Reference Manual LCOS 7.60

- Addendum 7.70
- Addendum 7.80

LANCOM Systems

LANCOM reference manual part 1

- Introduction
- System design
- Configuration and management
- Advanced Management
- Diagnosis
- Security

Version: LCOS 7.6 with addendum 7.7 (see appendix)
(last update August 2009)

LANCOM
Systems

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

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

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen
Deutschland

www.lancom.de

Würselen, August 2009

110650/0809

Contents

1 Preface

1.1 About this documentation

Constituents of this documentation

The documentation of this device includes the following:

- Installation Guide

  In this getting started guide you find answers to the following questions:

  - Which software needs to be installed for the configuration?
  - How needs the device to be connected?
  - How can the device be reached by LANconfig, WEBconfig or another interface?
  - How do you start a setup assistant (e.g. for providing an internet access)?
  - How do you make a hardware check?
  - Where can you find more information and help?

- User’s manual

  The user’s manual contains all information, which are important for starting up the device. In addition you find all technical specifications.

- Manual PBX functionalities (only models with VoIP support)

  In the manual PBX functionalities you find a detailed step-by-step guide for using a LANCOM VoIP Router as a telephone system for a location. Also there are described the most important advices for the user and the connection of end devices.

- Reference manual

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

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

  The description in the reference manual is geared to the configuration with LANconfig. For every LANconfig dialogue is given the associated path for the configuration with WEBconfig, e.g.:

  LANconfig: Wireless LAN ▶ 802.11i/WEP ▶ WPA or Private WEP settings

  WEBconfig: LCOS Menu Tree ▶ setup ▶ interfaces ▶ WLAN ▶ encryption

  The path for the configuration with console/telnet is not explicit written, but can be deduced. The telnet path for the encryption setting is e.g.:

  ```
  cd Setup/interfaces/WLAN/encryption
  ```

- Menu reference

The menu reference describes all parameter of LCOS, the operating system of all LANCOM devices. This description supports the user to configurate the devices with WEBconfig or telnet. The parameters in the menu reference are sorted the way they can be reached with WEBconfig. Every parameter is not only described, but you can find as well possible values and standards.

You find all documents, which are not attached to your device in a printed version, as an acrobat document under www.lancom.de/download or on the attached product CD.

LCOS, the operating system of LANCOM devices

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

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

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

Validity

The present reference manual applies to all LANCOM routers and LANCOM Router Access Points with firmware version 7.6 or better.

The functions and settings described in this reference manual are not supported by all models and/or all firmware versions. A table can be found in the appendix denoting the individual functions, from which firmware version they are supported in the respective devices ('Overview of functions by model and LCOS* version' → page 17-18).

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 6-1.

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

This documentation was created by …

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

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

Our online services www.lancom.eu are available to you around the clock should you have any queries regarding the topics discussed in this manual or require any further support. The area 'Support' will help you with many answers to frequently asked questions (FAQs). Furthermore, the knowledgebase offers you a large reserve of information. The latest drivers, firmware, utilities and documentation are constantly available for download.
In addition, LANCOM support is available. For telephone numbers and contact addresses of LANCOM support, please see the enclosed leaflet or the LANCOM Systems website.

Information symbols	
⚡	Very important instructions. Failure to observe this may result in damage.
!	Important instruction that should be observed.
ⓘ	Additional information that may be helpful but which is not required.

1.2 Release history

Because of the limited hardware possibilities there can not be upgraded all older models with the actual version of LCOS. You can find the information which firmware version is supported in the respective devices in the table in the appendix ('Overview of functions by model and LCOS* version' → page 17-18).

New functions with LCOS version 7.60

- Configuration
  - Telnet: 'Functions for editing commands' → page 3-36
  - Telnet: 'Function keys for the command line' → page 3-36
  - WEBconfig: 'New WEBconfig with search function, comprehensive device status, on-line help, etc.' → page 3-27
  - 'Load files directly from a TFTP or HTTP server into the device' → page 3-44
  - Managing rights for different administrators – 'Administrators without trace rights' → page 4-13
  - 'Asymmetric Firmsafe' → page 3-42
  - LANconfig: 'Transferring device configurations to similar models' → page 3-17
  - LANconfig: 'Automatic backup of configuration with LANconfig' → page 3-6
  - LANconfig: 'Customizing the toolbar' → page 3-6
  - LANconfig: Object-oriented definition of firewall rules (see Firewall)
  - LL2M: 'LANCOM Layer 2 Management protocol (LL2M)' → page 4-10
- Diagnosis
  - LANmonitor: 'Saving support files with trace data, device configuration, bootlog and sysinfo' → page 5-4
  - LANmonitor: 'Automatic backup of trace data' → page 5-4
  - LANmonitor: 'Trace configuration with Wizards' → page 5-4
  - LANmonitor: 'Display of show commands' → page 5-4
  - LANmonitor: 'Display of status information and statistics' → page 5-4
  - LANmonitor: 'SSL-encrypted Telnet connection' → page 5-4
  - Display of SYSLOG in LANmonitor and WEBconfig (→ page 5-9)
- WAN
  - Flexible selection of the PPP authentication protocols (→ page 7-35)
  - The Action table (→ page 7-51)
  - GnuDIP support (→ page 7-52)
  - COM port forwarding: 'Using the serial interface in the LAN' → page 7-56
  - Flexible definition of WAN-RIP remote stations by using place holder (→ page 7-46)
  - 'Interfaces tags for remote sites' → page 7-12
- VPN
  - Unlimited number of VPN remote sites
  - 'Extended Authentication Protocol (XAUTH)' → page 10-54
  - 'Backup via alternative VPN connection' → page 10-55
  - 'Multi-level certificates for SSL/TLS' → page 10-46
- Firewall
  - Object-oriented definition of firewall rules with LANconfig (→ page 8-22)
  - Restricting the firewall rule to backup connections (→ page 8-26)
  - Restricting the firewall rule to one station's connections (→ page 8-26)
  - Specification of a maximum number of connections (→ page 8-26)
  - Specification of a percentage of bandwidth (→ page 8-26)
- Voice over IP

  New parameters for SIP provider lines (→ page 13-20) and SIP-PBX lines (→ page 13-26)

  - Local port number
  - (Re-) registration
  - Line monitoring
  - Monitoring interval
  - Trusted

- □ Privacy method

  New parameter for ISDN (→ page 13-16) and SIP users (→ page 13-14)

  - □ CLIR

  New parameters for Analog users (→ page 13-17)

  - □ Caller-ID Signaling
  - □ Caller-ID Transmission Requirements

- WLAN
  - □ WLAN: Packet forwarding adjustable per SSID (→ page 11-22)
  - □ 'DFS 2: Non-use of channels for weather radar' → page 11-78
  - □ 'Multi-level certificates for PublicSpots' → page 11-78
  - □ 'DFS 2: Non-use of channels for weather radar' → page 11-78
  - □ Central WLAN management: 'Internal script storage (script management without an HTTP server)' → page 11-77
- Messaging
  - □ SNMP traps: configurable trap version
- RADIUS
  - □ VLAN ID in the table for RADIUS users
  - □ Masking of calling and called users in the RADIUS user table
- DHCP
  - □ BOOTP: Assignment of fixed IP addresses or boot images to specific workstations depending on the IP network (ARF)
- Other changes
  - □ Access lists with routing tags

New functions with LCOS version 7.50

- Changes with the LANtools
  - □ 'Better overview in LANconfig with more columns' → page 3-8
  - □ 'Tracing with LANmonitor' → page 5-4
  - □ 'WLAN configuration with the wizards in LANconfig' → page 3-13
  - □ 'User-specific settings for LANconfig' → page 3-5
- 'RADSEC' → page 16-35
- 'Multi-level certificates for SSL/TLS' → page 10-46
- LANCOM WLAN Controller
  - □ 'Automatic RF optimization with LANCOM WLAN Controllers' → page 11-74
  - □ 'Central firmware and script management' → page 11-75
- New configuration wizard
  - □ 'Rollout Wizard' → page 4-8
- Improvements in WLAN
  - □ 'Connecting point-to-point remote stations by station name' → page 11-53
- GPS
  - □ 'Location verification by ISDN or GPS' → page 6-6

New functions in LCOS version 7.20

- 'Advanced Routing and Forwarding' → page 7-9
- 'Named loopback addresses' → page 4-18
- 'VLAN tags for DSL interfaces' → page 12-7
- 'VLAN Q-in-Q tagging' → page 12-3
- 'The roaming table' → page 11-42
- 'The beaconing table' → page 11-42
- 'DFS connections without the mandatory interruption' (→ page 11-13)
- 'Reset button behavior' (→ page 3-46)
- 'Extensions to the RADIUS server' (→ page 16-25)
- 'Certificate enrollment via SCEP' → page 10-47

- 'The rapid spanning tree protocol' → page 7-46
- 'TCP port tunnel' → page 4-17
- 'PBX functions for LANCOM VoIP Router' → page 13-38
- New functions in LANconfig and LANmonitor
  - '1-Click-VPN for networks (site-to-site)' → page 10-12
  - '1-Click-VPN for LANCOM Advanced VPN Client' → page 10-13
  - 'Storing and uploading certificates' → page 10-36
  - 'LANconfig behavior at Windows startup' → page 3-12z
- Other services
  - 'CRON jobs with time delay' → page 16-20

New functions in LCOS version 6.28

- WLAN
  - Checking the quality of the connection with LANmonitor (→ page 3-22)
- Changes with the LANtools
  - Choosing assistant or configuration dialogue (→ page 3-13)

New functions in LCOS version 6.24

- WLAN
  - 'Background WLAN scanning' → page 11-20
  - 'Rogue AP and rogue client detection with the WLANmonitor' → page 3-25
  - 'Indoor function for WLAN channels' (→ page 11-21)
  - 'Signal-quality display via LEDs' (→ page 11-50)
- VPN
  - 'Simplified network connection with certificates – proadaptive VPN' → page 10-44
  - 'Request certificates using CERTREQ' → page 10-45
  - 'Establishing Security Associations collectively' → page 10-23
- VoIP
  - 'Analog lines' (→ page 13-29)
  - 'Analog users' (→ page 13-17)
  - 'Call hold, transfer call, connect call' → page 13-12
  - 'Transfer of DTMF tones' → page 13-12
  - 'Transfer toll information to the internal ISDN buses' → page 13-13
- Management
  - 'Configuring daylight-saving time change according to UTC' → page 16-19
  - 'SSH authentication' → page 3-38
- LANconfig, LANmonitor, WLANmonitor
  - 'Switch graphical user interface language' → page 3-3
  - 'Download script from device' → page 4-3
  - 'Device-specific settings for communications protocols' → page 3-11

New functions in LCOS version 6.10

- 'Certificate revocation list - CRL' → page 10-45
- 'Simplified RAS with certificates' → page 10-43
- 'QoS for WLANs according to IEEE 802.11e (WMM/WME)' → page 9-13
- 'RADIUS' → page 16-25
- Voice over IP
  - 'Supporting digital calls' → page 13-13
  - 'ISDN interface configuration' → page 13-51
  - 'The LANCOM VoIP Router at a P2P (point-to-point) connection' → page 13-74
  - 'SIP trunking' → page 13-76
  - 'Remote gateway' → page 13-77
- 'VLAN tags on layer 2/3 in the Ethernet' → page 12-7

- 'Configuring the printer server in the LANCOM' → page 16-36

New functions in LCOS version 6.00

- 'Voice over IP (VoIP)' → page 13-1

New functions in LCOS version 5.20

- 'Backup Solutions and Load Balancing with VRRP' → page 14-7
- 'PPPoE Servers' → page 16-22
- 'WAN RIP' → page 7-46
- 'Routing tags for VPN and PPTP connections' → page 7-4
- 'NAT Traversal (NAT-T)' → page 10-52
- 'Configurable VLAN IDs' → page 12-6
- 'Vendor Class and User Class Identifier' → page 16-9
- 'Bandwidth limits in the WLAN' → page 11-78
- 'The rapid spanning tree protocol' → page 7-46
- 'Demilitarized Zone (DMZ)' → page 7-19

New functions in LCOS version 5.00

- 'Scripting' → page 4-1
- 'Working with digital certificates' → page 10-24
- 'Client-bridge support' → page 11-37
- 'DSL port mapping' → page 7-23
- 'Dynamic load balancing' → page 7-25
- 'Policy-based Routing' → page 7-26
- 'Monitoring the switch' → page 5-14
- 'ISDN location verification' → page 6-6
- 'Group configuration with LANconfig' → page 3-14
- 'Visualization of larger WLANs with WLANmonitor' → page 3-23

New functions in LCOS version 4.00

- 'Encrypted configuration with SSH access' → page 3-37
- 'VPN connections: High availability with VPN load balancing' → page 10-63
- 'Managing rights for different administrators' → page 4-13
- 'Manual definition of the MTU' → page 7-45
- 'LEPS – LANCOM Enhanced Passphrase Security' → page 11-18
- 'Multi-PPPoE' → page 7-22
- 'IKE config mode' → page 10-15
- 'SYSLOG storage in the device' (→ page 5-9)

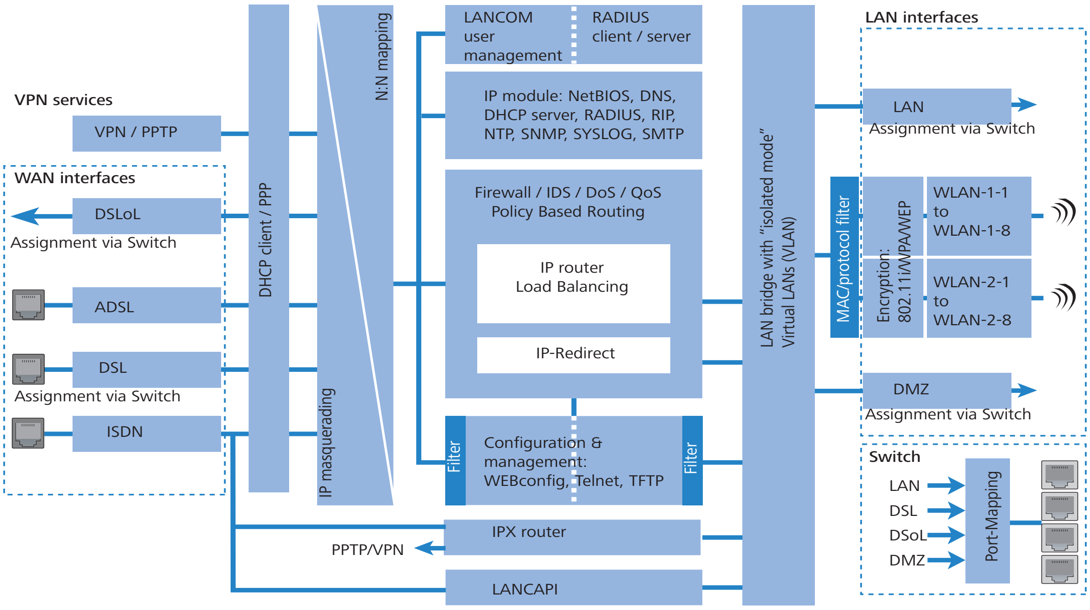
2 System design

2.1 Introduction

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

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

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



Notes regarding the respective modules and interfaces:

- The IP router takes care of routing data on IP connections between the interfaces from LAN and WAN.
- With IP redirect requests in the LAN are redirected to a specific computer
- The firewall (with the services "Intrusion Detection", "Denial of Service" and "Quality of Service") encloses the IP router like a shield. All connections via the IP router automatically flow through the firewall as well.
- LANCOM devices provide either a separate LAN interface or an integrated switch with multiple LAN interfaces as interfaces to the LAN.
- LANCOM Router access points resp. LANCOM routers with wireless modules offer additionally one or, depending on the respective model, also two wireless interfaces for the connection of Wireless LANs. Depending on the model every wireless interface can build up to eight different wireless networks ("multi SSID").
- A DMZ interface enables for some models a 'demilitarized zone' (DMZ), which is also physically separated within the LAN bridge from other LAN interfaces.
- The LAN bridge provides a protocol filter that enables blocking of dedicated protocols on the LAN. Additionally, single LAN interfaces can be separated by the "isolated mode". Due to VLAN functions, virtual LANs may be installed in the LAN bridge, which permit the operating of several logical networks on a physical cabling.
- Applications can communicate with different IP modules (NetBIOS, DNS, DHCP server, RADIUS, RIP, NTP, SNMP, SYSLOG, SMTP) either via the IP router, or directly via the LAN bridge.
- The functions "IP masquerading" and "N:N mapping" provide suitable IP address translations between private and public IP ranges, or also between multiple private networks.
- Provided according authorization, direct access to the configuration and management services of the devices (WEBconfig, Telnet, TFTP) is provided from the LAN and also from the WAN side. These services are protected by filters and login barring, but **do not** require any processing by the firewall. Nevertheless, a direct access from WAN to LAN (or vice versa) using the internal services as a bypass for the firewall is **not** possible.
- The IPX router and the LANCAPI access on the WAN side only the ISDN interface. Both modules are independent from the firewall, which controls only data traffic through the IP router.

- The VPN services (including PPTP) enable data encryption in the Internet and thereby enable virtual private networks over public data connections.
- Depending on the specific model, either xDSL/Cable, ADSL or ISDN are available as different WAN interfaces.
- The DSLoL interface (DSL over LAN) is no physical WAN interface, but more a “virtual WAN interface”. With appropriate LCOS settings, it is possible to use on some models a LAN interface as an **additional** xDSL/Cable interface.

3 Configuration and management

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

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

3.1 Configuration tools and approaches

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

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

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

What is the difference between these three possibilities?

On the 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 computer with a serial port. The preconditions are most extensive for ISDN remote configuration: In addition to an ISDN capable LANCOM, an ISDN card is needed in the configuration PC or alternatively, access via LANCAPI to an additional LANCOM that is ISDN capable.

3.2 Configuration software

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

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

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

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

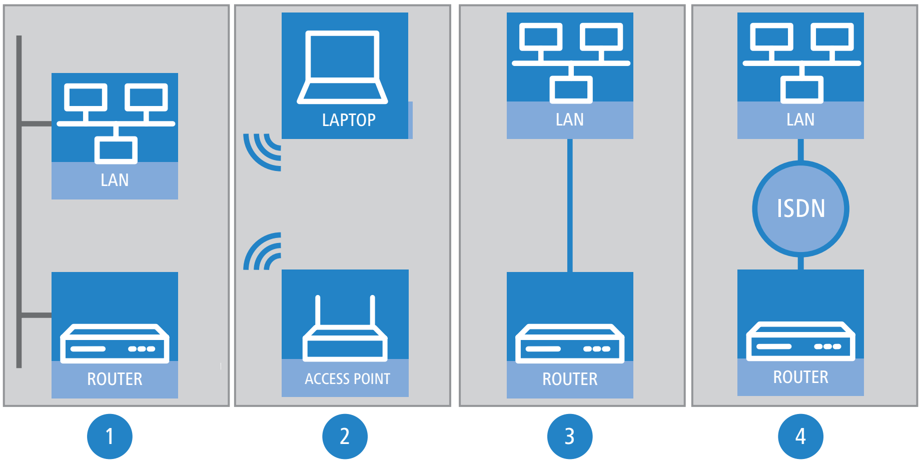
Please note that all procedures access the same configuration data. For example, if you change the settings in LANconfig, this will also have a direct effect on the values under WEBconfig and Telnet.

3.3 Searching and configuring devices

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

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

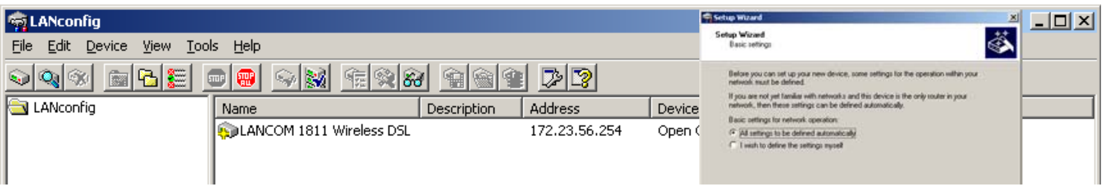
- Via the local network (LAN) ➊.
- Via the wireless network (WLAN) ➋, if the WLAN encryption (e.g. WEP) of a device with a wireless interface and in the configuration PC has been adjusted correctly and/or has been deactivated.
- Via the serial configuration interface ➌.
- Via a ISDN connection ➍



3.4 Configuration with LANconfig

3.4.1 Starting LANconfig

Start LANconfig by, for example, using the Windows Start menu: **Start** ▶ **Programme** ▶ **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.



Name	Description	Address	Device
LANCOM 1811 Wireless DSL		172.23.56.254	Open (

Setup Wizard

Setup Wizard
Basic settings

Before you can set up your new device, some settings for the operation within your network must be defined.

If you are not yet familiar with networks and this device is the only router in your network, then these settings can be defined automatically.

Basic settings for network operation:

● All settings to be defined automatically
○ I wish to define the settings myself

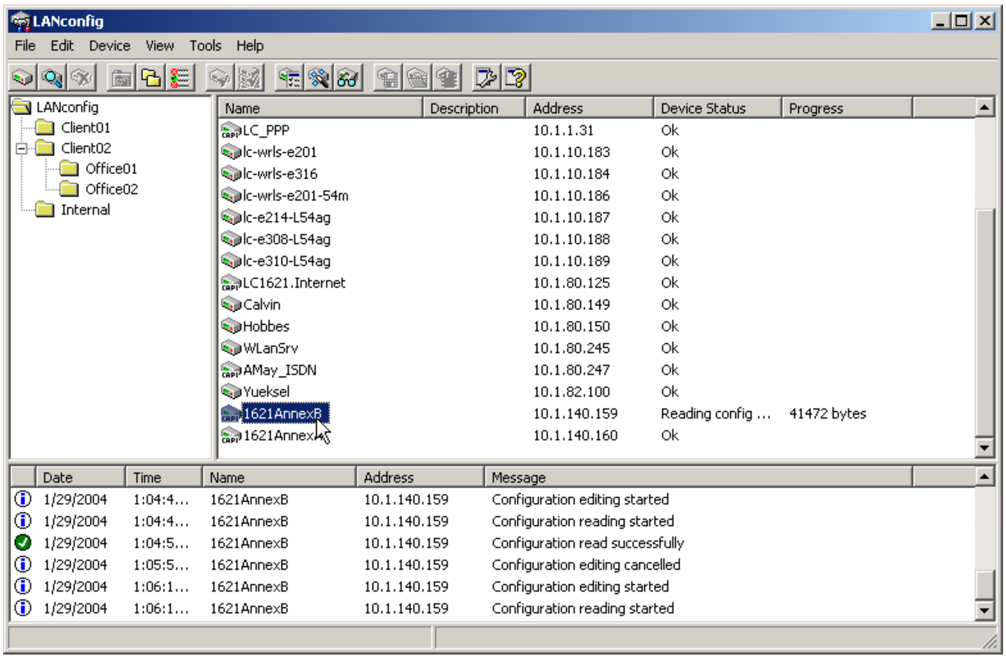
If the firewall is activated the LANconfig might not be able to find the new device in the LAN. In this occasion deactivate the firewill whilst the configuration.

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

Find new devices

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

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



Name	Description	Address	Device Status	Progress
LC_PPP		10.1.1.31	Ok	
lc-wrls-e201		10.1.10.183	Ok	
lc-wrls-e316		10.1.10.184	Ok	
lc-wrls-e201-54m		10.1.10.186	Ok	
lc-e214-L54ag		10.1.10.187	Ok	
lc-e308-L54ag		10.1.10.188	Ok	
lc-e310-L54ag		10.1.10.189	Ok	
LC1621.Internet		10.1.80.125	Ok	
Calvin		10.1.80.149	Ok	
Hobbes		10.1.80.150	Ok	
WLanSrv		10.1.80.245	Ok	
AMay_ISDN		10.1.80.247	Ok	
Yueksel		10.1.82.100	Ok	
1621AnnexB		10.1.140.159	Reading config ...	41472 bytes
1621Annex		10.1.140.160	Ok	

Date	Time	Name	Address	Message
1/29/2004	1:04:4...	1621AnnexB	10.1.140.159	Configuration editing started
1/29/2004	1:04:4...	1621AnnexB	10.1.140.159	Configuration reading started
1/29/2004	1:04:5...	1621AnnexB	10.1.140.159	Configuration read successfully
1/29/2004	1:05:5...	1621AnnexB	10.1.140.159	Configuration editing cancelled
1/29/2004	1:06:1...	1621AnnexB	10.1.140.159	Configuration editing started
1/29/2004	1:06:1...	1621AnnexB	10.1.140.159	Configuration reading started

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

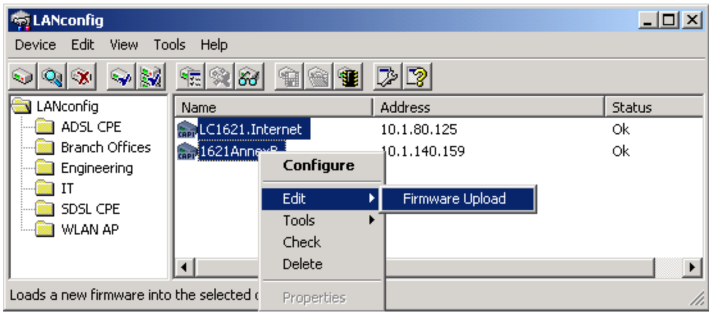
The remainder of the program's operation is self-explanatory or you can use the online help. You can click on the 'Help' button top right in any window or right-click on an unclear term at any time to call up context-sensitive help.

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 Access Points.

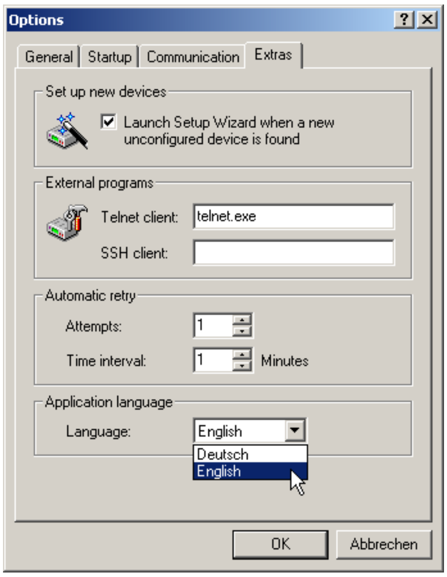


Name	Address	Status
LC1621.Internet	10.1.80.125	Ok
1621AnnexB	10.1.140.159	Ok

Loads a new firmware into the selected (

3.4.2 Switch graphical user interface language

The language for the LANconfig, LANmonitor or WLANmonitor graphical user interface can be set to 'German' or 'English'.



☑ Launch Setup Wizard when a new unconfigured device is found

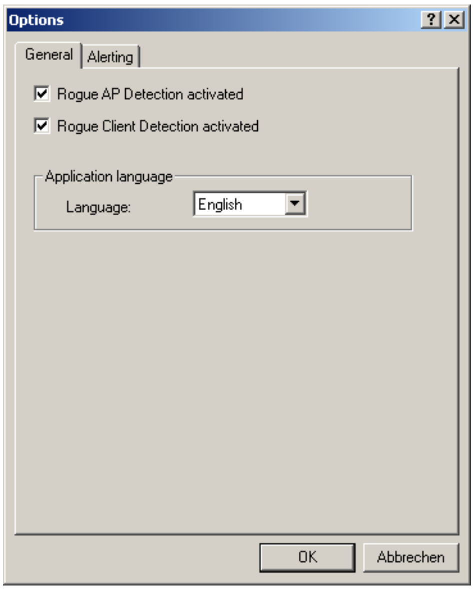
Telnet client: telnet.exe

SSH client:

Attempts: 1

Time interval: 1 Minutes

Language: English



☑ Rogue AP Detection activated

☑ Rogue Client Detection activated

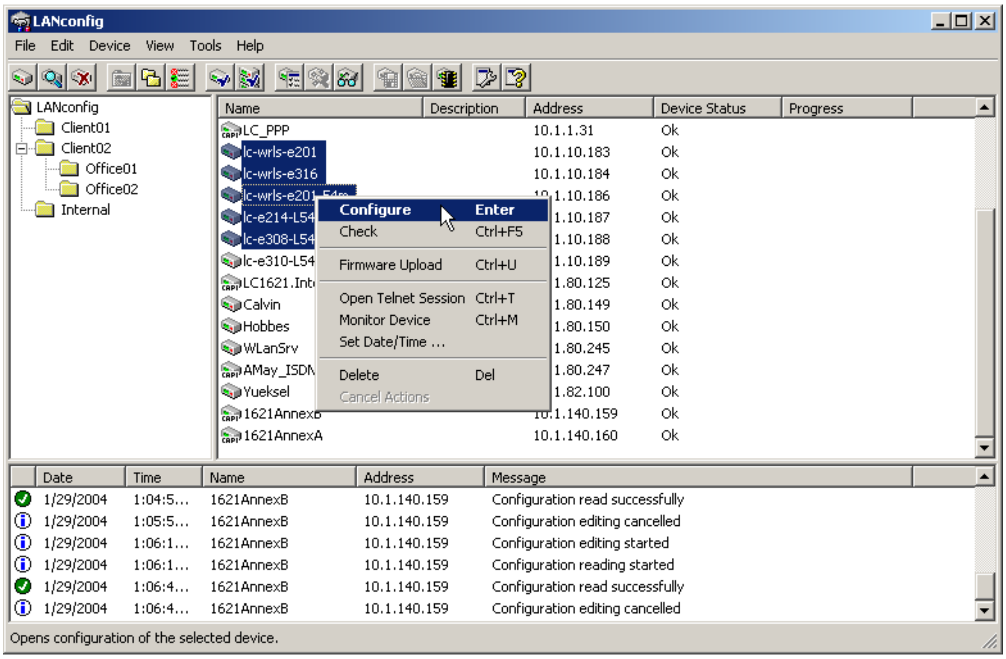
Language: English

LANconfig: Tools ▶ Options ▶ Extras

LANmonitor and WLANmonitor: Tools ▶ Options ▶ General

3.4.3 Project management with LANconfig

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

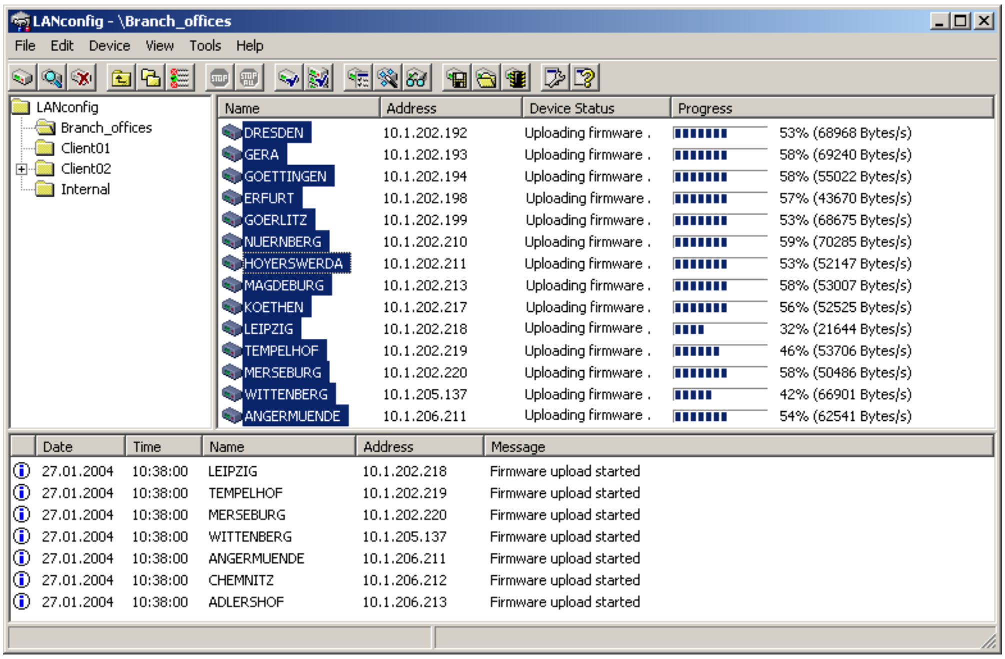


Name	Description	Address	Device Status	Progress
LC_PPP		10.1.1.31	Ok	
lc-wrls-e201		10.1.10.183	Ok	
lc-wrls-e316		10.1.10.184	Ok	
lc-wrls-e201-54m		1.10.186	Ok	
lc-e214-L54		1.10.187	Ok	
lc-e308-L54		1.10.188	Ok	
lc-e310-L54		1.10.189	Ok	
LC1621.Int		1.80.125	Ok	
Calvin		1.80.149	Ok	
Hobbes		1.80.150	Ok	
WLanSrv		1.80.245	Ok	
AMay_ISDN		1.80.247	Ok	
Yueksel		1.82.100	Ok	
1621AnnexB		10.1.140.159	Ok	
1621AnnexA		10.1.140.160	Ok	

	Date	Time	Name	Address	Message
✓	1/29/2004	1:04:5...	1621AnnexB	10.1.140.159	Configuration read successfully
ⓘ	1/29/2004	1:05:5...	1621AnnexB	10.1.140.159	Configuration editing cancelled
ⓘ	1/29/2004	1:06:1...	1621AnnexB	10.1.140.159	Configuration editing started
ⓘ	1/29/2004	1:06:1...	1621AnnexB	10.1.140.159	Configuration reading started
✓	1/29/2004	1:06:4...	1621AnnexB	10.1.140.159	Configuration read successfully
ⓘ	1/29/2004	1:06:4...	1621AnnexB	10.1.140.159	Configuration editing cancelled

Opens configuration of the selected device.

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



Name	Address	Device Status	Progress
DRESDEN	10.1.202.192	Uploading firmware .	53% (68968 Bytes/s)
GERA	10.1.202.193	Uploading firmware .	58% (69240 Bytes/s)
GOETTINGEN	10.1.202.194	Uploading firmware .	58% (55022 Bytes/s)
ERFURT	10.1.202.198	Uploading firmware .	57% (43670 Bytes/s)
GOERLITZ	10.1.202.199	Uploading firmware .	53% (68675 Bytes/s)
NUERNBERG	10.1.202.210	Uploading firmware .	59% (70285 Bytes/s)
HOYERSWERDA	10.1.202.211	Uploading firmware .	53% (52147 Bytes/s)
MAGDEBURG	10.1.202.213	Uploading firmware .	58% (53007 Bytes/s)
KOETHEN	10.1.202.217	Uploading firmware .	56% (52525 Bytes/s)
LEIPZIG	10.1.202.218	Uploading firmware .	32% (21644 Bytes/s)
TEMPELHOF	10.1.202.219	Uploading firmware .	46% (53706 Bytes/s)
MERSEBURG	10.1.202.220	Uploading firmware .	58% (50486 Bytes/s)
WITTENBERG	10.1.205.137	Uploading firmware .	42% (66901 Bytes/s)
ANGERMUENDE	10.1.206.211	Uploading firmware .	54% (62541 Bytes/s)

Date	Time	Name	Address	Message
27.01.2004	10:38:00	LEIPZIG	10.1.202.218	Firmware upload started
27.01.2004	10:38:00	TEMPELHOF	10.1.202.219	Firmware upload started
27.01.2004	10:38:00	MERSEBURG	10.1.202.220	Firmware upload started
27.01.2004	10:38:00	WITTENBERG	10.1.205.137	Firmware upload started
27.01.2004	10:38:00	ANGERMUENDE	10.1.206.211	Firmware upload started
27.01.2004	10:38:00	CHEMNITZ	10.1.206.212	Firmware upload started
27.01.2004	10:38:00	ADLERSHOF	10.1.206.213	Firmware upload started

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

> When setting the time, please observe the functions of the LANCOM as NTP client and NTP server ('Time server for the local net' → page 16-17).

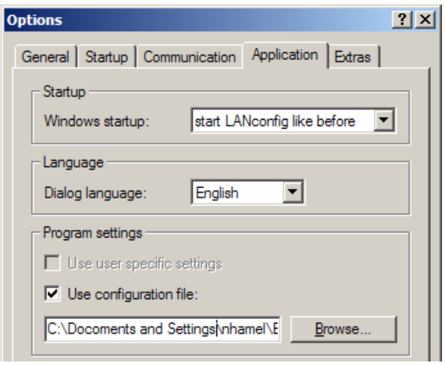
- Delete: Deletes the selected devices from the LANconfig list.

3.4.4 User-specific settings for LANconfig

The program settings for LANconfig are saved to the file 'lanconf.ini' located in the program directory when the program is ended. This includes, among others, the displayed devices, directory structure, selected language, etc. When the program is started, LANconfig reads this ini file and restores the previous status of the software. To save the ini file, the user needs a write authorization to the program directory.

As an alternative to the .ini file in the program directory, the program settings can be read from another source. The current user's user directory can be chosen, or indeed any other lanconf.ini from any location:

- By selecting the user directory, users can save their personal settings even if they don't have a write authorization for the program directory.
- Selecting an alternative storage location can be used, for example, to transfer program settings to any other LANconfig installation, or to save the program settings to a central location in the network for use by multiple users.



Startup
Windows startup: start LANconfig like before

Language
Dialog language: English

Program settings
□ Use user specific settings
☑ Use configuration file:
C:\Docoments and Settings\nhamel\E

LANconfig: **Options ▶ Application**

- **Use user-specific settings**

  Activates the use of the lanconf.ini file in the current user's directory `..\User\Application Files\LANCOM\LANconfig`.

  With this option activated, changes to the program settings are saved to this ini file.

- □ Possible values: On/off
- □ Default: Off

If this option is activated in parallel with the 'Use configuration file' option, then the file selected here will be used when the program starts and changes made to the program settings are stored to it.

- **Use configuration file**

  Activates the usage of the lanconf.ini from the given directory.

  With this option activated, changes to the program settings are saved to the ini file selected here.

  - □ Possible values: On/off and selection of the settings file
  - □ Default: Off

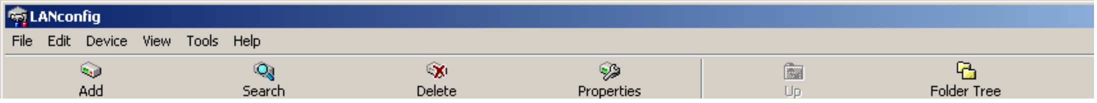
The file you select must be a valid LANconfig settings file.

If neither of the two options is activated, the ini file from the program directory will be used instead.

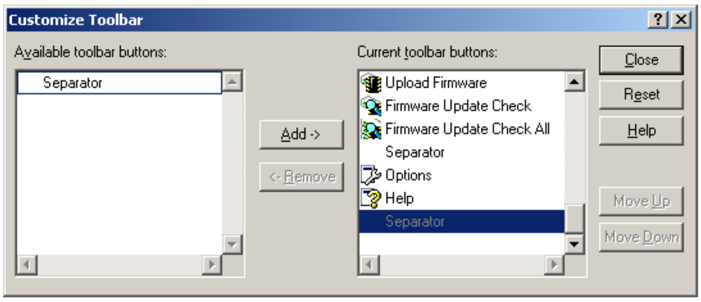
3.4.5 Customizing the toolbar

To customize the toolbar, select the following options in LANconfig under **View ▶ Toolbar**:

- Standard buttons: Hides/displays the buttons.
- Large icons: Shows a larger view of the icons.
- Show text: Text describing the action is displayed under each icon.



- Customize: Opens up a dialog enabling the displayed icons to be selected. A separator can be inserted between groups of icons. The order of the icons can also be changed.



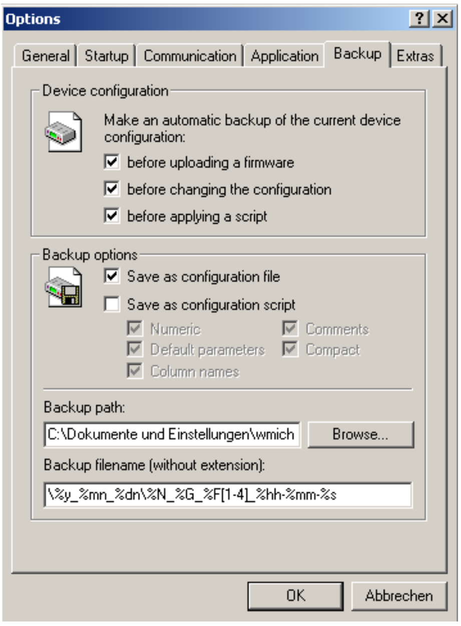
- Reset: Resets the settings for the toolbar to the default values.

