Debug messages generate a high data volume and interfere with the normal operation of the device. They should therefore be disabled during normal operation and should only be activated for troubleshooting.	DEBUG

- ⑤ After you have set all the parameters, confirm the entries with **OK**. The SYSLOG client is then entered with its parameters into the SYSLOG table.

### Facilities

All messages from LANCOM can be assigned to a facility with the **Facility mapping** button and then are written to a special log file by the SYSLOG client with no additional input.

Example

All facilities are set to 'local7'. Under Linux in the file `/etc/syslog.conf` the entry

```
local7.* /var/log/lancom.log
```

writes all outputs of the LANCOM to the file `/var/log/lancom.log`.

## 14 Virtual Private Networks—VPN

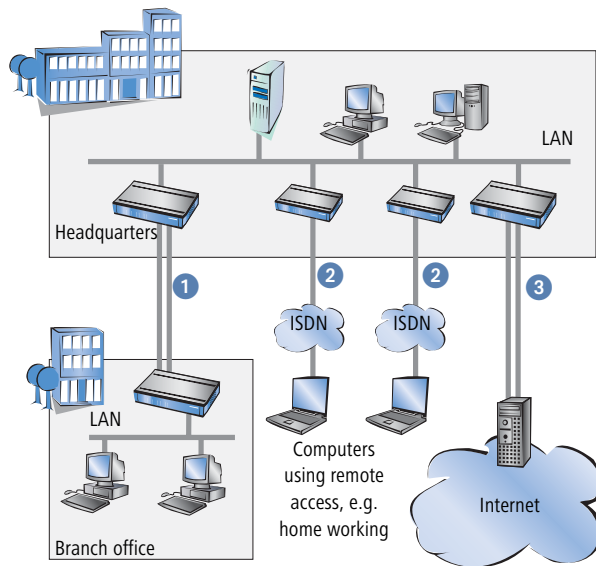
### 14.1 What does VPN offer?

A VPN (**V**irtual **P**rivate **N**etwork) can be used to set up cost-effective, public IP networks, for example via the Internet.

While this may sound unspectacular at first, in practice it has profound effects. To illustrate this, let's first look at a typical corporate network without VPN technology. In the second step, we will see how this network can be optimized by the deployment of VPN.

#### Conventional network infrastructure

First, let's have a look at a typical network structure that can be found in this form or similar forms in many companies:



The corporate network is based on the internal network (LAN) in the headquarters. This LAN is connected to the outside world in three ways:

- 1 A subsidiary is connected to the LAN, typically using a leased line.
- 2 PCs dial into the central network via modem or ISDN connections (Remote Access Service – RAS).

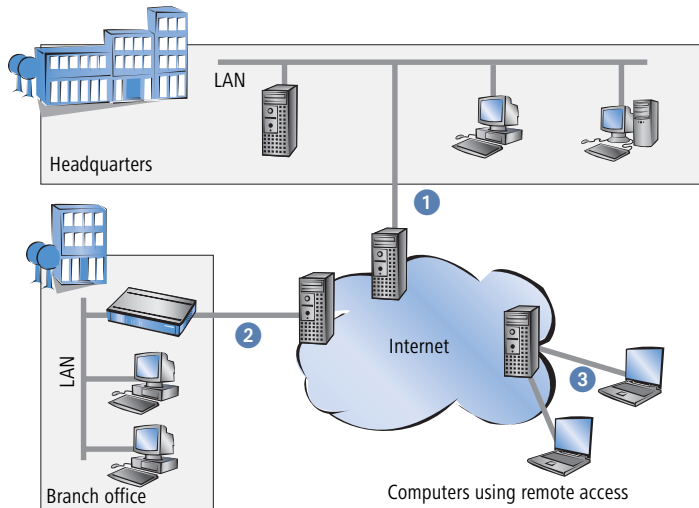
- 3 The central LAN has a connection to the Internet so that its users can access the Web, and send and receive e-mail.

All connections to the outside world are based on dedicated lines, i.e. switched or leased lines. Dedicated lines are very reliable and secure. On the other hand, they involve high costs. In general, the costs for dedicated lines are dependent on the distance. Especially in the case of long-distance connections, keeping an eye out of cost-effective alternatives can be worthwhile.

The appropriate hardware must be available in the headquarters for every type of required connection (analog dial-up, ISDN, leased lines). In addition to the original investment costs, ongoing costs are also incurred for the administration and maintenance of this equipment.

### Networking via the Internet

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



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

- 1 All that is required is the Internet connection of the LAN in the headquarters. Special switching devices or routers for dedicated lines to individual participants are superfluous.

- 2 The subsidiary also has its own connection to the Internet.
- 3 The RAS PCs connect to the headquarters LAN via the Internet.

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

The physical connection no longer exists directly between two participants; instead, the participants rely on their connection to the Internet. The access technology used is not relevant in this case: ideal is the use of broadband technologies such as DSL (Digital Subscriber Line) in combination with flatrate contracts. But also a conventional ISDN line can be used.

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

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

Two technical properties of the IP standard speak against using the Internet as a part of a corporate network, however:

- ▶ The necessity of public IP addresses for all participants
- ▶ The lack of data security of unprotected data transfers

### 14.1.1 Private IP addresses on the Internet?

The IP standard defines two types of IP addresses: public and private. A public IP address is valid worldwide, while a private IP address only applies within a closed LAN.

Public IP addresses must be unique on a worldwide basis. Private IP addresses can occur any number of times worldwide; they must only be unique within their own closed network.

Normally, PCs in a LAN only have private IP addresses, while the router to the Internet also has a public address. All PCs behind this router have access to the Internet via its public IP address (IP masquerading). In such a case, only the router itself is responsive via the Internet. PCs behind the router are not responsive to the Internet without intervention by the router.

### **Routing at the IP level with VPN**

IP connections must be established between routers with public IP addresses in order to link networks via the Internet. These routers provide the connections between multiple subnetworks. When a computer sends a packet to a private IP address in a remote network segment, the local router forwards the packet to the router of the remote network segment via the Internet.

VPN handles the conversion between private and public IP addresses. Without VPN, computers without public IP addresses would not be able to communicate with one another via the Internet.

### **14.1.2 Secure communications via the Internet?**

The idea of using the Internet for corporate communications has been met with skepticism. The reason for this is that the Internet lies beyond a company's field of influence. Unlike dedicated connections, data on the Internet travels through the network structures of third parties that are frequently unknown to the company.

In addition, the Internet is based on a simple form of data transfer using unencrypted data packets. Third parties can monitor and perhaps even manipulate the contents of these packets. Anyone can access the Internet. As a result, third parties may gain unauthorized access to the transferred data.

#### **VPN – Security through encryption**

VPN was developed as a solution to this security problem. If necessary, it can encrypt the complete data communications between two participants. The packets are then unreadable for third parties.

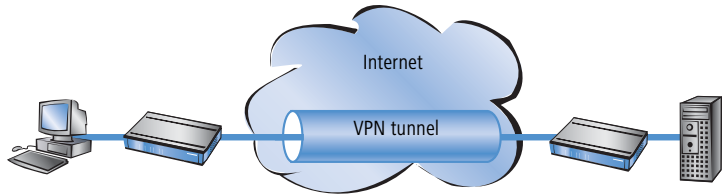
The latest and most secure encryption technologies can be used for VPN. A very high level of security can thus be reached. VPN-protected data traffic via the Internet offers a degree of security that at least corresponds to that of dedicated lines.

Codes usually referred to as "keys" are agreed upon between the participants and used for data encryption. Only the participants in the VPN know these keys. Without a valid key, it is not possible to decrypt the data. They thus remain "private", inaccessible to unauthorized parties.

#### **Send your data through the tunnel – for security's sake**

This also explains the nature of a virtual private network: A fixed, physical connection between the devices of the type required for a direct connection does not exist at any time. Rather, the data flows via suitable routes through

the Internet. With the proper technology, third parties can monitor and even record data traffic. As the packets are encrypted by VPN, the actual content of the packets is inaccessible. Experts compare this state to a tunnel: it's open at either end, but perfectly shielded in between. Secure connections within public IP networks are thus also referred to as "tunnels".



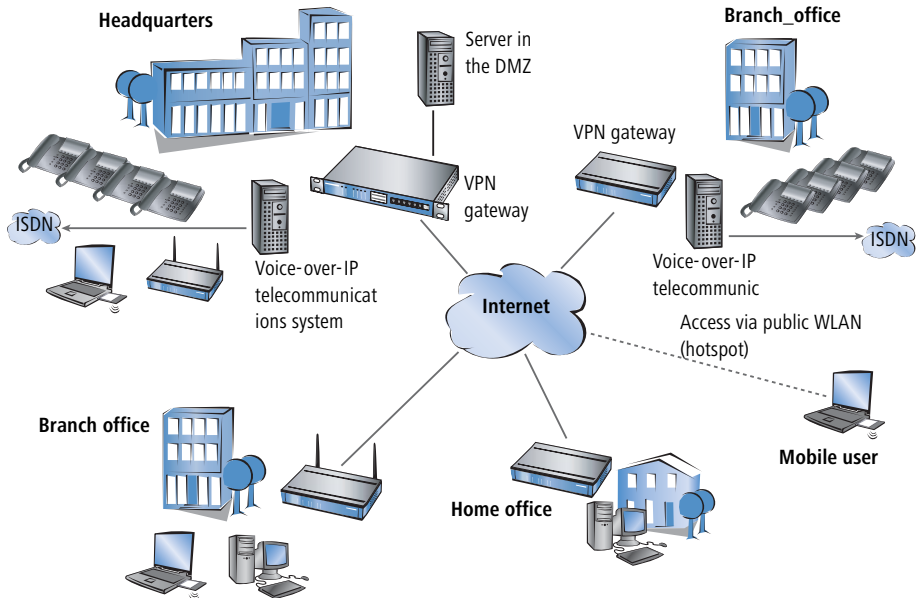
The goal of modern network structures has thus been achieved: secure connections via the largest and most low-cost public IP network: the Internet.

## 14.2 LANCOM VPN: an overview

### 14.2.1 VPN example application

VPN connections are used in many different fields of application. In most cases, a variety of communications technologies is used for transferring both data and audio, and VPN unites these systems into an integrated network. The

following example illustrates a typical application that is often used in practice.



The principal components and features of these applications:

- ▶ The coupling of networks, for example between headquarters and a branch office
- ▶ Connecting external locations without fixed IP addresses via VPN router
- ▶ Connecting home offices without fixed IPs via ISDN or analog modems
- ▶ Connecting to Voice-over-IP telephone exchanges
- ▶ Connecting mobile users, for example when using public WLAN access

### 14.2.2 Advantages of LANCOM VPN

LANCOM VPN solutions have numerous clear advantages over other VPN applications:

- ▶ When connecting remote stations with dynamic IP addresses (e.g. branch-office networks), LANCOM VPN can work with the “Main Mode” instead of the inferior “Aggressive Mode”. This mode offers a highly secure solution that is also easy to implement.



- ▶ When VPN clients are dialing in with the appropriate client software, extended functions in the IKE handshake of LANCOM VPN allow the use of different Preshared Keys (PSKs). Other conventional VPN client connections can use a single common PSK, a situation that is a compromise in terms of security.
- ▶ The use of LANCOM Dynamic VPN means that the headquarters with a static IP address can be connected to external locations that have neither fixed IP addresses nor flatrate Internet access. As these remote stations generally do not use dynamic DNS services, they cannot be reached via an IP address or via a name that can be resolved by DNS. The extensions provided by LANCOM Dynamic VPN make it possible to use ISDN signalling to establish connections.

Further information about these features can be found in the description of the applications.

### 14.2.3 LANCOM VPN functions

This section lists all of the functions and properties of LANCOM VPN. This overview will provide a great deal of information for VPN experts. It is very compact, but contains a lot of complex, specialized terminology. Knowledge of the technical basics of VPN are required to understand this section. Don't worry: it's no problem if you skip this section. The information contained here is not required to set up and use LANCOM VPN.