3.4.6 Automatic backup of configuration with LANconfig

LANconfig can automatically save backups of the current configuration prior to changes in firmware or configuration. Global settings to be used for all devices are available under **Tools ▶ Options ▶ Backup**. Additionally, special backup settings can be defined for individual devices. To access them, right-click the appropriate device and select entry **Properties ▶ Backup** from the context menu.

Select the following options here:

- Are the global or the device-specific backup settings for this device to be used (in device-specific dialogue only)?
- The event prior to which the configuration is to be saved (firmware upload, configuration change or script execution).
- In which format the configuration is to be saved (configuration file, script - possibly with options).
- In which directory the configuration is to be saved.
- How the file name of the backup file is to be structured. Placeholders can be used for device information (IP address, hardware type, etc.) and time information. Please refer to the online help function for further information on placeholders.



Device configuration

Make an automatic backup of the current device configuration:

☑ before uploading a firmware

☑ before changing the configuration

☑ before applying a script

Backup options

☑ Save as configuration file

☐ Save as configuration script

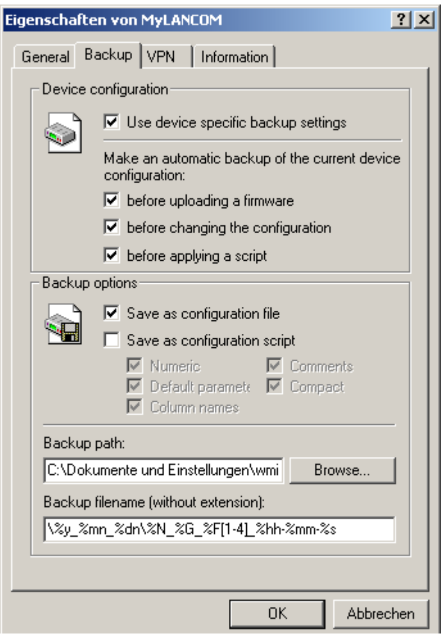
☑ Numeric ☑ Comments

☑ Default parameters ☑ Compact

☑ Column names

Backup path: C:\Dokumente und Einstellungen\wmich

Backup filename (without extension): \%y_%mn_%dn\%N_%G_%F[1-4]_%hh-%mm-%s



Device configuration

☑ Use device specific backup settings

Make an automatic backup of the current device configuration:

☑ before uploading a firmware

☑ before changing the configuration

☑ before applying a script

Backup options

☑ Save as configuration file

☐ Save as configuration script

☑ Numeric ☑ Comments

☑ Default paramete ☑ Compact

☑ Column names

Backup path: C:\Dokumente und Einstellungen\wmi

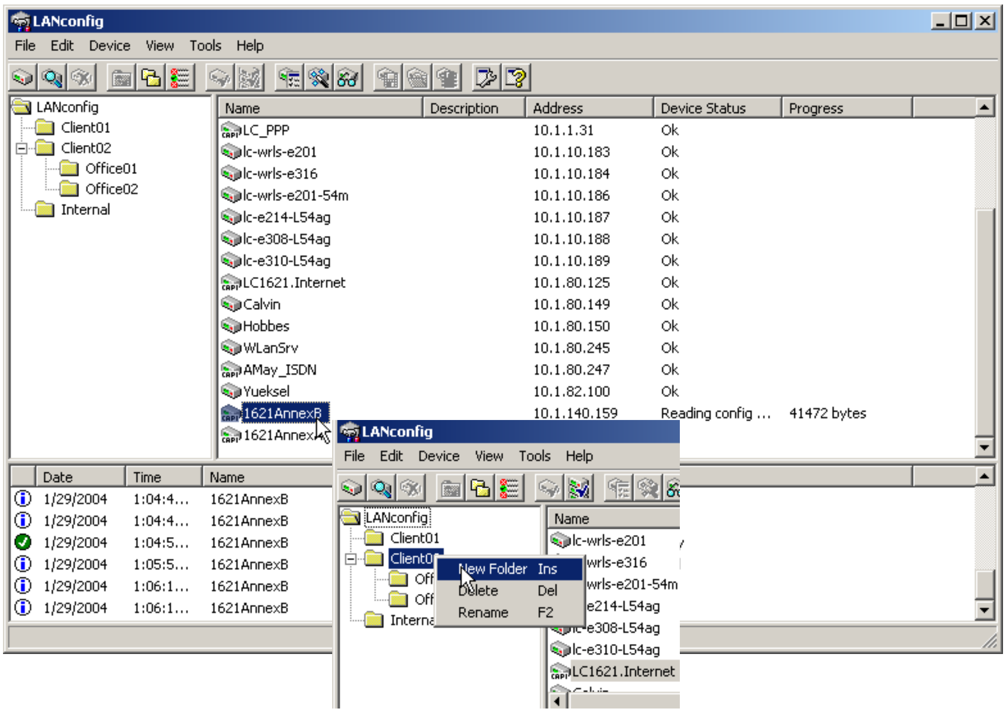
Backup filename (without extension): \%y_%mn_%dn\%N_%G_%F[1-4]_%hh-%mm-%s

3.4.7 Directory structure

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

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

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



Name	Description	Address	Device Status	Progress
LC_PPP		10.1.1.31	Ok	
lc-wrls-e201		10.1.10.183	Ok	
lc-wrls-e316		10.1.10.184	Ok	
lc-wrls-e201-54m		10.1.10.186	Ok	
lc-e214-L54ag		10.1.10.187	Ok	
lc-e308-L54ag		10.1.10.188	Ok	
lc-e310-L54ag		10.1.10.189	Ok	
LC1621.Internet		10.1.80.125	Ok	
Calvin		10.1.80.149	Ok	
Hobbes		10.1.80.150	Ok	
WLanSrv		10.1.80.245	Ok	
AMay_ISDN		10.1.80.247	Ok	
Yueksel		10.1.82.100	Ok	
1621AnnexB		10.1.140.159	Reading config ...	41472 bytes
1621Annex				

Date	Time	Name
1/29/2004	1:04:4...	1621AnnexB
1/29/2004	1:04:4...	1621AnnexB
1/29/2004	1:04:5...	1621AnnexB
1/29/2004	1:05:5...	1621AnnexB
1/29/2004	1:06:1...	1621AnnexB
1/29/2004	1:06:1...	1621AnnexB

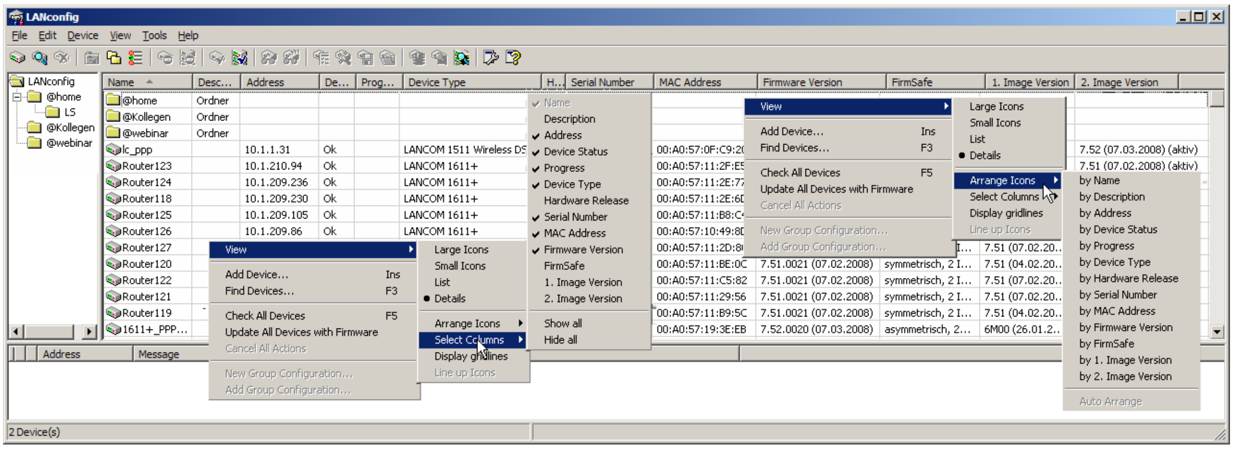
The directory structure in the left margin of the LANconfig window can be switched on and off with the **F6** function key or by using the menu **View** ▶ **Folder Tree**.

3.4.8 Better overview in LANconfig with more columns

Even for large-scale projects, a better overview and quicker orientation are facilitated in LANconfig by the columns featuring device-related details that can be displayed or concealed according to your needs. Simply click on the column header with the right-hand mouse button and use **Select columns**. The menu item **Arrange icons** allows you to sort the items as you prefer.

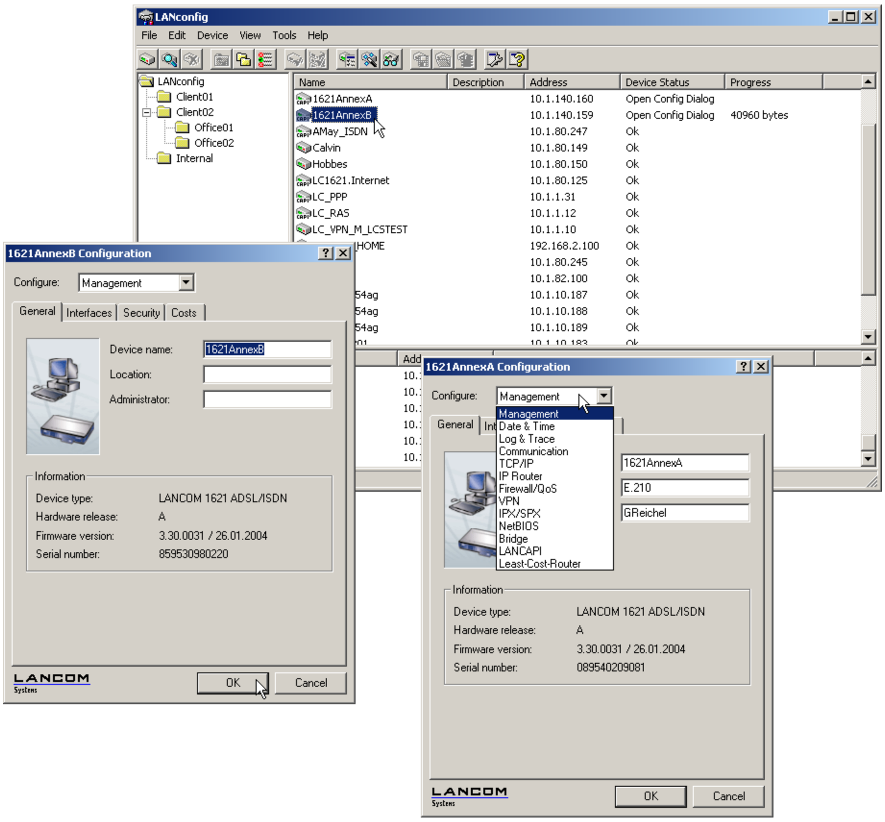
The following details can be displayed in the various columns:

- Device name
- Description
- Address
- Device status
- Progress
- Device type
- Hardware release
- Serial number
- MAC address
- Firmware version (active)
- Firmsafe
- 1. Image version
- 2. Image version


LANconfig
File Edit Device View Tools Help
LANconfig
@home
LS
@Kollegen
@webinar
Name
Desc…
Address
De…
Prog…
Device Type
H…
Serial Number
MAC Address
Firmware Version
FirmSafe
1. Image Version
2. Image Version
@home Ordner
@Kollegen Ordner
@webinar Ordner
lc_ppp 10.1.1.31 Ok LANCOM 1511 Wireless DS 00:A0:57:0F:C9:20 7.52 (07.03.2008) (aktiv)
Router123 10.1.210.94 Ok LANCOM 1611+ 00:A0:57:11:2F:E5 7.51 (07.02.2008) (aktiv)
Router124 10.1.209.236 Ok LANCOM 1611+ 00:A0:57:11:2E:77
Router118 10.1.209.230 Ok LANCOM 1611+ 00:A0:57:11:2E:6D
Router125 10.1.209.105 Ok LANCOM 1611+ 00:A0:57:11:B8:C4
Router126 10.1.209.86 Ok LANCOM 1611+ 00:A0:57:10:49:8D
Router127 00:A0:57:11:2D:8 7.51 (07.02.20…
Router120 00:A0:57:11:BE:0C 7.51.0021 (07.02.2008) symmetrisch, 2 I… 7.51 (04.02.20…
Router122 00:A0:57:11:C5:82 7.51.0021 (07.02.2008) symmetrisch, 2 I… 7.51 (07.02.20…
Router121 00:A0:57:11:29:56 7.51.0021 (07.02.2008) symmetrisch, 2 I… 7.51 (07.02.20…
Router119 00:A0:57:11:B9:5C 7.51.0021 (07.02.2008) symmetrisch, 2 I… 7.51 (04.02.20…
1611+_PPP… 00:A0:57:19:3E:EB 7.52.0020 (07.03.2008) asymmetrisch, 2… 6M00 (26.01.2…
View
Add Device… Ins
Find Devices… F3
Check All Devices F5
Update All Devices with Firmware
Cancel All Actions
New Group Configuration…
Add Group Configuration…
Large Icons
Small Icons
List
● Details
Arrange Icons
Select Columns
Display gridlines
Line up Icons
✓ Name
Description
✓ Address
✓ Device Status
✓ Progress
✓ Device Type
Hardware Release
✓ Serial Number
✓ MAC Address
✓ Firmware Version
FirmSafe
1. Image Version
2. Image Version
Show all
Hide all
by Name
by Description
by Address
by Device Status
by Progress
by Device Type
by Hardware Release
by Serial Number
by MAC Address
by Firmware Version
by FirmSafe
by 1. Image Version
by 2. Image Version
Auto Arrange
Address
Message
2 Device(s)

3.4.9 Multithreading

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



LANconfig

Name	Description	Address	Device Status	Progress
1621AnnexA		10.1.140.160	Open Config Dialog	
1621AnnexB		10.1.140.159	Open Config Dialog	40960 bytes
AMay_ISDN		10.1.80.247	Ok	
Calvin		10.1.80.149	Ok	
Hobbes		10.1.80.150	Ok	
LC1621.Internet		10.1.80.125	Ok	
LC_PPP		10.1.1.31	Ok	
LC_RAS		10.1.1.12	Ok	
LC_VPN_M_LCSTEST		10.1.1.10	Ok	
HOME		192.168.2.100	Ok	
		10.1.80.245	Ok	
		10.1.82.100	Ok	
54ag		10.1.10.187	Ok	
54ag		10.1.10.188	Ok	
54ag		10.1.10.189	Ok	
01		10.1.10.183	Ok	

1621AnnexB Configuration

Configure: Management

Device name: 1621AnnexB

Location:

Administrator:

Information

Device type: LANCOM 1621 ADSL/ISDN

Hardware release: A

Firmware version: 3.30.0031 / 26.01.2004

Serial number: 859530980220

1621AnnexA Configuration

Configure: Management

1621AnnexA

E.210

GReichel

Information

Device type: LANCOM 1621 ADSL/ISDN

Hardware release: A

Firmware version: 3.30.0031 / 26.01.2004

Serial number: 089540209081

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

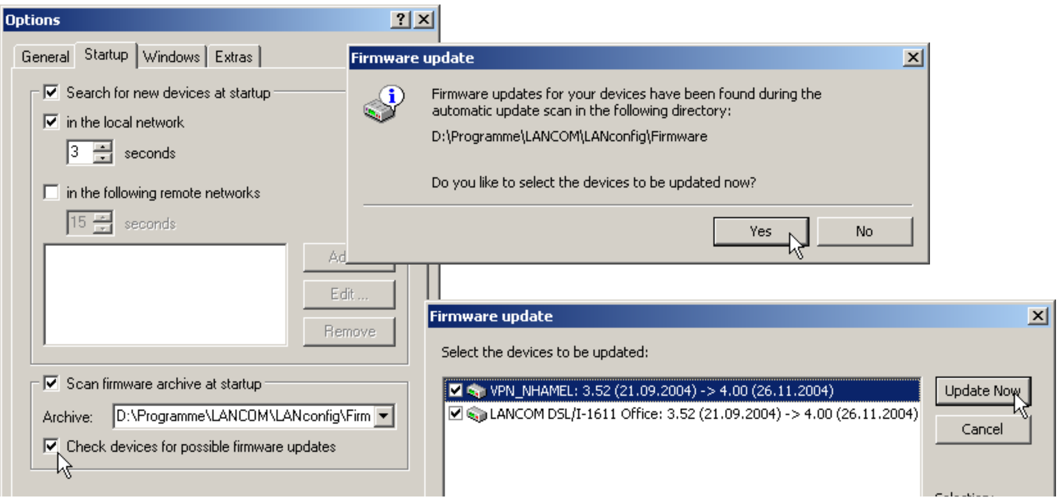
Multithreading allows changes to both the internal configurations of the available devices and to the configuration files. Each configuration is written separately to the file and to the device when the dialog is closed.

3.4.10 Manual and automatic searches for firmware updates

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

Automatic search for firmware updates

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



Options

☑ Search for new devices at startup

☑ in the local network

3 seconds

□ in the following remote networks

15 seconds

☑ Scan firmware archive at startup

Archive: D:\Programme\LANCOM\LANconfig\Firm

☑ Check devices for possible firmware updates

Firmware update

Firmware updates for your devices have been found during the automatic update scan in the following directory:

D:\Programme\LANCOM\LANconfig\Firmware

Do you like to select the devices to be updated now?

Firmware update

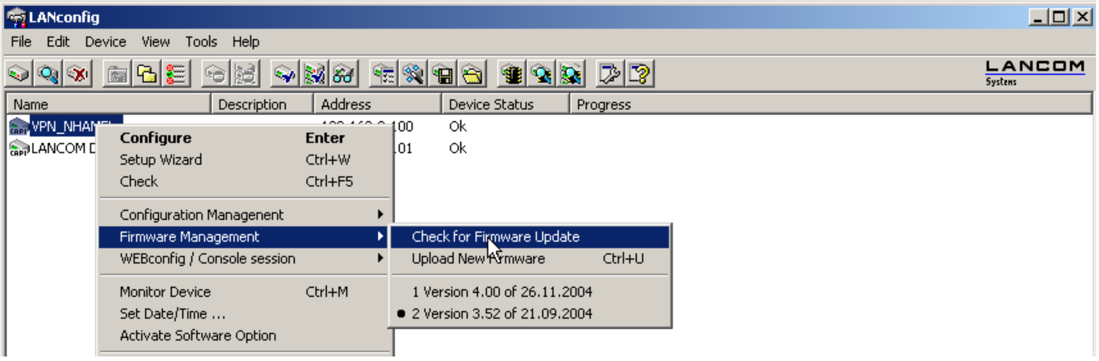
Select the devices to be updated:

☑ VPN_NHAMEL: 3.52 (21.09.2004) -> 4.00 (26.11.2004)

☑ LANCOM DSL/I-1611 Office: 3.52 (21.09.2004) -> 4.00 (26.11.2004)

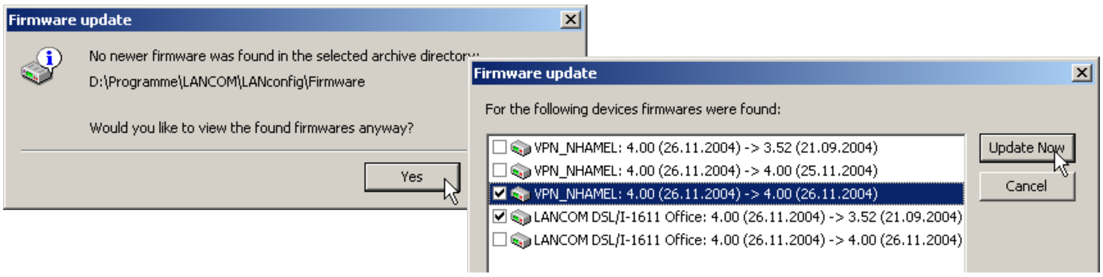
Manual search for firmware updates

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



View a full list of all firmware versions

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


Firmware update

No newer firmware was found in the selected archive directory:
D:\Programme\LANCOM\LANconfig\Firmware

Would you like to view the found firmwares anyway?

Firmware update

For the following devices firmwares were found:

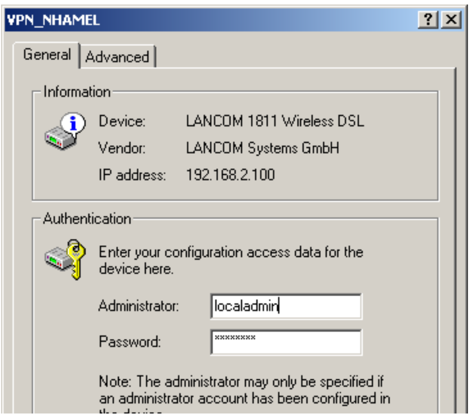
□ VPN_NHAMEL: 4.00 (26.11.2004) -> 3.52 (21.09.2004)
□ VPN_NHAMEL: 4.00 (26.11.2004) -> 4.00 (25.11.2004)
☑ VPN_NHAMEL: 4.00 (26.11.2004) -> 4.00 (26.11.2004)
☑ LANCOM DSL/I-1611 Office: 4.00 (26.11.2004) -> 3.52 (21.09.2004)
□ LANCOM DSL/I-1611 Office: 4.00 (26.11.2004) -> 4.00 (26.11.2004)

3.4.11 Password protection for SNMP read-only access.

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

LANmonitor

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



Device: LANCOM 1811 Wireless DSL
Vendor: LANCOM Systems GmbH
IP address: 192.168.2.100

Enter your configuration access data for the device here.

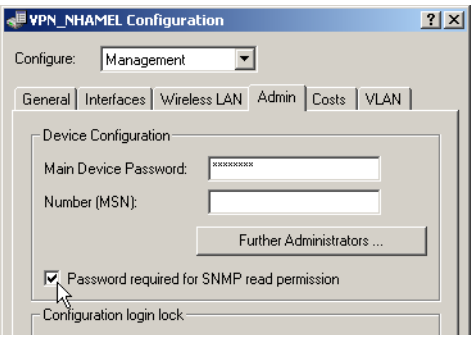
Administrator: localadmin
Password: ********

Note: The administrator may only be specified if an administrator account has been configured in the device.

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

- A supervisor has full access to the information in LANmonitor and can execute actions such as closing a connection, among others.
- A local administrator also has full access to the information in LANmonitor and can execute actions such as closing a connection, among others.
- A user with read-only rights can view the information in LANmonitor but cannot take any actions such as closing a connection.

- A user without rights has no SNMP access to the device's information.



Main Device Password: ********

Number (MSN):

☑ Password required for SNMP read permission

LANconfig: Management ▶ General

WEBconfig: LCOS menu tree ▶ Setup ▶ Config modul ▶ Password-required-for-SNMP-read-access

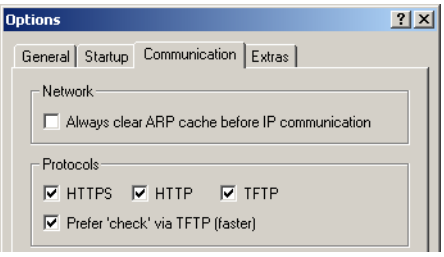
3.4.12 Device-specific settings for communications protocols

With LANconfig, all device actions are conducted using the TFTP protocol. Since this protocol has disadvantages compared to other protocols when transmitting large volumes of data, the protocols HTTPS and HTTP can also be used as alternatives.

The use of the protocols can be set either globally for all devices managed by a LANconfig or specifically for each individual device. The global settings overwrite the specific settings here – therefore, in the specific device settings, only the settings allowed in the global configuration can take effect.

Configuration of the global communication settings

When setting up the communications protocols, one must differentiate between the protocol that is used solely for checking the device and for other operations such as a firmware upload, etc.:



☐ Always clear ARP cache before IP communication

☑ HTTPS ☑ HTTP ☑ TFTP

☑ Prefer 'check' via TFTP (faster)

LANconfig: Tools ▶ Options ▶ Communication

- **HTTPS, HTTP, TFPT**

  When this is selected, the individual protocols are enabled for the operations firmware upload, configuration up/download, and script up/download. In these operations, LANconfig attempts to use these protocols in the order HTTPS, HTTP and TFTP. If the transfer fails when using a selected protocol, then the next protocol is automatically attempted.

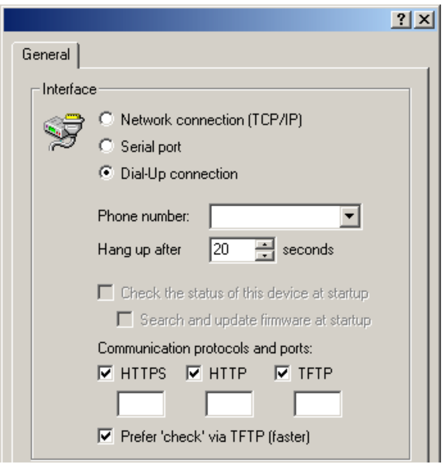
- **Prefer checks via TFTP**

  When checking the devices, only small amounts of data are transferred with the system information. As such, device checks could be performed using the TFTP protocol, particularly in the LAN. When this option is activated, the TFTP protocol is used to check the device first, regardless of the previously set communications protocols. If the check via TFTP fails, then the protocols HTTPS and HTTP are attempted in that order.

The device-specific settings are subordinate to the global communications settings. This allows, for example, the use of a protocol to be restricted centrally.

Configuration of the specific communication settings

For configuring the specific communications settings, the properties dialog of a device is opened via the context menu (right-click on mouse):



General

Interface

○ Network connection (TCP/IP)
○ Serial port
● Dial-Up connection

Phone number:

Hang up after 20 seconds

□ Check the status of this device at startup
□ Search and update firmware at startup

Communication protocols and ports:

☑ HTTPS ☑ HTTP ☑ TFTP

☑ Prefer 'check' via TFTP (faster)

- **HTTPS, HTTP, TFPT**

  Select the communications protocols as described in the global settings:

  In the fields under the protocols, the port to be used can be entered using the following default values:

  - HTTPS: 443
  - HTTP: 80
  - TFTP: 69

- **Prefer checks via TFTP**

  Preferred checking via TFTP as described in the global settings.

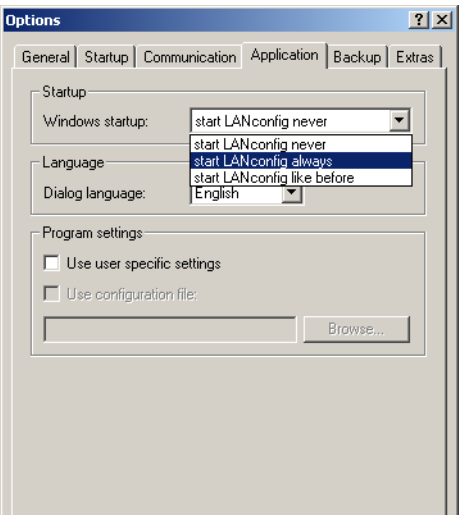
For all specific communications settings, the global settings are considered to be superordinate. A protocol can therefore only be used for operating a device when it is also activated in the global settings.

3.4.13 LANconfig behavior at Windows startup

LANconfig can be automatically started when the operating system starts.

Configuring the behavior of LANconfig at startup

The following parameters are used to configure the startup behavior of LANconfig:



Options

General | Startup | Communication | Application | Backup | Extras

Startup

Windows startup: start LANconfig never

start LANconfig never
start LANconfig always
start LANconfig like before

Language

Dialog language: English

Program settings

□ Use user specific settings
□ Use configuration file:

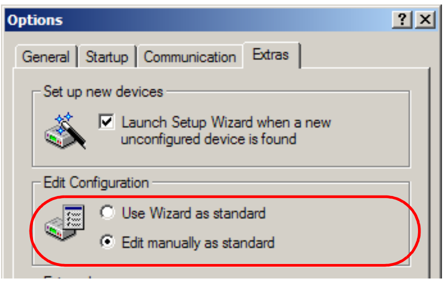
LANconfig: Options ▶ Extras ▶ Application

- **Windows system startup**
  - Start LANconfig never: LANconfig does not start automatically with the operating system, and it has to be started manually.
  - Start LANconfig always: LANconfig always starts automatically after Windows starts successfully.
  - Start LANconfig like last time: LANconfig starts in the program in the same status as when Windows was shut down the last time: If LANconfig was active then it will be started again; if inactive, LANconfig will not be automatically restarted.

When changing to a setting that enables LANconfig to be started automatically, a change is made to the operating system's registry. Personal firewalls on the computer or the operating system itself (Windows XP or Windows Vista^{TM}) may interpret this change as an attack and may issue a warning or even prevent the entry from being made. In order for LANconfig's startup behavior to be controlled as desired, you can ignore these warnings and allow the changes to be made.

3.4.14 Choice of Wizard or configuration dialog

You can define how LANconfig reacts when an entry in the list of devices is double-clicked, i.e. whether a Setup Wizard or the dialog for manually editing the configuration appears.



Set up new devices

☑ Launch Setup Wizard when a new unconfigured device is found

Edit Configuration

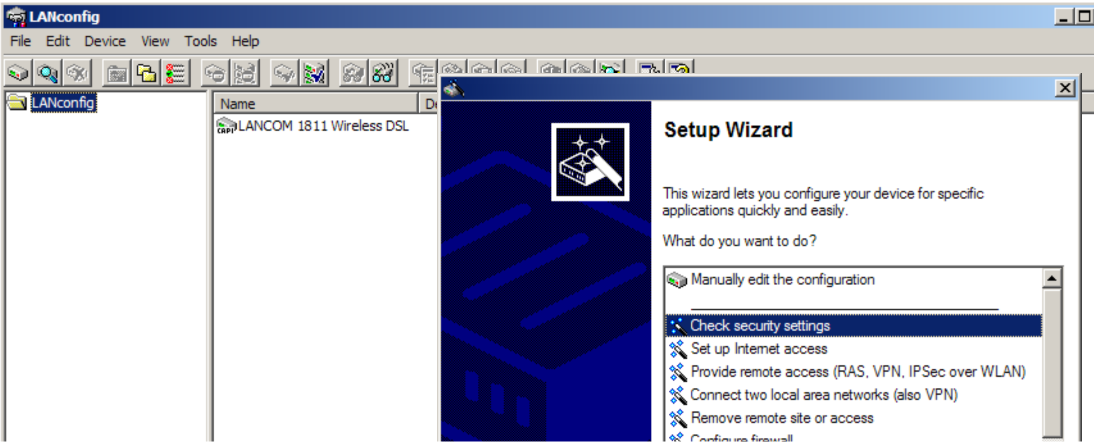
○ Use Wizard as standard

● Edit manually as standard

The standard behavior of LANconfig can be set under:

LANconfig: Tools ▶ Options ▶ Extras

- **Editing the configuration**
  - □ Use Wizard as standard: Double-clicking on a device entry in LANconfig will open up a dialog offering a choice of Wizards. As an alternative, the option 'Manually edit the configuration' can be selected here.



LANCOM 1811 Wireless DSL

Setup Wizard

This wizard lets you configure your device for specific applications quickly and easily.

What do you want to do?

- Manually edit the configuration
- Check security settings
- Set up Internet access
- Provide remote access (RAS, VPN, IPSec over WLAN)
- Connect two local area networks (also VPN)
- Remove remote site or access
- Configure firewall

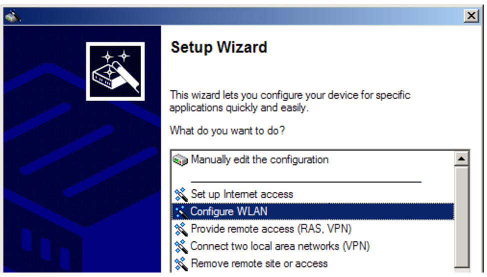
  - □ Edit manually as standard: Double-clicking on a device entry in LANconfig will open up a dialog for editing the configuration manually.

3.4.15 WLAN configuration with the wizards in LANconfig

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

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

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



Setup Wizard

This wizard lets you configure your device for specific applications quickly and easily.

What do you want to do?

- Manually edit the configuration
- Set up Internet access
- Configure WLAN
- Provide remote access (RAS, VPN)
- Connect two local area networks (VPN)
- Remove remote site or access

② In the selection menu, select the Setup Wizard, **Configure WLAN interface** and confirm the selection with **Continue**.

③ Make the settings as requested by the wizard and as described as follows.

Country settings

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

WLAN module operation

The WLAN modules can be operated in various operating modes:

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

  For further information please refer to section → Client Mode.

Physical WLAN settings

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

Logical WLAN networks

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

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

Point-to-point settings

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

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

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

3.5 Group configuration with LANconfig

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

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

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

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

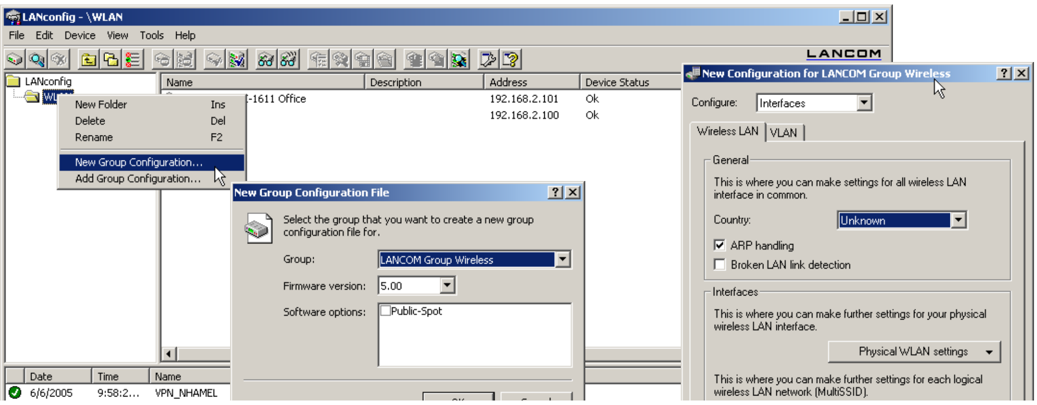
3.5.1 Create a group configuration

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

Group configuration with a new partial configuration file

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

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



Name	Description	Address	Device Status
-1611 Office		192.168.2.101	Ok
		192.168.2.100	Ok

Date	Time	Name
6/6/2005	9:58:2...	VPN_NHAMEL

New Group Configuration File

Select the group that you want to create a new group configuration file for.

Group: LANCOM Group Wireless

Firmware version: 5.00

Software options: □ Public-Spot

New Configuration for LANCOM Group Wireless

Configure: Interfaces

Wireless LAN | VLAN

General

This is where you can make settings for all wireless LAN interface in common.

Country: Unknown

☑ ARP handling

□ Broken LAN link detection

Interfaces

This is where you can make further settings for your physical wireless LAN interface.

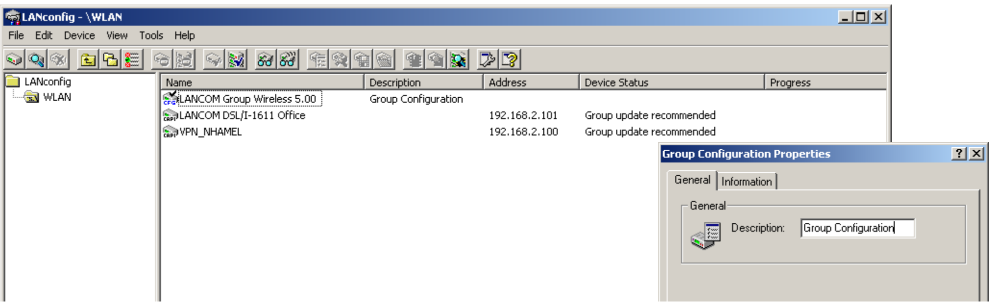
Physical WLAN settings

This is where you can make further settings for each logical wireless LAN network (MultiSSID).

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

The group configuration then saves all parameters to a partial configuration file. Those parameters which were not changed are also set to the standard values. Use the scripting function ('Scripting' → page 4-1) to read out non-standard settings from a device and transfer them to other devices, if required.

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



Name	Description	Address	Device Status	Progress
LANCOM Group Wireless 5.00	Group Configuration			
LANCOM DSL/I-1611 Office		192.168.2.101	Group update recommended	
VPN_NHAMEL		192.168.2.100	Group update recommended	

Group Configuration Properties

General | Information

General

Description: Group Configuration

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

Use an existing partial configuration file

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

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

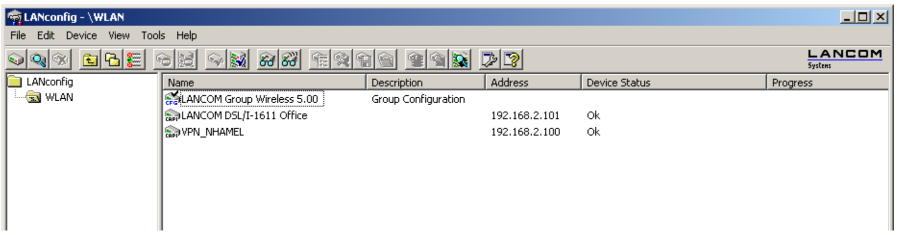
② In the subsequent dialog, select the existing partial configuration file to create a link to this file in the folder.

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

3.5.2 Update device configurations

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

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



Name	Description	Address	Device Status	Progress
LANCOM Group Wireless 5.00	Group Configuration			
LANCOM DSL/I-1611 Office		192.168.2.101	Ok	
VPN_NHAMEL		192.168.2.100	Ok	

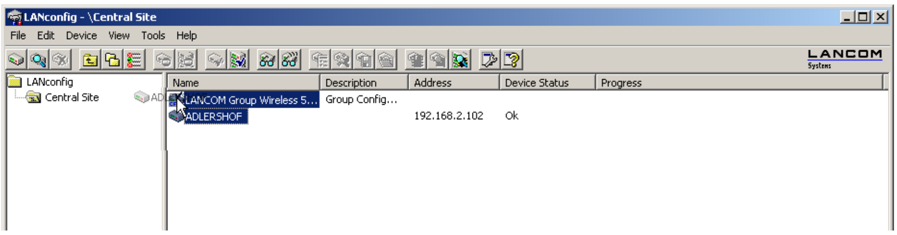
It is also possible to use the partial configuration for a device as a group configuration. Simply drag the device entry onto the group configuration entry.

3.5.3 Update group configurations

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

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

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

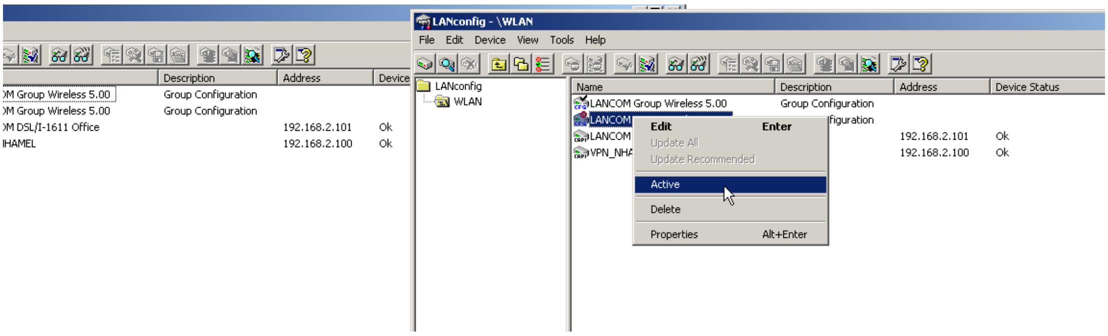


Name	Description	Address	Device Status	Progress
LANCOM Group Wireless 5...	Group Config...			
ADLERSHOF		192.168.2.102	Ok	

3.5.4 Using multiple group configurations

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

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



3.5.5 Transferring device configurations to similar models

When changing to a different device type, it is often necessary to adopt aspects of the configuration of the previous model. To do this, LANconfig offers the ability to load the configuration file (*.lcf) of a source device onto a similar destination device. All of the configuration parameters available on both source and destination devices assume the previously used values where possible:

- If the destination device has the appropriate parameter, and the value lies within the possible range, the value of the source device is taken.
- If the value of a parameter available on the destination device is not supported, the default value is used. Example:
  - The source device has four Ethernet interfaces.
  - The destination device only has two Ethernet interfaces.
  - The interface for an IP network is set to LAN-4 on the source device.
  - This value is not supported on the destination device. The value is therefore set to default value "LAN-1" on loading the configuration file.
- All destination-device parameters that were not available on the source device retain their respective values.

Proceed as follows to transfer the configuration onto a new device:

① The firmware levels of the source and destination devices should be matched as closely as possible. Every new LCOS firmware version features new parameters. Using the same firmware on the two devices allows the greatest possible matching of available parameters.

② Save the configuration of the source device with LANconfig , e.g. via **Device** ▶ **Configuration Management** ▶ **Save as File**.

③ Disconnect the source device from the network to avoid address conflicts.

④ Load the configuration onto the destination device using **Device** ▶ **Configuration Management** ▶ **Restore from File**. Messages on the conversion of the configuration are displayed in an information window.

Please note that this function is intended primarily for replacement devices and not for the configuration of new devices to be operated in parallel with the source device in the same network. Because key communication settings, such as the IP address of the device and DHCP settings, are transferred to the destination device, parallel operation of the source and destination devices in one network may result in conflicts. The configuration of several devices in one network is facilitated by group configuration and configuration via scripts.

3.6 LANmonitor—know what's going on

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

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

Explanations about the LANmonitor messages and helpful tips can be found in the appendix under 'Error messages in LANmonitor' → page 17-7.

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

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

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

3.6.1 Extended display options

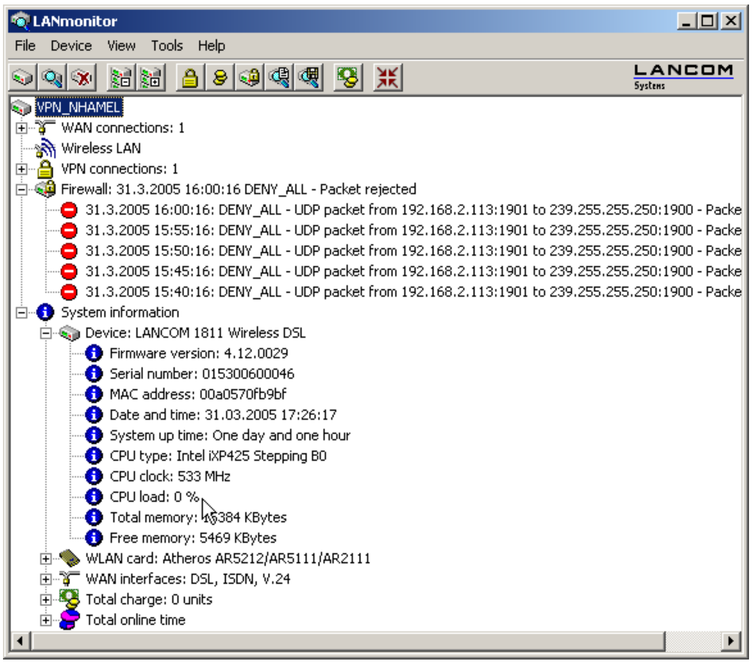
Under **View** ▶ **Show Details** you can activate and deactivate the following display options:

- 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.

3.6.2 Enquiry of the CPU and Memory utilization over SNMP

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



```
VPN_NHAMEL
 + WAN connections: 1
   Wireless LAN
 + VPN connections: 1
 - Firewall: 31.3.2005 16:00:16 DENY_ALL - Packet rejected
     31.3.2005 16:00:16: DENY_ALL - UDP packet from 192.168.2.113:1901 to 239.255.255.250:1900 - Packe
     31.3.2005 15:55:16: DENY_ALL - UDP packet from 192.168.2.113:1901 to 239.255.255.250:1900 - Packe
     31.3.2005 15:50:16: DENY_ALL - UDP packet from 192.168.2.113:1901 to 239.255.255.250:1900 - Packe
     31.3.2005 15:45:16: DENY_ALL - UDP packet from 192.168.2.113:1901 to 239.255.255.250:1900 - Packe
     31.3.2005 15:40:16: DENY_ALL - UDP packet from 192.168.2.113:1901 to 239.255.255.250:1900 - Packe
 - System information
     - Device: LANCOM 1811 Wireless DSL
         Firmware version: 4.12.0029
         Serial number: 015300600046
         MAC address: 00a0570fb9bf
         Date and time: 31.03.2005 17:26:17
         System up time: One day and one hour
         CPU type: Intel iXP425 Stepping B0
         CPU clock: 533 MHz
         CPU load: 0 %
         Total memory: 16384 KBytes
         Free memory: 5469 KBytes
     + WLAN card: Atheros AR5212/AR5111/AR2111
     + WAN interfaces: DSL, ISDN, V.24
     + Total charge: 0 units
     + Total online time
```

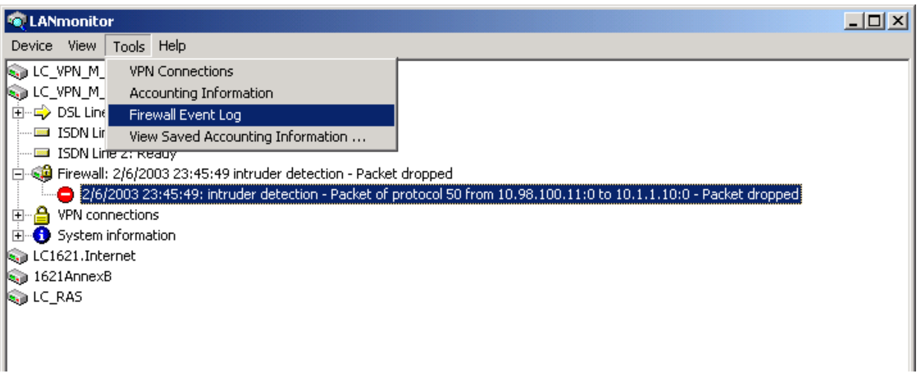
3.6.3 Monitor Internet connection

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

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

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

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



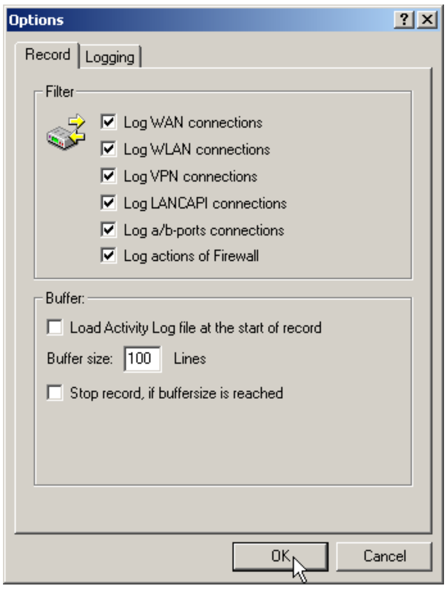
LC_VPN_M_
LC_VPN_M_
DSL Line
ISDN Lir
ISDN Line 2: Ready
Firewall: 2/6/2003 23:45:49 intruder detection - Packet dropped
2/6/2003 23:45:49: intruder detection - Packet of protocol 50 from 10.98.100.11:0 to 10.1.1.10:0 - Packet dropped
VPN connections
System information
LC1621.Internet
1621AnnexB
LC_RAS

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

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

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

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



Filter
☑ Log WAN connections
☑ Log WLAN connections
☑ Log VPN connections
☑ Log LANCAPI connections
☑ Log a/b-ports connections
☑ Log actions of Firewall

Buffer:
☐ Load Activity Log file at the start of record
Buffer size: 100 Lines
☐ Stop record, if buffersize is reached

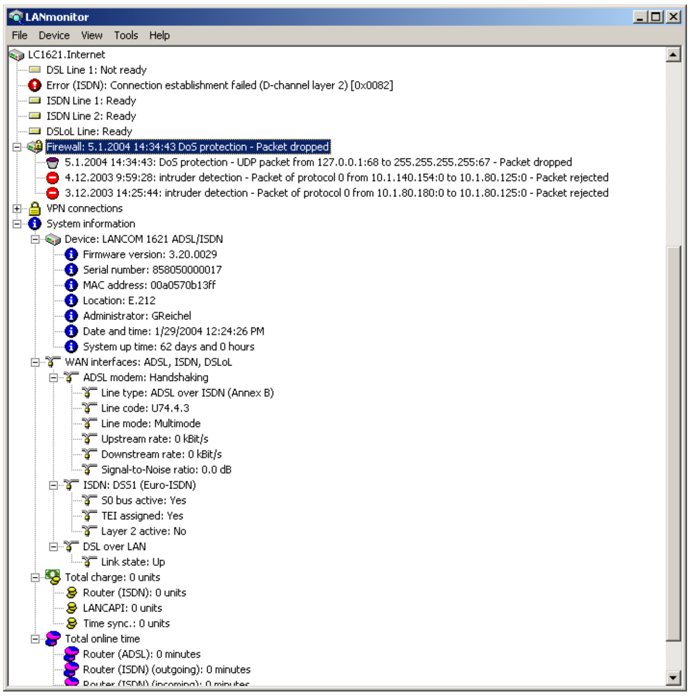
On the 'Protocol' tab you can define whether the following activities should be protocolled:

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

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

3.6.4 Display functions in LANmonitor

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



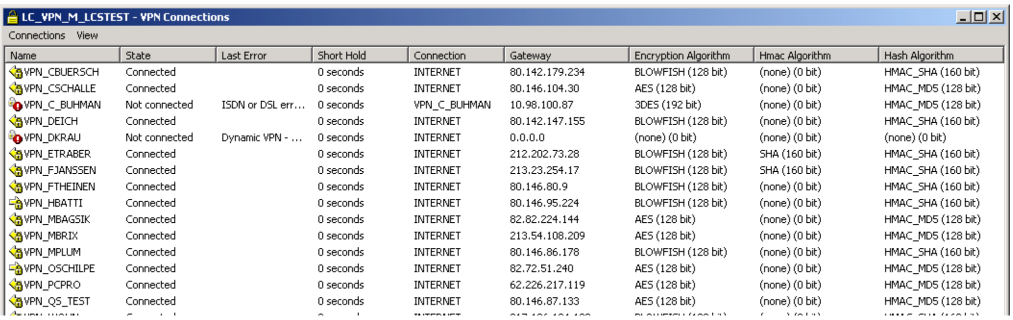
```
LC1621.Internet
    DSL Line 1: Not ready
    Error (ISDN): Connection establishment failed (D-channel layer 2) [0x0082]
    ISDN Line 1: Ready
    ISDN Line 2: Ready
    DSLoL Line: Ready
    Firewall: 5.1.2004 14:34:43 DoS protection - Packet dropped
        5.1.2004 14:34:43: DoS protection - UDP packet from 127.0.0.1:68 to 255.255.255.255:67 - Packet dropped
        4.12.2003 9:59:28: intruder detection - Packet of protocol 0 from 10.1.140.154:0 to 10.1.80.125:0 - Packet rejected
        3.12.2003 14:25:44: intruder detection - Packet of protocol 0 from 10.1.80.180:0 to 10.1.80.125:0 - Packet rejected
    VPN connections
    System information
        Device: LANCOM 1621 ADSL/ISDN
            Firmware version: 3.20.0029
            Serial number: 858050000017
            MAC address: 00a0570b13ff
            Location: E.212
            Administrator: GReichel
            Date and time: 1/29/2004 12:24:26 PM
            System up time: 62 days and 0 hours
        WAN interfaces: ADSL, ISDN, DSLoL
            ADSL modem: Handshaking
                Line type: ADSL over ISDN (Annex B)
                Line code: U74.4.3
                Line mode: Multimode
                Upstream rate: 0 kBit/s
                Downstream rate: 0 kBit/s
                Signal-to-Noise ratio: 0.0 dB
            ISDN: DSS1 (Euro-ISDN)
                S0 bus active: Yes
                TEI assigned: Yes
                Layer 2 active: No
            DSL over LAN
                Link state: Up
        Total charge: 0 units
            Router (ISDN): 0 units
            LANCAPI: 0 units
            Time sync.: 0 units
        Total online time
            Router (ADSL): 0 minutes
            Router (ISDN) (outgoing): 0 minutes
            Router (ISDN) (incoming): 0 minutes
```

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

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

- VPN connections

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

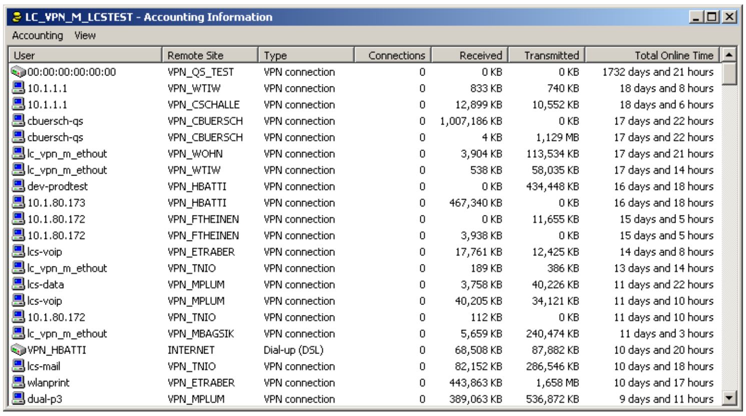


Name	State	Last Error	Short Hold	Connection	Gateway	Encryption Algorithm	Hmac Algorithm	Hash Algorithm
VPN_CBUERSCH	Connected		0 seconds	INTERNET	80.142.179.234	BLOWFISH (128 bit)	(none) (0 bit)	HMAC_SHA (160 bit)
VPN_CSCHALLE	Connected		0 seconds	INTERNET	80.146.104.30	AES (128 bit)	(none) (0 bit)	HMAC_MD5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

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

- Accounting information

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

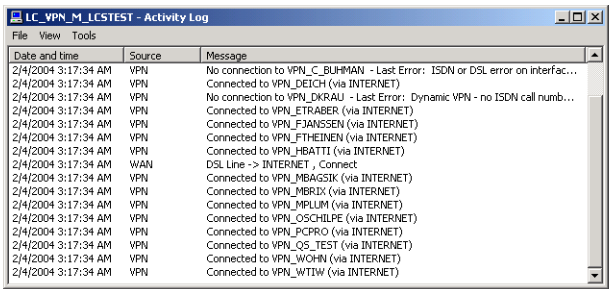


User	Remote Site	Type	Connections	Received	Transmitted	Total Online Time
00:00:00:00:00:00	VPN_QS_TEST	VPN connection	0	0 KB	0 KB	1732 days and 21 hours
10.1.1.1	VPN_WTIW	VPN connection	0	833 KB	740 KB	18 days and 8 hours
10.1.1.1	VPN_CSCHALLE	VPN connection	0	12,899 KB	10,552 KB	18 days and 6 hours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

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

■ Activity log

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

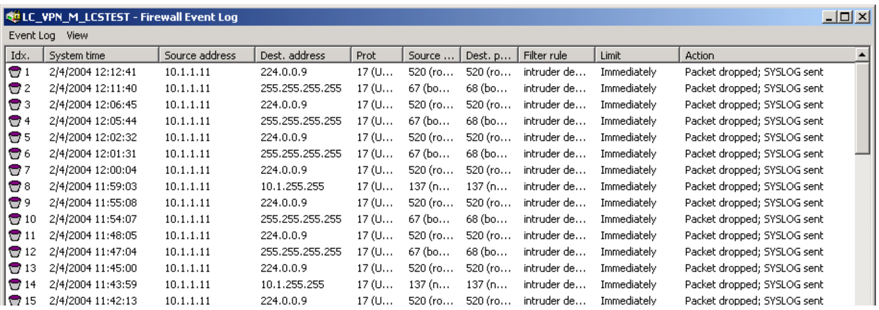


Date and time	Source	Message
2/4/2004 3:17:34 AM	VPN	No connection to VPN_C_BUHMAN - Last Error: ISDN or DSL error on interfac...
2/4/2004 3:17:34 AM	VPN	Connected to VPN_DEICH (via INTERNET)
2/4/2004 3:17:34 AM	VPN	No connection to VPN_DKRAU - Last Error: Dynamic VPN - no ISDN call numb...
2/4/2004 3:17:34 AM	VPN	Connected to VPN_ETRABER (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_FJANSSEN (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_FTHEINEN (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_HBATTI (via INTERNET)
2/4/2004 3:17:34 AM	WAN	DSL Line -> INTERNET , Connect
2/4/2004 3:17:34 AM	VPN	Connected to VPN_MBAGSIK (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_MBRIX (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_MPLUM (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_OSCHILPE (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_PCPRO (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_QS_TEST (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_WOHN (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_WTIW (via INTERNET)

- □ Date and time
- □ Source
- □ Message

■ Firewall actions log

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



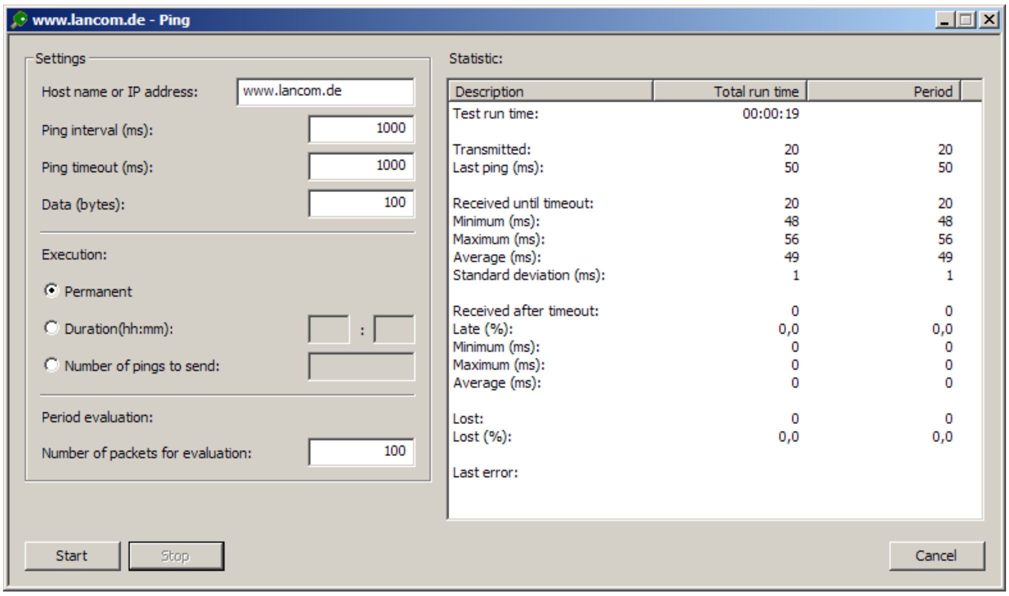
Idx.	System time	Source address	Dest. address	Prot	Source ...	Dest. p...	Filter rule	Limit	Action
1	2/4/2004 12:12:41	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
2	2/4/2004 12:11:40	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
3	2/4/2004 12:06:45	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
4	2/4/2004 12:05:44	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
5	2/4/2004 12:02:32	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
6	2/4/2004 12:01:31	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
7	2/4/2004 12:00:04	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
8	2/4/2004 11:59:03	10.1.1.11	10.1.255.255	17 (U...	137 (n...	137 (n...	intruder de...	Immediately	Packet dropped; SYSLOG sent
9	2/4/2004 11:55:08	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
10	2/4/2004 11:54:07	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
11	2/4/2004 11:48:05	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
12	2/4/2004 11:47:04	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
13	2/4/2004 11:45:00	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
14	2/4/2004 11:43:59	10.1.1.11	10.1.255.255	17 (U...	137 (n...	137 (n...	intruder de...	Immediately	Packet dropped; SYSLOG sent
15	2/4/2004 11:42:13	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent

- □ Time
- □ Source and destination address
- □ Protocol with source and destination port
- □ Activated filter rule and exceeded limit
- □ Action carried out

3.6.5 Connection diagnosis with LANmonitor

LANmonitor can be used to check the connection quality between stations in the LAN, WAN or WLAN. LANmonitor sends pings from the computer on which it is installed to the remote site at regular intervals. The responses it receives are the basis for a compiled report.

To enter the parameters and display the results, a dedicated dialog has been implemented in LANmonitor.



Host name or IP address: www.lancom.de
Ping interval (ms): 1000
Ping timeout (ms): 1000
Data (bytes): 100

Execution:
● Permanent
○ Duration(hh:mm): :
○ Number of pings to send:

Period evaluation:
Number of packets for evaluation: 100

Description	Total run time	Period
Test run time:	00:00:19	
Transmitted:	20	20
Last ping (ms):	50	50
Received until timeout:	20	20
Minimum (ms):	48	48
Maximum (ms):	56	56
Average (ms):	49	49
Standard deviation (ms):	1	1
Received after timeout:	0	0
Late (%):	0,0	0,0
Minimum (ms):	0	0
Maximum (ms):	0	0
Average (ms):	0	0
Lost:	0	0
Lost (%):	0,0	0,0
Last error:		

LANmonitor: Tools ▶ Ping... or via the context menu

Configuring Ping execution

- **Host name or IP address**

  The remote station which is to be queried by Ping is entered here. The following information can be entered for all of the different network devices (servers, clients, routers, printers, etc.) which can be reached via LAN, WAN or WLAN.

ⓘ If a device is selected when the Ping dialog is opened with **Device ▶ Ping...** or via the context menu in LANmonitor, then the IP address of this device is assumed to be the remote site.

- **Ping interval**

  The time interval between two consecutive pings in [ms].

ⓘ The interval between two pings cannot be less than the packet transmission time, i.e. before sending a ping, the previous ping must have been answered or the ping timeout must have expired.

- **Ping timeout**

  The time waited for the response to a ping to arrive [ms]. If this time expires and no response was received then the ping is assumed to be lost.

- **Data**

  The size of a ping packet [bytes]. A "ping" is an ICMP packet which is generally transmitted without any content, i.e. it is just a header. To increase the load of the packets used for testing a connection, a payload can be created artificially. The overall packet size then consists of an IP header (20 bytes), an ICMP header (8 bytes) and the payload.

ⓘ The packets will be fragmented if the payload of the ICMP packets exceeds the maximum IP packet size.

- **Execution**

  Repeat mode for the ping command.

Evaluation

The right-hand portion of the Ping dialog displays the results of the ping test. The first column shows the sum values over the entire test; the second column shows only the values collected over the evaluation period, i.e. the sum of the most recent packets. Unanswered pings are not included in the evaluation.

The period evaluation considers only the pings sent during the defined period.

The following information is displayed for evaluation:

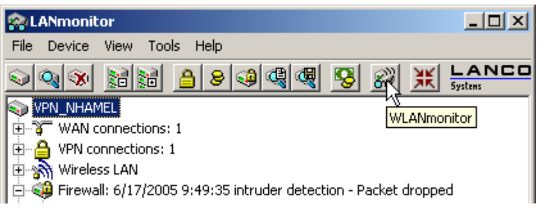
- **Test run time**
  - The total run time [hr./ min./ sec.]
- **Transmitted**
  - Total number of pings sent
  - Run time of the last ping [ms]
- **Received until timeout**
  - The number of pings answered in the timeout period
  - Minimum runtime
  - Maximum runtime
  - Average
  - Standard deviation from the mean run time
- **Received after timeout**
  - The number of pings answered after the timeout period
  - Late packets as a proportion of the total number
  - Minimum runtime
  - Maximum runtime
  - Average
- **Lost**
  - The number of lost packets
  - Lost packets as a proportion of the total number

3.7 Visualization of larger WLANs with WLANmonitor

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

3.7.1 Start the LANCOM WLANmonitor

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



VPN_NHAMEL
WAN connections: 1
VPN connections: 1
Wireless LAN
Firewall: 6/17/2005 9:49:35 intruder detection - Packet dropped

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

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

3.7.2 Search for access points

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

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

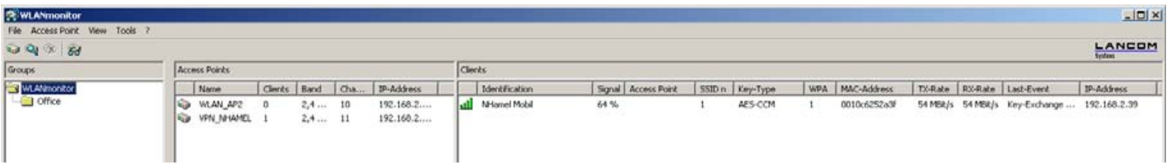
The right-hand column (client list) lists the clients that are logged in to the selected access point. The following information is shown for each client:

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

  LANconfig: WLAN Security ▶ Stations ▶ Stations

  Telnet: Setup/WLAN/Access-List

  WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN ▶ Access-List
- Signal: Connection signal strength
- Access point: Name of the access point that the client is logged on to
- SSID: Identifier for the WLAN network
- Encryption: Type of encryption used for the wireless connection
- WPA version (WPA-1 or WPA-2)
- MAC address: Hardware address of the WLAN client
- TX rate: Transmission data rate
- RX rate: Reception data rate
- Last event, e.g. 'Authentification successful', 'RADIUS successful'
- IP addresss of the WLAN clients



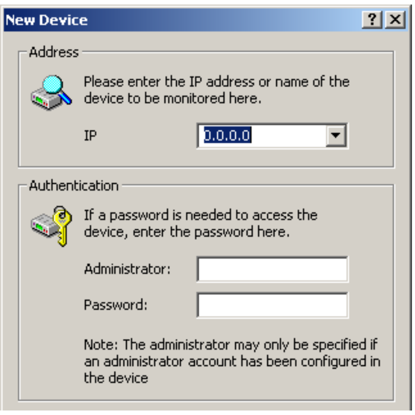
Name	Clients	Band	Cha...	IP-Address
WLAN_AP2	0	2,4 ...	10	192.168.2....
VPN_NHAMEL	1	2,4 ...	11	192.168.2....

Identification	Signal	Access Point	SSID n	Key-Type	WPA	MAC-Address	TX-Rate	RX-Rate	Last-Event	IP-Address
NHamel Mobil	64 %		1	AES-CCM	1	0010c6252a3f	54 MBit/s	54 MBit/s	Key-Exchange ...	192.168.2.39

3.7.3 Add access points

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

.



Please enter the IP address or name of the device to be monitored here.

IP: 0.0.0.0

If a password is needed to access the device, enter the password here.

Administrator:

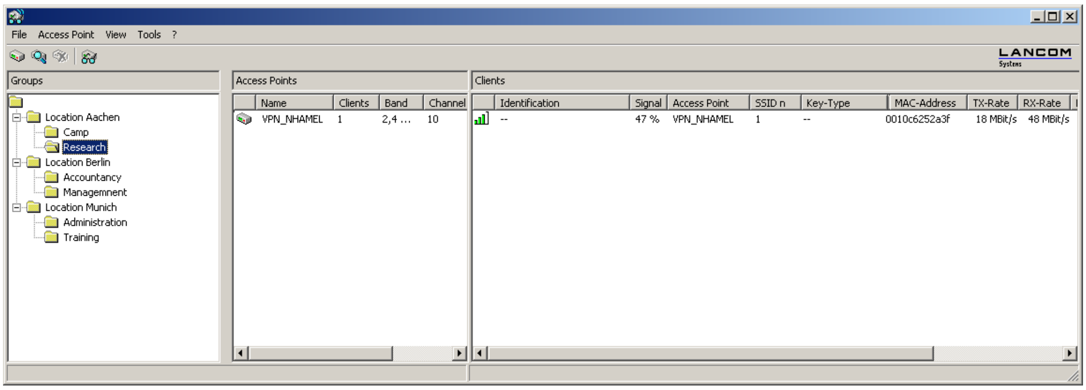
Password:

Note: The administrator may only be specified if an administrator account has been configured in the device

3.7.4 Organize access points

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

The groups are shown in the left column in WLANmonitor. Starting from the top group 'WLANmonitor', you can use the menu item **File ▶ Add group** to create new sub-groups and so build up a structure. Access points found during a search are assigned to the currently selected group in the group tree. Access points that have been recognized already can be moved to the another group with drag and drop.



Access Points

Name	Clients	Band	Channel
VPN_NHAMEL	1	2,4 ...	10

Clients

Identification	Signal	Access Point	SSID n	Key-Type	MAC-Address	TX-Rate	RX-Rate
--	47 %	VPN_NHAMEL	1	--	0010c6252a3f	18 MBit/s	48 MBit/s

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

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

3.7.5 Rogue AP and rogue client detection with the WLANmonitor

WLAN devices that make unauthorized attempts at accessing a WLAN by posing as an access point or client are called rogues.

- Rogue clients are computers equipped with WLAN adapters that are located within the range of a WLAN and attempt to log on to one of the access points, for example, in order to use the Internet connection or in order to receive access to secured areas on the network.
- An example of rogue APs are access points that a company's employees connect to the network without the knowledge or permission of the system administrators, thereby consciously or unconsciously making the network vulnerable to potential attackers via unsecured WLAN access. Not quite as dangerous, but disruptive all the same are access points that belong to third-party networks yet are within the range of the local WLAN. If such devices also use the same SSID and channel as the local AP (default settings), then local clients could attempt to log on to external networks.

Unidentified access points within the range of the local network frequently pose a possible threat and security gap. At the very least they are a disturbance, and so they need to be identified to decide whether further measures in securing the local network need to be introduced. Information about the clients within range of your network is automatically stored to an internal table in the LANCOM Wireless Router. Once activated, background scanning records neighboring access points and records them to the scan table. WLANmonitor presents this information visually. The access points and clients found can be categorized in groups such as 'known', 'unknown' or 'rogue'.

Further information can be found under 'Background WLAN scanning' → page 11-20.

Rogue AP detection

The WLANmonitor sorts all of the access points found into predefined subgroups under 'Rogue AP Detection' while displaying the following information:

- Time of first and last detection
- BSSID, the MAC addresse of the AP for this WLAN network
- Network name
- Type of encryption used
- Frequency band used
- Radio channel used
- Use of 108Mbps mode

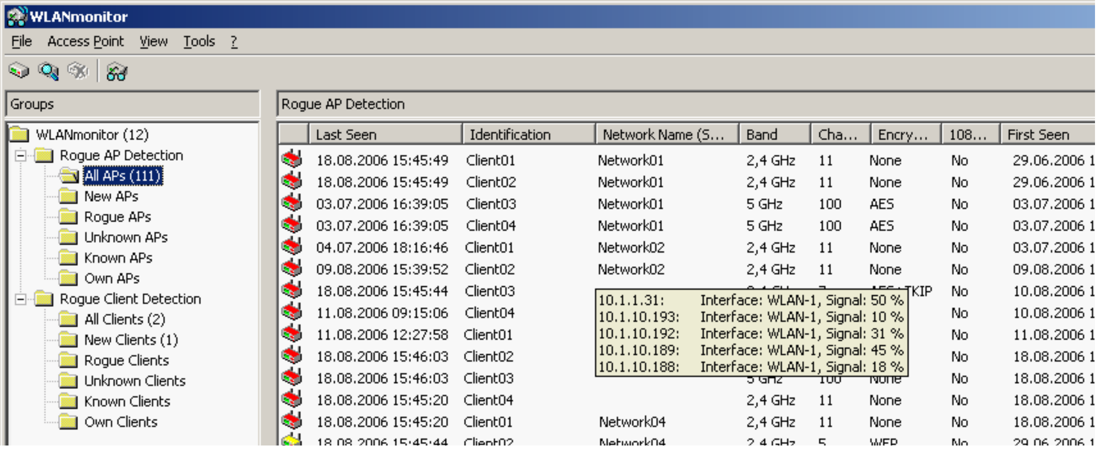
To use rogue AP detection, background scanning has to be activated in the LANCOM Wireless Router.

The WLANmonitor uses the following groups for sorting the APs that are found:

- All APs: List of all scanned WLAN networks grouped as follows
- New APs: New unknown and unconfigured WLAN networks are automatically grouped here (APs displayed in yellow)
- Rogue APs: WLAN networks identified as rogue and in need of urgent observation (APs displayed in red)

- Unknown APs: WLAN networks which are to be further analyzed (APs displayed in gray)
- Known APs: WLAN networks which are not a threat (APs displayed in gray)
- Own APs: New affiliated WLAN networks from access points monitored by WLANmonitor are automatically grouped here (APs displayed in green)

The WLANs that have been found can be placed into a corresponding group depending on their status. You can set up your own network groups within the individual groups by using the context menu (right mouse button) (except for the group 'All APs').



	Last Seen	Identification	Network Name (S...	Band	Cha...	Encry...	108...	First Seen
	18.08.2006 15:45:49	Client01	Network01	2,4 GHz	11	None	No	29.06.2006 1
	18.08.2006 15:45:49	Client02	Network01	2,4 GHz	11	None	No	29.06.2006 1
	03.07.2006 16:39:05	Client03	Network01	5 GHz	100	AES	No	03.07.2006 1
	03.07.2006 16:39:05	Client04	Network01	5 GHz	100	AES	No	03.07.2006 1
	04.07.2006 18:16:46	Client01	Network02	2,4 GHz	11	None	No	03.07.2006 1
	09.08.2006 15:39:52	Client02	Network02	2,4 GHz	11	None	No	09.08.2006 1
	18.08.2006 15:45:44	Client03				TKIP	No	10.08.2006 1
	11.08.2006 09:15:06	Client04					No	10.08.2006 1
	11.08.2006 12:27:58	Client01					No	11.08.2006 1
	18.08.2006 15:46:03	Client02					No	18.08.2006 1
	18.08.2006 15:46:03	Client03		5 GHz	100	None	No	18.08.2006 1
	18.08.2006 15:45:20	Client04		2,4 GHz	11	None	No	18.08.2006 1
	18.08.2006 15:45:20	Client01	Network04	2,4 GHz	11	None	No	18.08.2006 1
	18.08.2006 15:45:44	Client02	Network04	2,4 GHz	5	WEP	No	29.06.2006 1

```
10.1.1.31:      Interface: WLAN-1, Signal: 50 %
10.1.10.193:    Interface: WLAN-1, Signal: 10 %
10.1.10.192:    Interface: WLAN-1, Signal: 31 %
10.1.10.189:    Interface: WLAN-1, Signal: 45 %
10.1.10.188:    Interface: WLAN-1, Signal: 18 %
```

If a parameter is changed on an AP, e.g. the security settings, then it is displayed again as a newly discovered AP.

Rogue client detection

The WLANmonitor presents all of the clients found into predefined subgroups under 'Rogue Client Detection' while displaying the following information:

- Time of first and last detection
- MAC address of the client
- Network name

No configuration of the LANCOM Wireless Router is necessary to make use of rogue client detection.

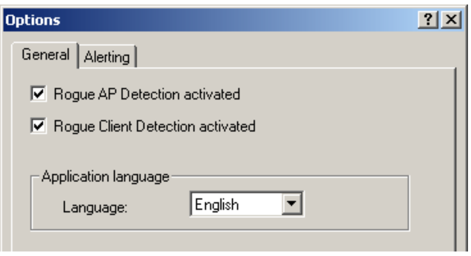
The WLANmonitor uses the following groups for sorting the clients that are found:

- All clients: List of all found clients grouped as follows (clients are colored according to their group)
- New clients: New unknown clients are automatically grouped here (clients displayed in yellow)
- Rogue clients: Clients identified as rogue and in need of urgent observation (clients displayed in red)
- Unknown clients: Clients which are to be further analyzed (clients displayed in gray)
- Known clients: Clients which are not a threat (clients displayed in gray)
- Own clients: New affiliated clients associated with access points monitored by WLAN monitor are automatically grouped here (APs displayed in green)

The clients that have been found can be placed into a corresponding group depending on their status. You can set up your own network groups within the individual groups by using the context menu (right mouse button) (except for the group 'All clients').

Activating rogue-AP and rogue-client detection

The functions for rogue-AP and rogue-client detection can be switched on or off in WLANmonitor.



☑ Rogue AP Detection activated

☑ Rogue Client Detection activated

Language: English

:WLANmonitor: Tools ▶ Options ▶ General

- **Rogue AP detection activated**

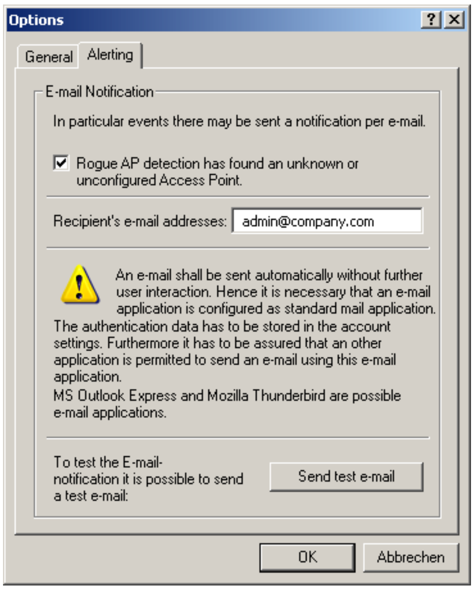
  Activate this option if WLANmonitor is to display unknown or unconfigured access points.

- **Rogue client detection activated**

  Activate this option if WLANmonitor is to display unknown or unconfigured clients.

Configuring the alert function in the WLANmonitor

The WLANmonitor can inform the administrator automatically via e-mail whenever an unknown or unconfigured access point is discovered.



Options

General | Alerting

E-mail Notification

In particular events there may be sent a notification per e-mail.

☑ Rogue AP detection has found an unknown or unconfigured Access Point.

Recipient's e-mail addresses: admin@company.com

An e-mail shall be sent automatically without further user interaction. Hence it is necessary that an e-mail application is configured as standard mail application. The authentication data has to be stored in the account settings. Furthermore it has to be assured that an other application is permitted to send an e-mail using this e-mail application.
MS Outlook Express and Mozilla Thunderbird are possible e-mail applications.

To test the E-mail-notification it is possible to send a test e-mail:

WLANmonitor: Tools ▶ Options ▶ Alerts

- **E-mail messaging**

  Activate this option if you would like the WLANmonitor to report unknown or unconfigured access points via e-mail.

- **Recipient e-mail addresses**

  Enter the e-mail address(es) of the administrators here that should be informed in the event of rogue AP detection. Multiple e-mail addresses should be separated by commas.

In order to send e-mail alerts, the computer on which WLANmonitor is running requires a standard e-mail client (MS Outlook Express or Mozilla Thunderbird) that allows automatic mail transmission to be configured and running.

- **Send a test e-mail**

  Some mail clients require a confirmation from the user before sending via third-party applications. Test the alarm function with this button.

3.8 Configuration with WEBconfig

New with LCOS 7.6:

- New WEBconfig with search function, comprehensive device status, on-line help, etc.

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

Secure with HTTPS

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

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

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

Access with WEBconfig

To carry out a configuration with WEBconfig, you need to know how to contact the device. Device behavior and accessibility for configuration via a Web browser depend on whether the DHCP server and DNS server are active in the LAN already, and whether these two server processes share the assignment in the LAN of IP addresses to symbolic names.