- ▶ VPN in accordance with IPSec standard
- ▶ VPN tunnel via leased lines, switched connections and IP networks
- ▶ IPSec main and aggressive mode
- ▶ LANCOM Dynamic VPN: Public IP addresses can be static or dynamic (initiation of a connection towards remote sites with dynamic IP addresses requires ISDN)
- ▶ IPSec protocols AH and ESP in transport and tunnel mode
- ▶ Hash algorithms:
  - ▷ HMAC-MD5-96, Hash length 128 bit
  - ▷ HMAC-SHA-1-96, Hash length 160 bit
- ▶ Symmetrical encryption methods
  - ▷ AES, key length 128 bit
  - ▷ Triple-DES, key length 168 bit
  - ▷ Blowfish, key length 128 - 448 bit
  - ▷ CAST, key length 128 bit

- ▷ DES, key length 56 bit
- ▶ IKE key exchange with Preshared Keys
- ▶ Key exchange via Oakley, Diffie-Hellman algorithm with key lengths 768 bit, 1024 bit or 1536 bit, well-known groups 1, 2 and 5
- ▶ Key management in accordance with ISAKMP
- ▶ Apart from conventional IPSec implementations, LANCOM devices offer extended functionality, such as the LANCOM Dynamic VPN that allows the use of the high-security IKE Main Mode even with dynamic IP addresses.
- ▶ In combination with the LANCOM Advanced VPN Client, a separate pre-shared key can be used for each connection even when using IKE Aggressive Mode connections.

## 14.3 VPN connections in detail

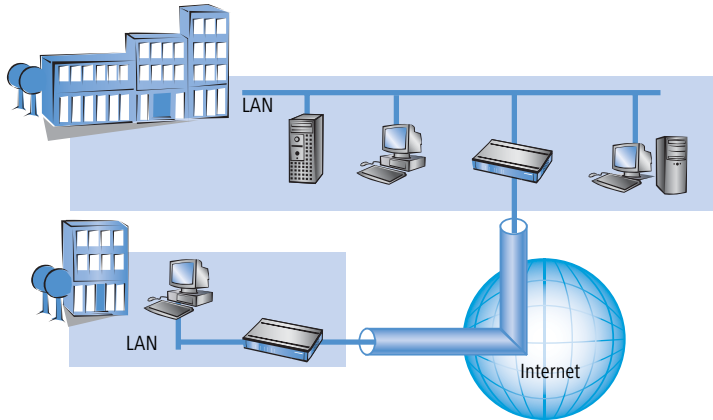
Two types of VPN connections are available:

- ▶ VPN connections linking two local networks. This type of connection is also known as a "LAN-LAN coupling".
- ▶ The connection of an individual computer with a network, generally via a dial-in connection (Remote Access Service – RAS).

### 14.3.1 LAN-LAN coupling

The coupling of two remote networks is known as a LAN-LAN coupling. With such a connection, the devices in one LAN can access those of the remote LAN (assuming they have the necessary access rights).

In practice, LAN-LAN couplings are frequently used between company headquarters and subsidiaries, or for connections to partner companies.



A VPN-enabled router (VPN gateway) is located at either end of the tunnel. The configuration of both VPN gateways must be matched to one another.

The connections are transparent for the remaining devices in the local networks, i.e., they appear to have a direct connection. Only the two gateways must be configured for the VPN connection.

### Internet access in parallel

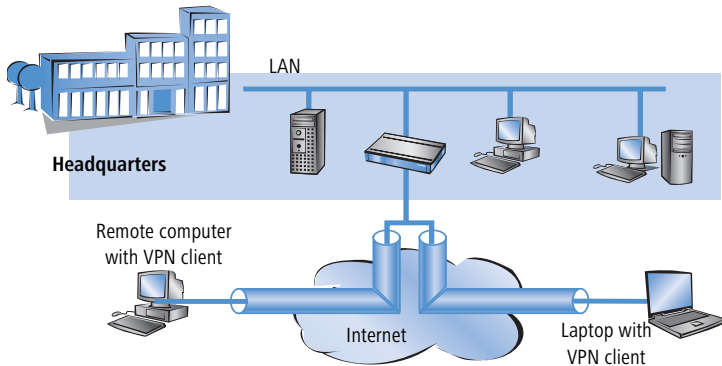
The Internet access for VPN can be used simultaneously for other Internet applications, such as web-browsing or e-mail. For security reasons, the parallel Internet access may be unwanted in some cases. For instance, if a branch office should be enforced to access the Internet only via a central firewall. For such applications the parallel Internet access can be disabled as well.

### 14.3.2 Dial-in connections (Remote Access Service)

Individual remote computers (hosts) can access the resources of the LAN via dial-up connections. Practical examples of this are employees working from home or field staff that dial into the company network.

If the dial-up connection of an individual computer to a LAN is to be realized via VPN, that computer first connects to the Internet. A special VPN client

software then sets up a tunnel to the VPN gateway of the LAN using this Internet connection.



The VPN gateway of the LAN must support the establishment of VPN tunnels with the VPN client software of the remote PC.

## 14.4 What is LANCOM Dynamic VPN?

LANCOM Dynamic VPN is a patent-pending LANCOM Systems technology which permits VPN tunnels to be connected **to** remote stations that do not have a static, but only a dynamic IP address.

Who needs LANCOM Dynamic VPN and how does it work? We will answer this question in two steps: First, a look at the basics of IP addressing will show the problem of static IP addresses. The second step shows the solution thereof with LANCOM Dynamic VPN.

### 14.4.1 A look at IP addressing

Every participant on the Internet needs an IP address. Participants even need a special kind of IP address - a public one. The administration of public IP addresses is handled from central locations in the Internet. Each public IP address may only occur once on the entire Internet.

Local IP-based networks do not use public, but private IP addresses. For this reason, a number of address ranges within the entire IP address range have been reserved for private IP addresses.

A computer connected to both a local network and directly to the Internet therefore has two IP addresses: a public one for communication with the rest

of the Internet and a private one by which the computer can be reached within the local network.

### **Static and dynamic IP addresses**

Public IP addresses must be applied for and managed, which involves costs. There is also only a limited number of public IP addresses. For this reason, not every Internet user has his or her own fixed (static) IP address.

The alternative to static IP addresses are the so-called dynamic IP addresses. A dynamic IP address is assigned to an Internet user by the Internet Service Provider (ISP) upon dialling-in, and remains valid for the duration of the connection. The ISP takes an unused address selected at random from their pool of IP addresses. This IP address is only temporarily assigned to the user for the duration of a given connection. When the connection is ended, the IP address is once again free and the ISP can assign it to another user.

Many flatrate connections, too, are realised with via dynamic IP addresses. Every 24 hours or so, the connection is forcibly interrupted. The new connection is generally assigned with a new and different IP address.

### **Advantages and disadvantages of dynamic IP addresses**

This process has a very important advantage for ISPs: they only need relatively small pools of IP addresses. Dynamic IP addresses are also favorable for users: it's not necessary for them to apply for static IP addresses in advance - they can connect to the Internet immediately. It's also not necessary for them to manage IP addresses. This saves trouble and costs. The other side of the coin: A user without a static IP address cannot be addressed directly from the Internet.

This is a major problem when setting up VPNs. If, for example, Computer A would like to communicate with Computer B using a VPN tunnel on the Internet, Computer A needs the remote computer's IP address. If B only has a dynamic address, A cannot know that address and therefore cannot contact B. The LANCOM Dynamic VPN offers the answer here.

#### **14.4.2 This is how LANCOM Dynamic VPN works**

Let's use two examples to explain how LANCOM Dynamic VPN works (designations refer to the IP addressing type of the two VPN gateways):

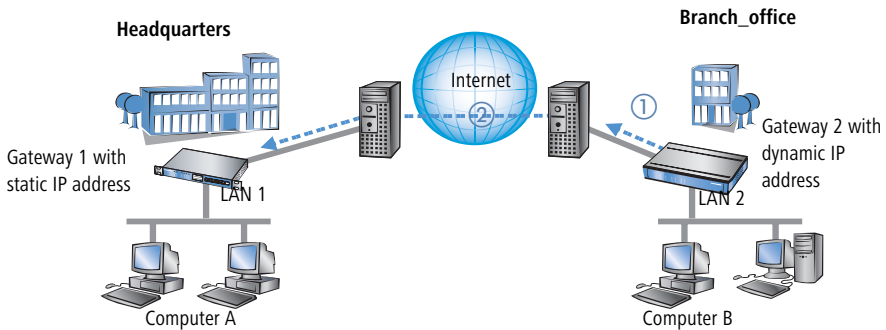
- ▶ dynamic – static

- ▶ static – dynamic
- ▶ dynamic – dynamic

### Dynamic – static

If a user on computer B in LAN 2 wishes to connect to computer A in LAN 1, then gateway 2 receives a request and tries to establish a VPN tunnel to gateway 1. Gateway 1 has a static IP address and can be directly contacted over the Internet.

A problem arises in that the IP address from gateway 2 is assigned dynamically, and gateway 2 must communicate its current IP address to gateway 1 when attempting to connect. In this case, LANCOM Dynamic VPN takes care of transmitting the IP address during connection establishment.



- ① Gateway 2 connects to the Internet and is assigned a dynamic IP address.
- ② Gateway 2 contacts Gateway 1 via its known public IP address. LANCOM Dynamic VPN enables the identification and transmission of the actual IP address of Gateway 2. Gateway 1 initiates the VPN tunnel then.

The great advantage of LANCOM devices with this application: Instead of the “Aggressive Mode” that is normally used when connecting VPN clients to the headquarters, the far more secure “Main Mode” can be applied. Although with Main Mode more unencrypted messages can be exchanged during the IKE handshake, the method is overall more secure than Aggressive Mode.

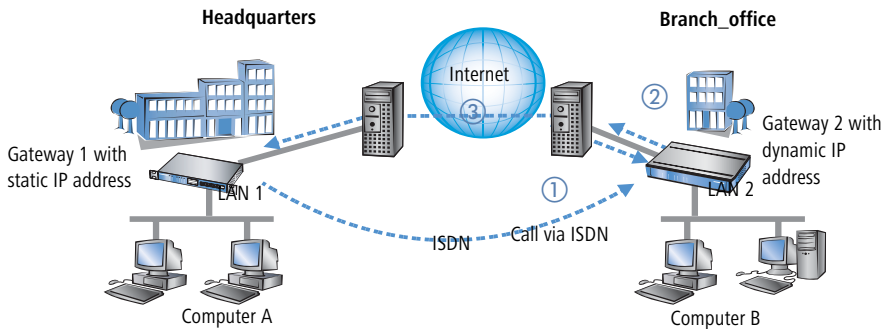


An ISDN line is not necessary for establishing this type of connection. The dynamic end communicates its IP address encrypted via the Internet protocol ICMP (or alternatively via UDP).

### Static – dynamic

If, on the other hand, computer A in LAN 1 requires a connection to computer B in LAN 2, for example when headquarters carries out remote maintenance at the external locations, then gateway 1 receives the request and attempts to establish a VPN tunnel to gateway 2. Gateway 2 only has a dynamic IP address and cannot be directly contacted over the Internet.

With LANCOM Dynamic VPN, the VPN tunnel can be set up nevertheless. The connection is established in three steps:



- ① Gateway 1 calls Gateway 2 via ISDN. It takes advantage of the ISDN functionality of sending its own subscriber number via the D-channel free of charge. Gateway 2 determines the IP address of Gateway 1 from the preconfigured VPN remote stations using the received subscriber number.

If Gateway 2 does not receive a subscriber number via the D-channel (if that particular ISDN service feature is not available, for example) or an unknown number is transferred, the authentication will be performed via the B-channel. Once the negotiation was successful, Gateway 1 sends its IP address and closes the connection on the B-channel immediately.

- ② Now it's Gateway 2's turn: It first connects to its ISP and is assigned a dynamic IP address.
- ③ Gateway 2 can now establish the VPN tunnel to Gateway 1. The static IP address of gateway 1 is known, of course.

The advantage of LANCOM devices, for example when connecting from the headquarters to branch offices: The functions in LANCOM Dynamic VPN also allow access to networks without a flatrate, i.e. networks that are not always online. The ISDN connection and an associated MSN act to substitute the another address, such as a static IP address or the dynamic address

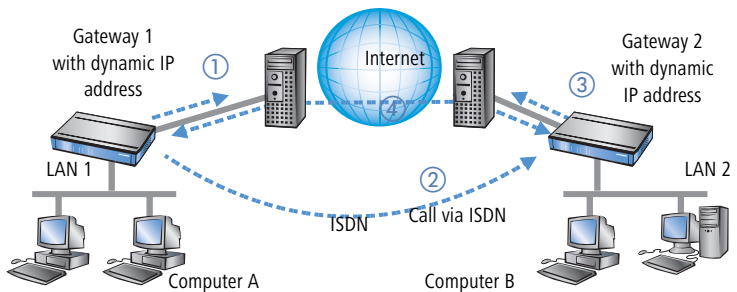
translation via dynamic DNS services, a solution often used with flatrate connections.