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

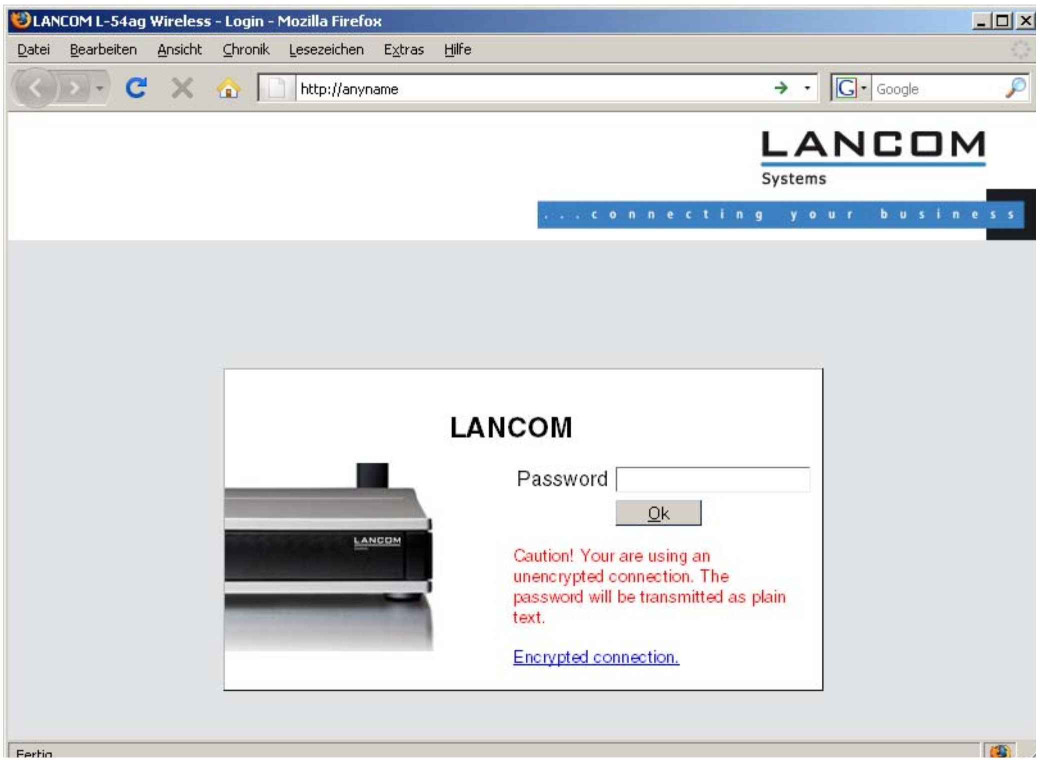
If a LANCOM Wireless Router or LANCOM Access Point is centrally managed from a LANCOM WLAN Controller, the DHCP mode is switched from auto-mode to client mode upon provision of the WLAN configuration.

Network without a DHCP server

Not for centrally managed LANCOM Wireless Routers or LANCOM Access Points

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

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



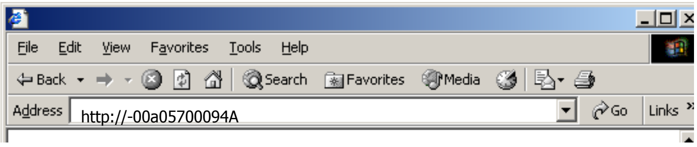
Caution! Your are using an unencrypted connection. The password will be transmitted as plain text.

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

Network with DHCP server

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

- If the LAN also has a DNS server for name resolution and this communicates the IP address/name assignment to the DHCP server, the device can be reached under name "-<MAC address>", e.g. "-00a057xxxxxx".



http://-00a05700094A

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

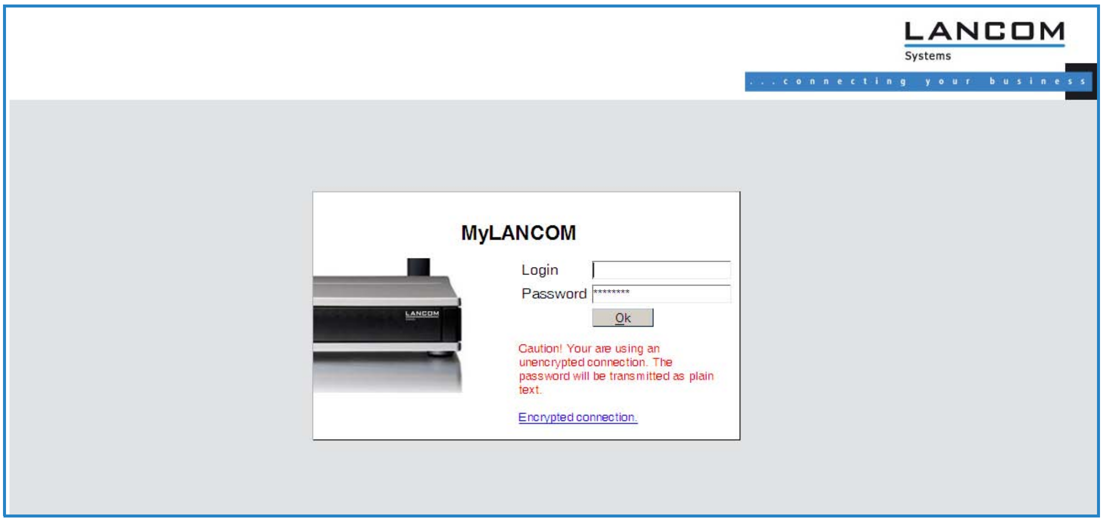
- If there is no DNS server in the LAN, or if it is not coupled to the DHCP server, the device cannot be reached via the name. In this case the following options remain:
  - Use LANconfig's “Find Device” function, or perform WEBconfig's “Device Search” from another yet accessible LANCOM.
  - Use suitable tools to find out the IP address assigned to the LANCOM by DHCP and access the device directly using this IP address.
  - Use the serial configuration interface to connect a computer running a terminal program to the device.

Login

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

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

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



MyLANCOM

Login

Password ********

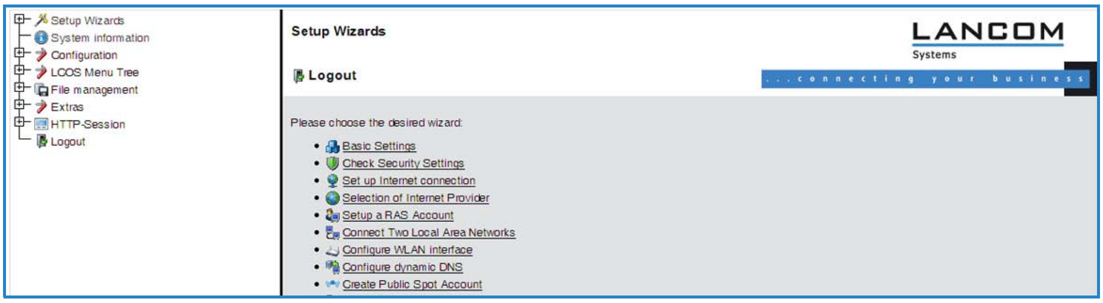
Ok

Caution! Your are using an unencrypted connection. The password will be transmitted as plain text.

Encrypted connection.

Setup Wizards

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



Setup Wizards

Logout

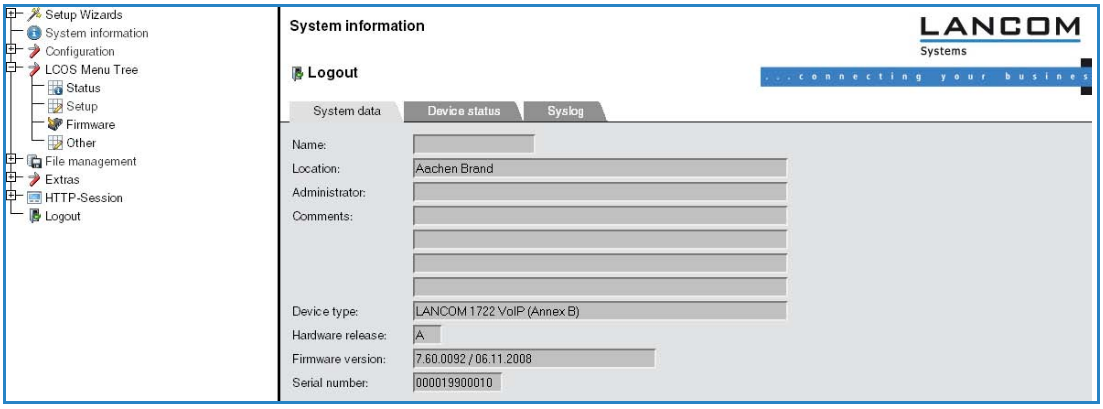
Please choose the desired wizard:

- Basic Settings
- Check Security Settings
- Set up Internet connection
- Selection of Internet Provider
- Setup a RAS Account
- Connect Two Local Area Networks
- Configure WLAN interface
- Configure dynamic DNS
- Create Public Spot Account

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

System information

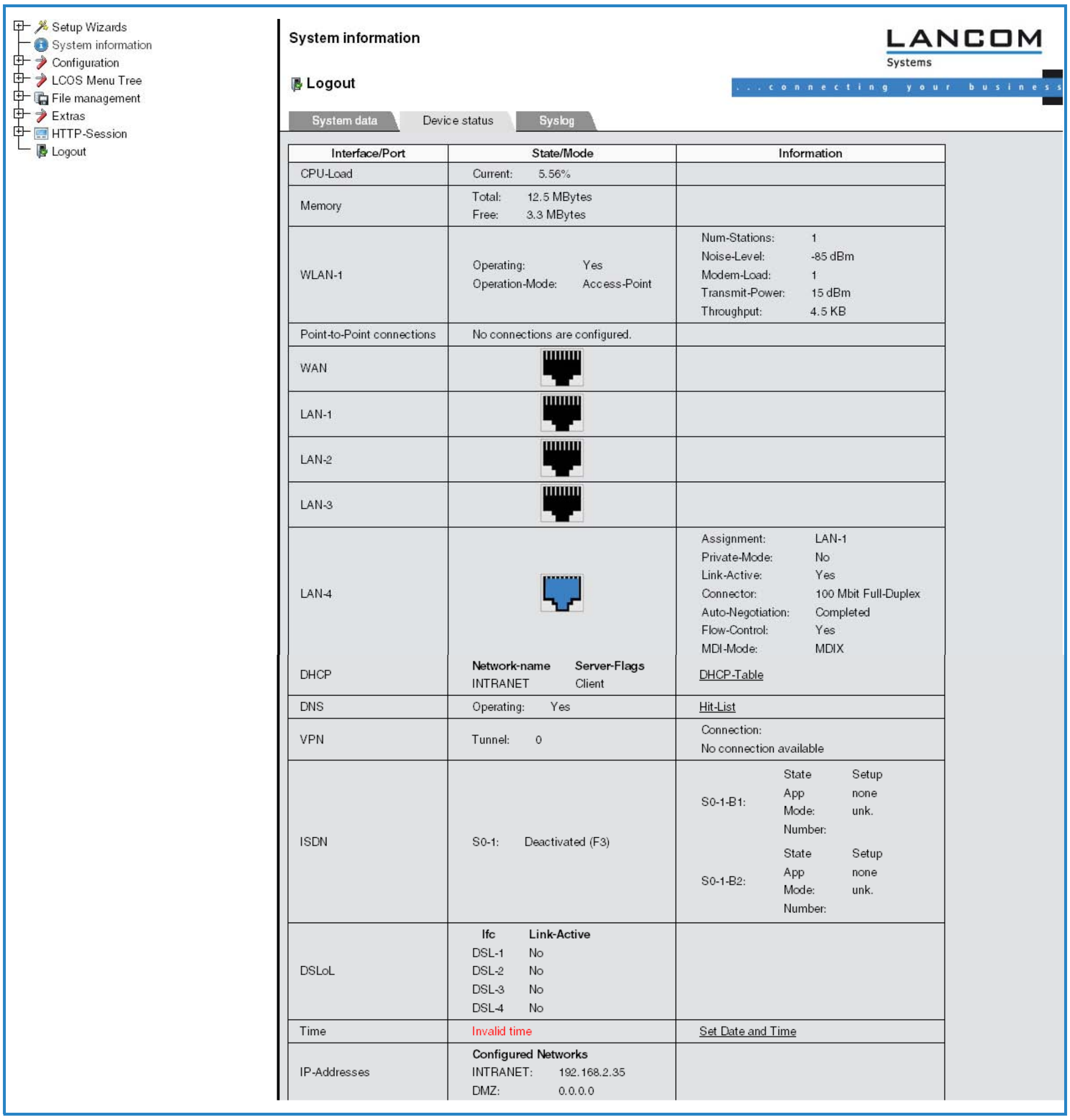
Under the "System Data" tab on the system information screen displays general information on the device including its location, the firmware version, the serial number, etc.



System information

Name:	
Location:	Aachen Brand
Administrator:	
Comments:	
Device type:	LANCOM 1722 VoIP (Annex B)
Hardware release:	A
Firmware version:	7.60.0092 / 06.11.2008
Serial number:	000019900010

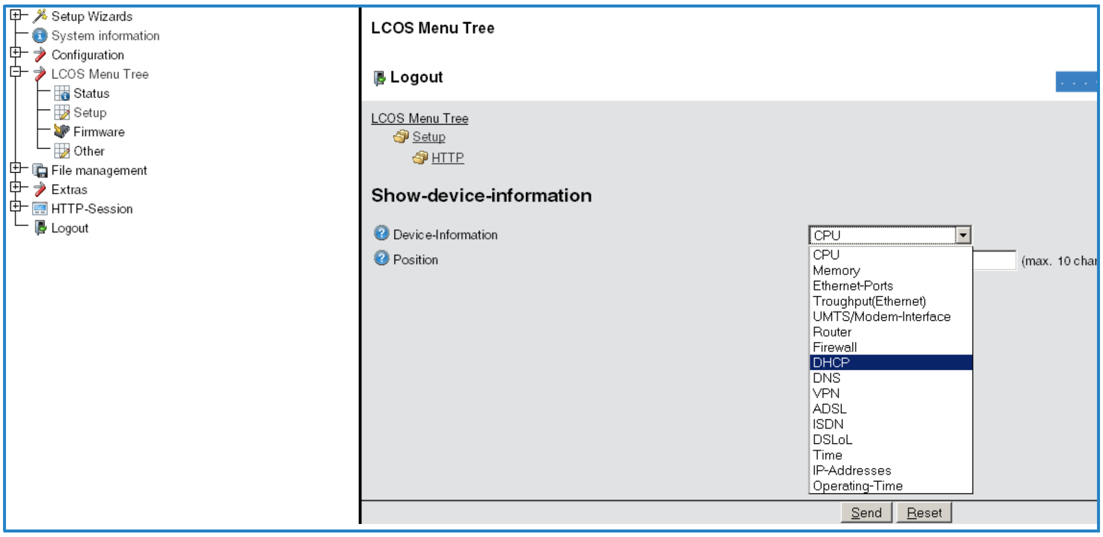
The "Device status" tab contains comprehensive information on the current operating state of the device. This includes, for example, a visual representation of the interfaces with information on the networks active on them. Appropriate links can be used to call up further relevant statistics (such as DHCP table). For significant configuration deficiencies (such as invalid time setting), a direct link to the appropriate configuration parameters is provided.



System information

Interface/Port	State/Mode	Information
CPU-Load	Current: 5.56%	
Memory	Total: 12.5 MBytes Free: 3.3 MBytes	
WLAN-1	Operating: Yes Operation-Mode: Access-Point	Num-Stations: 1 Noise-Level: -85 dBm Modem-Load: 1 Transmit-Power: 15 dBm Throughput: 4.5 KB
Point-to-Point connections	No connections are configured.	
WAN		
LAN-1		
LAN-2		
LAN-3		
LAN-4		Assignment: LAN-1 Private-Mode: No Link-Active: Yes Connector: 100 Mbit Full-Duplex Auto-Negotiation: Completed Flow-Control: Yes MDI-Mode: MDIX
DHCP	Network-name Server-Flags INTRANET Client	DHCP-Table
DNS	Operating: Yes	Hit-List
VPN	Tunnel: 0	Connection: No connection available
ISDN	S0-1: Deactivated (F3)	S0-1-B1: State Setup App none Mode: unk. Number: S0-1-B2: State Setup App none Mode: unk. Number:
DSLoL	Ifc Link-Active DSL-1 No DSL-2 No DSL-3 No DSL-4 No	
Time	Invalid time	Set Date and Time
IP-Addresses	Configured Networks INTRANET: 192.168.2.35 DMZ: 0.0.0.0	

The amount of information shown on this screen can be defined under Setup/HTTP/Show device information. An index number is also used to specify the display sequence.



LCOS Menu Tree

Logout

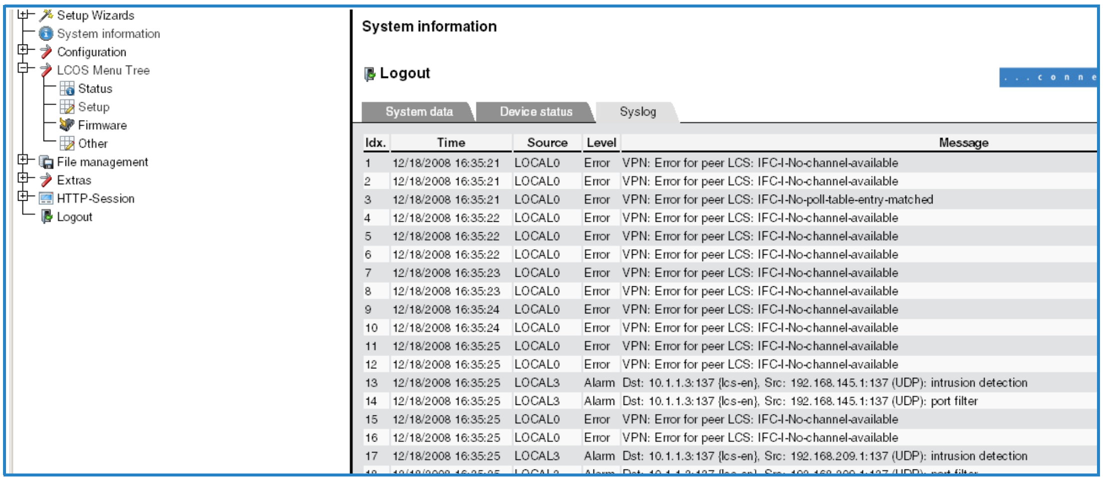
LCOS Menu Tree
Setup
HTTP

Show-device-information

Device-Information: CPU

Position (max. 10 char

LANCOM devices also store syslog information to the main memory (see Syslog). You can also view the latest syslog entries in WEBconfig under "System information".



System information

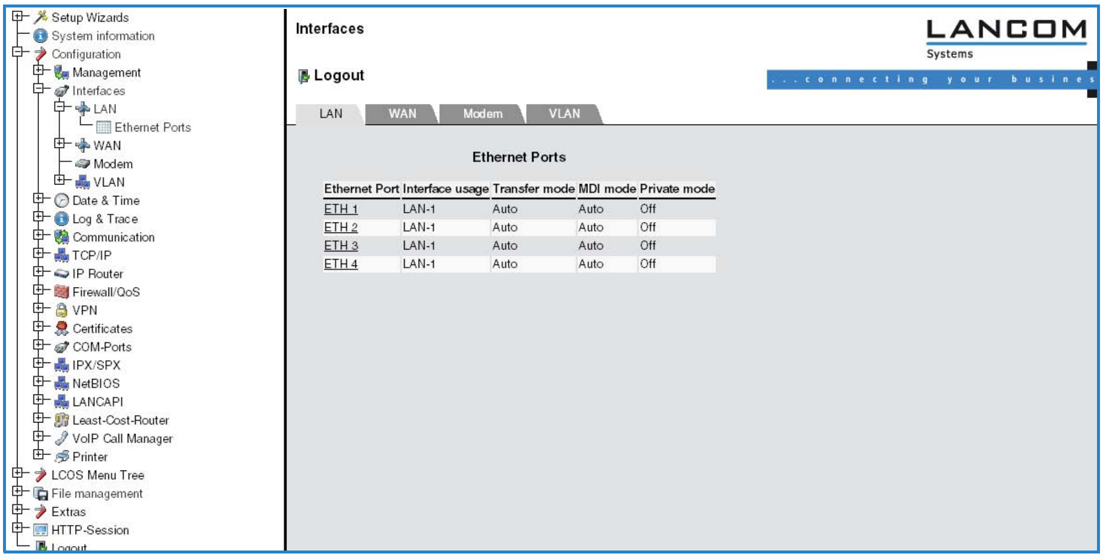
Logout

Idx.	Time	Source	Level	Message
1	12/18/2008 16:35:21	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-channel-available
2	12/18/2008 16:35:21	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-channel-available
3	12/18/2008 16:35:21	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-poll-table-entry-matched
4	12/18/2008 16:35:22	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-channel-available
5	12/18/2008 16:35:22	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-channel-available
6	12/18/2008 16:35:22	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-channel-available
7	12/18/2008 16:35:23	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-channel-available
8	12/18/2008 16:35:23	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-channel-available
9	12/18/2008 16:35:24	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-channel-available
10	12/18/2008 16:35:24	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-channel-available
11	12/18/2008 16:35:25	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-channel-available
12	12/18/2008 16:35:25	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-channel-available
13	12/18/2008 16:35:25	LOCAL3	Alarm	Dst: 10.1.1.3:137 {lcs-en}, Src: 192.168.145.1:137 (UDP): intrusion detection
14	12/18/2008 16:35:25	LOCAL3	Alarm	Dst: 10.1.1.3:137 {lcs-en}, Src: 192.168.145.1:137 (UDP): port filter
15	12/18/2008 16:35:25	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-channel-available
16	12/18/2008 16:35:25	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-channel-available
17	12/18/2008 16:35:25	LOCAL3	Alarm	Dst: 10.1.1.3:137 {lcs-en}, Src: 192.168.209.1:137 (UDP): intrusion detection

Configuration

Menu area “Configuration” provides the configuration parameters in the same structure as they are used in LANconfig.

Please note that not all settings can be configured from this configuration view.



Interfaces

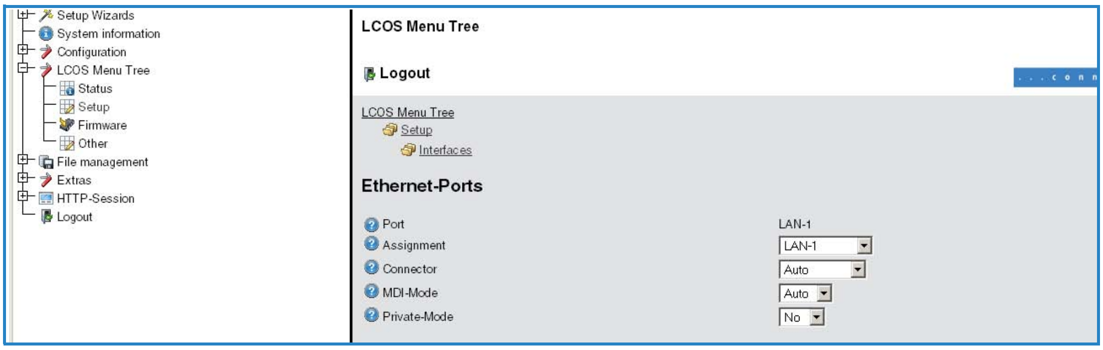
Logout

Ethernet Ports

Ethernet Port	Interface usage	Transfer mode	MDI mode	Private mode
ETH 1	LAN-1	Auto	Auto	Off
ETH 2	LAN-1	Auto	Auto	Off
ETH 3	LAN-1	Auto	Auto	Off
ETH 4	LAN-1	Auto	Auto	Off

LCOS menu tree

Menu area “LCOS menu tree” provides the configuration parameters in the same structure as they are used under Telnet. Clicking the question mark calls up help for each configuration parameter.



LCOS Menu Tree

LCOS Menu Tree
Setup
Interfaces

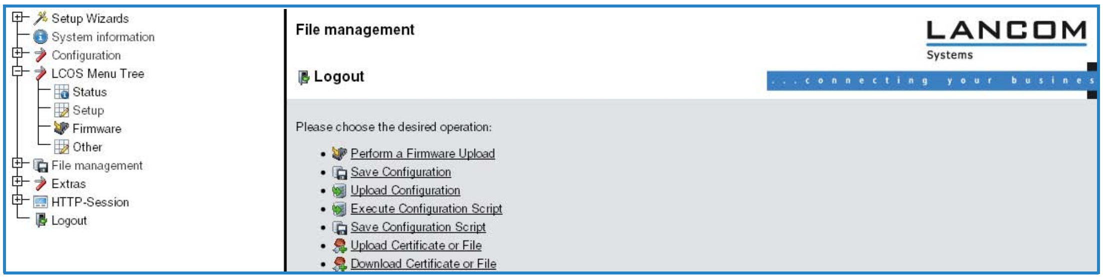
Ethernet-Ports

Port	LAN-1
Assignment	LAN-1
Connector	Auto
MDI-Mode	Auto
Private-Mode	No

File management

The menu area “File management” contains all actions with which files are downloaded from the device and uploaded to the device:

- Uploading new firmware
- Saving configuration
- Uploading configuration
- Using configuration script
- Saving configuration script
- Uploading certificate or file
- Downloading certificate or file



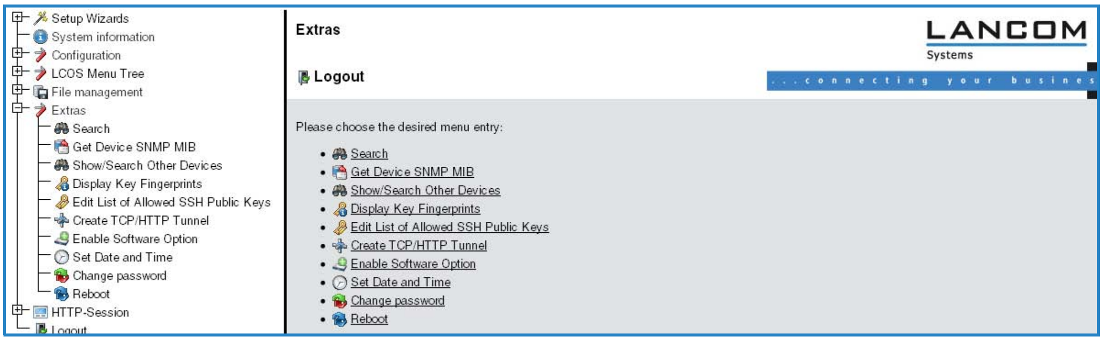
File management

Please choose the desired operation:

- Perform a Firmware Upload
- Save Configuration
- Upload Configuration
- Execute Configuration Script
- Save Configuration Script
- Upload Certificate or File
- Download Certificate or File

Extras

The menu area "Extras" contains a few functions that simplify device configuration.

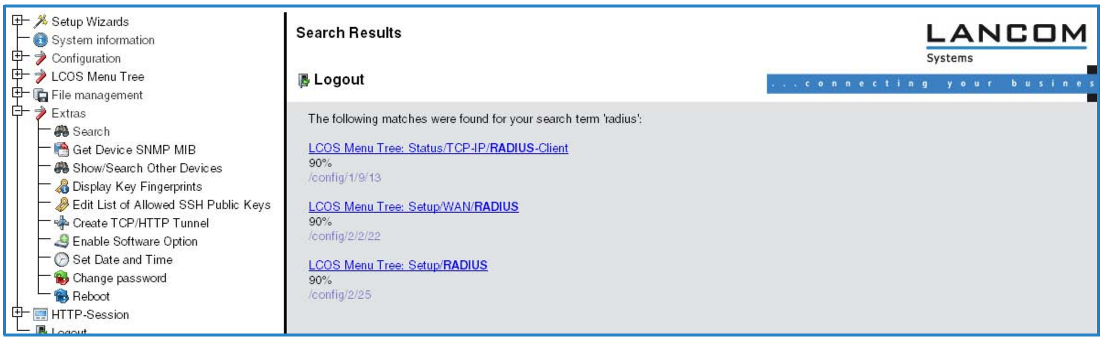


Extras

Please choose the desired menu entry:

- Search
- Get Device SNMP MIB
- Show/Search Other Devices
- Display Key Fingerprints
- Edit List of Allowed SSH Public Keys
- Create TCP/HTTP Tunnel
- Enable Software Option
- Set Date and Time
- Change password
- Reboot

The search function can be used, for example, to search the names for all configuration parameters. If you know the name for a particular configuration parameter, but do not know which menu is used to reach this entry, you can quickly locate the required place in the LCOS menu in this way.



Search Results

Logout

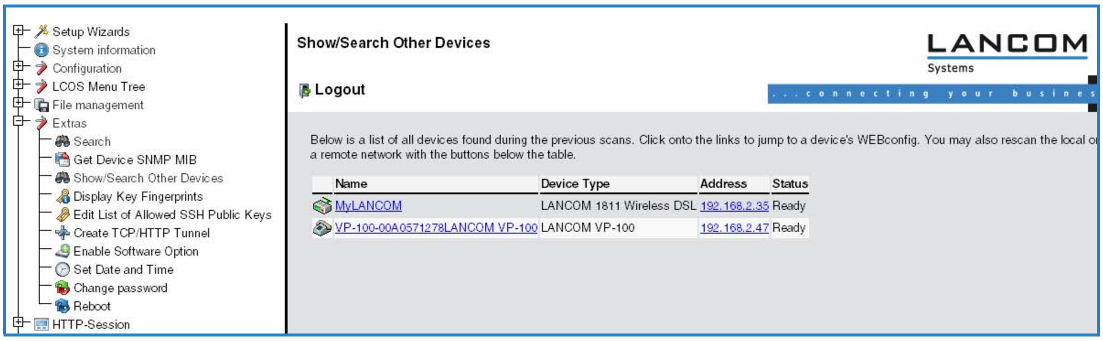
The following matches were found for your search term 'radius':

LCOS Menu Tree: Status/TCP-IP/RADIUS-Client
90%
/config/1/9/13

LCOS Menu Tree: Setup/WAN/RADIUS
90%
/config/2/2/22

LCOS Menu Tree: Setup/RADIUS
90%
/config/2/25

Using the Show/Search function, you can search for other LANCOM devices in your network and switch directly to the configuration of the devices located via a corresponding link.



Show/Search Other Devices

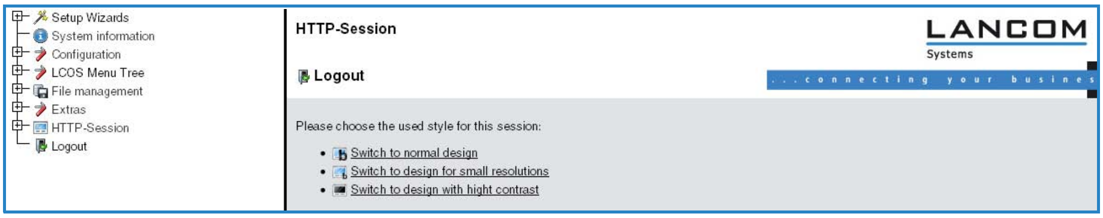
Logout

Below is a list of all devices found during the previous scans. Click onto the links to jump to a device's WEBconfig. You may also rescan the local o
a remote network with the buttons below the table.

Name	Device Type	Address	Status
MyLANCOM	LANCOM 1811 Wireless DSL	192.168.2.35	Ready
VP-100-00A0571278LANCOM VP-100	LANCOM VP-100	192.168.2.47	Ready

HTTP session

Menu area “HTTP session” allows you to customize the display of the WEBconfig interface to your output device for improved readability, e. g. by lowering the resolution or increasing the contrast.



HTTP-Session

Logout

Please choose the used style for this session:

- Switch to normal design
- Switch to design for small resolutions
- Switch to design with hight contrast

3.9 Configuration with other tools

3.9.1 Telnet

New with LCOS 7.6:

- Extended functions for editing commands
- Function keys

Open Telnet session

To commence the configuration, start Telnet from the Windows command line with command:

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

Telnet establishes a connection to the device with the IP address entered.

After entering the password (assuming one has been set to protect the configuration) all of the configuration commands are available to you.

Linux and Unix additionally support Telnet sessions via SSL-encrypted connections. Depending on the distribution it may be necessary to replace the standard Telnet application with an SSL-capable version. Start the encrypted Telnet connection with the following command:

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

Changing the console language

The terminal mode operates with the languages English and German. LANCOM devices are set with English as the standard console language. If necessary, change the console language with the following commands:

WEBconfig: LCOS menu tree ▶ Config-Module ▶ Language

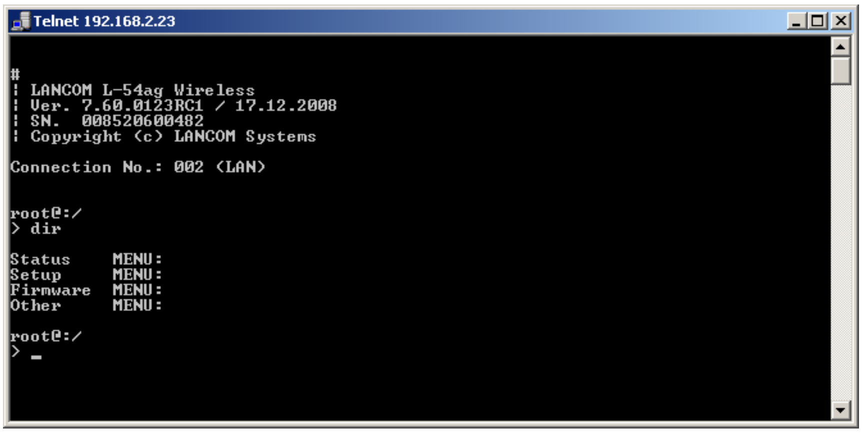
Close the Telnet session

To close the Telnet session, enter the command `exit` at the command prompt:

```
C:\>exit
```

Structure of the command-line interface

The LANCOM command-line interface is always structured as follows:



```
#
| LANCOM L-54ag Wireless
| Ver. 7.60.0123RC1 / 17.12.2008
| SN.  008520600482
| Copyright (c) LANCOM Systems

Connection No.: 002 (LAN)

root@:/
> dir

Status     MENU:
Setup      MENU:
Firmware   MENU:
Other      MENU:

root@:/
> _
```

- **Status**
  Contains the status and statistics of all internal modules in the device
- **Setup**
  Contains all adjustable parameters of all internal modules in the device
- **Firmware**
  Contains the firmware management
- **Others**
  Contains actions for establishing and terminating connections, reset, reboot and upload.

Command-line commands

The LANCOM command-line interface can be operated with the following DOS- or UNIX-style commands. The LCOS menu commands that are available to you can be displayed at any time by entering HELP at the command line.

ⓘ Supervisor rights are necessary to execute some commands.

Command	Description
beginscript	Resets the console session to script mode. In this state, commands entered are not transferred directly to the LANCOM's configuration RAM but initially to the device's script memory.
cd [PATH]	Switch to the current directory. Various abbreviations can be used, such as replacing " cd ../.." with "cd ...", etc.
del [PATH]*	Deletes the table in the branch of the menu tree defined with `Path`.
default [-r] [PATH]	Resets individual parameters, tables or entire menu trees back to their default configuration. If `PATH` indicates a branch of the menu tree, then the option `-r` (recursive) must be entered.
dir [PATH] list [PATH] ls [PATH] ll [PATH]	Displays the current directory content. The suffix parameter "-a" lists the SNMP IDs associated with the content of the query. The output begins with the SNMP ID of the device followed by the SNMP ID of the current menu. The SNMP IDs of the subordinate items can be read from the individual entries.
do [PATH] [<Parameter>]	Executes the action [PATH] in the current directory. Other parameters can be entered in addition.
echo <ARG>...	Display argument on console
exit/quit/x	Ends the command line session
feature <code>	Activation of a software feature with the feature code as entered
flash Yes/No	Changes to the configuration using commands in the command line are written directly to the boot-resistant Flash memory of the devices as standard (flash yes). If updating the configuration is suppressed in Flash (flash no), changes are only stored in RAM (deleted on booting).
history	Displays a list of recently executed commands. Command "!#" can be used to directly call the list commands using their number (#): For example, "!3" runs the third list command.

Command	Description
killscript	Deletes the script session contents yet to be processed. The script session is selected by its name.
loadconfig	Load configuration into device via TFTP client
loadfirmware	Load firmware into device via TFTP client
loadscript	Load script into device via TFTP client
passwd	Change password
passwd -n new [old]	Change password (no prompt)
ping [IP address or name]	Sends an ICMP echo request to the IP address specified
readconfig	Display of the entire configuration in the device syntax
readmib	Display of the SNMP Management Information Base
readscript [-n] [-d] [-c] [-m] [PATH]	In a console session, the readscript command generates a text dump of all commands and parameters required to configure the LANCOM in its current state.
repeat <INTERVAL> <Command>	Repeats the command every INTERVAL seconds until the process is ended with new input
sleep [-u] value[suffix]	Delays the processing of configuration commands by a particular time or terminates them at a particular time. Permissible suffixes are `s`, `m` and `h` for seconds, minutes and hours. If no suffix is defined, the command uses milliseconds. With option switch `-u`, the sleep command accepts times in format `MM/DD/YYYY hh:mm:ss` (English) or in format `TT.MM.JJJJ hh:mm:ss` (German). Date configuration is only accepted if the system time is set.
stop	Ends the PING command
set [PATH] <value(s)>	Sets a configuration parameter to a particular value. If the configuration parameter is a table value, a value must be specified for each column. Entering the "*" character leaves any existing table entry unchanged.
set [PATH] ?	Listing of the possible input values for a configuration parameter. If no name is specified, the possible input values for all configuration parameters in the current directory are specified.
setenv <NAME> <VALUE>	Set environment variable
unsetenv <NAME>	Delete environment variable
getenv <NAME>	Display environment variable (no line feed)
printenv	Display the entire environment
show <options>	Display of special internal data. show ? displays all available information, such as most recent boot processes ('bootlog'), firewall filter rules ('filter'), VPN rules ('VPN') and memory usage ('mem' and 'heap')
sysinfo	Display of system information (e.g. hardware/software version)
testmail	Sends an e-mail. See 'testmail ?' for parameters
time	Set time (DD.MM.YYYY hh:mm:ss)
trace [...]	Configuration of the diagnostics display.
who	List active sessions
writeconfig	Load a new configuration file in the device syntax. All subsequent lines are interpreted as configuration values until two blank lines occur
writeflash	Load a new firmware file (only via TFTP)
!!	Repeat last command
!<num>	Repeat command <num> times
!<prefix>	Repeat last command beginning with <prefix>
#<blank>	Comment

- PATH:
  - Path name for a menu or parameter, separated by / or \
  - .. means one level higher
  - . means the current level
- VALUE:
  - Possible input value
  - "" is a blank input value
- NAME:
  - Sequence of characters (made up of _ 0..9 A..Z)
  - First character cannot be a digit
  - Case insensitive

- All commands and directory/parameter names can be entered using their short-forms as long as they are unambiguous. For example, command "`sysinfo`" can be shortened to "`sys`" and "`cd Management`" to "`c ma`". Input "`cd /s`" is not valid, however, since it corresponds to both "`cd /Setup`" and "`cd /Status`".
- Names that contain spaces must be enclosed within quotation marks ("").
- A command-specific help function is available for actions and commands (call the function with a question mark as the parameter). For example, '`ping ?`' shows the options of the integrated ping command.
- Enter '`?`' on the command line for a complete listing of the console commands available.

Functions for editing commands

The following commands can be used to edit commands on the command line. The "ESC key sequences" show (for comparison) the shortcuts used on typical VT100/ANSI terminals

Function	Esc key sequences	Description
Up arrow	ESC [A	In the list of commands last run, jumps one position up (in the direction of older commands).
Down arrow	ESC [B	In the list of commands last run, jumps one position down (in the direction of newer commands).
Right arrow	Ctrl-F ESC [C	Moves the insert cursor one position to the right.
Left arrow	Ctrl-B ESC [D	Moves the insert cursor one position to the left.
Home or Pos1	Ctrl-A ESC [A ESC [1˜ (	Moves the insert cursor to the first character in the line.
End	Ctrl-E ESC [F ESC OF ESC [4˜	Moves the insert cursor to the last character in the line.
Ins	ESC [ESC [2˜	Switches between input and overwrite modes.
Del	Ctrl-D ESC <BS>ESC [3˜	Deletes the character at the current position of the insert cursor or ends the Telnet session if the line is blank.
erase	<BS><DEL>	Deletes the next character to the left of the insert cursor.
erase-bol	Ctrl-U	Deletes all characters to the left of the insert cursor.
erase-eol	Ctrl-K	Deletes all characters to the right of the insert cursor.
Tabulator		Completes the input from the current position of the insert cursor for a command or path of the LCOS menu structure: ■ If there is only one possibility of completing the command/path, this is accepted by the line. ■ If there is more than one possibility of completing the command/path, this is indicated by an audible sound when pressing the Tab key. Pressing the Tab key again displays a list of all possibilities to complete the entry. Then enter another character, for example, to allow unambiguous completion of the input. ■ If there is no possibility of completing the command/path, this is indicated by an audible sound when pressing the Tab key. No further actions are run.

Function keys for the command line

- Telnet: Setup ▶ Config ▶ Function keys

The function keys enable the user to save frequently used command sequences and to call them easily from the command line. In the appropriate table, commands are assigned to function keys F1 to F12 as they are entered in the command line.

- **Key**

  Name of function key.

  Possible values:

  □ Selection from function keys F1 to F12.

  Default:

  □ F1

- **Mapping**

  Description of the command/shortcut to be run on calling the function key in the command line.

  Possible values:

  □ All commands/shortcuts possible in the command line

  Default:

  □ Blank

  Special values:

- □ The caret symbol ^ is used to represent special control commands with ASCII values below 32.^a
- □ ^A stands for Ctrl-A (ASCII 1)
- □ ^Z stands for Ctrl-Z (ASCII 26)
- □ ^[stands for Escape (ASCII 27)
- □ ^^ A double caret symbol stands for the caret symbol itself.

If a caret symbol is entered in a dialog field or editor followed directly by another character, the operating system may possibly interpret this sequence as another special character. A Windows operating system makes, for example, an Â from input caret symbol + A. To call the caret symbol itself, enter a space before the following character. Sequence ^A is then formed from caret symbol + space + A.

3.9.2 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.

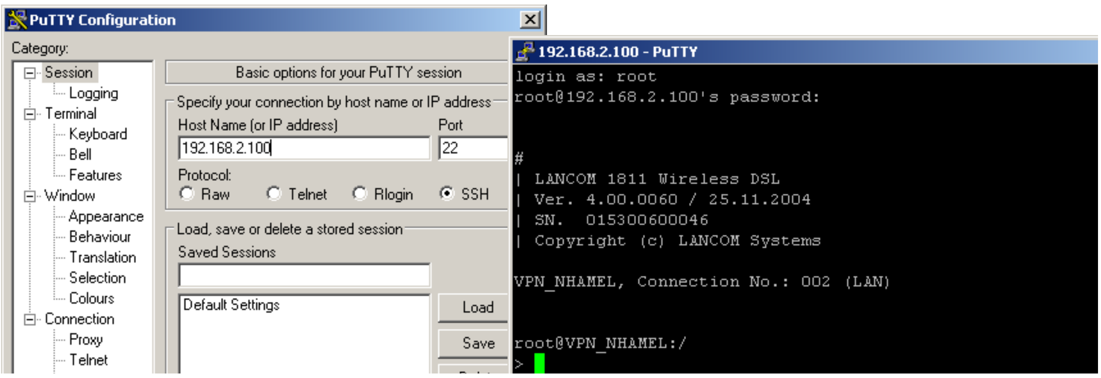
Your LANCOM can export a so-called device MIB file (**M**anagement **I**nformation **B**ase) for use in SNMP programs.

WEBconfig: Extras ▶Get Device SNMP MIB

3.9.3 Encrypted configuration with SSH access

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

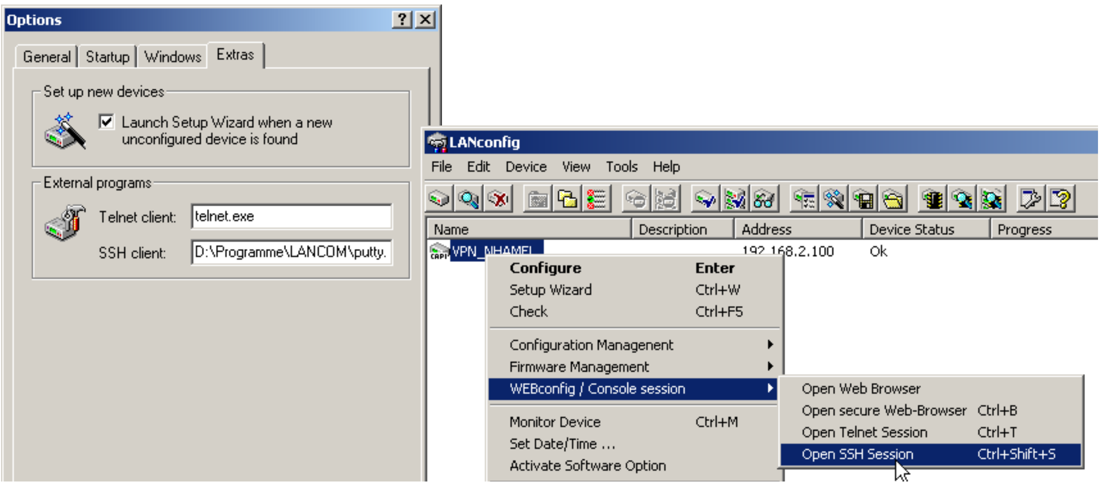
Start PuTTy (for example) and enter the LANCOM device's IP address as the host name. Use the command prompt that follows to log in by entering your user data.



Host Name (or IP address): 192.168.2.100
Port: 22
Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

```
login as: root
root@192.168.2.100's password:


#
| LANCOM 1811 Wireless DSL
| Ver. 4.00.0060 / 25.11.2004
| SN.  015300600046
| Copyright (c) LANCOM Systems

VPN_NHAMEL, Connection No.: 002 (LAN)


root@VPN_NHAMEL:/
>
```

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



☑ Launch Setup Wizard when a new unconfigured device is found

Telnet client: telnet.exe

SSH client: D:\Programme\LANCOM\putty.

The configuration is carried out with the same commands as used under Telnet or other terminal program ('Command-line commands' → page 3-34).

3.9.4 SSH authentication

The SSH protocol generally allows two different authentication mechanisms:

- With user name and password
- With the help of a public key

In the public key method, a key pair is used that is made up of a private and public key – a digital certificate. Detailed information about the keys mentioned here can be found under the section 'Digital certificates' in the chapter on VPN in the reference manual. The private part of the key pair is saved on the client (frequently protected with a password), the public part is loaded into the LANCOM Router.

The LANCOM Router supports both RSA and DSS/DSA keys. RSA keys are somewhat smaller, thereby allowing somewhat faster operation.

Generating key pairs

The pairs consisting of public and private keys can be generated with the help of OpenSource software OpenSSH, for example. The following command from a Linux operating system creates a key pair from the public part '`id_rsa.pub`' and the private part '`id_rsa`':

```
ssh-keygen -t rsa
```

Entering users into the public key

The public keys are generated in the following syntax:

```
<Encryption algorithm> <Public key> <User> [Further users]
```

In order to grant access to additional users with this key, the respective user names are simply attached to the existing key file.

Installing the private key on the SSH client

The private part of the key must be installed on the SSH client. Refer to the documentation for information on the steps required for your SSH client.

Load public key into the LANCOM Router

The public key(s) can be uploaded to the LANCOM Router using WEBconfig. For this, select the entry **Upload certificate or file** on the WEBconfig start page. In the following dialog, select the type of key ('SSH RSA key' or 'SSH DSA key'), select the file and enter the password if required. Entering the Upload command initiates the transfer to LANCOM.

! The uploaded file replaces an existing list of accepted keys in the device. Another way is to choose the entry **edit list of allowed puplic keys** at the start page og WEBconfig and edit the key directly. You can as well edit single keys to the existing list.

Configuring the authentication methods

The authentication methods permitted for SSH access can be set separately for LAN, WAN and WLAN.

Configuration tool	Call
WEBconfig, Telnet	LCOS menu tree > Setup > Config > SSH authentication methods

- **Methods**
  - □ All: Allows authentication using password and digital certificate.
  - □ Password: Allows authentication with a password.
  - □ Public key: Only allows authentication with a digital certificate.

Certificate check on SSH access

When establishing the SSH connection, the client first asks the LANCOM Router which authentication methods are permitted for this connection. If the public key method is allowed, the client searches for private keys that have been installed and transfers these with the user name to the LANCOM Router. When the LANCOM Router finds an entry in the list that includes the user name that corresponds to its public SSH key, the SSH connection is permitted. If the client does not have a suitable private key installed or if the LANCOM Router does not have a corresponding entry with the user name or public key, the SSH client can revert to authentication with user name/password – as long as this authentication method is permitted.

3.9.5 ISDN Remote configuration via Dial-Up Network

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

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

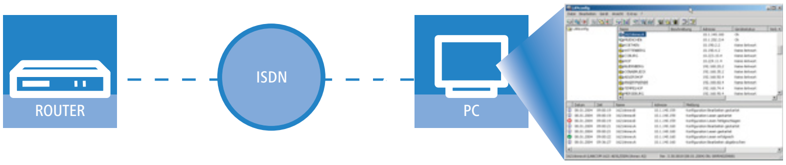
You can also reserve a special calling number for remote configuration. Then the support technician can always access the router even if it is really no longer accessible due to incorrect settings.

This is what you need for ISDN remote configuration

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

The first remote connection using Dial-Up Networking

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



LANCOM
with ISDN-interface
for the configuration

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

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

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

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

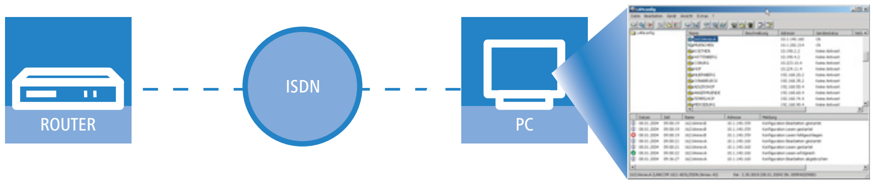
When an entry in the device list is deleted, the related connection in the Windows Dial-Up Network is also deleted.

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

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

The first remote connection using a PPP client and Telnet

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



LANCOM
with ISDN-interface
for the configuration

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

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

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

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

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

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

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

```
passwd
```

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

The default layer for remote field installations

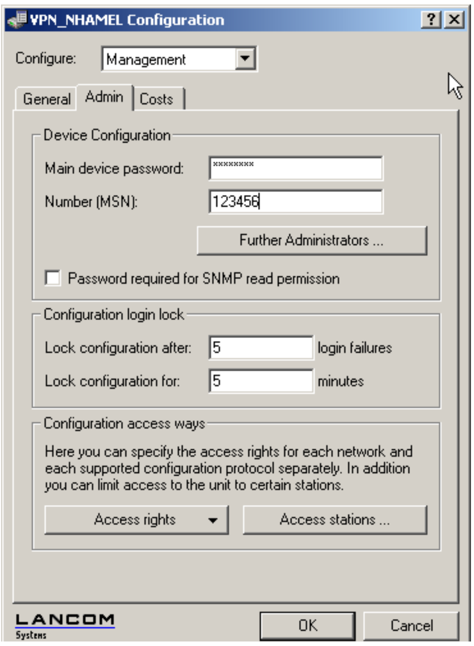
The PPP connection of any other remote site to the router, of course, will only succeed if the device answers every call with the corresponding PPP settings. This is the case using the factory default settings because the default protocol (default layer) is set to PPP.

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

The administrator access for ISDN remote management

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

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



VPN_NHAMEL Configuration

Configure: Management

General | Admin | Costs

Device Configuration

Main device password: ********

Number (MSN): 123456

Further Administrators ...

□ Password required for SNMP read permission

Configuration login lock

Lock configuration after: 5 login failures

Lock configuration for: 5 minutes

Configuration access ways

Here you can specify the access rights for each network and each supported configuration protocol separately. In addition you can limit access to the unit to certain stations.

Access rights | Access stations ...

OK | Cancel

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

Alternatively, enter the following command:

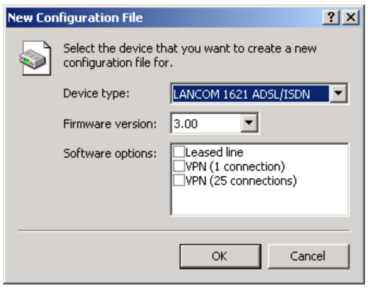
```
set /setup/config/Farconfig 123456
```

As long as no MSN is entered for the configuration access, a non-configured LANCOM accepts the calls on all MSNs. As soon as the first change is saved in the configuration, the device only takes calls on the configured MSN!
If no MSN configuration is entered the remote access is switched off and the device is protected against access over ISDN.

3.10 Working with configuration files

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

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



New Configuration File

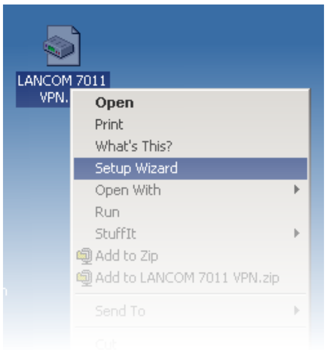
Select the device that you want to create a new configuration file for.

Device type: LANCOM 1621 ADSL/ISDN

Firmware version: 3.00

Software options: □ Leased line □ VPN (1 connection) □ VPN (25 connections)

OK | Cancel



Backup copies of configuration

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

Convenient series configuration

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

Running function

LANconfig:

Device ▶ Configuration Management ▶ Save to File
Device ▶ Configuration Management ▶ Restore from File
Edit ▶ New Configuration File
Edit ▶ Edit Configuration File
Device ▶ Configuration Management ▶ Print ...

WEBconfig: Save Configuration ▶ Load Configuration (in main menu)

3.11 New firmware with FirmSafe

New with LCOS 7.60:

- Asymmetric firmsafe

3.11.1 This is how FirmSafe works

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

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

- 'Immediate': The first option is to load the new firmware and activate it immediately. The following situations can result:
  - The new firmware is loaded successfully and works as desired. Then all is well.
  - The device no longer responds after loading the new firmware. If an error occurs during the upload, the device automatically reactivates the previous firmware version and reboots the device.
- 'Login': To avoid problems with faulty uploads there is the second option with which the firmware is uploaded and also immediately booted.
  - In contrast to the first option, the device will wait for the adjusted firmsafe timeout (using WEBconfig in the menu **LCOS menu tree ▶ Firmware ▶ Timeout-firmsafe**, using Telnet adjust with 'Firmware/Timeout-firmsafe') until it is logged on over Telnet, a terminal program or WEBconfig. Only if this login attempt is successful does the new firmware remain active permanently.
  - If the device no longer responds or it is impossible to log in, it automatically loads the previous firmware version and reboots the device with it.
- 'Manual': With the third option you can define a time period during which you want to test the new firmware yourself. The device will start with the new firmware and wait for the preset period until the loaded firmware is manually activated and therefore becomes permanently effective. Activate the new firmware using LANconfig with **Device ▶ Firmware Management ▶ Activate Firmware running in Test Mode**, using Telnet under 'firmware/ firmsafe table' with the command 'set # active' (# is the position of the firmware in the firmsafe table). Using WEBconfig you can find the firmsafe table under **LCOS menu tree▶ Firmware**.

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

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

3.11.2 Asymmetric Firmsafe

Because of large range of functions in the firmware, some models are unable to simultaneously store two complete versions of the firmware. These devices use the asymmetric Firmsafe. Here, the device always contains a complete version and a minimal version of the firmware. The minimal version normally remains unused, but it allows local access to the device after a failed upload of the complete firmware version (e.g. as a result of a power cut during the upload process) so as to load an executable version of the firmware onto the device. The minimal firmware can not be configurated. Changes in the configuration over LANconfig, WEBconfig or Telnet are not saved in the device

Advanced functions, such as remote administration, are not available whilst the minimal firmware is active. However, the LL2M server is also active in a minimal firmware version and offers access to the device provided it is reachable from an LL2M client over layer 2 (Ethernet).

Switching over to asymmetric Firmsafe

To switch devices to asymmetric Firmsafe, converter firmware is first loaded onto the device. This converts the firmware currently **not activated** in the device into a minimal firmware version, creating room for new and more comprehensive firmware. This process only has to be performed once.

You can then load a new, complete firmware version onto the device, which becomes active after a successful upload. The minimal firmware remains in the device to ensure that the device can be accessed.

Firmware upgrade with asymmetric Firmsafe

The subsequent firmware upload automatically overwrites the **active** firmware with new firmware.

3.11.3 How to load new software

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

- LANconfig
- WEBconfig
- Terminal program
- TFTP

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

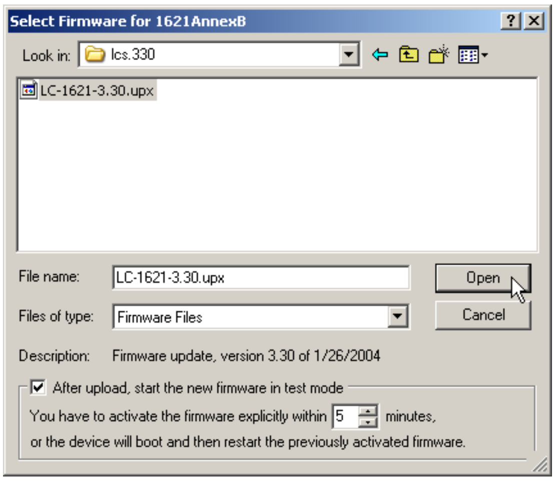
If the newly installed release contains parameters which are not present in the device's current firmware, the device will add the missing values using the default settings.

LANconfig

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

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

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



Look in: lcs.330

LC-1621-3.30.upx

File name: LC-1621-3.30.upx

Files of type: Firmware Files

Description: Firmware update, version 3.30 of 1/26/2004

☑ After upload, start the new firmware in test mode

You have to activate the firmware explicitly within 5 minutes,
or the device will boot and then restart the previously activated firmware.

WEBconfig

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

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

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

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

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

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

TFTP

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

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

Firmware upload via the serial interface with configuration reset

The serial interface can also be used to load firmware into the device. Entering the serial number instead of the configuration password results in the device configuration being reset to its ex-factory settings. In this way you can re-open the device in the case that the configuration password is lost and the reset button has been set to 'Ignore' or 'Boot only'.

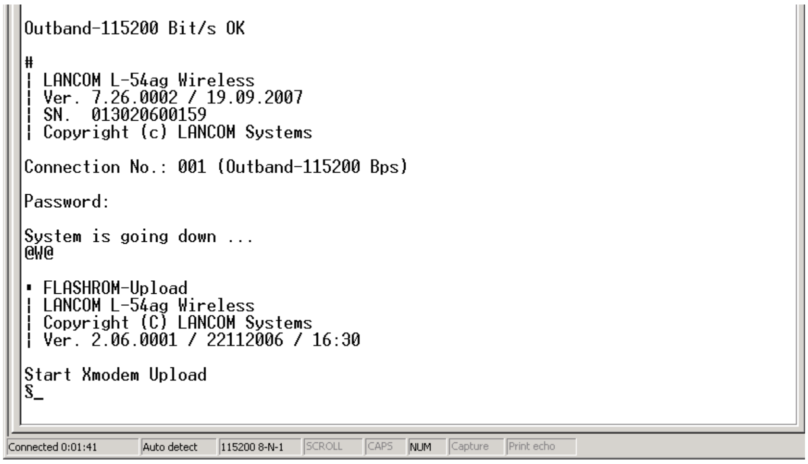
① Use the serial configuration cable to connect the device to a computer.

② On the computer, start a terminal program such as Hyperterminal.

③ Open a connection with the settings 115200bps, 8n1, hardware handshake (RTS/CTS).

④ In the terminal program's welcome screen, press the Return key until the request to enter the password appears.

⑤ Enter the serial number that is displayed under the firmware version and press Return again.



```
Outband-115200 Bit/s OK

#
¦ LANCOM L-54ag Wireless
¦ Ver. 7.26.0002 / 19.09.2007
¦ SN.  013020600159
¦ Copyright (c) LANCOM Systems

Connection No.: 001 (Outband-115200 Bps)

Password:

System is going down ...
@W@

▪ FLASHROM-Upload
¦ LANCOM L-54ag Wireless
¦ Copyright (C) LANCOM Systems
¦ Ver. 2.06.0001 / 22112006 / 16:30

Start Xmodem Upload
§_
```

⑥ The device now expects a firmware upload. To initiate this, in Hyperterminal you click on **Transfer** ▶ **Send** file and select X-Modem as the transfer protocol.

Uploading the firmware in this way completely deletes the configuration, which is returned to its ex-factory settings! Consequently, this option should only be used if the configuration password is no longer available.

3.12 Load files directly from a TFTP or HTTP server into the device

New in LCOS 7.60:

- Specification of server, path and file in URL notation
- Loading files into the device from an HTTP(S) server

Certain functions cannot be run satisfactorily, or not at all, via Telnet. These functions include those where entire files are transferred, such as the upload of firmware, and saving or restoring configuration data. TFTP or HTTP(S) is used in these cases.

3.12.1 TFTP

TFTP is available in Windows operating systems as standard. It enables the simple transfer of files to/from other devices over the network.

The syntax of the TFTP call is dependent on the operating system. The syntax under Windows:

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

The ASCII format is pre-configured on many TFTP clients. Binary transmission therefore usually needs to be selected explicitly for the transfer of binary data (suchas firmware). Parameter '-i' is used for this in this example under Windows.

If the device is password-protected, user name and password must be included in the TFTP command. The file name is either made up of the master password and the command to be executed (for supervisors), or of the combined user name and password separated by a colon (for local administrators), with the command as a suffix. A command sent by TFTP therefore resembles the following:

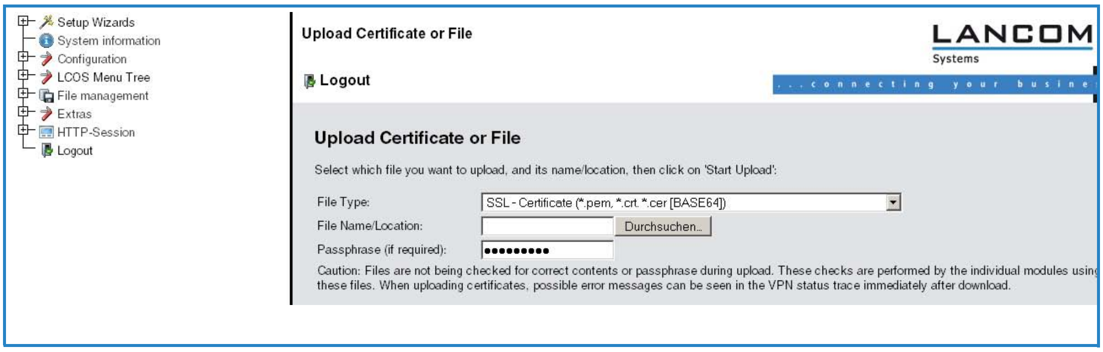
- <Master password><Command> or
- <User name>:<Password>@<Command>

The rights to use TFTP can be restricted for administrators—see also “Managing rights for different administrators”.

3.12.2 Loading firmware, device configuration or script via HTTP(S)

By supporting HTTP and in particular HTTPS, downloads of firmware, device configurations or scripts can also be used by LANCOM devices for automated processes (e.g. self-provisioning) that source files from the Internet. In practice it is far simpler to provide a cental HTTPS server with a unique Internet address (URI) than a comparable TFTP server, and an existing Web server can be modified to offer this function.

A certificate used optionally for the HTTPS server is uploaded by WEBconfig to the device as the SSL root CA certificate:



Upload Certificate or File

Select which file you want to upload, and its name/location, then click on 'Start Upload':

File Type: SSL - Certificate (*.pem, *.crt. *.cer [BASE64])

File Name/Location:

Passphrase (if required): ●●●●●●●●●●

Caution: Files are not being checked for correct contents or passphrase during upload. These checks are performed by the individual modules using these files. When uploading certificates, possible error messages can be seen in the VPN status trace immediately after download.

3.12.3 Loading firmware, device configuration or script via HTTP(S) or TFTP

Along with the option to load firmware or a configuration file into a device using LANconfig or WEBconfig, Telnet and SSH can also be used to directly upload the relevant files from an HTTP(S) or TFTP server. This process can simplify device administration in larger installations with regular firmware update and/or configuration. HTTP(S) and TFTP can also be used to load scripts (e.g. with partial configurations) into devices.

For this, the firmware and configuration files or scripts are stored on an HTTP(S) or TFTP server. A TFTP server is identical to an FTP server in terms of functionality, but uses a different protocol for data transmission. When using an HTTPS server, a certificate used to check the identity of the server can be stored on the device. The files can be retrieved from this server with the following commands:

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

The server, the directory and the file can be specified in two ways:

- By using the TFTP protocol with parameters -s and -f:
  - `-s <Server IP address or server name>`
  - `-f <File path and file name>`
- To use TFTP or HTTP(S), the command can be specified in the usual URL notation (either TFTP or HTTP(S) is entered as the protocol):
  - `Command protocol://server/directory/file name`

  When accessing a password-protected area on an HTTP(S) server, user name and password are entered accordingly:

□ `Command protocol://user name:password@server/directory/file name`

When using HTTPS, a certificate can be specified with which the identity of the server is checked.

□ `-c <Certificate name>`

The following variables are permitted in the file name (including path):

- %m - LAN MAC address (hexadecimal, lowercase, no separators)
- %s - Serial number
- %n - Device name
- %l - Location (from the configuration file)
- %d - Device type

Examples:

The following Telnet command loads a firmware file named 'LC-1811-5.00.0019.upx' into the device from directory 'LCOS/500' on the server with IP address '192.168.2.200':

- `LoadFirmware -s 192.168.2.200 -f LCOS/500/LC-1811-5.00.0019.upx`

The following command in a Telnet session loads a script consistent with the MAC address from the server with IP address '192.168.2.200' into the device:

- `LoadScript -s 192.168.2.200 -f %m.lcs`

The following command in a Telnet session loads into the device a firmware file named 'LC-1811-5.00.0019.upx' from directory 'download' on the HTTPS server with IP address 'www.myserver.com'. The identity of the server is checked with the “sslroot.crt” certificate.

- `LoadFirmware -c sslroot.crt https://www.myserver.com/download/LC-1811-5.00.0019.upx`

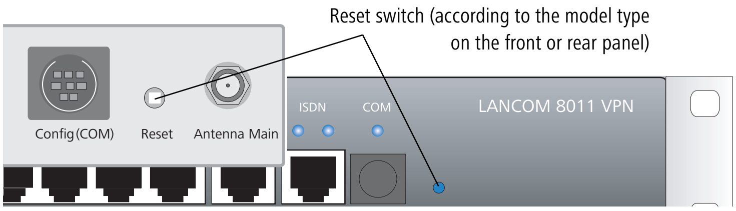
If the parameters `-s` and/or `-f` are not specified, the device uses default values set in path `/setup/config/TFTP-Client`:

- `Config address`
- `Config file name`
- `Firmware address`
- `Firmware file name`

These default values can be used if the latest configurations and firmware versions are always stored under the same name in the same location. In this case, the simple commands `LoadConfig` and `LoadFirmware` can be used to load the relevant files.

3.13 How to reset the device?

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


Reset switch (according to the model type
on the front or rear panel)
Config (COM)
Reset
Antenna Main
ISDN
COM
LANCOM 8011 VPN

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

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

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

Some devices simply cannot be installed under lock and key. There is consequently a risk that the configuration will be deleted by someone pressing the reset button too long. With the suitable setting, the behavior of the reset button can be controlled accordingly (only for devices with serial configuration interface):

WEBconfig: LCOS Menu Tree ▶ Setup ▶ Config

- **Reset button**

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

  □ Ignore: The button is ignored.

Please observe the following notice: The settings 'Ignore' or 'Boot only' makes it impossible to reset the configuration to the factory settings using the reset button. If the password is lost for a device with this setting, there is no way to access the configuration! In this case the serial communications interface can be used to upload a new firmware version to the device-this resets the device to its factory settings, which results in the deletion of the former configuration. Instructions on firmware uploads via the serial configuration interface are available here (→ page 3-44).

□ Reset-or-boot (standard setting): Press the button briefly to restart the device. Pressing the button for 5 seconds or longer restarts the device and resets the configuration to its factory settings. All LEDs on the device light up continuously. Once the switch is released the device will restart with the restored factory settings.

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

Please notice that also the WLAN encryption settings of the device will get lost in case of a reset and the standard WEP key comes into effect again. The wireless configuration of a device with WLAN interface will only succeed after a reset, if the standard WEP key is programmed into the WLAN adapter! After a reset, the LANCOM access point returns to managed mode, in which case the configuration cannot be directly accessed via the WLAN interface!

4 Advanced management

4.1 Scripting

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

4.1.1 Applications

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

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

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

- Edit the configuration with a simple text editor

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

- Edit sections of the configuration

  Instead of the entire configuration, smaller sections of it can be read out from a device instead (e.g. just the firewall settings). Just as with complete configurations, sections can be edited and transferred to one or more devices. This allows the particular settings in a device to be uploaded to other models or devices with a different version of the firmware.

- Automized configuration updates

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

- Convenient roll-out for larger installations

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

- Storage of configuration to volatile memory only

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

- Configuration changes in test mode

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

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

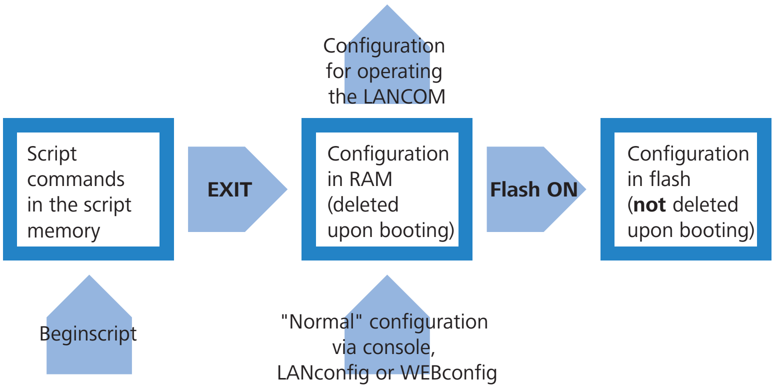
4.1.2 Scripting function

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

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

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

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


Configuration for operating the LANCOM
Script commands in the script memory
EXIT
Configuration in RAM (deleted upon booting)
Flash ON
Configuration in flash (not deleted upon booting)
Beginscript
"Normal" configuration via console, LANconfig or WEBconfig

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

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

4.1.3 Generating script files

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

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

Read out the configuration via the console

① Log on to the console with Supervisor rights.

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

③ At the command prompt, execute the command `readscript`. Observe the optional command extensions ('Scripting commands' → page 4-5).

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

Via TFTP from the command line interface (DOS box)

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

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

② Enter the following command at the prompt:

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

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

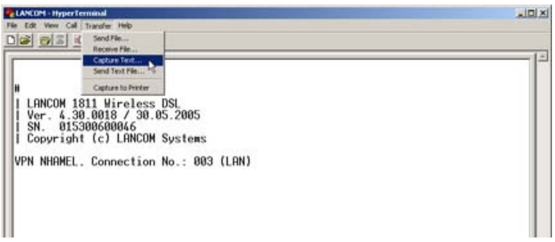
Please be aware that device passwords will be clearly visible as plain text while entering this command!

Via Hyperterminal

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

① Set up a connection to the device with Hyperterminal.

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



```
#
| LANCOM 1811 Wireless DSL
| Ver. 4.30.0018 / 30.05.2005
| SN.  015300600046
| Copyright (c) LANCOM Systems

VPN NHAMEL. Connection No.: 003 (LAN)
```

③ At the command prompt, execute the command `readscript`. Observe the optional command extensions ('Scripting commands' → page 4-5).

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

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

Download script from device

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

Detailed information about scripting can be found under the section 'scripting' in the chapter on Network Management with LANtools in the reference manual.

In addition to manually setting a script and console read-outs, script files can also be read out from a device with the help of LANconfig. For this, right click on the corresponding entry in the device list and select the entry **Configuration management ▶ Save script to file** from the context menu. Select the following options here:

- **Numeric sections**

  Enable this option if you do not want the configuration sections in the script to be displayed in cleartext (e.g. `/setup/wlan/ppp`), but numerically (`/2/2/5`).

- **Default parameters**

  Unless defined otherwise, the only parameters saved in a script are those that deviate from the default values. Enable this option if the standard values should also be entered into the script.

- **Column names**

  Unless defined otherwise, the fields of a table are initially entered as column names in the scripts and, thereafter, only the respective values are inserted into the rows. Enable this option when every value in the table should explicitly receive the description of the column in which it is inserted.

- **Comments**

  Activate this option when additional comments should be included in the script file.

- **Compact formatting**

  □ Enable this option if spaces and tabs should be suppressed.

- **Download only selected sections**

  Without further entries, the entire device configuration will always be saved in the script. In contrast, entering the sections also makes it possible to save partial configurations. Enter the sections to which the script should be transferred into this field, e.g. `/setup/wlan`.

4.1.4 Uploading configuration commands and script files

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

- The commands can be manually entered at a console in script mode (with the command "beginscript"). In this way the commands are written directly from the console to the intermediate memory. After all of the commands are ready, they are processed by entering the command "exit" and are then transferred to the RAM.

- The required command sequence can be saved to a text file. This text file is then sent to the intermediate memory by using an appropriate tool (LANconfig, terminal program, TFTP). If the necessary commands are included in the file, the transfer of the configuration to the RAM will be started automatically.

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

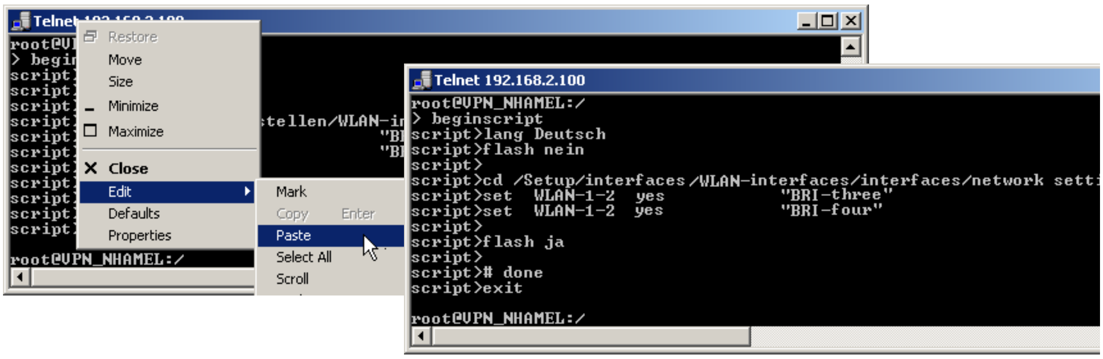
Command input via console session (Telnet, SSH)

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

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

② Log on to the console with Supervisor rights.

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



```
root@VPN_NHAMEL:/
> beginscript
script>lang Deutsch
script>flash nein
script>
script>cd /Setup/interfaces/WLAN-interfaces/interfaces/network setti
script>set  WLAN-1-2  yes                "BRI-three"
script>set  WLAN-1-2  yes                "BRI-four"
script>
script>flash ja
script>
script># done
script>exit

root@VPN_NHAMEL:/
```

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

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

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

Upload script with TFTP client

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

① Log on to the console with Supervisor rights.

② Enter the following command at the prompt:

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

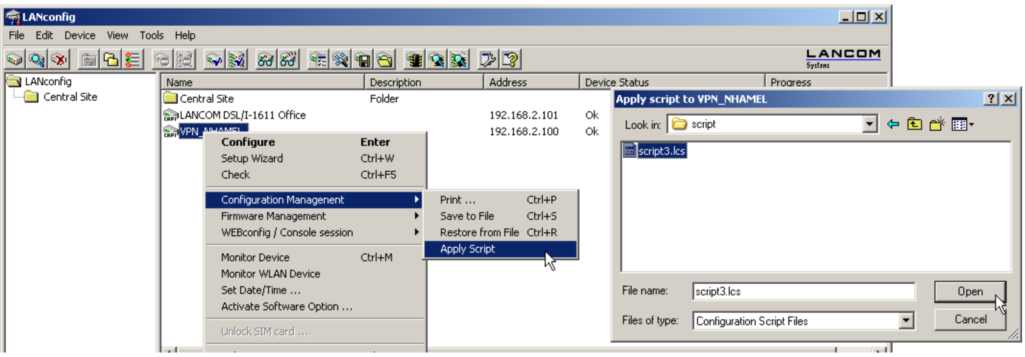
- □ IP address is the address of the TFCTP server where the script file is stored.
- □ script.lcs is the name of the script file on the TFTP server

Upload script with LANconfig

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

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

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



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

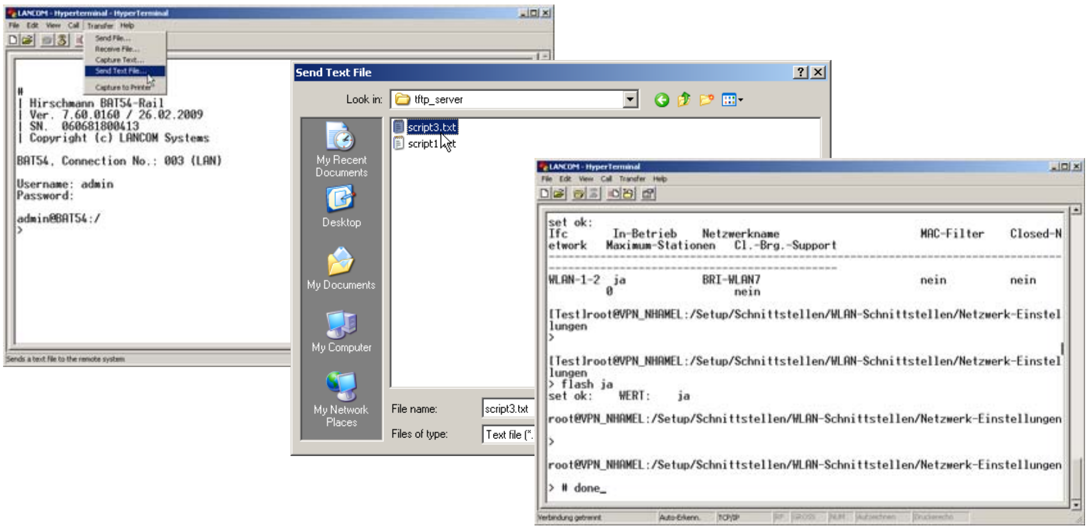
Upload script with Hyperterminal

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

① Set up a connection to the device with Hyperterminal.

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

③ Choose the required script file and start the transfer.



```
#
| Hirschmann BAT54-Rail
| Ver. 7.60.0160 / 26.02.2009
| SN.  060681800413
| Copyright (c) LANCOM Systems

BAT54, Connection No.: 003 (LAN)

Username: admin
Password:

admin@BAT54:/
>
```

```
set ok:
Ifc       In-Betrieb    Netzwerkname                      MAC-Filter    Closed-N
etwork   Maximum-Stationen   Cl.-Brg.-Support
--------------------------------------------------------------------------------
-------------------------------------------------
WLAN-1-2  ja            BRI-WLAN7                         nein          nein
         0                   nein

[Test]root@VPN_NHAMEL:/Setup/Schnittstellen/WLAN-Schnittstellen/Netzwerk-Einstel
lungen
>

[Test]root@VPN_NHAMEL:/Setup/Schnittstellen/WLAN-Schnittstellen/Netzwerk-Einstel
lungen
> flash ja
set ok:    WERT:    ja

root@VPN_NHAMEL:/Setup/Schnittstellen/WLAN-Schnittstellen/Netzwerk-Einstellungen

>

root@VPN_NHAMEL:/Setup/Schnittstellen/WLAN-Schnittstellen/Netzwerk-Einstellungen

> # done_
```

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

4.1.5 Multiple parallel script sessions

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

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

4.1.6 Scripting commands

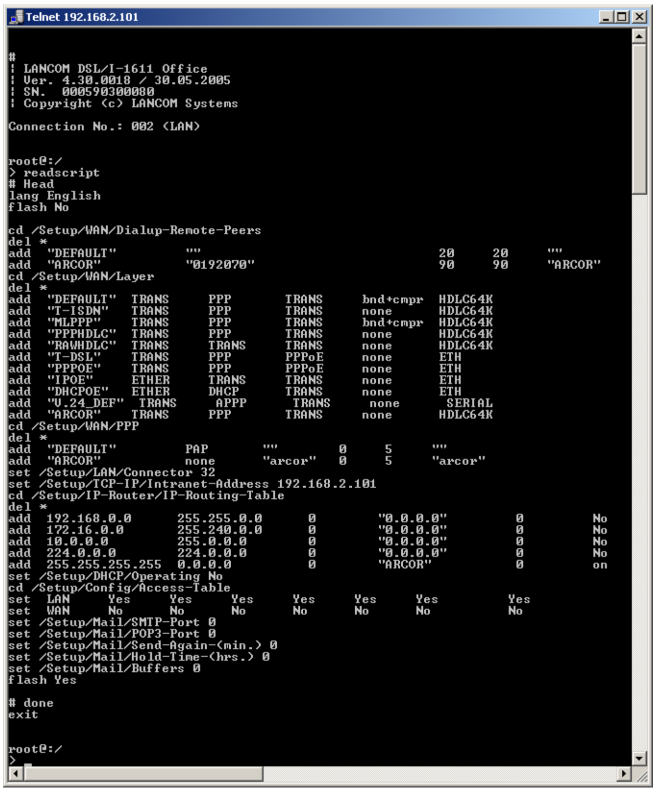
- `readscript`

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

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

Supervisor rights are necessary to execute this command.