The described connection set up requires an ISDN connection for both VPN gateways. But usually no charges will arise for this procedure.

### Dynamic – dynamic

With LANCOM Dynamic VPN, VPN tunnels can also be set up between two gateways that both only have dynamic IP addresses. Let's modify the previous example so that in this case Gateway 1 also has a dynamic IP address. Once again, Computer A would like to connect to Computer B:



- ① Gateway 1 connects to its ISP and is assigned a public, dynamic IP address.
- ② It then calls Gateway 2 via ISDN to send this dynamic address. Three procedures are used to send the address:

- ▶ **As information in the LLC element of the D-channel.** In the D-channel protocol of Euro-ISDN (DSS-1), the so-called LLC (**L**ower **L**ayer **C**ompatibility) element can be used to send additional information to the remote station. This transfer takes place before the B-channel connection is established. Once the address has been sent successfully, the remote station rejects the call. Charges are thus not incurred for a B-channel connection. The IP address is sent nevertheless for free in this case.



The LLC element is generally available as a standard feature in Euro-ISDN that does not require registration or activation. It may be disabled by telephone companies or individual exchanges, however.



The LLC element is not available in 1TR6, the German national ISDN. The procedure described above thus will not work with 1TR6.

- ▷ **As a subaddress via the D-channel.** If it is not possible to send the address via the LLC element, Gateway 1 will attempt to send the address as a so-called subaddress. Like the LLC element, the subaddress is an information element of the D-channel protocol that permits short items of information to be sent free of charge. In this case, the telephone company must enable the 'subaddressing' feature first; this is generally subject to a charge. As with the LLC element, the call is rejected by the remote station once the IP address has been transferred successfully. The connection thus remains free of charge.
- ▷ **Via the B-channel.** If both attempts to send the IP address via the D-channel fail, then a conventional connection via the B-channel must be established to send the IP address. The connection is dropped immediately after the IP address has been sent. This connection is subject to the usual charges.

③ Gateway 2 connects to the ISP and receives a dynamic IP address.

④ Gateway 2 now sets up the VPN tunnel to Gateway 1.



Dynamic VPN works only between LANCOM that each feature at least one ISDN port that can be used for the ISDN connection.

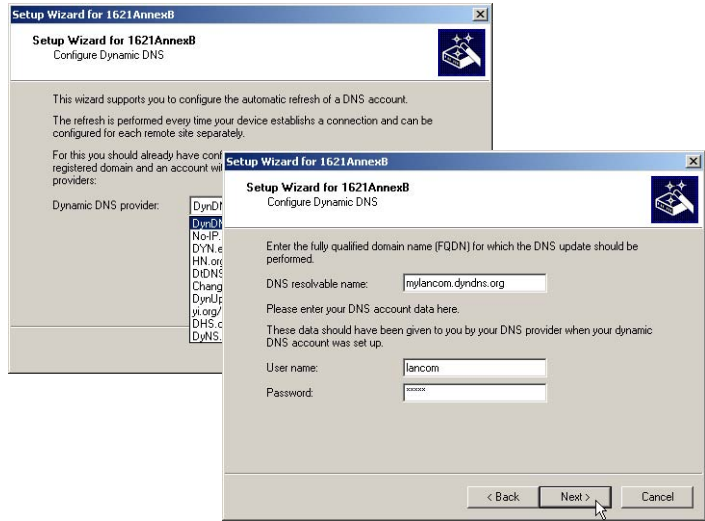
### Dynamic IP addresses and DynDNS

It is also possible to establish a connection between two stations using dynamic IP addresses by using so-called dynamic DNS services (DynDNS). The address of the tunnel end-point is not defined as an IP number (which is, of course, dynamic and subject to frequent change) but as a static name instead (e.g. MyLANCOM@DynDNS.org).

Two things are needed for translating a name to its current IP address: A dynamic DNS server and a dynamic DNS client:

- ▶ The first, available from numerous providers in the Internet, is a server that is in communication with Internet DNS servers.
- ▶ The dynamic DNS client is integrated in the device. It can make contact to any one of a number of dynamic-DNS service providers and, assuming that a user account has been set up, automatically update its current IP

address for the DNS name translation. This can be set up very conveniently with a Wizard under LANconfig (also see 'Dynamic DNS' auf Seite 284):



For reasons of security and availability, LANCOM recommends the use of Dynamic VPN in preference to dynamic DNS-based VPN solutions. Dynamic VPN is based on direct connections via the ISDN network and ensures a higher degree of availability than dynamic DNS services in the Internet.

## 14.5 Configuration of VPN connections

Two questions are answered in the configuration of VPN connections:

- ▶ Between which VPN gateways (remote stations) is the connection established?
- ▶ What security parameters are used to secure the VPN tunnel between the two gateways?
- ▶ Which networks or computers can intercommunicate via these tunnels?



This section introduces the basic considerations for configuring VPN connections. Considered first of all is the simple connection of two local networks. Special cases such as dialling in to LANs with

individual computers (RAS) or the connection of structured networks will be covered subsequently.

### 14.5.1 VPN tunnel: Connections between VPN gateways

Virtual Private Networks (VPNs) are used to interconnect local networks over the Internet. This involves the routing of the private LAN IP addresses via an Internet connection between two gateways with public IP addresses.

For the secure routing of private IP addresses over the Internet, a VPN connection, also known as a VPN tunnel, is established between the two LANs.

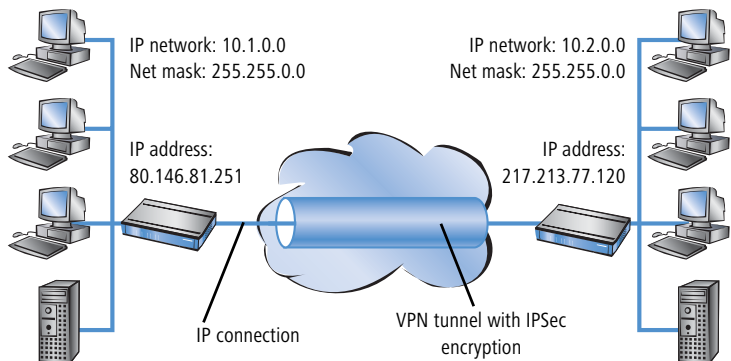
The VPN tunnel has two important tasks:

- ▶ To shield the transported data from unauthorized access
- ▶ To route private IP addresses via an Internet connection that can normally only be used to route public IP addresses.

The VPN connection between the two gateways is defined by the following parameters:

- ▶ The end-points of the tunnel, the VPN gateways, each of which are accessible via public IP addresses (static or dynamic)
- ▶ The IP connection between the two gateways
- ▶ The private IP address range that are to be routed between the VPN gateways
- ▶ Setting relevant to security, such as passwords, IPSec keys etc. to shield the VPN tunnel

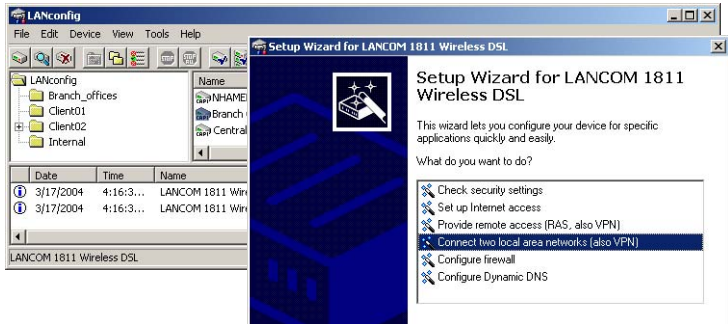
This information is contained in the so-called VPN rules.



## 14.5.2 Set up VPN connections with the Setup Wizard

If possible, make use of the Setup Wizard within LANconfig to set up VPN connections between local networks. The Wizard guides you through the configuration and makes all the necessary settings for you. Carry out the configuration on both routers, one after the other.

- 1 Choose your device from the selection window in LANconfig and select the **Setup Wizard** button or use the menu bar **Tools ▶ Setup Wizard**.



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

This Wizard automatically sets up the VPN connections essential for typical LAN-LAN coupling. In the following situations, the VPN connections will have to be configured manually:

- ▶ Where no Windows computer with LANconfig is available. In this case, the necessary parameters are set with WEBconfig or via the Telnet console.
- ▶ Where only selected portions of the LAN (intranet) are to communicate with other computers via the VPN connection. This is the case where, for example, the intranet is connected to further subnets with routers, or when only selected portions of the intranet should have access to the VPN connection. In such cases, additional parameters are defined supplementary to those entered in the Setup Wizard.
- ▶ Configuring VPN connections to third-party devices.

### 14.5.3 Inspect VPN rules

VPN rules represent a combination of various pieces of information and they are not directly defined in a LANCOM device; instead, they are compiled from a variety of sources. This is why it is not possible to inspect the VPN rules with LANconfig or any other configuration tool.

Information about the current VPN rules in the device can be retrieved with the Telnet console. Start a Telnet connection to the VPN gateway and enter the command **show vpn** in the console:

```
Telnet 192.168.2.100
#
! LANCOM 1811 Wireless DSL
! Ver. 3.52.0015 / 02.03.2004
! SN. 01530000046
! Copyright (c) LANCOM Systems

VPN_MHAMEL, Connection No.: 002 (LAN)
Password:
VPN_MHAMEL:/
> show vpn
> show vpn

VPN PH SPD and Ike configuration:
# of connections = 1
Connection #1          ipsec 192.168.2.0/255.255.255.0<->10.0.0.0/255.0.0.0 any
Name:                  VPN-GW-2
Unique Id:             ipsec-1-VPN-GW-2-pr0-10-r0
Flags:                 ps main-mode
Local Network [0]:    IPV4_ADDR_SUBNET<any:0, 192.168.2.0/255.255.255.0>
Local Gateway:        IPV4_ADDR<any:0, 80.146.81.251>
Remote Gateway:       IPV4_ADDR<any:0, 217.213.77.120>
Remote Network [0]:   IPV4_ADDR_SUBNET<any:0, 10.0.0.0/255.0.0.0>
```

The output informs you of the network relationships that are relevant to VPN connections to other networks.

In this example, the local network at a branch office (network 192.168.2.0, netmask 255.255.255.0) is connected to the network at the headquarters (network 10.0.0.0, netmask 255.255.255.0). The public IP address of the local gateway is 80.146.81.251, and that of the remote VPN gateway is 217.213.77.120.



Entering “any:0” displays the protocols and ports that can be used over the connection.

Further output is displayed by the command “show vpn long”. The information displayed here covers network relationships and also the parameters that are relevant to security, such as IKE and IPSec proposals.

### 14.5.4 Manually setting up VPN connections

Manually setting up VPN connections involves the tasks described previously:

- ▶ Definition of the tunnel endpoints
- ▶ Definition of the security-related parameters (IKE and IPSec)
- ▶ Definition of the VPN network relationships, i.e. the IP address ranges to be connected. Should the IP ranges overlap at both ends of the connection, please refer to the section 'N:N mapping' auf Seite 80.
- ▶ When coupling Windows networks (NetBIOS/IP): Without WINS servers at both ends of the VPN connection (such as when linking a home office), the LANCOM can take over the necessary NetBIOS proxy functions. To this end, the NetBIOS module in the LANCOM must be activated, and the corresponding VPN remote site must be entered into the NetBIOS module as the remote site. Should WINS servers be present in both of the coupled networks, then the NetBIOS module should be deactivated so that the LANCOM does not perform NetBIOS proxy functions.
- ▶ When using LANCOM Dynamic VPN: Entry for the corresponding remote site in the PPP list with a suitable password for the Dynamic VPN handshake. The username entered here must correspond with the name entered in the remote device that describes the VPN connection to this local device. Activate "IP routing". If Windows networks are also to be coupled, then the NetBIOS entry should be activated here.

The tunnel endpoints, i.e. the local VPN gateway and each of the VPN remote stations, are entered into the VPN connection list.

Manually configuring the VPN connection involves the following steps:

- ① Create an entry for the remote VPN gateway in the connection list and enter its public IP address.
- ② The security parameters for the VPN connection are normally taken from the prepared list, and all that is required here is to define an IKE key.
- ③ For a Dynamic VPN connection, create a new entry in the PPP list with the name of the remote VPN gateway as the remote station, with the name of the local VPN gateway as the User Name, and set a suitable password. Be sure to activate the IP routing for this PPP connection and, if required, the routing of "NetBIOS over IP" as well. The remaining PPP parameters, such as the procedure for checking the remote station, can be defined in the same way as for other PPP connections.
- ④ The main task in setting up VPN connections is in defining the network relationships. Which IP address ranges at each end of the VPN tunnel should be included in the secured connection?

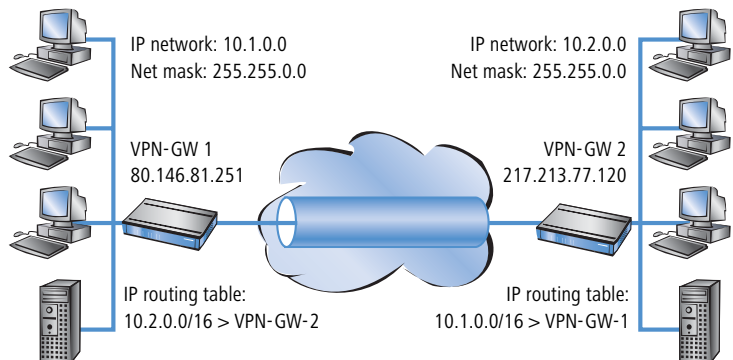
## 14.5.5 Prepare VPN network relationships

The firewall integrated into LANCOM routers is a powerful instrument for defining source and target address ranges between which data transfer (and limitations to it) can be enabled or prohibited. These functions are also used for setting up the network relationships for the VPN rules.

In the simplest case, the firewall can generate the VPN rules automatically.

- ▶ The local intranet serves as the source network, i.e. the same private IP address range that the local VPN gateway itself belongs to.
- ▶ For automatically generated VPN rules, the target networks are those network ranges that have a remote VPN gateway set as their router.

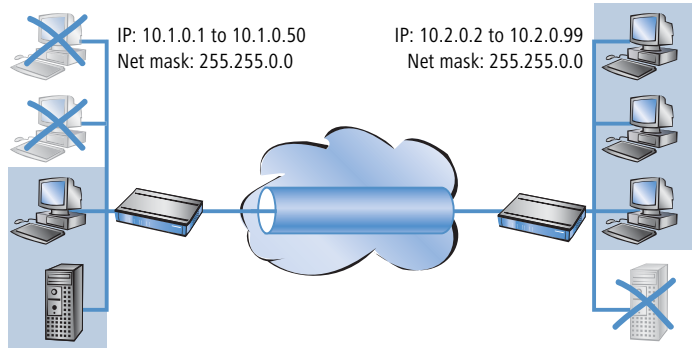
To activate the automated rule generation, simply switch on the corresponding option in the firewall<sup>1</sup>. When coupling two simple local networks, the automatic VPN can interpret the necessary network relationships from the IP address range in its own LAN and from the entry for the remote LAN in the IP routing table.



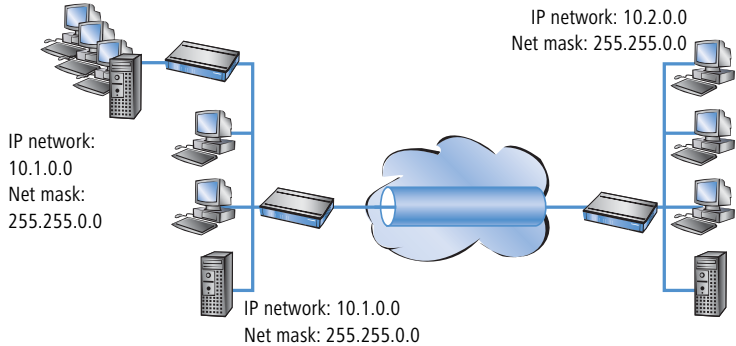
The description of the network relationships is more complicated if the source and target networks are not only represented by the intranet address ranges of the connected LANs:

1. automatic when using the VPN installation Wizard under LANconfig

- ▶ When only a portion of the local intranet is to be available to the remote network, then the automatic method is unsuited as the IP address range that is open to the VPN connection is too large.



- ▶ In many network structures, the local network is connected by further routers to sections of other networks with their own IP address ranges. Additional settings are required to include these address ranges in the network relationship.




In these cases, the network relationships that describe the source and target networks must be entered manually. Depending on the situation, the scope of the automatically generated VPN rules may be extended, although sometimes it is better to deactivate the automatic VPN system to prevent unwanted network relationships.

The necessary network relationships are defined by the appropriate firewall rules under the following circumstances:

- ▶ In the firewall rules, the option “Consider this rule when generating VPN rules” must be activated.




---

 The firewall rules for generating VPN rules are active even when the actual firewall function in the LANCOM device is not required and is switched off!


- ▶ Make sure that the firewall action is set to “Transfer”.
- ▶ Sources and targets for the connection can be entered as individual stations, certain IP address ranges, or whole IP networks.

---

 It is vital that target networks are defined in the IP routing table so that the router in the LANCOM devices can forward the appropriate data packets to the other network. You can make use of the entries that already exist there and simply enter a higher-level network as the target. The intersecting portion of the target network defined by the firewall and the subordinate entries in the IP routing table is integrated into the network relationships for the VPN rules.


**Example:** The target networks 10.2.1.0/24, 10.2.2.0/24 and 10.2.3.0/24 are entered into the IP routing table and can be accessed via the router VPN-GW 2. An entry for the target network 10.2.0.0/16 is sufficient for these three subnets to be included in the VPN rules.

---

 The definition of source and target networks must agree at both ends of the VPN connection. It is not possible, for example, to map a larger target address range to a smaller source address range at the opposite end. Decisive here are the IP address ranges allowed by the VPN rules and not the networks defined in the firewall rules. These can be very different from the network relationships in the VPN rules because of the intersecting ranges.

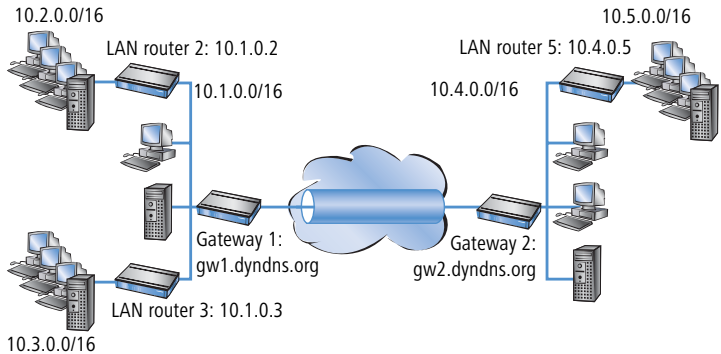
- ▶ VPN connections can also be limited to certain services or protocols according to your requirements. This means that the VPN connection can be limited to use only with a Windows network, for example.

---

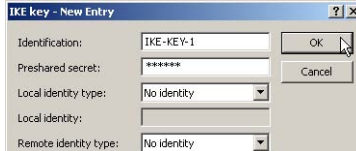
 These limitation should be defined by a separate set of rules that applies only to the firewall and that will not be used in generating VPN rules. Combined firewall/VPN rules can very quickly become highly complex and difficult to comprehend.

## 14.5.6 Configuration with LANconfig

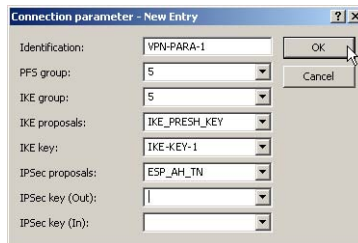
The section demonstrates how LANconfig can be used to configure a LAN-LAN coupling with additional subnets. In this section, VPN gateway 1 will be configured and then the configuration of gateway 2 with the help of WEBconfig will be demonstrated.



- 1 When configuring VPN, access the “IKE param.” tab and create a new IKE key for the connection:



- 2 Under the “General” tab, create a new entry in the list of Connection parameters. Select the IKE key created earlier for this. PFS and IKE groups can also be selected in the same way as IKE and IPSec proposals from the options prepared earlier.



- 3 You should then generate a new entry in the Connection list with the name of the remote gateway as “name for the connection”. For the “Remote

gateway”, enter the public address of the remote station: either the fixed IP address or the name for translation by DNS.

**Connection list - New Entry**

Name of connection: VPN-GATEWAY-2

Short hold time: 0 seconds

Dead Peer Detection: 0 seconds

Extranet address: 0.0.0.0

Remote gateway: gw2.dyndns.org

Connection parameter: VPN-PARA-1

Rule Creation: Auto

Dynamic VPN connection (only with compatible remote stations):

- No dynamic VPN
- Dynamic VPN (a connection is created to transmit IP addresses)
- Dynamic VPN (IP addresses are transmitted without establishing a connection if possible)
- Dynamic VPN (an ICMP packet will be sent to transmit IP addresses)
- Dynamic VPN (an UDP packet will be sent to transmit IP addresses)

IKE exchange (only in conjunction with "No dynamic VPN"):

- Main mode
- Aggressive mode

- ④ When using LANCOM Dynamic VPN: Change to the “Communication” configuration area. Using the “Protocols” tab, make a new entry in the PPP list. Select the remote VPN gateway as the remote site, enter the User Name as the name of the VPN connection that the remote VPN gateway uses to address the local device, and enter a suitable password that is identical at both locations.

**PPP list - New Entry**

Remote site: VPN-GATEWAY-2

User name: VPN-GATEWAY-1

Password: \*\*\*\*\*

Activate IP routing

Activate NetBIOS over IP

Activate IPX routing

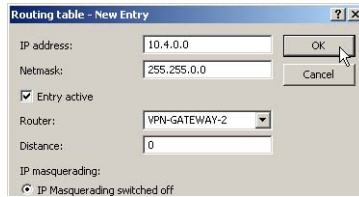
Authentication of the remote site:

- No active authentication. However, the remote site (your Internet Service Provider for example) can do his own authentication.
- Authenticate the remote site via PAP.
- Authenticate the remote site via CHAP.

Be sure to activate "IP routing" and, if required, "NetBIOS over IP" (→page 310).

- ⑤ Change to the “IP Router” configuration area. On the “Routing” tab, make a new entry in the routing table for those parts of networks that are to be

accessible in the remote and in the local LAN. In each case, define the router as the remote VPN gateway and switch the IP masquerading off.



For the "VPN gateway 1", the following entries are necessary so that the remote network sections can be reached.

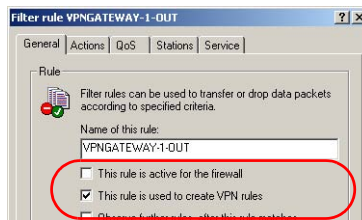
IP address	Net mask	Router	IP masquerading
10.4.0.0	255.255.0.0	VPN gateway 2	No
10.5.0.0	255.255.0.0	VPN gateway 2	No


For those subnetworks connected to your own LAN, define the router as the IP address for the appropriate LAN router.

IP address	Net mask	Router	IP masquerading
10.2.0.0	255.255.0.0	10.1.0.2	No
10.3.0.0	255.255.0.0	10.1.0.3	No

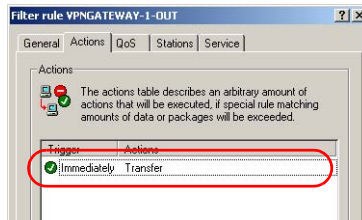
These entries enable VPN gateway 1 to forward packets arriving from the remote network to the correct sections of the local network.

- Change to the "Firewall/QoS" configuration area. On the "Rules" tab, add a new firewall rule with the name "VPN GATEWAY 1 OUT" and activate the option "This rule is used to create VPN rules". This ensures that IP networks described in this rule will be used in establishing VPN network relationships.

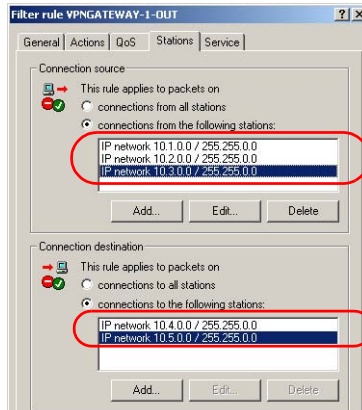


 As a rule, it is recommended that you keep the rules used for making network relationships separate from those firewall rules that affect the services used in communications, for example.

- ⑦ On the “Actions” tab for these firewall rules, set the “Packet Action” to “Transmit”.