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



```
#
| LANCOM DSL/I-1611 Office
| Ver. 4.30.0018 / 30.05.2005
| SN.  000590300080
| Copyright (c) LANCOM Systems

Connection No.: 002 (LAN)


root@:/
> readscript
# Head
lang English
flash No

cd /Setup/WAN/Dialup-Remote-Peers
del *
add  "DEFAULT"         ""                               20     20     ""
add  "ARCOR"           "0192070"                        90     90     "ARCOR"
cd /Setup/WAN/Layer
del *
add  "DEFAULT"  TRANS     PPP       TRANS     bnd+cmpr  HDLC64K
add  "T-ISDN"   TRANS     PPP       TRANS     none      HDLC64K
add  "MLPPP"    TRANS     PPP       TRANS     bnd+cmpr  HDLC64K
add  "PPPHDLC"  TRANS     PPP       TRANS     none      HDLC64K
add  "RAWHDLC"  TRANS     TRANS     TRANS     none      HDLC64K
add  "T-DSL"    TRANS     PPP       PPPoE     none      ETH
add  "PPPOE"    TRANS     PPP       PPPoE     none      ETH
add  "IPOE"     ETHER     TRANS     TRANS     none      ETH
add  "DHCPOE"   ETHER     DHCP      TRANS     none      ETH
add  "V.24_DEF"  TRANS     APPP      TRANS     none      SERIAL
add  "ARCOR"    TRANS     PPP       TRANS     none      HDLC64K
cd /Setup/WAN/PPP
del *
add  "DEFAULT"         PAP       ""        0     5     ""
add  "ARCOR"           none      "arcor"   0     5     "arcor"
set /Setup/LAN/Connector 32
set /Setup/TCP-IP/Intranet-Address 192.168.2.101
cd /Setup/IP-Router/IP-Routing-Table
del *
add  192.168.0.0      255.255.0.0      0        "0.0.0.0"         0         No
add  172.16.0.0       255.240.0.0      0        "0.0.0.0"         0         No
add  10.0.0.0         255.0.0.0        0        "0.0.0.0"         0         No
add  224.0.0.0        224.0.0.0        0        "0.0.0.0"         0         No
add  255.255.255.255  0.0.0.0          0        "ARCOR"           0         on
set /Setup/DHCP/Operating No
cd /Setup/Config/Access-Table
set  LAN     Yes     Yes     Yes     Yes     Yes     Yes         Yes
set  WAN     No      No      No      No      No      No          No
set /Setup/Mail/SMTP-Port 0
set /Setup/Mail/POP3-Port 0
set /Setup/Mail/Send-Again-(min.) 0
set /Setup/Mail/Hold-Time-(hrs.) 0
set /Setup/Mail/Buffers 0
flash Yes

# done
exit


root@:/
>
```

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

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

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

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

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

The following options can be used with the readscript command:

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

- #

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

The space after the # is obligatory.

- `del *`

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

  Syntax: `del [PATH]*`

- `default`

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

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

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

Supervisor rights are necessary to execute this command.

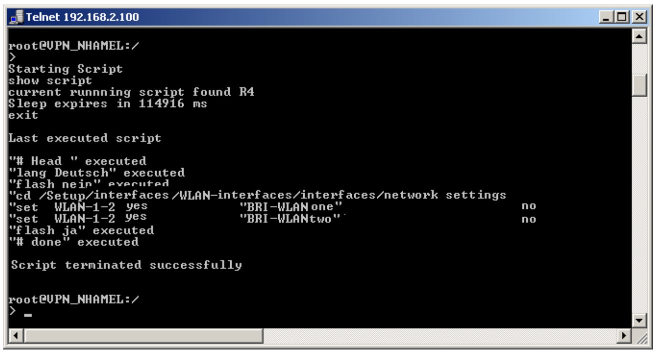
- `beginscript`

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

Supervisor rights are necessary to execute this command.

- `show script`

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



```
root@VPN_NHAMEL:/
>
Starting Script
show script
current runnning script found R4
Sleep expires in 114916 ms
exit

Last executed script

"# Head " executed
"lang Deutsch" executed
"flash nein" executed
"cd /Setup/interfaces/WLAN-interfaces/interfaces/network settings
"set  WLAN-1-2 yes              "BRI-WLAN one"                  no
"set  WLAN-1-2 yes              "BRI-WLANtwo"                   no
"flash ja" executed
"# done" executed

 Script terminated successfully


root@VPN_NHAMEL:/
> _
```

Supervisor rights are necessary to execute this command.

- `killscript`

  The command killscript deletes the content of a script session that has not yet been executed. The script session is selected by its name.

Supervisor rights are necessary to execute this command.

- `flash Yes/No`

  When configuring a device with scripts, any add-, set- or del- command can lead to an (unintentional) update of the configuration in flash; to prevent this, the update to flash function can be deactivated. After concluding the configuration, this function can be activated again with `flash Yes`. Changes in the RAM configuration are then written to flash. The status `flash Yes/No` is stored globally.

Supervisor rights are necessary to execute this command.

- `sleep`

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

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

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

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

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

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

4.2 Rollout Wizard

In complex scenarios with multiple LANCOM devices at different locations, on-site technicians may not be available to carry out the installation and configuration of a LANCOM. A large part of the configuration can be prepared at headquarters. All that has to be set up on-site are a few location-dependent parameters. The Rollout Wizard allows non-expert, on-site employees to carry out these last-minute adjustments with the help of a browser. After running the Rollout Wizard the device is either operational or it can independently retrieve the rest of its configuration from a central storage location.

The parameters for configuration can be found under the following paths:

WEBconfig: LCOS menu tree ▶ Setup ▶ HTTP ▶ Rollout-Wizard

4.2.1 General settings in the Rollout Wizard

- **Operating**

  Switches the Rollout Wizard on or off. After being switched on the Wizard appears directly on the WEBconfig start page.

  - Possible values: On, off
  - Default: Off

- **Title**

  The name for the Rollout Wizard that appears on the start page of WEBconfig.

  - Possible values: Maximum 64 alphanumerical characters
  - Default: Roll-out

4.2.2 Variables

Maximum ten variables can be defined with Index, Ident, Title, Type, Min-Value, Max-Value and Default-Value.

- **Index**

  Index for the variable. The Rollout Wizard displays the variables in ascending order.

  - Possible values: 1 to 2^{32} - 1
  - Default: 0

- **Ident**

  Unique identifier of variables that are referenced during the execution of actions. Identifiers are not required for fields that are not used by users to enter their data (e.g. label).

  - Possible values: Maximum 64 alphanumerical characters
  - Default: blank

- **Title**

  Name of the variable as displayed by the Rollout Wizard in WEBconfig.

  - Possible values: Maximum 64 alphanumerical characters
  - Default: blank

- **Type**

  Name of the variable as displayed by the Rollout Wizard in WEBconfig.

- □ Possible values: Label, Integer, String, Password, Checkmark
- □ Label: Text that is displayed to provide explanations of the other variables. Min.-Value and Max.-Value are of no further significance for these entries.
- □ Integer: Allows the entry of a positive integer number between 0 and 2^{32} - 1. By entering the Min.-Value and Max.-Value, the range of entries can be limited. Also, a default value can be defined. This default value must be between the Min. and Max.-Values.
- □ String: Enables text to be entered. By entering the Min.-Value and Max.-Value, the length of the string can be limited. Also, a default value can be defined. This default text must be shorter than the maximum length, otherwise it will be truncated.
- □ Password: splayed while being entered. Entering a password has to be repeated. The Rollout Wizard will execute no actions if the passwords do not agree.
- □ Checkmark: Simple option that can be switched on or off. Min.-Value and Max.-Value are of no further significance for these entries. Checkmarks are activated as standard if the default value is not empty.
- □ Default: Label

■ **Min-Value**

Minimum value for the current variable (if type = integer) or minimum number of characters (where type = String or Password).

- □ Possible values: 0 to 2^{32} - 1
- □ Default: 0

■ **Max-Value**

Maximum value for the current variable (if type = integer) or maximum number of characters (where type = String or Password).

- □ Possible values: 0 to 2^{32} - 1
- □ Default: 0

■ **Default value**

Default value of the current variable.

- □ Possible values: Maximum 64 alphanumerical characters
- □ Default: blank

4.2.3 Actions to be executed by the Rollout Wizard

Max. 19 definitions of actions (with index and action) which are to be executed by the Rollout Wizard after the user data has been entered.

■ **Index**

Index for the action. The Rollout Wizard executes the actions in ascending order.

- □ Possible values: 1 to 2^{32} - 1
- □ Default: 0

■ **Action**

Action to be executed by the Rollout Wizard after the user data has been entered.

- □ Possible values: Similar to Cron commands, actions are entered in the syntax `[Protocol:]Argument`. If no protocol is entered, 'exec.' is applied.
- □ exec: Executes any command just as it is used in Telnet to configure a LANCOM. The following example sets the name of the device to 'MyLANCOM':

```
exec: set /setup/name MyLANCOM
```

- □ mailto: Enables an e-mail to be sent upon entry of the address, subject and body text, for example:

```
mailto:admin@mylancom.de?subject=Rollout?body=LANCOM setup completed
```

ⓘ To make use of the mail function, an SMTP account must be set up in the device.

- □ http and http: Enables a Web site to be accessed, for example to carry out an action there.

```
<http:|http:>//[user[:pass]@]hostname[:port]/...
```

- □ Variables in the actions: When actions are executed, the values as defined with the Rollout Wizard can be referenced. To this end, the variable's identifier is used for the action with a leading percent character. The identifier must be enclosed by curly brackets if other alphanumeric characters are included in the action. The following example sets the name of the device to the format 'Site (branch)', if the location of the device is being queried as a variable with the identifier 'Location':

```
exec: set /setup/name %{Location}(Branch)
```

For variables of the type Integer or String, the value as entered by the user is used. In the case of variables of the type Checkmark, '1' (switched on) or '0' (switched off) is used.

ⓘ If the expression for the action contains spaces then the expression must be enclosed by quotation marks.

- □ Default: blank

4.2.4 Actions for managing the Rollout Wizard

- **Renumber variables**
- **Renumber actions**

  As explained above, variables and actions are displayed or processed in the order of their index. Occasionally, variables/actions with neighboring index numbers require a new entry to be entered between them. With this action, the indices can automatically be renumbered with a certain interval between them.

  When being executed, the arguments can be defined with the start value and increment. This action renumbers the entries starting with the start value and continuing with the increment as chosen. If the start value and increment are not defined, both are set automatically to 10. If no arguments are entered, the action renumbers the indices with 10, 20, 30, etc.

4.3 LANCOM Layer 2 Management protocol (LL2M)

4.3.1 Introduction

As a pre-requisite for all methods of configuring a LANCOM, an IP connection must exist between the configuration computer and the LANCOM. No matter whether LANconfig, WEBconfig or Telnet is used, no configuration commands can be sent to the device without an IP connection. In the event of erroneous configuration of the TCP/IP settings or VLAN parameters, this IP connection may be impossible to establish. The only option in this case is to access the device via the serial configuration interface (not available on all devices) or to reset the device to its factory settings. However, both options require physical access to the device—this may not always be the case for concealed installation of Access Points and can represent considerable overhead for larger-scale installations.

The LANCOM Layer 2 Management Protocol (LL2M) is used to also enable configuration access to a device even without an IP connection. All this protocol requires is a connection on layer 2 (i.e. via Ethernet directly or via layer-2 switches) to establish a configuration session. LL2M connections are supported on LAN or WLAN connections, but not via WAN. Connections via LL2M are password protected and are resistant to replay attacks.

LL2M establishes a client-server structure for this purpose: The LL2M client sends requests or commands to the LL2M server that responds to the requests or runs the commands. The LL2M client is integrated into LCOS and is run from the command line. The LL2M server is also integrated into LCOS and is usually only enabled for a brief period after device power-on. In this time frame, an administrator can use the LL2M client to perform changes to the configuration of the device running the LL2M server.

4.3.2 Configuration of the LL2M server

WEBconfig: LCOS Menu Tree/Setup/Config/LL2M

- **Operating**

  Enables/disables the LL2M server. An LL2M client can contact an enabled LL2M server for the duration of the time limit following device boot/power-on.

  Possible values:

  - □ Yes, No

  Default:

  - □ Yes

- **Time limit**

  Defines the period in seconds during which an enabled LL2M server can be contacted by an LL2M client after device boot/power-on. The LL2M server is disabled automatically after expiry of the time limit.

  Possible values:

  - □ 0 to 4294967295

Default:

- □ 0

Special values:

- □ 0 disables the time limit. The LL2M server stays permanently enabled in this state.

4.3.3 Commands for the LL2M client

For every LL2M command, an encrypted tunnel is set up that protects the log-in information transferred on transmission. To use the integrated LL2M client, start a Telnet session on a LANCOM that has local access to the LL2M server via the available physical medium (LAN, WLAN). The following commands can be used to contact the LL2M server in this console session.

You must have root rights on the LL2M server to run commands on the LL2M client.

- ■ **LL2Mdetect**

  The LL2M client uses this command to send a SYSINFO request to the LL2M server. The server then sends its system information, such as hardware and serial number, back to the client for display. The LL2Mdetect command can be restricted using the following parameters.

  - □ -a <MAC address>: Restricts the command to those devices with the specified MAC address only. The MAC address is specified in format “00a057010203”, “00-a0-57-01-02-03” or “00:a0:57:01:02:03”.

  If no MAC limitations are set, the detect is sent as a multicast (or optionally as a broadcast) to all LL2M-compatible devices.
  To contact groups of MAC addresses, * and x can by used as placeholders in individual MAC address positions, e.g. “00-a0-57-xx-xx-xx” for all LANCOM MAC addresses.

  - □ -t <device type>: Restricts the command to those devices of the corresponding hardware type only.
  - □ -r <hardware release>: Restricts the command to those devices with the corresponding hardware release only.
  - □ -f <version>: Restricts the command to those devices with the corresponding firmware version only.
  - □ -s <serial number>: Restricts the command to those devices with the corresponding serial number only.
  - □ -b : Sends the LL2Mdetect request as a broadcast and not as a multicast.
  - □ -v <VLAN ID>: Only sends the LL2Mdetect request on the VLAN specified. If no VLAN ID is specified, the VLAN ID of the first defined IP network is used.

  Example:

  - □ ll2mdetect -r A: This command sends a SYSINFO request to all devices with hardware release “A”.

  The response from the LL2M server contains the following information:

  - □ Device name
  - □ Device type
  - □ Serial number
  - □ MAC address
  - □ Hardware release
  - □ Firmware version with date

- ■ **LL2Mexec**

  The LL2M client uses this command to send a single-line command to run on the LL2M server. Several commands can be combined in one LL2M command by using semicolons as separators. Depending on the command, either the actions are run on the remote device and the responses from the remote device are sent to the LL2M client for display. The LL2Mexec command conforms to the following syntax:

  - □ ll2mexec <user>[:<password>]@<MAC address>

  The LL2Mexec command can be restricted using the following parameters.

  - □ -v <VLAN ID>: Only sends the LL2Mexec command on the VLAN specified. If no VLAN ID is specified, the VLAN ID of the first defined IP network is used.

  Example:

  - □ ll2mexec root@00a057010203 set name MyLANCOM: This command logs the LL2M client on to the LL2M server with MAC address “00a057010203” as user “root”. The user is prompted for the password in the console session. The LL2M client then sets the name of the remote device to “MyLANCOM”.

4.4 Messaging

The action table contains the following variables for control over messaging when certain events occur in the LANCOM:

- **%a**
  WAN IP address of the WAN connection relating to the action.
- **%H**
  Host name of the WAN connection relating to the action.
- **%h**
  as %h, except the hostname is in small letters
- **%c**
  Connection name of the WAN connection relating to the action.
- **%n**
  Device name
- **%s**
  Device serial number
- **%m**
  Device MAC address (as in Sysinfo)
- **%t**
  Time and date in the format YYYY-MM-DD hh:mm:ss

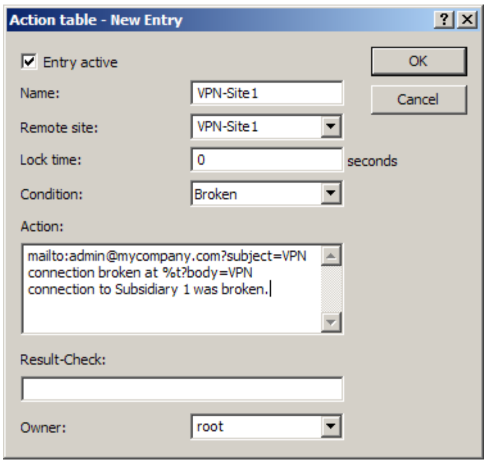
Example: Broken connection alert as an SMS to a mobile telephone

The placeholder %t allows the current time of an event to be incorporated into a message. For example, an alert about the interruption of an important VPN connection can be sent by e-mail or as an SMS to a system administrator's mobile telephone.

The following requirements have to be met for messaging:

- The status of the VPN connection must be monitored, for example by means of "dead-peer-detection" (DPD).
- The LANCOM has to be configured as an NTP client in order to have the current system time.
- An SMTP account must be set up for transmitting e-mails.

Once these requirements are fulfilled, messaging can be set up. This is done with a new entry in the action table; e. g. with LANconfig under **Communication ▶ General ▶ Action table**.



☑ Entry active

Name: VPN-Site1

Remote site: VPN-Site1

Lock time: 0 seconds

Condition: Broken

Action:

mailto:admin@mycompany.com?subject=VPN connection broken at %t?body=VPN connection to Subsidiary 1 was broken.

Result-Check:

Owner: root

Select the remote site for the relevant connection. As Condition select 'Broken' and enter the action as the transmission of an e-mail.

`mailto:admin@mycompany.com?subject=VPN connection broken at %t?body=VPN connection to Subsidiary 1 was broken.`

If the connection is broken, this action sends an e-mail to the administrator with the time of the event in the subject line.

ⓘ If the mail is sent to an appropriate Mail2SMS gateway the alert can be sent directly to a mobile telephone.

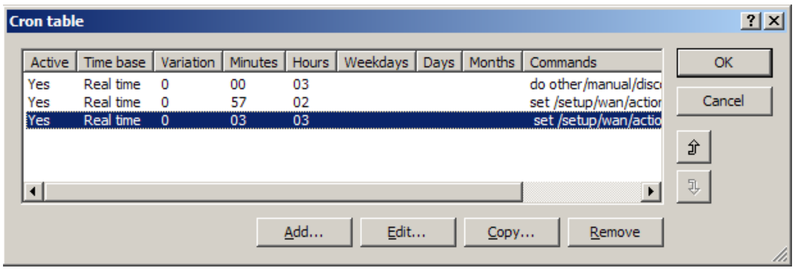
(!) For complex scenarios with several subsidiaries, each of the remote sites is given a corresponding entry in the central LANCOM. For monitoring the central device itself, an action is entered into a device at one of the subsidiaries. In this way the administrator receives an alert even if the VPN gateway at the central location fails, which could potentially prevent any messages from being transmitted.

Suppress messaging in case of re-connects with a DSL connection

Some providers interrupt the DSL connection used for the VPN connections once every 24 hours. To avoid informing the administrator of these regular interruptions, messaging can be disabled at the time when the re-connect occurs.

First of all an action is required to force the re-connect to occur at a fixed time; generally at night when the Internet connection is not in use. The entry defines, for example, 03:00h and the Internet connection is broken with the command `do other/manual/disconnect internet`.

With two more cron commands `set /setup/wan/action-table/1 yes/no` the corresponding entry in the action table is switched off three minutes before 03:00h and switched on again three minutes after 03:00h. The number 1 following the path to the action table is an index that stands for the first entry in the table.



Cron table

Active	Time base	Variation	Minutes	Hours	Weekdays	Days	Months	Commands
Yes	Real time	0	00	03				do other/manual/disc
Yes	Real time	0	57	02				set /setup/wan/actior
Yes	Real time	0	03	03				set /setup/wan/actio

4.5 Managing rights for different administrators

New in LCOS 7.60:

- Administrators without trace rights

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

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

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

If more than one administrator is set up in the admin table, the main menu features an additional button **Change administrator**, which makes it possible to switch to a different user ID (with different rights, if applicable).

4.5.1 Rights for the administrators

Two different groups are differentiated regarding administrators' rights.

- Each administrator belongs to a certain group that has globally defined rights assigned to it.
- Each administrator also has "function rights" that determine personal access to certain functions such as the Setup Wizards.

Administrator groups

Description under Telnet/Terminal	Description under LANconfig	Rights
Supervisor	All	Supervisor - member of all groups
Admin-RW	Limited	Local administrator with read and write access
Admin-RW limit	Limited without trace rights	Local administrator with read and write access but without trace rights
Admin-RO	Read only	Local administrator with read access but no write access
Admin-RO limit	Read only without trace rights	Local administrator with read access but no write access and no trace rights
None	None	No access to the configuration

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

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

- Local administrator with read and write rights but without trace rights: Also has full access to the configuration, although the following options are prohibited:
  - Upload firmware onto the device
  - Upload configuration onto the device
  - Configuration with LANconfig
  - Trace output via Telnet or LANmonitor

Local administrators with write access but without trace rights cannot create administrators with trace rights.

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

Function rights

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

- Basic Settings Wizard
- Security Settings Wizard
- Internet Connection Wizard
- Selection of Internet Provider Wizard
- RAS Account Wizard
- LAN-LAN Connection Wizard
- Change time and date
- Search for further devices
- WLAN link test
- a/b Wizard

4.5.2 Administrators' access via TFTP and SNMP

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

Access with LANconfig

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

Access with TFTP

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

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

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

- Read the configuration from the device (supervisor only)

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

- Write the configuration to the device (supervisor only)

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

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

```
tftp mylancom.intern GET localadmin:Admin@readmib mylancom.mib
```

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

Access with SNMP management systems

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

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

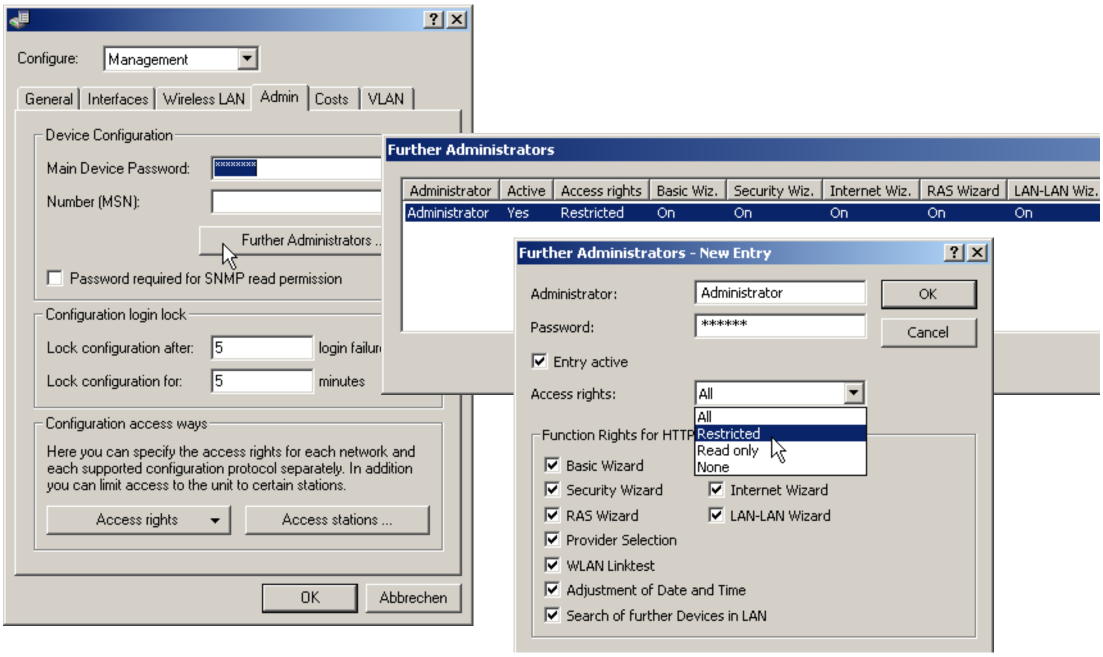
The community 'public' corresponds with the rights of a local administrator with read-only access, as long as the SNMP read access without password is enabled (). If this access is not allowed, then the 'public' community will have access to no menus at all.

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

4.5.3 Configuration of user rights

LANconfig

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



Configure: Management

Device Configuration

Main Device Password: ********

Number (MSN):

□ Password required for SNMP read permission

Configuration login lock

Lock configuration after: 5 login failur

Lock configuration for: 5 minutes

Configuration access ways

Here you can specify the access rights for each network and each supported configuration protocol separately. In addition you can limit access to the unit to certain stations.

Further Administrators

Administrator	Active	Access rights	Basic Wiz.	Security Wiz.	Internet Wiz.	RAS Wizard	LAN-LAN Wiz.
Administrator	Yes	Restricted	On	On	On	On	On

Further Administrators - New Entry

Administrator: Administrator

Password: ******

☑ Entry active

Access rights: All

All
Restricted
Read only
None

Function Rights for HTTP

☑ Basic Wizard

☑ Security Wizard ☑ Internet Wizard

☑ RAS Wizard ☑ LAN-LAN Wizard

☑ Provider Selection

☑ WLAN Linktest

☑ Adjustment of Date and Time

☑ Search of further Devices in LAN

Enter the following values:

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

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

WEBconfig, Telnet or terminal program

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

WEBconfig: LCOS menu tree ▶ Setup ▶ Config-module ▶ Admin.-table

The different user groups are represented by the following values:

Description	Rights
Supervisor	Supervisor - member of all groups
Admin-RW	Local administrator with read and write access
Admin-RW limit	Local administrator with read and write access but without trace rights
Admin-RO	Local administrator with read access but no write access
Admin-RO limit	Local administrator with read access but no write access, without trace rights
None	No access to the configuration

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

Value	Rights
0x00000001	The user can run the Basic Settings Wizard
0x00000002	The user can run the Security Wizard
0x00000004	The user can run the Internet Wizard
0x00000008	The user can run the Wizard for selecting Internet providers
0x00000010	The user can run the RAS Wizard
0x00000020	The user can run the LAN-LAN Coupling Wizard
0x00000040	The user can set the date and time (also applies for Telnet and TFTP)
0x00000080	The user can search for additional devices
0x00000100	The user can run the WLAN Link test (also applies for Telnet)
0x00000200	The user can run the a/b Wizard
0x00000400	The user can run the WTP Assignment Wizard
0x00000800	The user can run the Public Spot Wizard
0x00001000	The user can run the WLAN Wizard
0x00002000	The user can run the Rollout Wizard
0x00004000	The user can run the Dynamic DNS Wizard
0x00008000	The user can run the VoIP Call Manager Wizard
0x00010000	The user can run the WLC Profile Wizard

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

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

For this example, enter the the function rights as "0000015a".

Put differently, this is an OR operator with the following hexadecimal values:

Description	Value
Security Settings Wizard	0x00000002
Selecting the provider	0x00000008
RAS Account Wizard	0x00000010
Changing the time	0x00000040
WLAN link test	0x00000100
OR operated	0x0000015a

Examples:

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

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

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

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

4.5.4 Limitation of the configuration commands

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

Command	Supervisor	Local administrator	Remark
activateimage	✔		
cfgreset	✔		
linktest	✔		The 'linktest' command can also be executed if the user possesses the function right to carry out a WLAN link test
readconfig	✔		
writeconfig	✔		
writeflash	✔		
setenv	✔	✔	
testmail	✔	✔	
time	✔	✔	The 'time' command can also be executed if the user possesses the function right to set the system time
unsetenv	✔	✔	
delete/rm	✔	✔	
readmib	✔	✔	
WLA	✔	✔	
set	✔	✔	

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

ⓘ The commands listed above are not available in all LCOS versions nor LANCOM models.

4.5.5 TCP port tunnel

In some cases it can be useful to enable temporary remote access to a station within a LAN, e.g. via HTTP (TCP port 80) or TELNET (TCP port 23). For example, if questions come up concerning network devices such as a LANCOM VP-100, the Support department is best able to assist with direct access to the device in the customer's LAN. The standard method for accessing LAN devices via inverse masquerading (port forwarding) sometimes requires a special configuration of the firewall—changes are made which, if they are not deleted again afterwards, can represent a security risk.

As an alternative to permanent access which is based on port forwarding, a temporary remote-maintenance access can be set up that automatically closes again after certain periods of inactivity. To this end, a support staff member requiring access to a device in the customer's network, for example, creates a "TCP/HTTP" tunnel using TCP port 80 to provide this access.

! This access only applies to the IP address that was the source of the tunnel. Network access to devices released in this way is not transferable!

Configuring the TCP/HTTP tunnel

The following parameters are available for configuring TCP/HTTP tunnel in LANCOM:

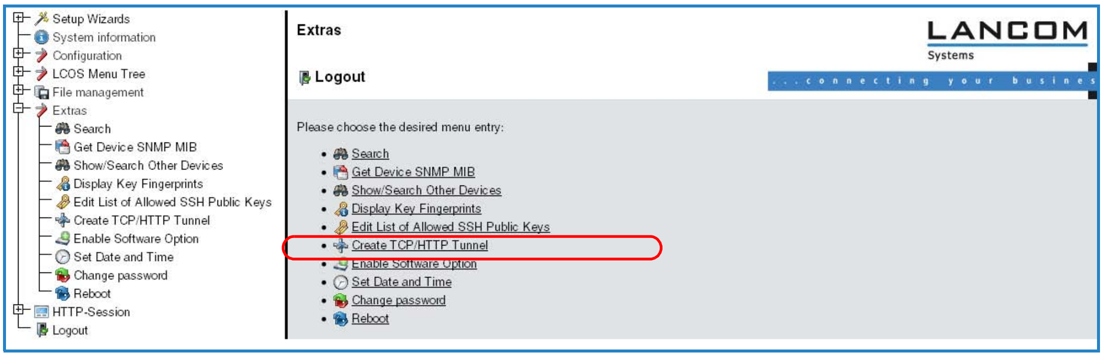
WEBconfig: LCOS menu tree ▶ Setup ▶ HTTP

- **Max. tunnel connections**
  The maximum number of simultaneously active TCP/HTTP tunnels
- **Tunnel idle timeout**
  Life-expectancy of an inactive tunnel. After expiry of this time period the tunnel closes automatically unless data transfer is actively taking place.

Create the TCP/HTTP tunnel

① HTTP tunnels are set up on the start page of WEBconfig. In WEBconfig log on to the LANCOM Wireless behind which the device to be released is located. If necessary obtain the required login data from the responsible administrator.

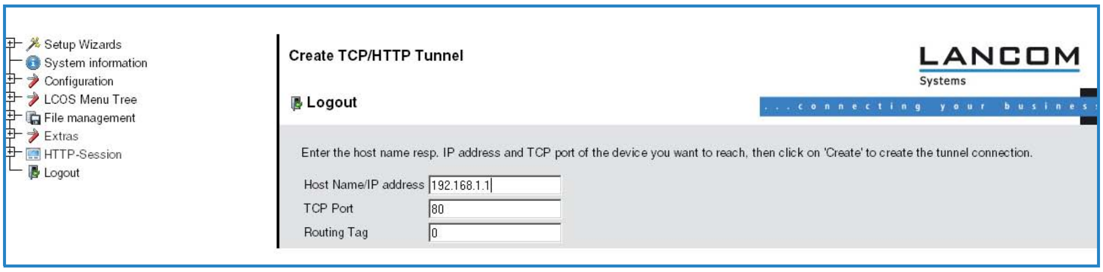
② In the area 'Extras', select the entry **Create TCP/HTTP tunnel**



Please choose the desired menu entry:

- Search
- Get Device SNMP MIB
- Show/Search Other Devices
- Display Key Fingerprints
- Edit List of Allowed SSH Public Keys
- Create TCP/HTTP Tunnel
- Enable Software Option
- Set Date and Time
- Change password
- Reboot

③ Enter the name or IP address of the device that is to be temporarily available via HTTP.

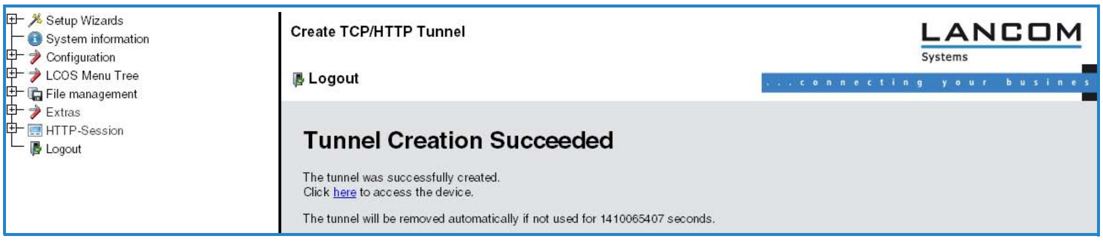


Enter the host name resp. IP address and TCP port of the device you want to reach, then click on 'Create' to create the tunnel connection.

Host Name/IP address: 192.168.1.1
TCP Port: 80
Routing Tag: 0

④ Select a port for the HTTP tunnel and, if applicable, enter the routing tag of the IP network in which the device is located and confirm your entries with **Create**.

⑤ The dialog that follows displays a confirmation of the newly created tunnel and provides a link to the device.



Tunnel Creation Succeeded

The tunnel was successfully created.
Click here to access the device.

The tunnel will be removed automatically if not used for 1410065407 seconds.

Apart from HTTP or HTTPS-based access, remote maintenance can also be based on any other TCP service such as telnet connections (TCP port 23) or SSH (TCP port 22).

Deleting the tunnel prematurely

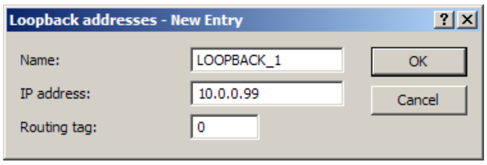
The newly created HTTP tunnel is deleted automatically if the tunnel remains inactive for the duration of the tunnel idle timeout. To delete the tunnel earlier, click on **LCOS menu tree** ▶ **Status** ▶ **TCP-IP** ▶ **HTTP** to access the list of active tunnels and delete the one you no longer require.

Although active TCP connections in this tunnel are **not** terminated immediately, no new connections can be established.

4.6 Named loopback addresses

A LANCOM Wireless can be set with up to 16 loopback addresses with which it can be addressed, for example for the management of large network structures. To use the loopback addresses for certain networks (e.g. in the context of

Advanced Routing and Forwarding), these addresses can be assigned with routing tags. To simplify the identification in other configuration units, the loopback addresses can be given freely definable names:


Loopback addresses - New Entry

Name: LOOPBACK_1
IP address: 10.0.0.99
Routing tag: 0

LANconfig: TCP/IP ▶ General ▶ Loopback addresses

WEBconfig: LCOS menu tree > Setup > TCP-IP > Loopback list

- **Name**

  A freely definable name for the loopback address.

- **Loopback address**

  Loopback address for the device.

- **Routing tag**

  Routing tag of the loopback address. Loopback addresses with the routing tag '0' (untagged) are visible to all networks. Loopback addresses with a different routing tag are only visible to networks with the same routing tag.

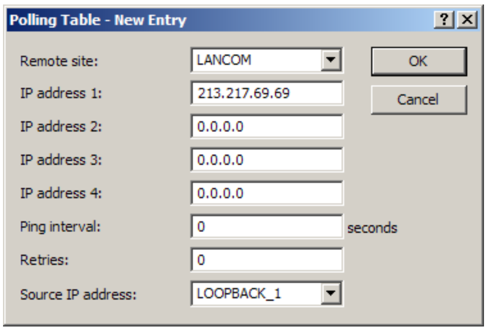
4.6.1 Loopback addresses with ICMP polling

Similar to LCP monitoring, ICMP polling transmits regular requests to a remote site. Ping commands are transmitted and the answers to them are monitored. Unlike LCP monitoring, the target site for ICMP pings can be freely defined. Pinging a router in a remote network thus provides monitoring for the entire connection and not just the section to the Internet provider.

A ping interval is defined for the remote site in the polling table. Further, for the event that replies are missed, the number of retries before the transmission of a new LCP request is defined. Should the transmitter not receive any reply to the retries, the target for the ping requests is classified as unavailable.

Up to four different IP addresses can be entered for each remote site that will be checked in the remote network in parallel. Only if all of the IP addresses are unavailable is the connection considered to have failed.

With the ICMP polling, an entire connection can be monitored from end to end.


Polling Table - New Entry

Remote site: LANCOM
IP address 1: 213.217.69.69
IP address 2: 0.0.0.0
IP address 3: 0.0.0.0
IP address 4: 0.0.0.0
Ping interval: 0 seconds
Retries: 0
Source IP address: LOOPBACK_1

LANconfig: Communication ▶ Remote Sites ▶ Polling table

WEBconfig: LCOS menu tree ▶ Setup ▶ WAN ▶ Polling table

- **Peer**

  Name of the remote station which is to be checked with this entry.

- **IP address 1 - 4**

  IP addresses for targeting with ICMP requests to check the remote site.

If no IP address is entered for a remote site that can be checked with a ping, then the IP address of the DNS server that was determined during the PPP negotiation will be checked instead.

- **Ping interval**

  The time entered into the polling table defines the time interval between ping requests. If the value "0" is entered, then the standard value of 30 seconds applies.

- **Retries**

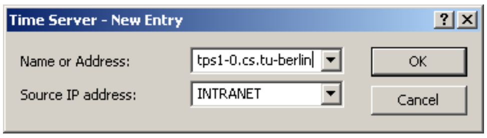
If no reply to a ping is received then the remote site will be checked in shorter intervals. The device then tries to reach the remote site once a second. The number of retries defines how many times these attempts are repeated. If the value "0" is entered, then the standard value of 5 retries applies.

- **Loopback address**

  Sender address sent with the ping; this is also the destination for the answering ping.

4.6.2 Loopback addresses for time servers

LANCOM Wirelesss can retrieve time information from public time servers in the Internet (NTP server). The LANCOM can then be provided the time to all stations in the local network. When defining the time server, the name or IP address of the NTP server being queried by the LANCOM Wireless can be entered as well as loopback addresses.



Name or Address: tps1-0.cs.tu-berlin
Source IP address: INTRANET

LANconfig: Date & time ▶ Synchronization ▶ Time server

WEBconfig: LCOS Menu Tree ▶ LCOS menu tree ▶ Setup ▶ NTP ▶ RQ address

- **Name**

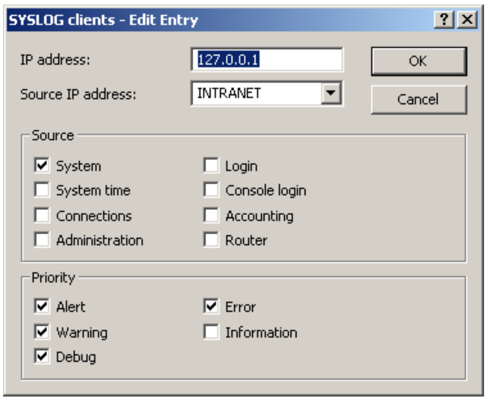
  Name or IP address of the NTP server. The LANCOM Wireless attempts to reach the servers in the order that they are entered.

- **Loopback address**

  Sender address sent with the NTP request; this is also the destination for the NTP answer.

4.6.3 Loopback addresses for SYSLOG clients

The SYSLOG module enables the logging of accesses to the LANCOM Wireless. SYSLOG clients are set up to be able to receive the SYSLOG messages.