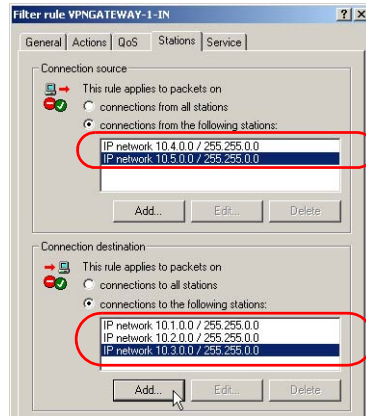


- ⑧ On the “Stations” tab for these firewall rules, define the source of the data transfers as the subnets at the local site, and set the destination as all of the subnets at the remote site.



- ⑨ Now for the incoming data transmissions, generate a firewall rule named “VPN GATEWAY 1 IN” with the same parameters as the rule just described.

The only difference is that the source and the destination networks are swapped.

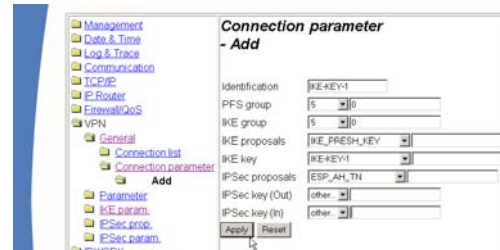


## 14.5.7 Configuration with WEBconfig

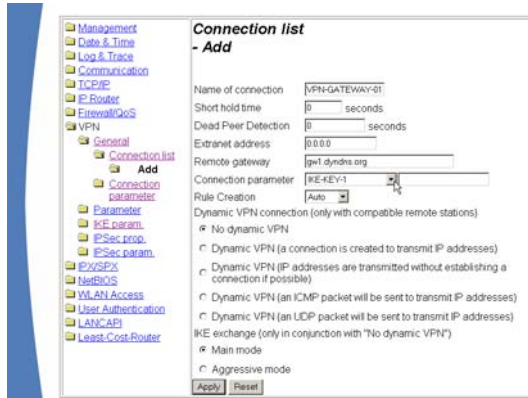
- ① Under **Configuration ▶ VPN ▶ IKE-Param. ▶ IKE key** set a new IKE key for the connection:



- ② Under **Configuration ▶ VPN ▶ General ▶ Connection parameters** define a new "VPN layer" for the connection parameters. Select the IKE key created earlier for this.



- ③ Under **Configuration ▶ VPN ▶ Connection list** generate a new entry with the name of the remote gateway set to "Name". For the "Remote gateway", enter the public address of the remote station: either the fixed IP address or the name for translation by DNS.



- ④ When using LANCOM Dynamic VPN: Under **Configuration ▶ Setup ▶ WAN module ▶ PPP list** make a new entry. Select the remote VPN gateway as the remote site, enter the User Name as the name of the VPN connection that the remote VPN gateway uses to address the local device, and enter a suitable password that is identical at both locations.



Be sure to activate "IP routing" and, if required, "NetBIOS over IP" (→page 310).

- ⑤ Under **Configuration ▶ Setup ▶ IP router module ▶ IP routing table** generate a new entry for each network portion that should be

accessible in the remote and in the local LAN. In each case, define the router as the remote VPN gateway and switch the IP masquerading off.



For the “VPN gateway 2”, the following entries are necessary so that the remote network sections can be reached.

IP address	Net mask	Router	IP masquerading
10.1.0.0	255.255.0.0	VPN gateway 1	No
10.2.0.0	255.255.0.0	VPN gateway 1	No
10.3.0.0	255.255.0.0	VPN gateway 1	No

For those subnetworks connected to your own LAN, define the router as the IP address for the appropriate LAN router.

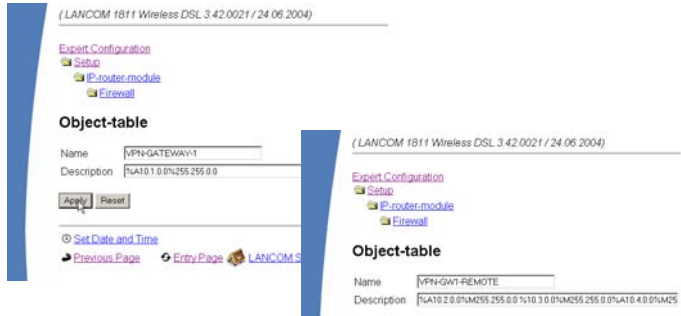
IP address	Net mask	Router	IP masquerading
10.5.0.0	255.255.0.0	10.4.0.5	No

These entries enable VPN gateway 2 to forward packets arriving from the remote network to the correct sections of the local network.

- Under **Configuration ▶ Firewall/QoS ▶ Object table** make an entry for each part of the network that should be used as a source or destination for the VPN connection via “VPN GATEWAY 1” (“VPN-GW1-LOCAL” and



“VPN-GW1-REMOTE”). Enter each subnet in the form “%A10.1.0.0%M255.255.0.0”.



- 7 Under **Configuration ▶ Firewall/QoS ▶ Rules table** define a new firewall rule named “VPN-GW1-OUT”. Set the objects to “CPN-GW1-LOCAL” and “VPN-GW1-REMOTE”, the protocol to “ANY” and the action to “ACCEPT”. Activate the option “VPN rule” so that the IP networks described in this rule will be used in establishing VPN network relationships.



**i** As a rule, it is recommended that you keep the rules used for making network relationships separate from those firewall rules that affect the services used in communications, for example.

- 8 Now for the incoming data transmissions, generate a firewall rule named “VPN-GW1-IN” with the same parameters as the rule just described. The

only difference is that the source and the destination networks are swapped.



### 14.5.8 Diagnosis of VPN connections

If the VPN connections fail to work after the configuration of the parameters, the following diagnostic methods can be applied:

- ▶ The command **show vpn spd** on the Telnet console calls the “Security Policy Definitions”.
- ▶ Use the command **show vpn sadb** to access information about the negotiated “Security Associations” (SAs).
- ▶ The command **trace + vpn** [status, packet] calls up the status and error messages for the current VPN negotiations.
  - ▷ The error message “No proposal chosen” indicates a fault in the configuration at the remote site.
  - ▷ The error message “No rule matched”, on the other hand, indicates a fault in the configuration of the local gateway.

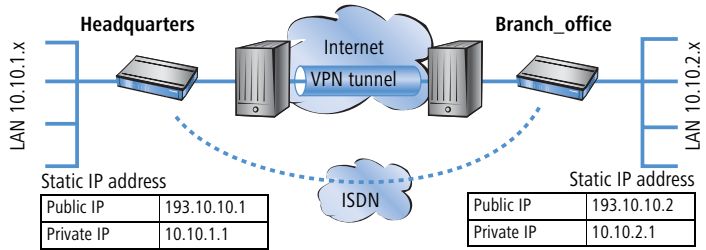
## 14.6 Specific examples of connections

This section covers the 4 possible types of VPN connections with concrete examples. These 4 different connection types are categorized by the type of IP address of the two VPN gateways:

- ▶ static/dynamic
- ▶ dynamic/static (the dynamic peer initiates the connection)
- ▶ static/dynamic (the static peer initiates the connection)
- ▶ dynamic/dynamic

There is a section for each of these types, together with a description of all required configuration information in the familiar table form.

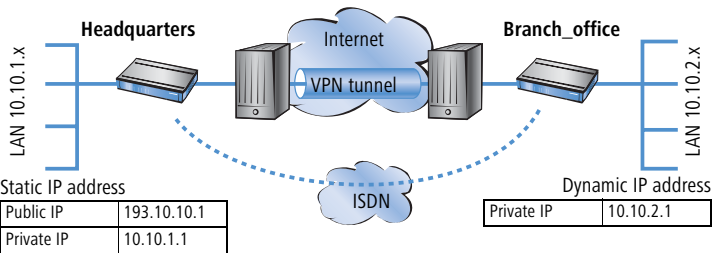
### 14.6.1 Static/static



A VPN tunnel via the Internet serves as the connection between the LANCOM **Headquarters** and **branch office**. Both gateways have static IP addresses. Thus, both can initiate the connection.

Entry	Headquarters		Branch_office
Type of local IP address	static	↔	static
Type of remote IP address	static	↔	static
Name of the local device	Headquarters	↔	Branch_office
Name of the remote device	Branch_office	↔	Headquarters
Shared Secret for encryption	secret	↔	secret
IP address of the remote device	193.10.10.2		193.10.10.1
IP-network address of the remote network	10.10.2.0		10.10.1.0
Netmask of the remote network	255.255.255.0		255.255.255.0

### 14.6.2 Dynamic/static



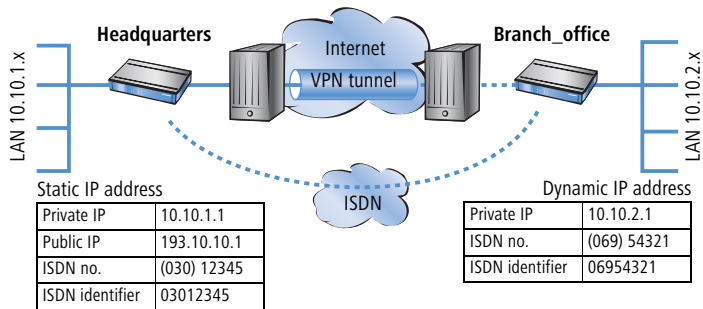
The VPN gateway **Branch office** initiates a VPN connection to the gateway **Headquarters**. **Branch office** has a dynamic IP address that was chosen and assigned by the Internet service provider upon dialling in, whereas

**Headquarters** has a fixed, static address. When the connection is set up, **Branch office** transmits its actual IP address to **Headquarters**. This is accomplished by a special ICMP packet (alternatively UDP, port 87).

Entry	Headquarters	Branch_office
Type of local IP address	static	dynamic
Type of remote IP address	dynamic	static
Name of the local device	Headquarters	Branch_office
Name of the remote device	Branch_office	Headquarters
Password for the secure transmission of the IP address	confidential	confidential
Shared Secret for encryption	secret	secret
IP address of the remote device	–	193.10.10.1
IP-network address of the remote network	10.10.2.0	10.10.1.0
Netmask of the remote network	255.255.255.0	255.255.255.0

### 14.6.3 Static/dynamic (with LANCOM Dynamic VPN)

In this case (other than the example above), the peer with the static IP address initiates the VPN connection.



The VPN gateway **Headquarters** initiates a VPN connection to **Branch office**. **Headquarters** has a static IP address, **Branch office** a dynamic one.



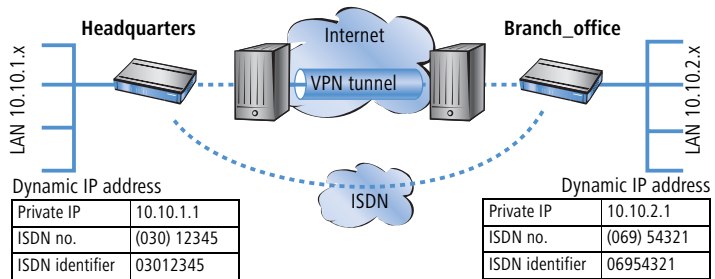
The entries for the ISDN connection are needed for the transmission of the actual dynamic IP address solely. The Internet access wizard configures the connection to the Internet.



Alternatively, this application can be solved with the help of dynamic DNS. In this constellation, the headquarters with its static IP address connects to the branch office with the help of a dynamic DNS name which is assigned to the current dynamic IP address. More information is available under 'Dynamic IP addresses and DynDNS' →page 305.

Entry	Headquarters	Branch_office
Type of local IP address	static	dynamic
Type of remote IP address	dynamic	static
Name of the local device	Headquarters	Branch_office
Name of the remote device	Branch_office	Headquarters
ISDN-calling number of the remote device	06954321	03012345
ISDN-caller ID of the remote device	06954321	03012345
Password for the secure transmission of the IP address	confidential	confidential
Shared Secret for encryption	secret	secret
IP address of the remote device		193.10.10.1
IP-network address of the remote network	10.10.2.0	10.10.1.0
Netmask of the remote network	255.255.255.0	255.255.255.0

### 14.6.4 Dynamic/dynamic (with LANCOM Dynamic VPN)



A VPN tunnel via the Internet serves as the connection between the LANCOM **Headquarters** and **branch office**. Both sites have dynamic IP addresses. Thus, both can initiate the connection.



The entries for the ISDN connection are needed for the transmission of the actual dynamic IP address solely. The Internet access wizard configures the connection to the Internet.



Alternatively, this application can be solved with the help of dynamic DNS. Instead of a static IP address, a dynamic DNS name helps to find the dynamic IP address that is currently in use. More information is available under 'Dynamic IP addresses and DynDNS' →page 305.

Entry	Headquarters		Branch_office
Type of local IP address	dynamic		dynamic
Type of remote IP address	dynamic		dynamic
Name of the local device	Headquarters		Branch_office
Name of the remote device	Branch_office		Headquarters
ISDN-calling number of the remote device	06954321		03012345
ISDN-caller ID of the remote device	06954321		03012345
Password for the secure transmission of the IP address	confidential		confidential
Shared Secret for encryption	secret		secret
IP-network address of the remote network	10.10.2.0		10.10.1.0
Netmask of the remote network	255.255.255.0		255.255.255.0

## 14.7 How does VPN work?

In practice, a VPN must fulfill a number of requirements:

- ▶ Unauthorized third parties must not be able to read the data (encryption)
- ▶ It should not be possible to manipulate the data (data integrity)
- ▶ Unambiguous identification of the sender of data (authentication)
- ▶ Simple key management
- ▶ Compatibility to VPN devices from a variety of manufacturers

LANCOM VPN achieves these five major goals by applying the widely used IPSec standard.

### 14.7.1 IPSec—The basis for LANCOM VPN

The original IP protocol does not contain any provisions for security. Security problems are compounded by the fact that IP packets do not go directly to a specific recipient, but are sent scattershot to all computers on a given network segment. Anyone can help themselves and read the packets. This leaves the door open to the misuse of data.

IP has been developed further for this reason. A secure version is now available: IPSec. LANCOM VPN is based on IPSec.

IPSec stands for “**IP Security Protocol**” and was originally the name used by a working group of the IETF, the **Internet Engineering Task Force**. Over the years, this group has developed a framework for a secure IP protocol that is generally referred to as IPSec today.

It is important to note that IPSec itself is not a protocol, but merely the standard for a protocol framework. IPSec actually consists of a variety of protocols and algorithms for encryption, authentication and key management. These standards will be introduced in the following sections.

#### Security in an IP environment

IPSec has been implemented almost completely within level 3 of the OSI model, i.e. in the network layer. The transfer of data packets using the IP protocol is realized on level 3 of IP networks.

IPSec thus replaces the IP protocol. Under IPSec, the packets have a different internal structure than IP packets. Their external structure remains fully compatible to IP, however. IPSec packets can therefore be transported without problems by existing IP networks. The devices in the network responsible for the transport of the packets cannot distinguish IPSec packets from IP packets on the basis of their exterior structure.

The exceptions in this case are certain firewalls and proxy servers that access the contents of the packets. Problems can arise from the (often function dependent) incompatibilities of these devices to the existing IP standard. These devices must therefore be adapted to IPSec.

IPSec will be firmly implemented in the next generation of the IP standard (IPv6). For this reason, we can assume that IPSec will remain the most important standard for virtual private networks in the future.

## 14.7.2 Alternatives to IPsec

IPsec is an open standard. It is not dependent on individual manufacturers and is being developed by the IETF with input from the interested public. The IETF is a nonprofit organization that is open to everyone. The broad acceptance of IPsec is the result of this open structure which unites a variety of technical approaches.

Nevertheless, there are other approaches for the realization of VPNs. We will only mention the two most important of these here. They are not realized at the network level like IPsec, but at the connection and application levels.

### Security at the connection level – PPTP, L2F, L2TP

Tunnels can already be set up at the connection level (level 2 of the OSI model). Microsoft and Ascend developed the **Point-to-Point Tunneling Protocol (PPTP)** early on. Cisco presented a similar protocol with **Layer 2 Forwarding (L2F)**. Both manufacturers agreed on a joint effort and the IETF produced the **Layer 2 Tunnel Protocol (L2TP)**.

Their main advantage over IPsec is that any network protocol can be used with such a network connection, especially NetBEUI and IPX.

A major disadvantage of the described protocols is the lack of security at the packet level. What's more, these protocols were designed specifically for dial-up connections.

### Security at higher levels – SSL, S/MIME, PGP

Communications can also be secured with encryption at higher levels of the OSI model. Well known examples of this type of protocol are **SSL (Secure Socket Layer)** mainly used for web browser connections, **S/MIME (Secure Multipurpose Internet Mail Extensions)** for e-mails and **PGP (Pretty Good Privacy)** for e-mails and files.

In all of the above protocols, an application handles the encryption of the data, for example the Web browser on one end and the HTTP server on the other.

A disadvantage of these protocols is the limitation to specific applications. In addition, a variety of keys is generally required for the different applications. The configuration must be managed on the individual computers and can not be administered conveniently on the gateways only, as is the case with IPsec. Security protocols at the application level tend to be more intelligent as they know the significance of the data being transferred. They are usually much more complex, however.



All of these layer-2 protocols only support end-to-end connections; they are therefore not suitable for coupling entire networks.

On the other hand, these mechanisms do not require the slightest changes to the network devices or access software. And unlike protocols in lower network levels, they are still effective when the data content is already in the computer.

### **Combinations are possible**

All of the alternatives listed above are compatible to IPSec and can therefore be used parallel to it. This permits a further increase of the security level. It would be possible, for example, to dial into the Internet using an L2TP connection, set up an IPSec tunnel to a Web server and exchange HTTP data between the Web server and the browser in secure SSL mode.

Each additional encryption would reduce the data throughput, however. Users can decide on a case-by-case basis whether the security offered by IPSec alone is sufficient. Only in rare cases is a higher level of security really necessary. Particularly as the degree of security can be adjusted within IPSec.

## **14.8 The standards behind IPSec**

IPSec is based on a variety of protocols for the individual functions. These protocols are based on, and complement one another. The modularity achieved with this concept is an important advantage of IPSec over other standards. IPSec is not restricted to specific protocols but can be supplemented at any time by future developments. The protocols integrated to date also offer such a high degree of flexibility that IPSec can be perfectly adapted to virtually any requirements.

### **14.8.1 IPSec modules and their tasks**

IPSec has to perform a number of tasks. One or more protocols have been defined for each of these tasks.

- ▶ Authentication of packets
- ▶ Encryption of packets
- ▶ Transfer and management of keys

### **14.8.2 Security Associations – numbered tunnels**

A logical connection (tunnel) between two IPSec devices is known as an SA (**S**ecurity **A**ssociation). SAs are managed independently by the IPSec device. An SA consists of three values:

▶ **Security Parameter Index (SPI)**

ID to distinguish multiple logical connections to the same target device with the same protocols

▶ **Target IP address**

▶ **Security protocol used**

Designates the security protocol used for the connection: AH or ESP (further information will be provided on these protocols in the following sections).

An SA applies only to one communication direction of the connection (simplex). A complete send and receive connection requires two SAs. In addition, an SA only applies for one used protocol. Two separate SAs are also required if AH and ESP are used, i.e. two for each communication direction.

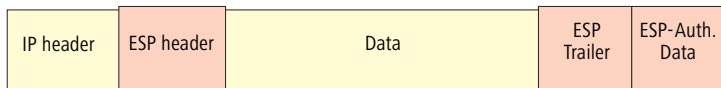
The SAs are managed in an internal database of the IPSec device that also contains the advanced connection parameters. These parameters include the algorithms and keys used, for example.

### 14.8.3 Encryption of the packets – the ESP protocol

The ESP protocol (**E**ncapsulating **S**ecurity **P**ayload) encrypts the packets as protection against unauthorized access. This was once the only function of ESP, but in the course of the further development of the protocol it was expanded with options for the protection of integrity and verification of authenticity. In addition, ESP also features effective protection against replayed packets. ESP thus offers all of the functions of AH – in some cases, however, the use of AH parallel to ESP is advisable.

#### How ESP works

The structure of ESP is more complex than that of AH. ESP also inserts a header behind the IP header as well its own trailer and a block of ESP authentication data.



#### Transport and tunnel mode

Like AH, ESP can be used in two modes: transport and tunnel mode.

In transport mode, the IP header of the original packet is left unchanged and the ESP header, encrypted data and both trailers are inserted.

The IP header contains the unchanged IP address. Transport mode can therefore only be used between two end points, for the remote configuration of a router, for example. It cannot be used for the coupling of networks via the Internet – this would require a new IP header with the public IP address of the recipient. In such cases, ESP can be used in tunnel mode.

In tunnel mode, the entire packet including the original IP header is encrypted and authenticated and the ESP header and trailers are added at the entrance of the tunnel. A new IP header is added to this new packet, this time with the public IP address of the recipient at the end of the tunnel.

### Encryption algorithms

As a higher-level protocol, IPSec does not require specific encryption algorithms. The manufacturers of IPSec products are thus free in their choice of the processes used. The following standards are common:

#### ▶ **AES – Advanced Encryption Standard**

AES is the official encryption standard for use by US authorities, and therefore one of the most important standards worldwide. Following a worldwide competition in the year 2000 to find the best of the numerous encryption algorithms, the **National Institute of Standards and Technology (NIST)** selected the Rijndael algorithm (pronounced: “Rinedoll”) and declared it as the AES in 2001.

AES is a symmetric key algorithm with variable block and encryption lengths. It has been developed by the Belgian scientists Joan Daemen and Vincent Rijmen, and features outstanding security, flexibility and efficiency.

#### ▶ **DES – Data Encryption Standard**

DES was developed by IBM for the NSA (National Security Agency) in the early 1970s and was the worldwide security standard for years. The key length of this symmetrical process is 56 bits. Today, it is considered to be insecure due to its short key length and in the year 2000 the NIST replaced it with the AES (Rijndael algorithm). It is no longer suitable for use.

#### ▶ **Triple DES (a.k.a. 3-DES)**

A further development of DES. The conventional DES algorithm is applied three times consecutively. Two or three different keys, each with a length of 56 bits are used. The key for the first run is reused for the third DES run.

The result is a nominal key length of 168 bit, with an effective key length of 112 bits.

Triple-DES combines the sophisticated DES technology with a sufficiently long key and is therefore considered to be highly secure. Triple-DES is slower than other processes, however.

▶ **Blowfish**

This development by the renowned cryptographer Bruce Schneier is a symmetrical encryption process. Blowfish achieves outstanding data throughput on multifunction processors. The process is reputed to be extremely efficient and secure.

▶ **CAST** (from the authors **Carlisle Adams** und **Stafford Tavares**)

is a symmetrical process with a key length of 128 bits. CAST permits the modification of parts of the algorithm at runtime.

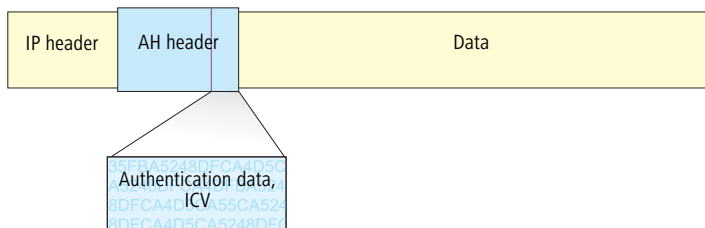


The encryption settings can be modified in the expert configuration within LANconfig. Modifications of this sort are generally only required when setting up VPN connections between devices from different manufacturers. LANCOM gateways offer the encryption as standard either after AES (128 bit), Blowfish (128 bit) or Triple-DES (168 bit).

## 14.8.4 Authentication – the AH protocol

The AH protocol (**A**uthentication **H**eder) guarantees the integrity and authenticity of the data. Integrity is frequently regarded as a component of authenticity. In the following, we will consider integrity to be a separate problem that is resolved by AH. In addition to integrity and authenticity, AH also provides effective protection against the replay of received packets (Replay Protection).

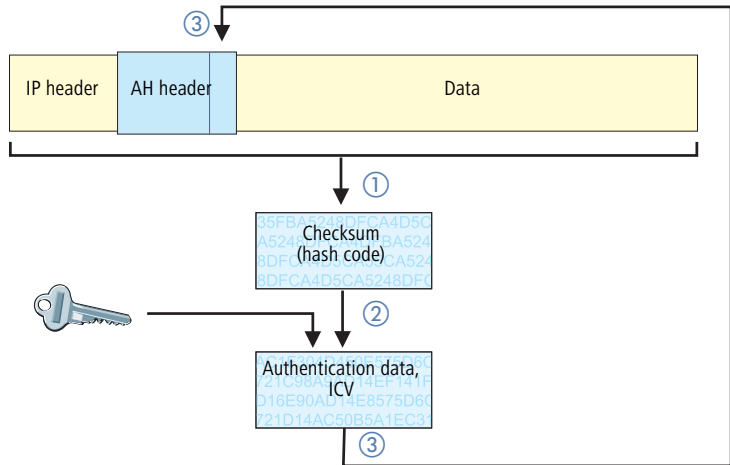
AH adds its own header to IP packets immediately after the original IP header. The most important part of this AH header is a field containing authentication data, often referred to as the **I**ntegrity **C**heck **V**alue (ICV).