IP address: 127.0.0.1
Source IP address: INTRANET

Source
☑ System
□ System time
□ Connections
□ Administration
□ Login
□ Console login
□ Accounting
□ Router

Priority
☑ Alert
☑ Warning
☑ Debug
☑ Error
□ Information

LANconfig: Log & Trace ▶ SYSLOG ▶ SYSLOG clients

WEBconfig: LCOS menu tree ▶ Setup ▶ SYSLOG ▶ SYSLOG table

- **IP address**

  IP address of the SYSLOG client.

- **Loopback address**

  Sender address entered into the SYSLOG message. No answer is expected to a SYSLOG message.

- **Source**
  - System: System messages (boot events, timer system, etc.)
  - Logins: Messages concerning the user's login or logout during the PPP negotiation, and any errors that occur during this.
  - System time: Messages about changes to the system time
  - Console logins: Messages about console logins (Telnet, Outband, etc.), logouts and any errors that occurred during this.
  - Connections: Messages about establishment and termination of connections and any errors that occurred (display trace)

  - Accounting: Accounting information stored after termination of a connection (user, online time, transfer volumes)
  - Administration: Messages on changes to the configuration, remotely executed commands, etc.
  - Router: Regular statistics about the most frequently used services (breakdown per port number) and messages about filtered packets, routing errors, etc.
- **Priority**
  - Alert: This is a collection of messages of interest to the administrator (general SYSLOG priority: PANIC, ALERT, CRIT).
  - Error: At this level all error messages which can occur under normal conditions are communicated; no special attention is required by the administrator, e.g. connection errors (general SYSLOG priority: ERROR).
  - Warning: This level communicates messages which do not compromise normal operating conditions (general SYSLOG priority: WARNING).
  - Information: At this level, all messages are sent that have a purely informational character (e.g. accounting) (general SYSLOG priority: NOTICE, INFORM).
  - Debug: Communication of all debug messages. Debug messages generate large data volumes and can compromise the device's operation. For this reason they should be disabled for normal operations and only used for trouble-shooting (general SYSLOG priority: DEBUG).

5 Diagnosis

5.1 Trace information—for advanced users

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

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

5.1.1 How to start a trace

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

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

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

5.1.2 Overview of the keys

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

5.1.3 Overview of the parameters

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

This parameter...	... brings up the following display for the trace:
Status	status messages for the connection
Error	error messages for the connection
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
IPX-RIP	IPX Routing Information Protocol
Firewall	Firewall activities
RIP	IP Routing Information Protocol
ARP	Address Resolution Protocol
ICMP	Internet Control Message Protocol
IP masquerading	processes in the masquerading module
DHCP	Dynamic Host Configuration Protocol
NetBIOS	NetBIOS management
DNS	Domain Name Service Protocol
Packet dump	display of the first 64 bytes of a package in hexadecimal form

This parameter...	... brings up the following display for the trace:
D-channel-dump	trace on the D channel of the connected ISDN bus
ATM-cell	spoofing at the ATM packet level
ATM-Error	ATM errors
ADSL	ADSL connections status
SMTP-Client	E-mail processing of the integrated mail client
Mail-Client	E-mail processing of the integrated mail client
SNTP	Simple Network Time Protocol information
NTP	Timeserver Trace
Connact	Messages from the activity protocol
Cron	cron table
RADIUS	RADIUS trace
Serial	Status of serial interface
USB	Status of USB interface
Load-Balancer	Load balancing information
VRRP	Information concerning Virtual Router Redundancy Protocol
Ethernet	Status of ethernet interface
VLAN	Information concerning virtual networks
IGMP	Information concerning Internet Group Management Protocol
WLAN	Information concerning wireless networks
IAPP	Trace for Inter Access Point Protocol, shows information concerning WLAN roaming.
DFS	Trace for Dynamic Frequency Selection
Bridge	Information concerningWLAN bridge
EAP	Trace for EAP
Spgtree	Information concerning Spanning Tree Protokoll
LANAUTH	LAN authentication (e.g. Public Spot)
SIP-Packet	SIP information which is exchanged between a LANCOM VoIP Router and a SIP provider or upstream SIP PBX
VPN-Status	IPSec and IKE negotiation
VPN-Packet	IPSec and IKE packets

5.1.4 Combination commands

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

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

5.1.5 Trace filters

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

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

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

An operator can be entered as any string of characters, such as the name of a remote station, protocols or ports. The trace filter then processes the output according to the operator rules, much like an Internet search engine. Examples of the application of filters can be seen under 'Examples of traces' → page 5-3.

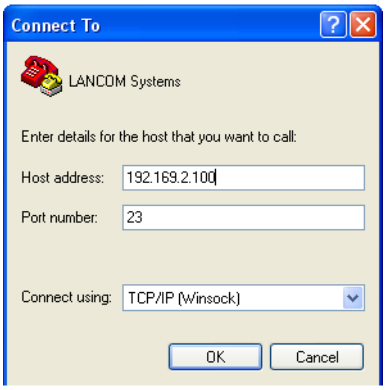
5.1.6 Examples of traces

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

5.1.7 Recording traces

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

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



Enter details for the host that you want to call:

Host address: 192.169.2.100

Port number: 23

Connect using: TCP/IP (Winsock)

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

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

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

5.2 Tracing with LANmonitor

New in LCOS 7.60:

- Saving support files with trace data, device configuration, bootlog and sysinfo
- Automatic backup of trace data
- Trace configuration with Wizards
- Display of show commands
- Display of status information and statistics
- SSL-encrypted Telnet connection

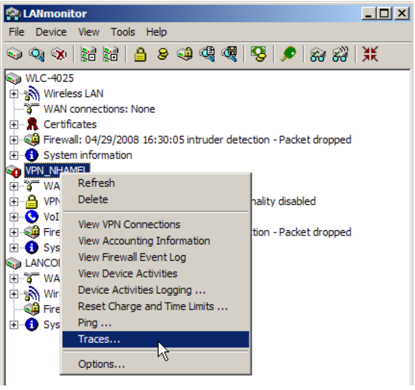
Traces can be executed very easily with LANmonitor. Simply click on the entry for the device with the right-hand mouse key and select **Traces** from the context menu.

> Telnet-access to the device must be enabled to carry out trace requests with LANmonitor. When starting the trace dialog, LANmonitor first attempts to establish an SSL-encrypted Telnet connection to the device. If the device does not support SSL connections, LANmonitor automatically switches to unencrypted Telnet.
> If SNMP access to the device is password-protected, the access data for an administrator with trace rights is also required.

Introduction

The trace function in LANmonitor exceeds the standard trace functions available from Telnet and offers greater convenience in the generation and analysis of traces. For example, the current trace configuration for activating the necessary trace commands can be stored to a configuration file. An experienced service technician can set up a trace configuration and provide it to a less experienced user for executing specialized trace requests for a device. The trace results can also be stored in a file and returned to the technician for analysis.

To open the trace window for a device, right-click the device entry in LANmonitor and select “Traces” from the context menu.



LANmonitor has the following buttons for operating the trace module:

Opens a pre-defined configuration for the trace command. This allows you to carry out trace commands precisely as required by the service technician, for example.

Stores the current trace configuration to be passed on to a user.

Opens a file with trace results for viewing in the trace module.

Saves the current trace results to a file.

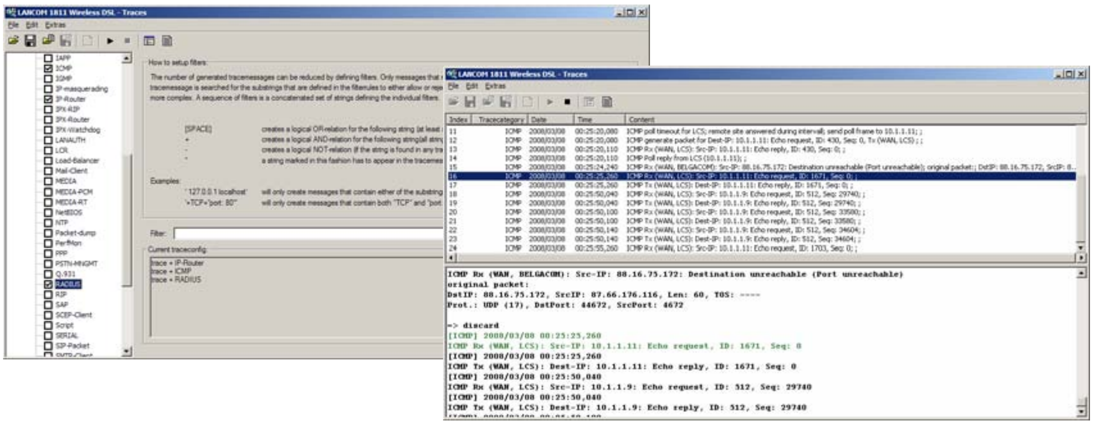
Clears the current display or trace results.

Starts outputting the trace results as produced by the current configuration and automatically switches to the trace-result display mode. As soon as the trace results are returned, the other buttons are deactivated.

Stops the output of trace results.

Switches to the mode for configuring the trace output.

Switches to the mode for displaying the trace output.



The number of generated tracemessages can be reduced by defining filters. Only messages that
tracemessage is searched for the substrings that are defined in the filterrules to either allow or reje
more complex. A sequence of filters is a concatenated set of strings defining the individual filters.

[SPACE]	creates a logical OR-relation for the following string (at least
+	creates a logical AND-relation for the following string(all string
-	creates a logical NOT-relation. If the string is found in any tra
"	a string marked in this fashion has to appear in the tracemes

Examples:

"127.0.0.1 localhost"	will only create messages that contain either of the substring
"+TCP+"port: 80"	will only create messages that contain both "TCP" and "port

Filter:

Current traceconfig:

```
trace + IP-Router
trace + ICMP
trace + RADIUS
```

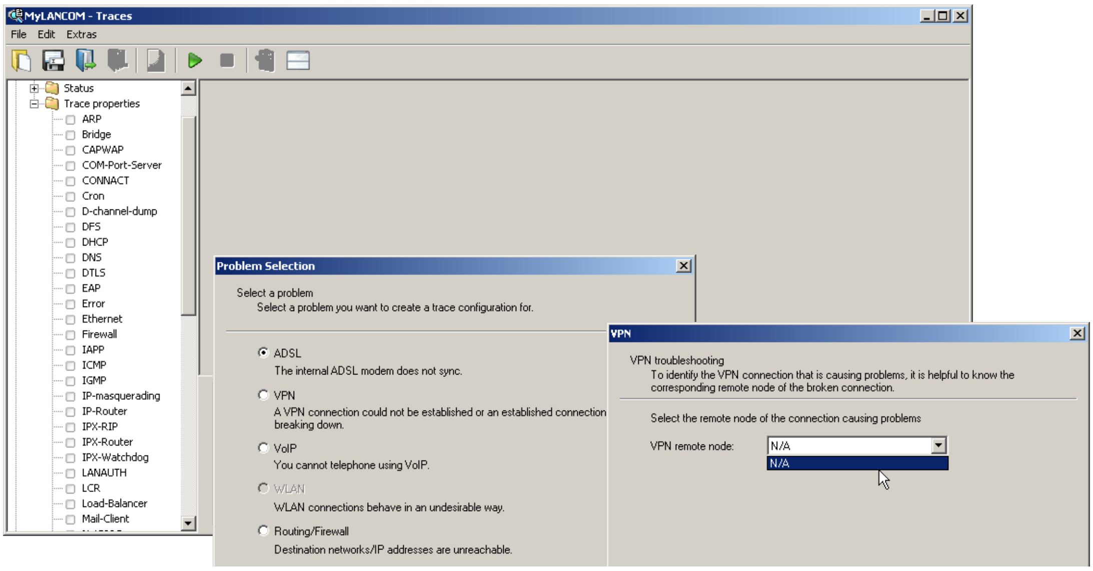
```
Index  Tracecategory  Date        Time          Content
11     ICMP           2008/03/08  00:25:20,080  ICMP poll timeout for LCS; remote site answered during intervall; send poll frame to 10.1.1.11; ;
12     ICMP           2008/03/08  00:25:20,080  ICMP generate packet for Dest-IP: 10.1.1.11: Echo request, ID: 430, Seq: 0, Tx (WAN, LCS) ; ;
13     ICMP           2008/03/08  00:25:20,110  ICMP Rx (WAN, LCS): Src-IP: 10.1.1.11: Echo reply, ID: 430, Seq: 0; ;
14     ICMP           2008/03/08  00:25:20,110  ICMP Poll reply from LCS (10.1.1.11); ;
15     ICMP           2008/03/08  00:25:24,240  ICMP Rx (WAN, BELGACOM): Src-IP: 88.16.75.172: Destination unreachable (Port unreachable); original packet:; DstIP: 88.16.75.172, SrcIP: 8...
16     ICMP           2008/03/08  00:25:25,260  ICMP Rx (WAN, LCS): Src-IP: 10.1.1.11: Echo request, ID: 1671, Seq: 0; ;
17     ICMP           2008/03/08  00:25:25,260  ICMP Tx (WAN, LCS): Dest-IP: 10.1.1.11: Echo reply, ID: 1671, Seq: 0; ;
18     ICMP           2008/03/08  00:25:50,040  ICMP Rx (WAN, LCS): Src-IP: 10.1.1.9: Echo request, ID: 512, Seq: 29740; ;
19     ICMP           2008/03/08  00:25:50,040  ICMP Tx (WAN, LCS): Dest-IP: 10.1.1.9: Echo reply, ID: 512, Seq: 29740; ;
20     ICMP           2008/03/08  00:25:50,100  ICMP Rx (WAN, LCS): Src-IP: 10.1.1.9: Echo request, ID: 512, Seq: 33580; ;
21     ICMP           2008/03/08  00:25:50,100  ICMP Tx (WAN, LCS): Dest-IP: 10.1.1.9: Echo reply, ID: 512, Seq: 33580; ;
22     ICMP           2008/03/08  00:25:50,140  ICMP Rx (WAN, LCS): Src-IP: 10.1.1.9: Echo request, ID: 512, Seq: 34604; ;
23     ICMP           2008/03/08  00:25:50,140  ICMP Tx (WAN, LCS): Dest-IP: 10.1.1.9: Echo reply, ID: 512, Seq: 34604; ;
24     ICMP           2008/03/08  00:25:55,260  ICMP Rx (WAN, LCS): Src-IP: 10.1.1.11: Echo request, ID: 1703, Seq: 0; ;
```

```
ICMP Rx (WAN, BELGACOM): Src-IP: 88.16.75.172: Destination unreachable (Port unreachable)
original packet:
DstIP: 88.16.75.172, SrcIP: 87.66.176.116, Len: 60, TOS: ----
Prot.: UDP (17), DstPort: 44672, SrcPort: 4672

-> discard
[ICMP] 2008/03/08 00:25:25,260
ICMP Rx (WAN, LCS): Src-IP: 10.1.1.11: Echo request, ID: 1671, Seq: 0
[ICMP] 2008/03/08 00:25:25,260
ICMP Tx (WAN, LCS): Dest-IP: 10.1.1.11: Echo reply, ID: 1671, Seq: 0
[ICMP] 2008/03/08 00:25:50,040
ICMP Rx (WAN, LCS): Src-IP: 10.1.1.9: Echo request, ID: 512, Seq: 29740
[ICMP] 2008/03/08 00:25:50,040
ICMP Tx (WAN, LCS): Dest-IP: 10.1.1.9: Echo reply, ID: 512, Seq: 29740
```

Configuring the trace dumps with the Trace Wizard.

The trace settings can be configured very easily with the Wizard. To do this, select **Accompanying Configuration** in the left-hand area of the trace dialog and click **Start Wizard** in the main window. The trace functions can be selected in the following dialogs (such as VPN) and the trace can be further restricted when required (such as to a particular VPN remote site). When ending the Wizard, select whether the Wizard should replace or extend the existing trace configuration.

With the exception of the bootleg trace (contained automatically), all previous trace settings are deleted when the trace configuration is replaced. Save the previous trace configuration for later use whenever required before running the Wizard.



Select a problem
Select a problem you want to create a trace configuration for.

● ADSL
The internal ADSL modem does not sync.

○ VPN
A VPN connection could not be established or an established connection breaking down.

○ VoIP
You cannot telephone using VoIP.

○ WLAN
WLAN connections behave in an undesirable way.

○ Routing/Firewall
Destination networks/IP addresses are unreachable.

VPN troubleshooting
To identify the VPN connection that is causing problems, it is helpful to know the corresponding remote node of the broken connection.

Select the remote node of the connection causing problems

VPN remote node: N/A

N/A

LCOS menu tree of the trace dumps

Going beyond the settings of the Wizard, traces and other displays can be set up precisely using the LCOS menu tree. The LCOS menu tree is divided into three areas:

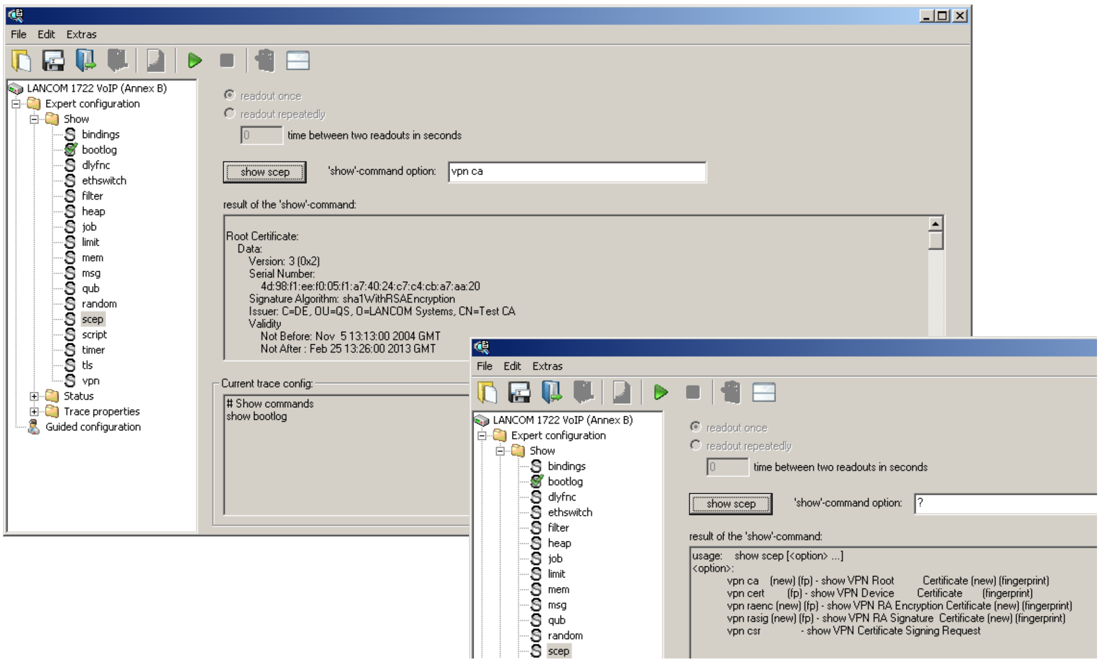
- Show

  Particular information can be retrieved for every device type using a Show command. Show commands are usually used on the command line (Telnet). The call of this Show command is very convenient from the graphical Windows interface in the advanced configuration of the trace.

  To access the current dump of the Show command, click the name of a Show command in the left-hand area of the trace dialog and then the Show button. You may have to/be able to specify additional parameters depending on the entry selected. Enter a question mark in the input field and then click the Show button for information on these parameters.

  To accept the dump of the Show command into the trace data, click the appropriate checkbox to the left of the entry name. For every Show command enabled, it is possible to set whether it is only run once on start of the trace or whether it is run at regular intervals (set in seconds).

The settings of the Show commands are stored in the trace configuration together with the actual trace settings.



● readout once
○ readout repeatedly
0 time between two readouts in seconds

'show'-command option: vpn ca

result of the 'show'-command:

```
Root Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      4d:98:f1:ee:f0:05:f1:a7:40:24:c7:c4:cb:a7:aa:20
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=DE, OU=QS, O=LANCOM Systems, CN=Test CA
    Validity
      Not Before: Nov  5 13:13:00 2004 GMT
      Not After : Feb 25 13:26:00 2013 GMT
```

Current trace config:

```
# Show commands
show bootlog
```

● readout once
○ readout repeatedly
0 time between two readouts in seconds

'show'-command option: ?

result of the 'show'-command:

```
usage:   show scep [<option> ...]
<option>:
         vpn ca    (new) (fp) - show VPN Root         Certificate (new) (fingerprint)
         vpn cert        (fp) - show VPN Device       Certificate       (fingerprint)
         vpn raenc (new) (fp) - show VPN RA Encryption Certificate (new) (fingerprint)
         vpn rasig (new) (fp) - show VPN RA Signature  Certificate (new) (fingerprint)
         vpn csr              - show VPN Certificate Signing Request
```

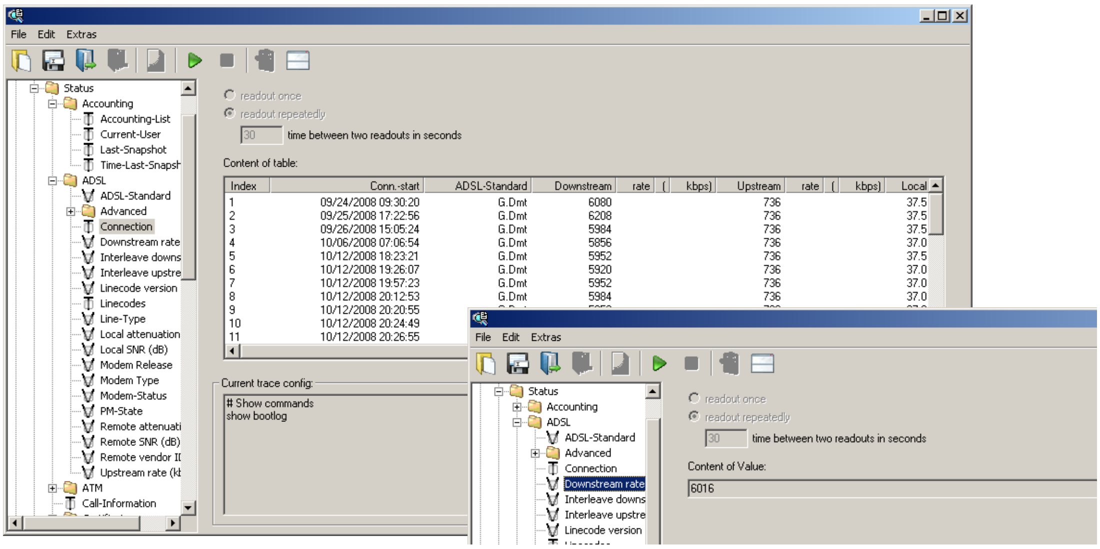
■ Status

Comprehensive status information and statistics on a device can be accessed from the command line (Telnet) or via WEBconfig. All available status information can also be shown via the trace dialog. Tables and individual values are shown using special icons.

To display the current contents of the table or value, click the name of a status entry in the left-hand area of the trace dialogue.

To accept the dump of the Status entry into the trace data, click the appropriate checkbox to the left of the entry name. For every Status entry enabled, a setting defines whether it is read out once only on starting the trace or whether it is read out at regular intervals (set in seconds).

The settings of the Status information are stored in the trace configuration together with the actual trace settings. Status information is stored together with the actual trace data.



○ readout once
● readout repeatedly
30 time between two readouts in seconds

Content of table:

Index	Conn.-start	ADSL-Standard	Downstream	rate	(	kbps)	Upstream	rate	(	kbps)	Local
1	09/24/2008 09:30:20	G.Dmt	6080				736				37.5
2	09/25/2008 17:22:56	G.Dmt	6208				736				37.5
3	09/26/2008 15:05:24	G.Dmt	5984				736				37.5
4	10/06/2008 07:06:54	G.Dmt	5856				736				37.0
5	10/12/2008 18:23:21	G.Dmt	5952				736				37.5
6	10/12/2008 19:26:07	G.Dmt	5920				736				37.0
7	10/12/2008 19:57:23	G.Dmt	5952				736				37.0
8	10/12/2008 20:12:53	G.Dmt	5984				736				37.0
9	10/12/2008 20:20:55										
10	10/12/2008 20:24:49										
11	10/12/2008 20:26:55										

Current trace config:

```
# Show commands
show bootlog
```

○ readout once
● readout repeatedly
30 time between two readouts in seconds

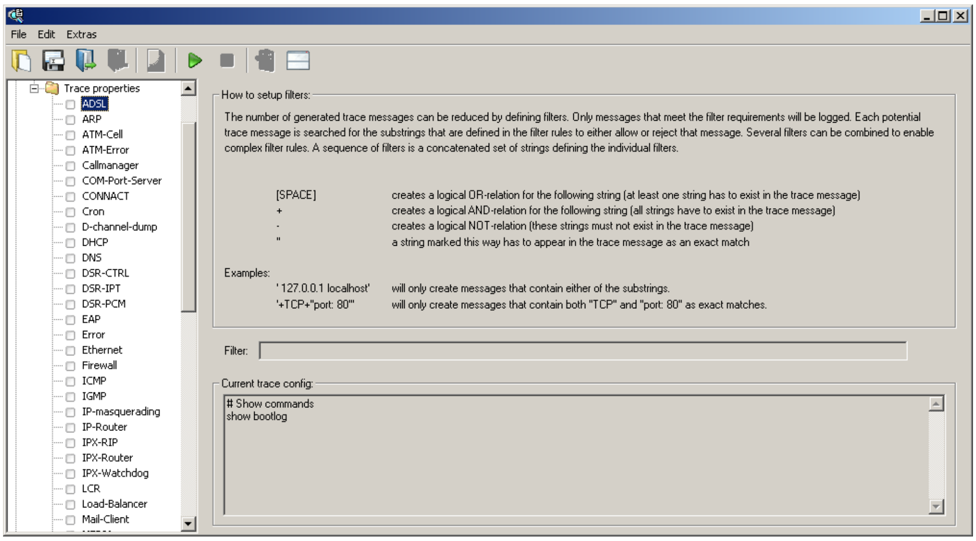
Content of Value:

6016

■ Trace settings

The traces to be dumped for the current device can be enabled in the trace settings area.

To accept the dump of the trace into the trace data, click the appropriate checkbox to the left of the entry name. A filter can be entered for every trace. For example, if you want to display only the IP traces of a particular workstation, enter the appropriate IP address as a filter of the IP router trace.



How to setup filters:

The number of generated trace messages can be reduced by defining filters. Only messages that meet the filter requirements will be logged. Each potential trace message is searched for the substrings that are defined in the filter rules to either allow or reject that message. Several filters can be combined to enable complex filter rules. A sequence of filters is a concatenated set of strings defining the individual filters.

[SPACE]	creates a logical OR-relation for the following string (at least one string has to exist in the trace message)
+	creates a logical AND-relation for the following string (all strings have to exist in the trace message)
-	creates a logical NOT-relation (these strings must not exist in the trace message)
"	a string marked this way has to appear in the trace message as an exact match

Examples:

' 127.0.0.1 localhost'	will only create messages that contain either of the substrings.
'+TCP+"port: 80"'	will only create messages that contain both "TCP" and "port: 80" as exact matches.

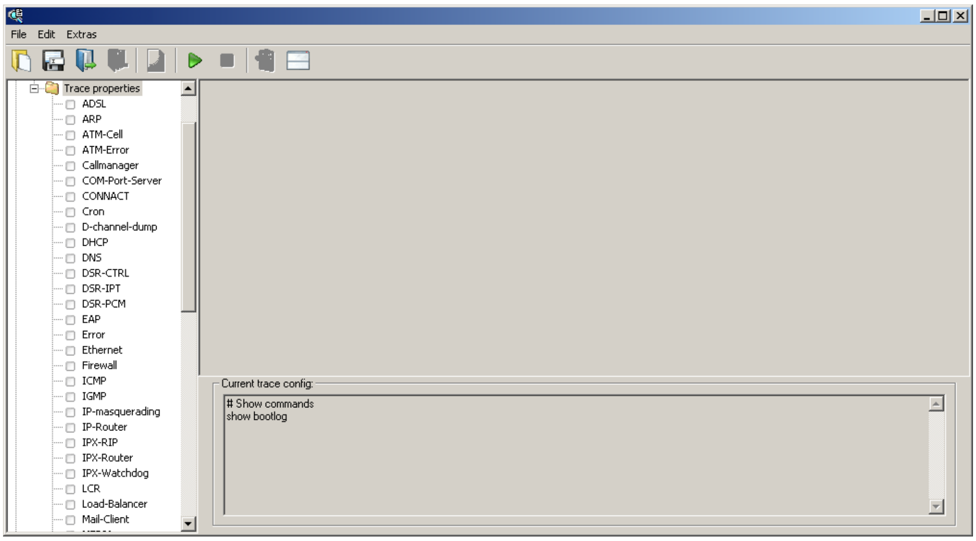
Filter:

Current trace config:

```
# Show commands
show bootlog
```

Display of trace data

The entire trace configuration is shown in the lower area of the dialog where all active Trace, Status and Show entries are listed with the respective filters and parameters.



Current trace config:

```
# Show commands
show bootlog
```

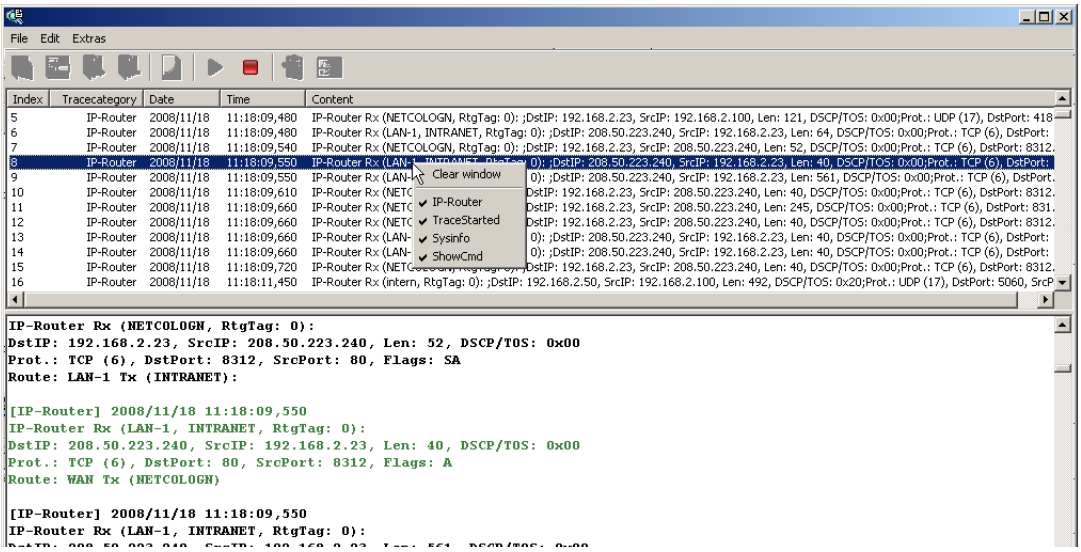
To start the dump of the trace data, change to Display mode with the Start button. The ongoing trace dumps are displayed in this view:

- The trace events are listed chronologically in the upper area.
- The lower area lists the results of the events in sequence.

For easier navigation within long trace dumps, click a trace event in the upper area. The appropriate result is then enabled in the list and highlighted green.

Right-clicking a trace event opens up a context menu from where individual trace results can be shown/hidden.

Trace data is collected as long as the trace dump is enabled. To prevent overloading the main workstation memory using LANmonitor, trace data is automatically written to a backup file. The time intervals and the maximum size of a backup file can be set with **Extras** ▶ **Other Settings** ▶ **Trace backup**.



Index	Tracecategory	Date	Time	Content
5	IP-Router	2008/11/18	11:18:09,480	IP-Router Rx (NETCOLOGN, RtgTag: 0): ;DstIP: 192.168.2.23, SrcIP: 192.168.2.100, Len: 121, DSCP/TOS: 0x00;Prot.: UDP (17), DstPort: 418
6	IP-Router	2008/11/18	11:18:09,480	IP-Router Rx (LAN-1, INTRANET, RtgTag: 0): ;DstIP: 208.50.223.240, SrcIP: 192.168.2.23, Len: 64, DSCP/TOS: 0x00;Prot.: TCP (6), DstPort:
7	IP-Router	2008/11/18	11:18:09,540	IP-Router Rx (NETCOLOGN, RtgTag: 0): ;DstIP: 192.168.2.23, SrcIP: 208.50.223.240, Len: 52, DSCP/TOS: 0x00;Prot.: TCP (6), DstPort: 8312.
8	IP-Router	2008/11/18	11:18:09,550	IP-Router Rx (LAN- 0): ;DstIP: 208.50.223.240, SrcIP: 192.168.2.23, Len: 40, DSCP/TOS: 0x00;Prot.: TCP (6), DstPort:
9	IP-Router	2008/11/18	11:18:09,550	IP-Router Rx (LAN- 0): ;DstIP: 208.50.223.240, SrcIP: 192.168.2.23, Len: 561, DSCP/TOS: 0x00;Prot.: TCP (6), DstPort.
10	IP-Router	2008/11/18	11:18:09,610	IP-Router Rx (NETC DstIP: 192.168.2.23, SrcIP: 208.50.223.240, Len: 40, DSCP/TOS: 0x00;Prot.: TCP (6), DstPort: 8312.
11	IP-Router	2008/11/18	11:18:09,660	IP-Router Rx (NETC DstIP: 192.168.2.23, SrcIP: 208.50.223.240, Len: 245, DSCP/TOS: 0x00;Prot.: TCP (6), DstPort: 831.
12	IP-Router	2008/11/18	11:18:09,660	IP-Router Rx (NETC DstIP: 192.168.2.23, SrcIP: 208.50.223.240, Len: 40, DSCP/TOS: 0x00;Prot.: TCP (6), DstPort: 8312.
13	IP-Router	2008/11/18	11:18:09,660	IP-Router Rx (LAN- 0): ;DstIP: 208.50.223.240, SrcIP: 192.168.2.23, Len: 40, DSCP/TOS: 0x00;Prot.: TCP (6), DstPort:
14	IP-Router	2008/11/18	11:18:09,660	IP-Router Rx (LAN- 0): ;DstIP: 208.50.223.240, SrcIP: 192.168.2.23, Len: 40, DSCP/TOS: 0x00;Prot.: TCP (6), DstPort:
15	IP-Router	2008/11/18	11:18:09,720	IP-Router Rx (NETC DstIP: 192.168.2.23, SrcIP: 208.50.223.240, Len: 40, DSCP/TOS: 0x00;Prot.: TCP (6), DstPort: 8312.
16	IP-Router	2008/11/18	11:18:11,450	IP-Router Rx (intern, RtgTag: 0): ;DstIP: 192.168.2.50, SrcIP: 192.168.2.100, Len: 492, DSCP/TOS: 0x20;Prot.: UDP (17), DstPort: 5060, SrcP

```
IP-Router Rx (NETCOLOGN, RtgTag: 0):
DstIP: 192.168.2.23, SrcIP: 208.50.223.240, Len: 52, DSCP/TOS: 0x00
Prot.: TCP (6), DstPort: 8312, SrcPort: 80, Flags: SA
Route: LAN-1 Tx (INTRANET):

[IP-Router] 2008/11/18 11:18:09,550
IP-Router Rx (LAN-1, INTRANET, RtgTag: 0):
DstIP: 208.50.223.240, SrcIP: 192.168.2.23, Len: 40, DSCP/TOS: 0x00
Prot.: TCP (6), DstPort: 80, SrcPort: 8312, Flags: A
Route: WAN Tx (NETCOLOGN)

[IP-Router] 2008/11/18 11:18:09,550
IP-Router Rx (LAN-1, INTRANET, RtgTag: 0):
DstIP: 208.50.223.240, SrcIP: 192.168.2.23, Len: 561, DSCP/TOS: 0x00
```

Backing up and restoring the trace configuration

The entire configuration of the trace dump can be written to a storage medium for later re-use or for transfer to another user. Click on **File ▶ Store trace configuration** and re-open it later with **File ▶ Load trace configuration**.

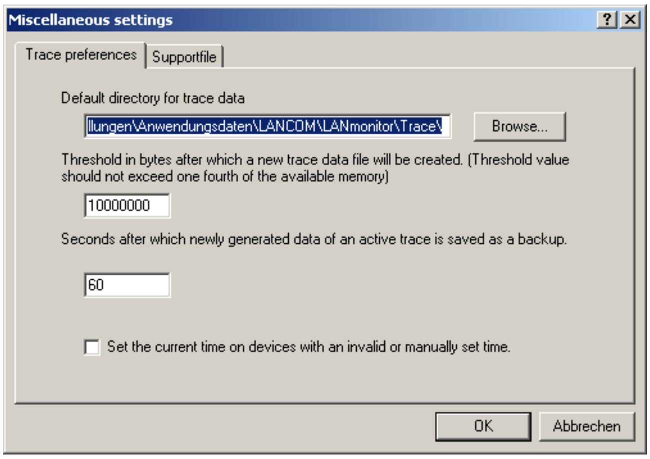
Backing up and restoring the trace data

For later editing, or for transfer to another user, the actual trace data can be written to a storage medium with **File ▶ Store trace data** and later re-opened with **File ▶ Load trace data** .

Backup settings for traces

When starting a trace with LANmonitor, a backup file with the current trace data is automatically saved. The settings for the trace backup can be configured with **Extras ▶ Other settings ▶ Trace backup**. Enter the following parameters:

- Directory for the trace backups
- Maximum size of a trace backup file. If this file size is reached with an active trace, another trace backup file is created automatically.
- Save interval of the trace backup file. When this time has elapsed, an updated version of the trace backup file is saved automatically. The trace backup file therefore does not contain the information from the most recent backup up to the current time.
- LANmonitor can set current workstation time as a time for the trace, for example when the traced device itself does not have valid time information.



Default directory for trace data

llungen\Anwendungsdaten\LANCOM\LANmonitor\Trace\

Threshold in bytes after which a new trace data file will be created. (Threshold value should not exceed one fourth of the available memory)

10000000

Seconds after which newly generated data of an active trace is saved as a backup.

60

□ Set the current time on devices with an invalid or manually set time.

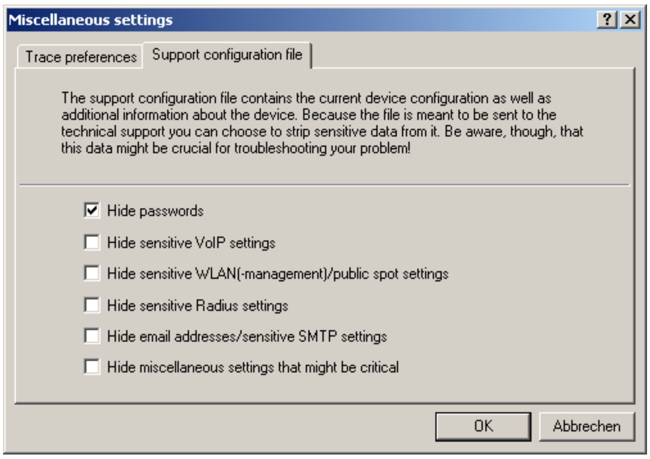
Saving support file

A support file enables all information pertaining to support to be easily written to one file:

- Trace data as configured in the current settings (such as with function “Save trace data”)
- Current device configuration
- Bootlog

- Sysinfo

When saving the device configuration, security-related information of no relevance to support can be hidden. Use **Extras ▶ Other settings ▶ Support file** in the trace window to select which information is not to be saved in the support file:



The support configuration file contains the current device configuration as well as additional information about the device. Because the file is meant to be sent to the technical support you can choose to strip sensitive data from it. Be aware, though, that this data might be crucial for troubleshooting your problem!

☑ Hide passwords
☐ Hide sensitive VoIP settings
☐ Hide sensitive WLAN(-management)/public spot settings
☐ Hide sensitive Radius settings
☐ Hide email addresses/sensitive SMTP settings
☐ Hide miscellaneous settings that might be critical

The support file created this way contains text-based information. The file can be opened using an editor or checked for any critical entries.