### The AH process in the sender

In the sender, the authentication data is generated in 3 steps.

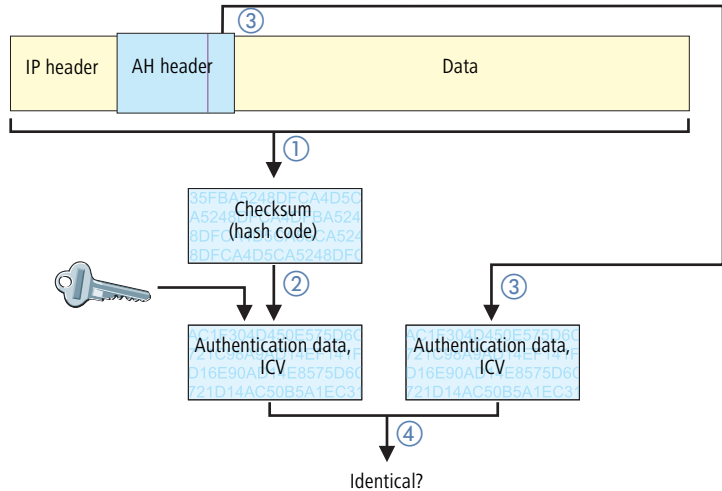
- ① A checksum is calculated for the complete package using a hash algorithm.
- ② This checksum is once again sent through a hash algorithm together with a key known to both the sender and the recipient.
- ③ This results in the required authentication data which is inserted in the AH header.



### Checking of integrity and authenticity by the recipient

The AH protocol works in a very similar manner at the recipient's end. The recipient also uses his key to calculate the authentication data for the received

packet. The comparison with the sent ICV of the packet determines the integrity and authenticity of the packet.



### Determining the checksum for the integrity check

AH adds a checksum to each packet before it is sent to guarantee the integrity of the transferred packets. At the recipient's end, AH checks whether the checksum and the contents of the package match. If this is not the case, the packet was either incorrectly transferred or deliberately manipulated. Such packets are discarded immediately and are not forwarded to higher protocol levels.

A variety of so-called hash algorithms are available to determine the checksum. Hash algorithms are distinguished by the fact that their results (the hash code) are a unique fingerprint of the original data. Conversely, the original data cannot be determined on the basis of the hash code. In addition, minimum changes of the input value entail a completely different hash code with a high-grade hash algorithm. Systematic analyses of several hash codes thus are made more difficult.

LANCOM VPN supports the two most common hash algorithms: MD5 and SHA-1. Both methods work without keys, i.e. on the basis of fixed algorithms. Keys do not play a role until a later step of AH: the final generation of the authentication data. The integrity checksum is only a necessary intermediate result on the way there.

### Generation of the authentication data

In the second step, AH generates a new hash code using the checksum and a key, the final authentication data. A variety of standards are available under IPSec for this process as well. LANCOM VPN supports HMAC (**H**ash-based **M**essage **A**uthentication **C**ode). The hash functions MD5 and SHA-1 are available as hash algorithms. The HMAC versions are accordingly known as HMAC-MD5-96 and HMAC-SHA-1-96.

This clarifies why AH leaves the packet itself unencrypted. Only the checksum of the packet and the local key are added to the packet together with the ICV, the authentication data, in encrypted form as a verification criterion.

### Replay protection – protection against replayed packets

In addition to the ICV, AH assigns a unique sequence number to each packet. The recipient can thus recognize which packets were intercepted by a third party and resent. Attacks of this type are known as “packet replay”.



AH does not cater for the masking of IPSec tunnels unless additional measures, such as NAT-Traversal or an outer Layer-2-Tunneling (e.g. PPPT/L2TP), are used that offer “changeable” IP headers.

## 14.8.5 Key management – IKE

The **I**nternet **K**ey **E**xchange Protocol (IKE) permits the integration of subprotocols for managing the SAs and for key administration.

Within IKE, two subprotocols are used in LANCOM VPN: Oakley for the authentication of partners and key administration, and ISAKMP for managing the SAs.

### Setting up the SAs with ISAKMP/Oakley

Establishing an SA involves a sequence of steps (with dynamic Internet connections, these steps follow the exchange of the public IP addresses):

- ① The initiator sends a plain-text message to the remote station via ISAKMP with the request to set up an SA and with proposals for the security parameters of the SA.
- ② The remote station replies with the acceptance of a proposal.
- ③ Both devices now generate key pairs, each consisting of a public and private key, for Diffie-Hellman encryption.

- ④ In two further messages, the devices exchange their public keys for Diffie-Hellman. The further communication is encrypted with Diffie-Hellman.
- ⑤ Both ends use numbers that have been transferred (with the Diffie-Hellman method) and the Shared Secret to generate a common secret key that is used to encrypt the subsequent communication. Both sides additionally authenticate their Shared Secrets by using hash codes. Phase 1 of the SA setup is thus completed.
- ⑥ Phase 2 is based on the encrypted and authenticated connection established in Phase 1. In Phase 2, the session keys for the authentication and symmetrical encryption of the actual data transfer are generated at random and transferred.



Symmetrical processes are used for the encryption of the actual data transfer. Asymmetrical processes (also known as public-key encryption) are more secure as they do not require the exchange of secret keys. However, they require considerable processing resources and are thus significantly slower than symmetrical processes. In practice, public-key encryption is generally only used for the exchange of key material. The actual data encryption is then performed using the fast symmetrical process.

### **The regular exchange of new keys**

ISAKMP ensures that new key material is regularly exchanged between the two devices during the SA. This takes place automatically and can be checked using the 'Lifetime' setting in the advanced configuration of LANconfig.



## 15 Appendix: Overview of functions for LANCOM models and LCOS versions

	800 1000 1100	I-10	821	1511	1521	1611	1621	1711	1811	1821	3050 3550	4000 4100	6000 6001 6021	7011	8011	L-2	IL-2	L-11	IL-11	L-54g	L-54ag
Stateful Inspection	2.80	2.80	2.80	✓	✓	2.80	2.80	✓	✓	✓	2.80	2.80	2.80	2.80	✓	2.80	2.80	2.80	2.80	2.80	2.80
Intrusion Detection, DoS Protection	2.80	2.80	2.80	✓	✓	2.80	2.80	✓	✓	✓	2.80	2.80	2.80	2.80	✓	2.80	2.80	2.80	2.80	2.80	2.80
Extended IP QoS	3.30	3.30	3.30	3.30	✓	3.30	3.30	✓	✓	✓	3.30	3.30	3.30	3.30	✓	3.30	3.30	3.30	3.30	3.30	3.30
N:N-Mapping						3.30	3.30	✓	3.30	✓	3.30	3.30	3.30	3.30	✓						
VLAN				3.30	✓			✓	3.30	✓	3.30							3.30	3.30	3.30	3.30
DMZ-Port			1)	1)	1)		1)	1)	1)	1)				✓	1)						
AES, 3-DES, DES, Blow-fish, CAST						3.32	3.32	✓	3.32	✓	✓ <sup>2)</sup>	✓ <sup>2)</sup>	✓	✓	✓						
VPN-5 Option						integr. 3.32	integr. 3.32	integrated	integr. 3.32	integrated	✓	✓									
VPN Hardware Acceleration								in combinatin with VPN-25	in combinatin with VPN-25	in combinatin with VPN-25					✓						
VPN 25 Option						✓	✓	✓	✓	✓	✓	✓									
VPN 100													✓								
VPN 200														✓	✓ <sup>4)</sup>						
ADSL Modem			✓		✓ <sup>5)</sup>		✓			✓ <sup>5)</sup>											
4 Port Switch			✓	✓	✓		✓	✓	✓	✓					✓						
ISDN Leased Line Option	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		integrated	integrated	integrated	integrated		✓		✓		
Faxmodem Option	✓	-	-	-	-	-	-	-	-	-	-	integrated	✓	-	-	-	✓		✓	-	-
Dynamic DNS	3.10	3.10	3.10	✓	✓	3.10	3.10	✓	✓	✓	3.10	3.10	3.10	3.10	✓			3.10	3.10	3.10	3.10
DSLolL			3.10		✓		3.10			✓								3.10	3.10	3.10	3.10
CRON	3.10	3.10	3.10	✓	✓	3.10	3.10	✓	✓	✓	3.10	3.10	3.10	3.10	✓	3.10	3.10	3.10	3.10	3.10	3.10
802.11b				✓	✓				✓	✓	✓					✓	✓	✓	✓	✓	✓
802.11g				✓	✓				✓	✓	✓									✓	✓
802.11a (incl. 108 Mbps Turbo Mode)									✓	✓	✓										✓
Multi SSID				3.42	3.42				3.42	3.42	3.42 <sup>3)</sup>					3.42	3.42	3.42	3.42	3.42	3.42
IP Redirect				3.42	3.42				3.42	3.42	3.42					3.42	3.42	3.42	3.42	3.42	3.42
Super A/G (108 Mbps 802.11a/g Turbo Mode & Bursting)				3.42	3.42				3.42	3.42	3.42 <sup>3)</sup>									3.42	3.42
DHCP Auto Client Mode	3.42	3.42	3.42	3.42	3.42	3.42	3.42	3.42	3.42	3.42	3.42	3.42	3.42	3.42	3.42	3.42	3.42	3.42	3.42	3.42	3.42
802.11i with Hardware AES				3.50	3.50				3.50	3.50	- / 3.50									3.50	3.50

1) Port Separation (Private Mode)  
 2) only if VPN option activated  
 3) not with in conjunction with 802.11b WLAN cards  
 4) optional VPN 500 and VPN 1000  
 5) compatible to ADSL and ADSL2

# 16 Index

## Numerics

1	
1 mapping	41, 84
3 DES	297, 331
3-DES	337
4-Port Switch	337
802.11i	213, 230
PMK caching	231
VoIP	231
802.11x	
Rekeying	222

## A

AAL-5	91
Access Control List	235
Access protection	58
for the configuration	58
by name or number	59
by number	59
via TCP/IP	55
Address administration	
IP address administration	272
Address pool	274
ADSL	28, 50
ADSL-Modem	337
AES	214, 297, 331, 337
AES-CCM	230
Aggressive mode	297
AH	297, 330, 332
Antenna gain	247
AOCD	286
ATM	28, 50
ATM adaptation layer	91
Auth.	99
Authentication	96, 214, 220
Authentication process	
TLS	222
TTLS	222

auto reconnect	98
Availability	268

## B

B-channel	
protocol	60
Blowfish	214, 297, 332
Bonk	164
Brute force	54
Bruttodatenrate	175

## C

Call charge	
information	286
limit	285
management	265, 285
Callback	58, 60
according to RFC 1570	100
Fast callback	61
for Microsoft CBCP	98
Callback procedure	
fast callback	99
Caller ID	58
Calling Line Identifier Protocol	60
Capab.	277
CAPI Faxmodem	270
CAPI interface	265
CAST	297, 332
Channel bundling	101
dynamic	102
static	102
Charge limiting	285
Charges	
information	102
units	102, 286
Client mode	211, 249
CLIP	60
Collision domain	192
Command line interface	32

Command line reference	33	Dial-Up Network	20
Common ISDN Application Programming Interface (CAPI)	265	Dial-Up Networking	59
Computer names	277	Differentiated Services – siehe DiffServ	
Conf	97	Differentiated Services Code Point – siehe DSCP	
Configuration		Diffie-Hellman method	336
procedure	15	DiffServ	169, 170
SNMP	20	Assured Forwarding	169, 170
Configuration files	29	Best Effort	170
Configuration interface	15	Class Selector	170
Connection limit	286	Expedited Forwarding	169, 170, 172
Cost reduction	285	IPSec	169
CRON	337	Distance of a route	68
<b>D</b>		DMZ	77, 79
D channel	28, 50, 60	IP address assignment	274
Data compression procedure		DMZ-Port	337
LZS	102	DNS	28, 50, 277
Data transfer	102	DNS forwarding	279
Denial of Service attacks		DNS server	272, 275, 277
Bonk	164	available information	279
Ping of Death	163	filter mechanism	278
Teardrop	164	DNS-table	282, 283
Denial-of-Service-Angriffe	162	Dynamic DNS	284
Fragrouter	164	Domain	277, 283
LAND	163	deny access	284
Smurf	162	Domain name service (DNS)	
SYN Flooding	162	DNS	277
DES	214, 298, 331	DoS	337
Device-name	96	Downstream rate	175
DHCP	27, 49, 91, 272	DSCP	170
assignment		DSLol	337
broadcast address	275	DSSS	204
DNS and NBNS server	275	Dynamic channel bundling	102
network mask	274	Dynamic DNS	284, 337
standard gateway	275	Dynamic Host Configuration Protocol (DHCP)	272
DHCP server	272, 278	Dynamic routing	66
mode	273	Dynamic VPN	
for WINS resolution	276	dynamic – dynamic	304, 325
period of validity	275		339

- Dynamic – static 302, 323
- Examples 323
- How it works 301
- ICMP 324
- Introduction 300
- PPP list 310
- Static – dynamic 303, 324
- UDP 324
  
- E**
- EAP 220
  - Process of a session secured by EAP 221
- RADIUS server 221
- EAP/802.1x 223
  - Master Secret 222
- E-mail virus 138
- Encapsulation 90
- Encryption 214, 294, 331, 336
  - asymmetric 215
  - symmetric 214
- Encryption methods
  - AES-CCM 230
- End address 274
- ESP 297, 330
- ETH-10 91
- Exclusion routes 67
- exposed host 79
- Extensible Authentication Protocol 220, 255
  
- F**
- Fail 97
- Fast callback 61
- Fax 270
- Fax Class 1 270
- Fax driver 270
- Fax transmission 271
- Faxmodem Option 337
- Filter 74
- Firewall 74, 209, 265
  
- Quell- und Zielobjekte 147
- Firmware-upload 31
  - with LANconfig 31
  - with terminal program 32
  - with TFTP 32
  - with WEBconfig 32
- Flash ROM memory 30
- Flat rate 97
- Fragrouter 164
- Frame tagging 193
- FTP
  - active FTP 182
  - passive FTP 182
  - TCP-secured transfer 177
- FTP data transfer 176
- FTP download 168
  
- G**
- Gateway 74, 272
- Gross data rate 175
  
- H**
- Hash algorithms 297
- HDLC 91
- Hidden station 253
- High telephone costs 285
- Host 277
- Host name table 281
- HTTPS 19
  
- I**
- IBBS 250
- ICMP 140, 324
- Identification control 58
- Identifying the caller 59
- IEEE 802.11a 204
- IEEE 802.11b 204
- IEEE 802.11g 205
- IEEE 802.1p/q 192
- IEEE 802.1x/EAP 255
- IEEE 802.3 91

IKE	298, 335	ISDN Festverbindungs-Option	337
Inband	15	<b>K</b>	
inband		Keep-Alive	97
Configuration via Inband	15	Key lengths	297
with Telnet	19	<b>L</b>	
Initial Vector	217	L2F	328
Install software	30	L2TP	328
Internet	74	LAN	
Internet access	95	Different organisations on one LAN	196
Intranet		logisch	194
IP address assignment	274	physikalisch	193
Intranet address	77	LANCOM FirmSafe	30
Intrusion Detection	160	LANconfig	16, 21, 31
Intrusion-Detection		Management of multiple devices	18
IP-Spoofing	160	LAND	163
Inverse masquerading	37, 78, 81	LANmonitor	23, 46
IP addresses		display options	24, 46
Dynamic	301	monitor Internet connection	24, 47
Static	301	system information	24, 46
IP broadcast	72	Layer-2	91
IP header	169	Layer-2-switch	192
IP masquerading	27, 37, 49, 74, 81, 209	Layer-3	91
simple masquerading	78	LCOS	10, 337
IP multicast	72	LCP echo reply	94
IP routing		LCP echo request	94
standard router	68	LCR	286
IP telephony	176	Least-cost routing	286
IP4 address	37, 80	LLC-MUX	90
IP-address	25, 47, 74, 94	Logging table	152
IP-routing-table	66	Logical LAN	194
IPSec	213, 297, 327	Logical sending direction	182
IPSec over WLAN	256	Logical wireless networks	234
IP-Spoofing	160	Login	31, 54
IPv6	327	Login barring	54
ISAKMP	298, 335	Loopback address	41, 84
ISDN		LZS data compression	102
B channel	304, 305	<b>M</b>	
D channel	60, 303, 305	MAC address filter	209
Euro-ISDN (DSS-1)	304		
LLC	304		

- MAC frame 194
- Mail server 282
- Main mode 297
- Maximum bandwidth 170, 172
- Microsoft Network 276
- Minimum bandwidth 169, 171, 172
  - Reception 171
  - Sending 171
- Modem 91
- Monitoring 23, 46
- MS-CHAP 92, 93
- Multi SSID 250
- Multilink PPP (MLPPP) 92, 101
- Multi-SSID 212
- N**
- N
- N mapping 37, 81
  - Configuration 42, 85
  - Decentralized mapping 41, 84
  - Firewall 43, 86
  - Loopback address 43, 86
  - NAT table 42, 85
  - Network coupling via VPN 39, 82
  - Routing table 43, 86
  - VPN rule 43, 86
- N-Mapping 337
- NAT 37, 74, 80
- NBNS server 272, 276
- Net data rate 175
- Net data transfer rate 205
- NetBIOS 28, 50, 278
- NetBIOS networks 278
- NetBIOS proxy 137, 310
- NetBIOS/IP 310
- Nettodatenrate 175
- Network Address Translation 37, 80
- Network coupling 38, 81
- Network names 277
- N-N mapping
  - Central mapping 41, 84
  - DNS forwarding 43, 86
  - No charge information 286
- O**
- OFDM 204
- Office communications 265
- Online minutes 285
- Outband 15
  - configuration via Outband 15
- Overhead 168
- P**
- Packet dump 28, 50
- passwd 54
- Password 23, 25, 47, 52, 58, 59, 96
- PAT 74
- Period 285
- Period of validity 273, 275
- Physical LAN 193
- Physical sending direction 182
- Physical WLAN interface 233
- Ping 140
- Ping blocking 123
- Ping of Death 163
- Ping-Blocking 123
- PMTU reduction 177
- Port 78
  - IP port 267
- Port Address Translation 37, 81
- Port-Separierung 337
- PPP 25, 47, 59, 91, 101
  - callback functions 98
  - checking the line with LCP 94
  - handshake 22
  - IP address assignment 94
  - LCP Extensions 100
- PPP client 21
- PPP connection 22
- PPPoE 91
- PPTP 213, 328

Precedence	170	with N	
Pre-Shared Key	214	N mapping	39, 83
Preshared key	298	Remote-ID	96
Priority control	268	Repetitions	97
Private Mode	337	Rijndael	331
Private WEP settings	239	RIP	27, 49
Protection		Router	209
for the configuration	52	Router-interface-list	103
for the LAN	74	Router-name	67
Protocol filter	237	RSA	215
PSK	214	RTS threshold	253
Public key	336	RTS/CTS protocol	253
<b>Q</b>		<b>S</b>	
QoS	176, 337	Security	52, 74
Direction of data transfer	182	Security Association	329
QoS –		Security checklist	61
siehe Quality-of-Service		Security Parameter Index	330
Quality of Service	168	Security procedures	59
Quality-of-Service	168	Security settings	11, 54
Queue	172	Serial port	15
Queues	172	Single user access	74
Secured queue	173	Smurf	162
Standard queue	173	SNMP	20
Urgent queue I	172	SNMP trap	40, 83
Urgent queue II	172	Stac data compression	102
<b>R</b>		Standard fax programs	270
Radio cell	208	Start address	274
RADIUS	221	Stateful Inspection	209, 337
RADIUS server	255	Static channel bundling	102
Range	205, 208	Static routing	66
RAS	291, 293	SYN Flooding	162
RC4	214	SYN/ACK speedup	73
Advantages	216	SYSLOG	287
Redirect	236, 254	<b>T</b>	
Remote access	20, 95	TCP	168
Remote configuration	15	TCP- control packets	172
Remote connection	21	TCP Stealth mode	124
Remote control	38, 81	TCP/IP	66
Remote maintenance		TCP/IP networks	277
			343

TCP-Stealth-Modus	124	VC-MUX	90
Teardrop	164	Virtual LAN	192
Telnet	21	Virtual Private Network	291
Temporal Key Integrity Protocol	224	VLAN	192, 337
Term	97	Allow all VLANs	199
Terminal program	31	Allow untagged frames	199
TFTP	19	Connection of WLAN stations	196
Throughput	102	Conversion in the interfaces	194
Time	97	Default ID	199
Time budget	286	Default-VLAN ID	194
Time dependent connection- limit	286	ID	194
Time-out	102, 103	Konfiguration	198
ToS	169, 170	Management of LAN traffic	196
High Reliability	169	Network table	198
IPSec	169	Port	199
Low Delay	169, 172	Port list	198
Priority	170	Port table	199
Trace		Priority	194
examples	29, 51	Shielding of SNMP traffic	196
keys and parameters	26, 48	Use of a central cabling	197
outputs	26, 48	Use tagging	199
starting	26, 48	VLAN D	198
Transfer rates	205	VLAN ID	194
Transmission rates	25, 48	Voice-over-IP	168, 171
Transport mode	297, 330	VoIP	79
Triple DES	297, 331	VoIP –	
Trojans	138	siehe Voice-over-IP	
Troubleshooting	24, 46	VPN	291, 337
Tunnel mode	297, 330	Client	139
Type-of-Service –		Configuration	306
siehe ToS		Configuration with LANconfig	314
<b>U</b>		Configuration with WEBconfig	318
UDP	168, 324	dynamic – dynamic	325
Upload	30	Dynamic – static	323
Upstream rate	175	Examples	322
User name	22, 59, 96	Gateway	139
<b>V</b>		Network coupling with N	
V.110	91	N mapping	38, 82
		Remote maintenance via N	
		N mapping	39, 83



Static – dynamic	324	Wireless LAN	
static - static	323	Ad-hoc	207
VPN client	299	operation modes	206
VPN connections		Wireless bridge	210
Diagnosis	322	Wireless LANs	
Manual set-up	309	Infrastructure network	207
Setup Wizard	308	WLAN	
VPN example application	295	Access point density	248
VPN network relationships	311	ACL	235
VPN rules	309	ad-hoc mode	206
<b>W</b>		ARP handling	244
WAN-layer	90	bridge mode	207
WEBconfig	16, 18, 31	Broken link detection	244
HTTPS	19	Channel number	246
Well known groups	298	Client mode	249
WEP	238, 241	client mode	207
Challenge-response procedure	218	Closed network mode	251
CRC checksums	217	Compatibility mode	246
Explanation of the process	215	Country setting	243
Initial Vector	217	DFS method	246
Key length	217	Frequency band	246
Passphrase	217	IBBS	250
Private WEP settings	238	infrastructure network	207
Process of encryption	215	IPSec over WLAN	256
RC4	215	Keep client connection alive	250
Sniffer tools	219	Maximum distance	248
Weak points of the process	218	Multi-SSID	207
WEP group keys	242	Network settings	251
WEP key		Network types	249
dynamic	220	Operation mode	245
WEPplus	220	Point-to-point connections	248
Limits	220	point-to-point mode	207
WiFi Alliance	223	Protocol filter	236
Wifi Protected Access	223	Radio settings	246
Wildcards	283	Redirect	254
Windows networks	310	Scan bands	250
WINS Address	276	SSID	251
WINS server	310	Subband	246
Wired Equivalent Privacy	215	Transmission power reduction	247
		Turbo mode	247

VPN pass-through	207
WEP group keys	241
WLAN interface	
logical	250
physical	244
WLAN security	214
802.11i	230
802.1x	220
AES	230
EAP	220
Sniffer tools	219
TKIP	223
WEP	215
WEPplus	219
WPA	223
WPA	213, 223
Group Key	227
Handshake procedure	223
Key handshake	226
Key mixing phase	225
Master Secret	224, 227
Michael	223
Michael hash algorithm	225
Michael key	225
Pairwise Key	227
Passphrase	228
Procedure for key handshake	227
Procedure for TKIP/Michael	224
Rekeying	228
TKIP	223, 224
TKIP session key	227
<b>Y</b>	
Y connection	103