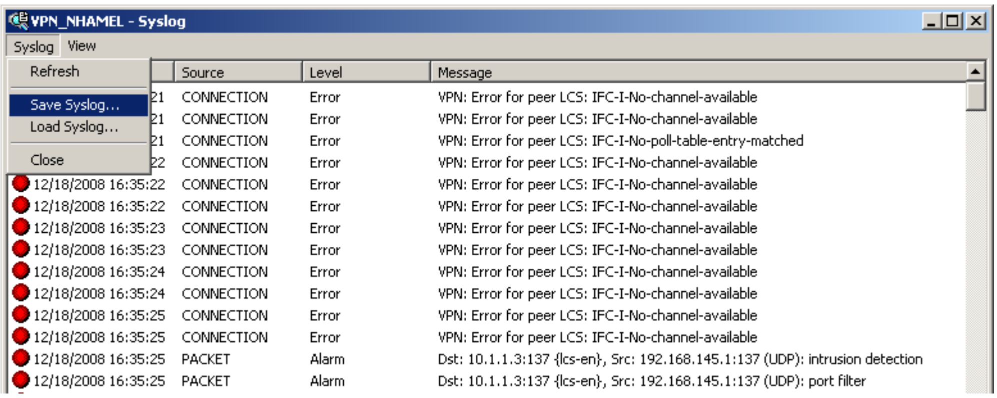
5.3 SYSLOG

5.3.1 Introduction

The SYSLOG protocol is used to log the activities of a LANCOM device. This function is especially interesting for system administrators as it records a a complete history of all activities in the device. The information captured in the SYSLOG log can be viewed in different ways:

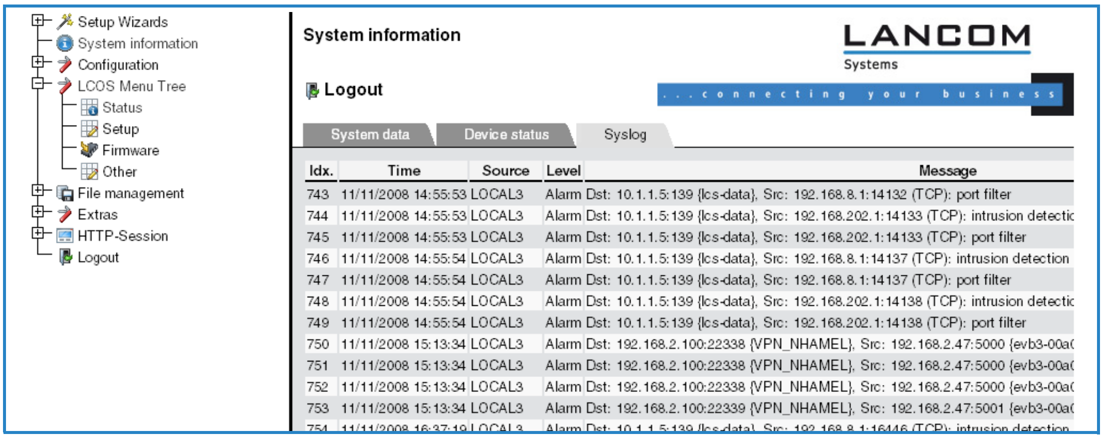
- SYSLOG messages can be sent to a central "collection point", a so-called SYSLOG client or SYSLOG daemon. This option is useful, for example, when messages from a large number of devices are to be logged.
  - Logging under UNIX/Linux is generally performed by the SYSLOG daemon that is set up as standard in these operating systems. The daemon either establishes contact with the console or writes its log to an appropriate SYSLOG file. The file `/etc/syslog.conf` contains a definition of which facilities (more on this term later) should be written to which log file. Please check your daemon's configuration to see if it explicitly listens to network connections.
  - Windows does not provide a corresponding system function. You require special software to provide the functionality of a SYSLOG daemon.
  - Syslog in the device memory.
- To extend the output of the SYSLOG information over an appropriate SYSLOG client, the most recent SYSLOG messages are stored in the device's RAM. Depending on the memory fitted, this can vary from 100 to 2048 syslog messages. These internal syslogs can be viewed in various ways:
  - In the device statistics via the command line, e.g. with telnet
  - In WEBconfig under /System information/Syslog
  - LANmonitor additionally lets you export the syslog from the device and save it to a file. Simply click on the entry for the device with the right mouse button and select **View Syslog** from the context menu. A snapshot of the current status is displayed. Clicking on **Refresh** exports a copy of the current syslog and this is dispayed in the window. **Save syslog...** stores the current display to a file. The content of syslog files can be viewed with **Load syslog...**.

SYSLOG messages will only be written to the device's internal memory if the LANCOM was entered as a SYSLOG client with the loopback address 127.0.0.1.



```
                     Source       Level   Message
21                   CONNECTION   Error   VPN: Error for peer LCS: IFC-I-No-channel-available
21                   CONNECTION   Error   VPN: Error for peer LCS: IFC-I-No-channel-available
21                   CONNECTION   Error   VPN: Error for peer LCS: IFC-I-No-poll-table-entry-matched
22                   CONNECTION   Error   VPN: Error for peer LCS: IFC-I-No-channel-available
12/18/2008 16:35:22  CONNECTION   Error   VPN: Error for peer LCS: IFC-I-No-channel-available
12/18/2008 16:35:22  CONNECTION   Error   VPN: Error for peer LCS: IFC-I-No-channel-available
12/18/2008 16:35:23  CONNECTION   Error   VPN: Error for peer LCS: IFC-I-No-channel-available
12/18/2008 16:35:23  CONNECTION   Error   VPN: Error for peer LCS: IFC-I-No-channel-available
12/18/2008 16:35:24  CONNECTION   Error   VPN: Error for peer LCS: IFC-I-No-channel-available
12/18/2008 16:35:24  CONNECTION   Error   VPN: Error for peer LCS: IFC-I-No-channel-available
12/18/2008 16:35:25  CONNECTION   Error   VPN: Error for peer LCS: IFC-I-No-channel-available
12/18/2008 16:35:25  CONNECTION   Error   VPN: Error for peer LCS: IFC-I-No-channel-available
12/18/2008 16:35:25  PACKET       Alarm   Dst: 10.1.1.3:137 {lcs-en}, Src: 192.168.145.1:137 (UDP): intrusion detection
12/18/2008 16:35:25  PACKET       Alarm   Dst: 10.1.1.3:137 {lcs-en}, Src: 192.168.145.1:137 (UDP): port filter
```

Alternatively you can view the current SYSLOG messages on the first page of WEBconfig on the SYSLOG tab:



```
Idx. Time                Source Level Message
743  11/11/2008 14:55:53 LOCAL3 Alarm Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.8.1:14132 (TCP): port filter
744  11/11/2008 14:55:53 LOCAL3 Alarm Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.202.1:14133 (TCP): intrusion detectic
745  11/11/2008 14:55:53 LOCAL3 Alarm Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.202.1:14133 (TCP): port filter
746  11/11/2008 14:55:54 LOCAL3 Alarm Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.8.1:14137 (TCP): intrusion detection
747  11/11/2008 14:55:54 LOCAL3 Alarm Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.8.1:14137 (TCP): port filter
748  11/11/2008 14:55:54 LOCAL3 Alarm Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.202.1:14138 (TCP): intrusion detectic
749  11/11/2008 14:55:54 LOCAL3 Alarm Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.202.1:14138 (TCP): port filter
750  11/11/2008 15:13:34 LOCAL3 Alarm Dst: 192.168.2.100:22338 {VPN_NHAMEL}, Src: 192.168.2.47:5000 {evb3-00a(
751  11/11/2008 15:13:34 LOCAL3 Alarm Dst: 192.168.2.100:22338 {VPN_NHAMEL}, Src: 192.168.2.47:5000 {evb3-00a(
752  11/11/2008 15:13:34 LOCAL3 Alarm Dst: 192.168.2.100:22338 {VPN_NHAMEL}, Src: 192.168.2.47:5000 {evb3-00a(
753  11/11/2008 15:13:34 LOCAL3 Alarm Dst: 192.168.2.100:22339 {VPN_NHAMEL}, Src: 192.168.2.47:5001 {evb3-00a(
754  11/11/2008 16:37:19 LOCAL3 Alarm Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.8.1:16446 (TCP): intrusion detection
```

5.3.2 Structure of SYSLOG messages

SYSLOG messages consist of three parts:

- Priority
- Header
- Contents

Priority

The priority in a SYSLOG message contains information about the the message severity and the facility (service or component that triggered the message).

The eight severity levels originally defined in SYSLOG have been reduced to five levels in the LANCOM. The table below shows the correlation between the LANCOM alarm level, the meaning and the SYSLOG severities.

Priority	Meaning	SYSLOG severity
Alarm	This category includes all messages requiring the system administrator's close attention.	PANIC, ALERT, CRIT
Error	All error messages which can occur under normal conditions are communicated at this level; no special attention is required by the administrator (e.g. connection errors).	ERROR
Warning	This level communicates messages which do not compromise normal operating conditions.	WARNING
Information	At this level, all messages are sent that have a purely informational character (e.g. accounting information).	NOTICE, INFORM
Debug	Communication of all debug messages. Debug messages generate large data volumes and can compromise the device's operation. For this reason they should be disabled for normal operations and only used for troubleshooting.	DEBUG

The table below provides an overview of the meaning of all internal message sources that you can set in the LANCOM. The final column in the table also provides the standard correlation between the internal sources of the LANCOM and the SYSLOG facilities. This mapping can be changed, if necessary.

Source	Meaning	Facility
System	System messages (boot events, timer system, etc.)	KERNEL
Logins	Messages concerning the user's login or logout during the PPP negotiation, and any errors that occur during this.	AUTH
System time	Messages about changes to the system time	CRON
Console logins	Messages about console logins (Telnet, Outband, etc.), logouts and any errors that occurred during this.	AUTHPRIV
Connections	Messages about establishment and termination of connections and any errors that occurred (display trace)	LOCAL0
Accounting	Accounting information stored after termination of a connection (user, online time, transfer volumes)	LOCAL1
Administration	Messages on changes to the configuration, remotely executed commands, etc.	LOCAL2
Router	Regular statistics about the most frequently used services (breakdown per port number) and messages about filtered packets, routing errors, etc.	LOCAL3

Header

The header contains the name or the IP address of the device which sent the SYSLOG message. The chronological sequence is also very important for evaluating the messages. Time information is only added to the messages at the SYSLOG client in order not to disturb their chronological consistency due to different device times.

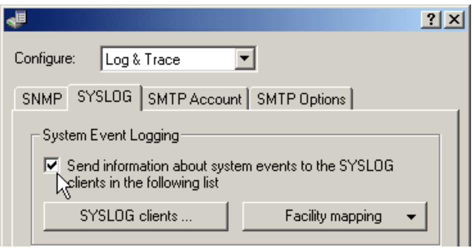
The LANCOM devices must have a valid time stamp for the evaluation of the SYSLOG messages in internal memory.

Contents

The actual contents of the SYSLOG messages describe the event, for example a login occurrence, the establishment of a WAN connection, or firewall activities.

5.3.3 Configuring SYSLOG using LANconfig

You can find the parameters to configure SYSLOG under LANconfig in the configuration area "Log & Trace" on the "SYSLOG" tab.



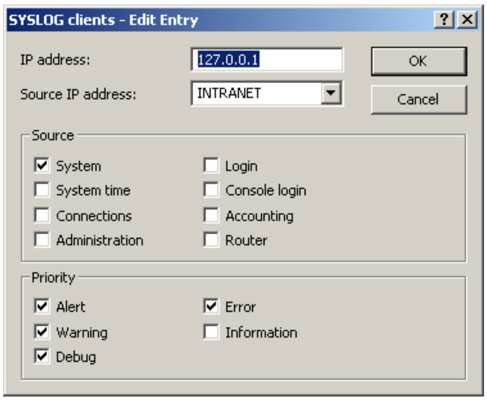
Configure: Log & Trace

System Event Logging

☑ Send information about system events to the SYSLOG clients in the following list

Creating SYSLOG clients

When setting up a SYSLOG client, first define the IP address to which SYSLOG messages are to be sent. As an option, you can define a different sending IP address. To do this, select which of the internal LANCOM sources are to send messages to this SYSLOG client. You can further restrict the volume of messages by selecting certain priorities, for example only alarm and error messages.



SYSLOG clients - Edit Entry

IP address: 127.0.0.1

Source IP address: INTRANET

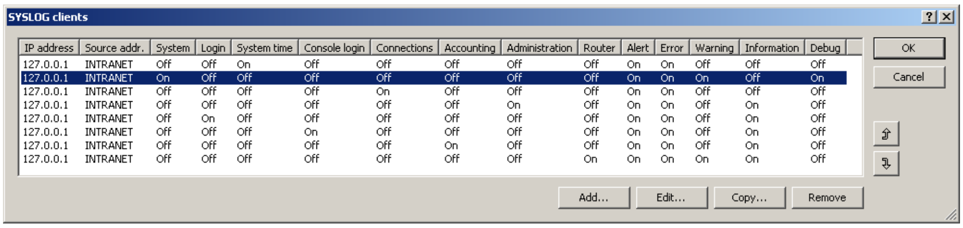
Source

☑ System ☐ Login
☐ System time ☐ Console login
☐ Connections ☐ Accounting
☐ Administration ☐ Router

Priority

☑ Alert ☑ Error
☑ Warning ☐ Information
☑ Debug

As of LCOS version 7.6 the table of syslog clients (factory settings) is set up to display important events which are relevant to diagnostics, and to save these to the internal syslog memory. The following screenshot shows these pre-defined syslog clients under LANconfig:



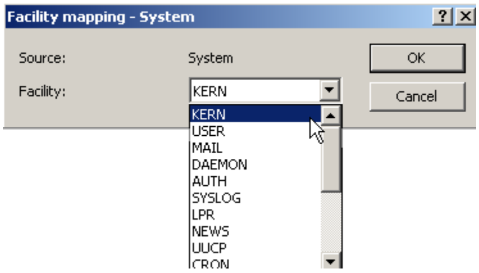
IP address	Source addr.	System	Login	System time	Console login	Connections	Accounting	Administration	Router	Alert	Error	Warning	Information	Debug
127.0.0.1	INTRANET	Off	Off	On	Off	Off	Off	Off	Off	On	On	Off	Off	Off
127.0.0.1	INTRANET	On	Off	Off	Off	Off	Off	Off	Off	On	On	On	Off	On
127.0.0.1	INTRANET	Off	Off	Off	Off	On	Off	Off	Off	On	On	Off	Off	Off
127.0.0.1	INTRANET	Off	Off	Off	Off	Off	Off	On	Off	On	On	Off	On	Off
127.0.0.1	INTRANET	Off	On	Off	Off	Off	Off	Off	Off	On	On	Off	On	Off
127.0.0.1	INTRANET	Off	Off	Off	On	Off	Off	Off	Off	On	On	Off	On	Off
127.0.0.1	INTRANET	Off	Off	Off	Off	Off	On	Off	Off	On	On	Off	On	Off
127.0.0.1	INTRANET	Off	Off	Off	Off	Off	Off	Off	On	On	On	On	On	Off

Further information about the meaning of the pre-defined syslog clients and the update options for existing LANCOM devices are to be found in the section "Table of syslog clients" for the configuration of syslog via telnet or WEBconfig.

Assigning internal LANCOM sources to SYSLOG facilities

The SYSLOG protocol uses certain designations for message sources, the so-called facilities. Each internal source in the LANCOM devices that can generate a SYSLOG message must therefore be assigned to a SYSLOG facility.

The standard mapping can be changed, if necessary. So, for example, all SYSLOG messages from a LANCOM can be sent with a certain facility (Local7). It is thus possible to collect all LANCOM messages in a common log file by configuring the SYSLOG client appropriately.



Source: System

Facility: KERN

5.3.4 Configuring SYSLOG using Telnet or WEBconfig

Path: Setup/SYSLOG

- **Active**

  Activates the dispatch of information about system events to the configured SYSLOG client.

- **Port**

  Port used for sending SYSLOG messages.

Facility mapping

Path: Setup/SYSLOG/Facility-Mapper

- **Facility**

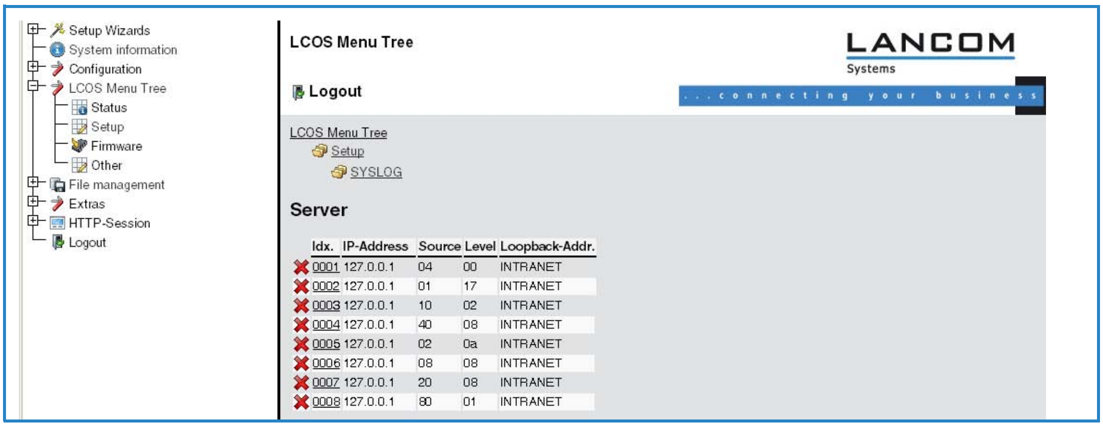
  Mapping sources to specific facilities.

- **Source**

  Mapping sources to specific facilities.

Table of SYSLOG clients

As of LCOS version 7.6 the table of syslog clients (factory settings) is set up to display important events which are relevant to diagnostics, and to save these to the internal syslog memory. The following screenshot shows these pre-defined syslog clients under WEBconfig:



Server

Idx.	IP-Address	Source	Level	Loopback-Addr.
0001	127.0.0.1	04	00	INTRANET
0002	127.0.0.1	01	17	INTRANET
0003	127.0.0.1	10	02	INTRANET
0004	127.0.0.1	40	08	INTRANET
0005	127.0.0.1	02	0a	INTRANET
0006	127.0.0.1	08	08	INTRANET
0007	127.0.0.1	20	08	INTRANET
0008	127.0.0.1	80	01	INTRANET

WEBconfig: LCOS menu tree ▶ Setup ▶ SYSLOG ▶ SYSLOG table

All pre-defined syslog clients transmit the messages to the IP address 127.0.0.1, i.e. to the LANCOM itself. The sender IP address is the IP address from the "INTRANET" network. Individual entries have the following functions:

Index	Source	Level	Meaning
0001	04	00	System time without a specifiied level
0002	01	17	System messages with the level alarm, error, alert or debug.
0003	10	02	Connection messages with the level error.
0004	40	08	Management messages with the level information.
0005	02	0a	Logins with the level error or information.
0006	08	08	Console logins with the level information.
0007	20	08	Accounting messages with the level information.
0008	80	01	Router messages with the level alarm.

If you update an existing device, the settings for SYSLOG are **not** set to this default value, so that any existing settings are retained. In this case you can enter the settings according to this table. Alternatively you will find a script for automatically installing pre-defined syslog clients on the LANCOM Web site in the "KnowledgeBase".

- **Idx.**
  Position of the entry in the table.
- **IP address**
  IP address of the SYSLOG client.
- **Source**
  Source that caused the message to be sent. Each source is represented by a certain code.
- **Level**
  SYSLOG level with which the message is sent. Each level is represented by a certain code.
- **Loopback address**
  This is where you can configure an optional sender address for use instead of that automatically selected for the destination address.

5.4 The ping command

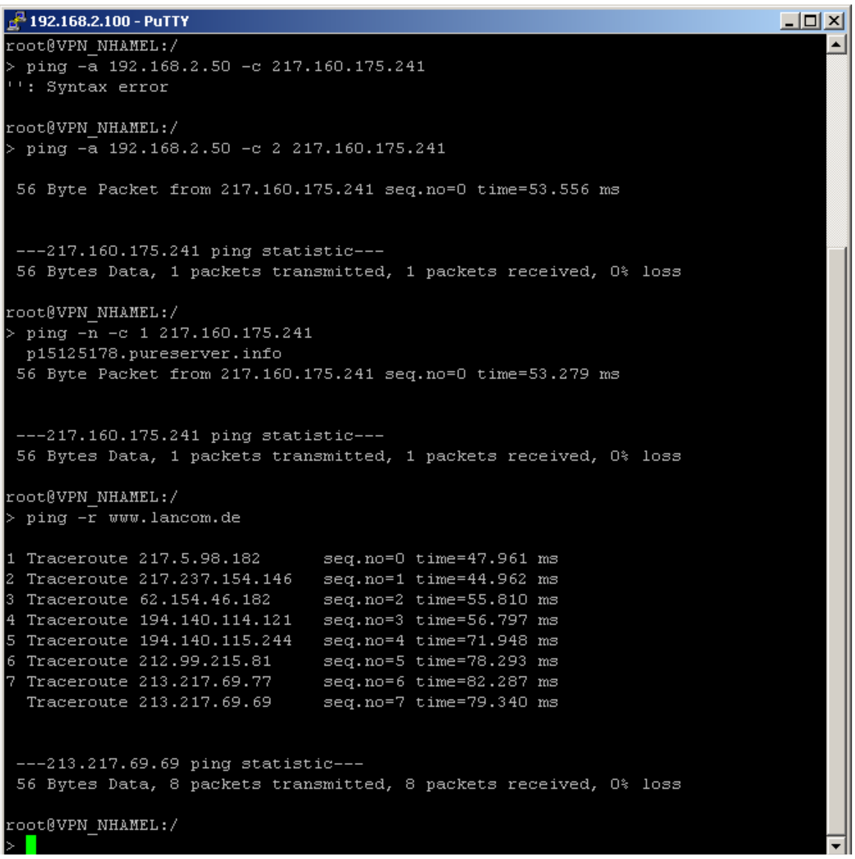
With the ping command in Telnet or in a terminal connection an „ICMP Echo Request" is sent to the addressed host. As long as the recipient provides the protocol and the request is not filtered by the firewall, the addressed host answers with an „ICMP Echo Reply". In case the host is not available, the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

The syntax of the ping commando is:

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

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

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



```
root@VPN_NHAMEL:/
> ping -a 192.168.2.50 -c 217.160.175.241
'': Syntax error

root@VPN_NHAMEL:/
> ping -a 192.168.2.50 -c 2 217.160.175.241

 56 Byte Packet from 217.160.175.241 seq.no=0 time=53.556 ms


 ---217.160.175.241 ping statistic---
 56 Bytes Data, 1 packets transmitted, 1 packets received, 0% loss

root@VPN_NHAMEL:/
> ping -n -c 1 217.160.175.241
  p15125178.pureserver.info
 56 Byte Packet from 217.160.175.241 seq.no=0 time=53.279 ms


 ---217.160.175.241 ping statistic---
 56 Bytes Data, 1 packets transmitted, 1 packets received, 0% loss

root@VPN_NHAMEL:/
> ping -r www.lancom.de

1 Traceroute 217.5.98.182      seq.no=0 time=47.961 ms
2 Traceroute 217.237.154.146   seq.no=1 time=44.962 ms
3 Traceroute 62.154.46.182     seq.no=2 time=55.810 ms
4 Traceroute 194.140.114.121   seq.no=3 time=56.797 ms
5 Traceroute 194.140.115.244   seq.no=4 time=71.948 ms
6 Traceroute 212.99.215.81     seq.no=5 time=78.293 ms
7 Traceroute 213.217.69.77     seq.no=6 time=82.287 ms
  Traceroute 213.217.69.69     seq.no=7 time=79.340 ms


 ---213.217.69.69 ping statistic---
 56 Bytes Data, 8 packets transmitted, 8 packets received, 0% loss

root@VPN_NHAMEL:/
>
```

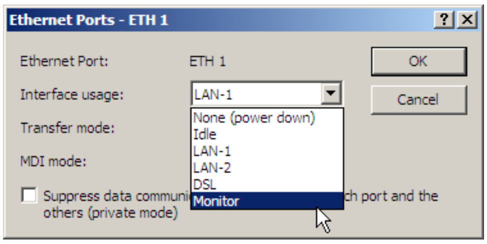
5.5 Monitoring the switch

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

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

LANconfig

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



Ethernet Ports - ETH 1

Ethernet Port: ETH 1

Interface usage: LAN-1

Transfer mode:

MDI mode:

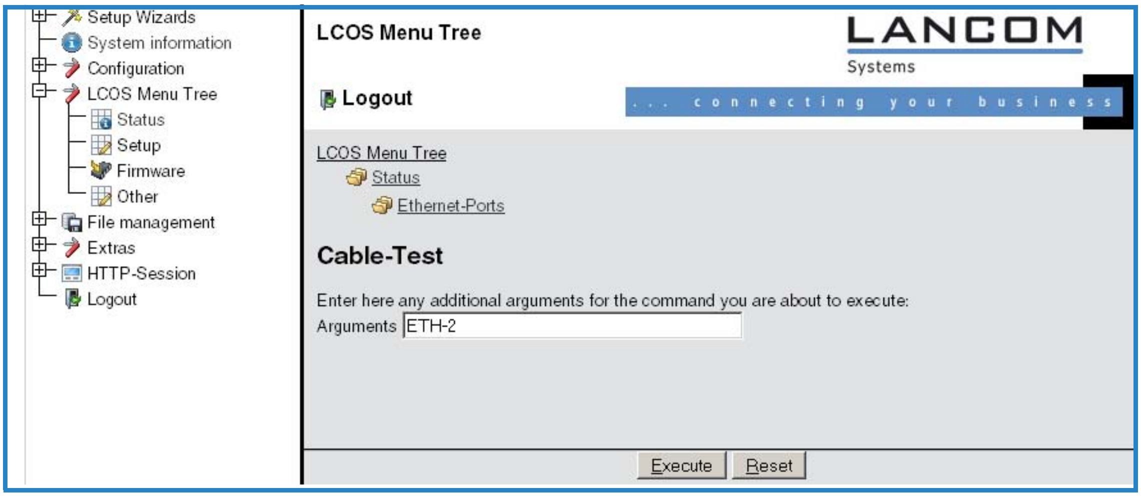
□ Suppress data communi… ch port and the others (private mode)

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ Ethernet-Ports.

5.6 Cable testing

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

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



LCOS Menu Tree

Logout

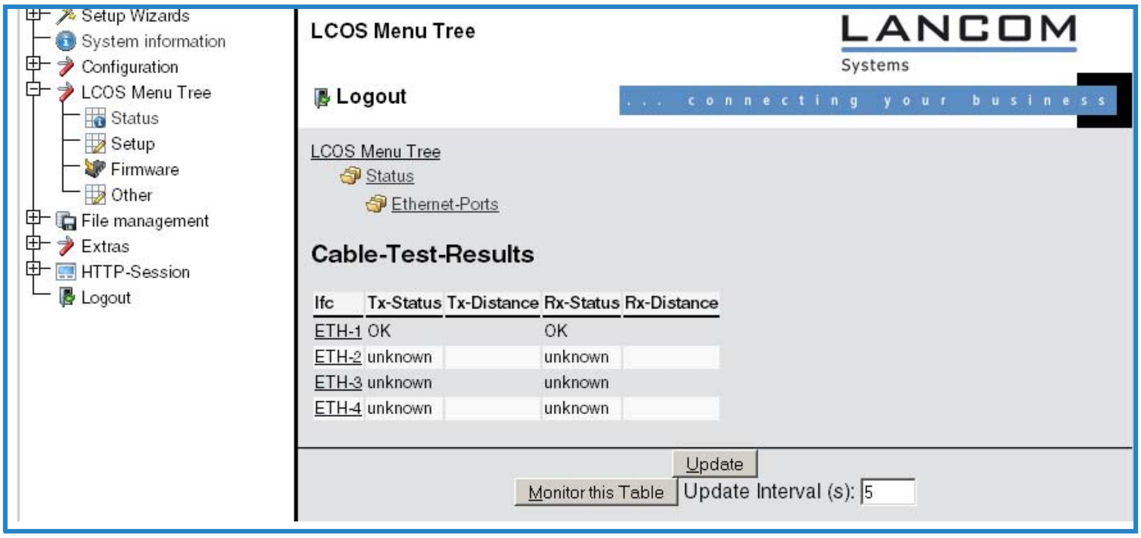
LCOS Menu Tree
Status
Ethernet-Ports

Cable-Test

Enter here any additional arguments for the command you are about to execute:

Arguments: ETH-2

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



LCOS Menu Tree

Logout

LCOS Menu Tree
Status
Ethernet-Ports

Cable-Test-Results

Ifc	Tx-Status	Tx-Distance	Rx-Status	Rx-Distance
ETH-1	OK		OK	
ETH-2	unknown		unknown	
ETH-3	unknown		unknown	
ETH-4	unknown		unknown	

Update Interval (s): 5

The following results can occur:

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

6 Security

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

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

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

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

- 'Firewall' → page 8-1
- 'IP masquerading' → page 7-16
- 'Virtual LANs (VLANs)' → page 12-1

6.1 Protection for the configuration

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

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

6.1.1 Password protection

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

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

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

Tips for proper use of passwords

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

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

Capital and small letters are distinguished in the configuration password.

- **Never use a password twice.**
  If you use the same password for several purposes, you reduce its security effect. If the other end is not secure, you also endanger all other connections for which you use this password at once.

- **Change the password regularly.**
  Passwords should be changed as frequently as possible. This requires effort, however considerably increases the security of the password.
- **Change the password immediately if you suspect someone else knows it.**
  If an employee with access to a password leaves the company, it is high time to change this password. A password should also always be changed when there is the slightest suspicion of a leak.

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

Entering the password

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

LANconfig: Management ▶ Admin ▶ Password

WEBconfig: Tool ▶ Change password

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.

LANconfig: Management ▶ Admin ▶ Password required for SNMP read permission

WEBconfig: LCOS menu tree ▶ Setup ▶ SNMP ▶ Password- required-for-SNMP-read-access

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`)

LANconfig: Management ▶ Admin

WEBconfig: LCOS menu tree ▶ Setup ▶ Config

6.1.3 Restriction of the access rights on the configuration

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

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

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

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

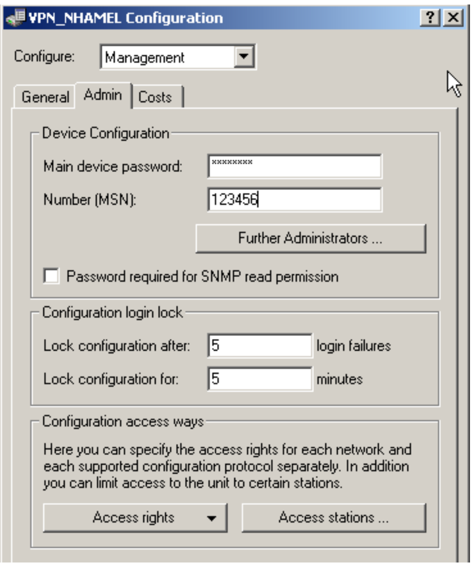
The use of the internal functions with a WAN interface of devices with VPN can be restricted merely for the VPN connection.

Restrictions on the ISDN administrative account

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

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

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


VPN_NHAMEL Configuration

Configure: Management

General | Admin | Costs

Device Configuration

Main device password: ********

Number (MSN): 123456

Further Administrators ...

□ Password required for SNMP read permission

Configuration login lock

Lock configuration after: 5 login failures

Lock configuration for: 5 minutes

Configuration access ways

Here you can specify the access rights for each network and each supported configuration protocol separately. In addition you can limit access to the unit to certain stations.

Access rights | Access stations ...

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

Enter alternatively the following instruction:

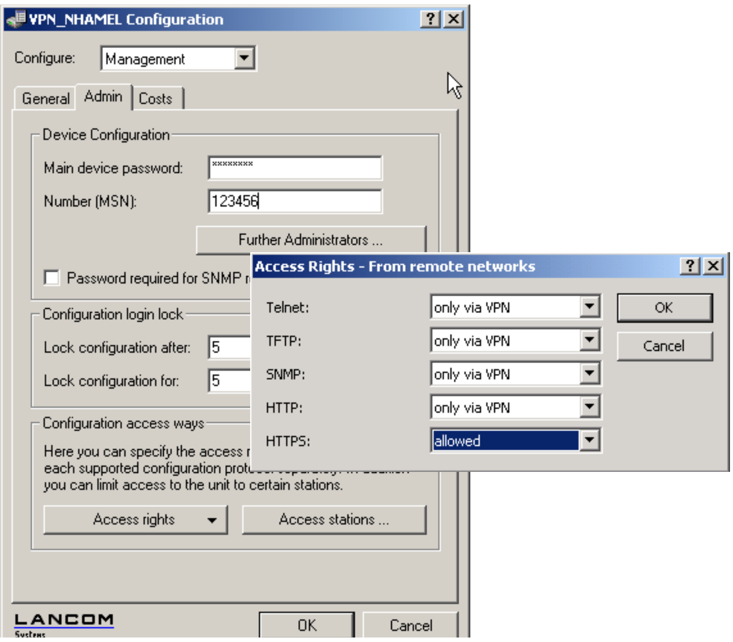
```
set /setup/config/farconfig-(EAZ-MSN) 123456
```

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

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

Limit the network configuration access

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


VPN_NHAMEL Configuration

Configure: Management

Main device password: ********

Number (MSN): 123456

Lock configuration after: 5

Lock configuration for: 5

Access Rights - From remote networks

Telnet:	only via VPN
TFTP:	only via VPN
SNMP:	only via VPN
HTTP:	only via VPN
HTTPS:	allowed

OK | Cancel

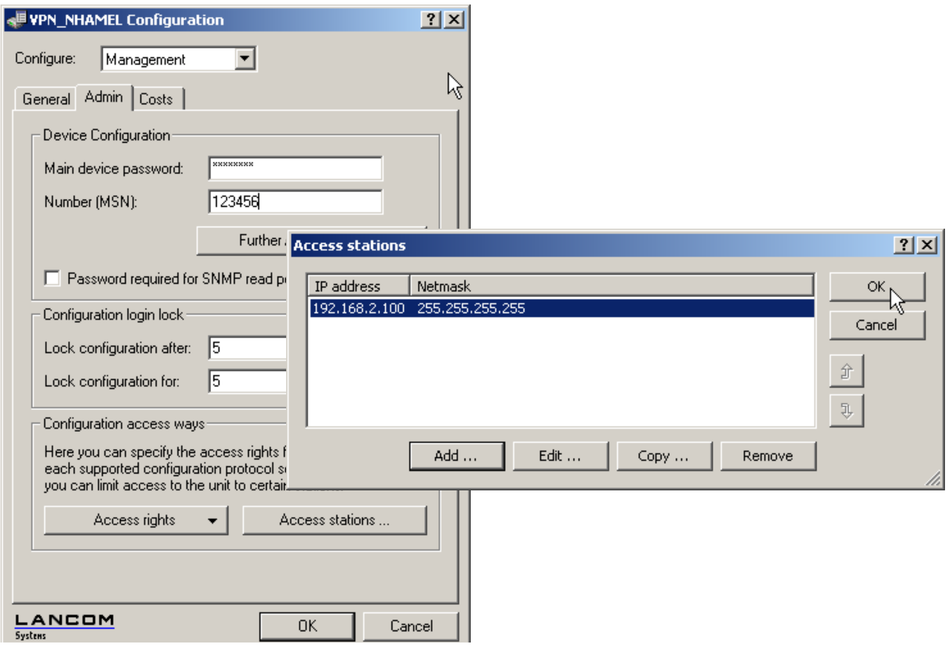
If you want to remove the network access to the router over the WAN completely, set the configuration access from distant nets for all methods to 'denied'.

LANconfig: Management ▶ Admin ▶ access rights

WEBconfig: LCOS menu tree ▶ Setup ▶Config ▶ Access-list

Restriction of the network configuration access to certain IP addresses

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



Configure: Management

Device Configuration

Main device password: ********

Number (MSN): 123456

□ Password required for SNMP read p

Configuration login lock

Lock configuration after: 5

Lock configuration for: 5

Configuration access ways

Here you can specify the access rights f
each supported configuration protocol s
you can limit access to the unit to certai

IP address	Netmask
192.168.2.100	255.255.255.255

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

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

LANconfig: Management ▶ Admin ▶ access stations

WEBconfig: LCOS menu tree ▶ Setup ▶ TCP-IP ▶Access-list

6.2 Protecting the ISDN connection

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

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

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

6.2.1 Identification control

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

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

LANconfig: Communication ▶ Call Management

WEBconfig: LCOS menu tree ▶ Setup ▶ WAN ▶ Protect

You have a choice of the following:

- all: Calls are accepted from any remote station.

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

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

Verification of name and password

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

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

The PPP list can be found as follows:

LANconfig: Communication ▶ Protocols ▶ PPP list

WEBconfig: LCOS menu tree ▶ Setup ▶ WAN ▶ PPP-list

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

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

Checking the number

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

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

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

6.2.2 Callback

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

LANconfig: Communications ▶ Remote site ▶ Remote Sites (ISDN/serial)

WEBconfig: LCOS menu tree ▶ Setup ▶ WAN ▶ dialup-peers

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

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

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

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

Additional information on callback can be found in section 'Callback functions' → page 7-38.

6.3 Location verification by ISDN or GPS

After being stolen, the device can theoretically be operated at another location by unauthorized persons. Password-protected device configurations offer no protection from the operation of the RAS access, LAN coupling or VPN connections that are set up in the device; a thief could gain access to a protected network.

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

6.3.1 GPS location verification

GPS location verification enables a geographical position to be defined within the device. After being switched on the device automatically activates the GPS module and checks if it is located at the "correct" position. The router module is only switched on if the check is positive. After location verification has been carried out the GPS module is deactivated again, unless it was switched on manually.

6.3.2 ISDN location verification

ISDN location verification can prevent the misuse of a router. Each time it is switched on, the router carries out a check by making an ISDN telephone call to itself to ensure that it is installed at the intended location. Only after successful location verification is the router module activated.

Prerequisites for successful ISDN location verification:

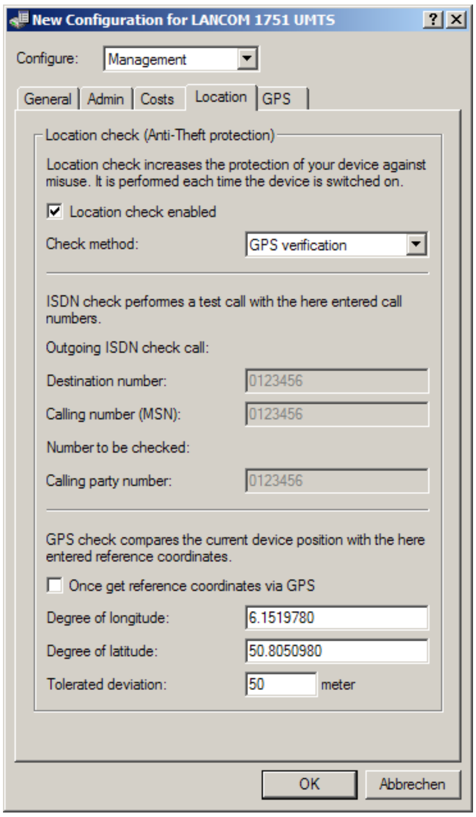
- The device must be reachable from the public ISDN telephone network.
- The device needs two free B channels for the duration of the check. If just one channel is free, e.g. one channel at a point-to-multipoint connection with two B channels is being used for a telephone call, then the device cannot make a call to itself via ISDN.

6.3.3 Configuring location verification

LANconfig

Parameters for location verification are to be found in LANconfig in the configuration area 'Management' on the 'Location' tab.

You can enable the GPS module on the 'GPS' tab independently from the location verification e. g. for monitoring the current GPS coordinates using LANmonitor.



New Configuration for LANCOM 1751 UMTS

Configure: Management

Location check (Anti-Theft protection)

Location check increases the protection of your device against misuse. It is performed each time the device is switched on.

☑ Location check enabled

Check method: GPS verification

ISDN check performes a test call with the here entered call numbers.

Outgoing ISDN check call:

Destination number: 0123456

Calling number (MSN): 0123456

Number to be checked:

Calling party number: 0123456

GPS check compares the current device position with the here entered reference coordinates.

☐ Once get reference coordinates via GPS

Degree of longitude: 6.1519780

Degree of latitude: 50.8050980

Tolerated deviation: 50 meter

- Activate location verification with the 'Enable location check' option.
- Select the method for the location check:

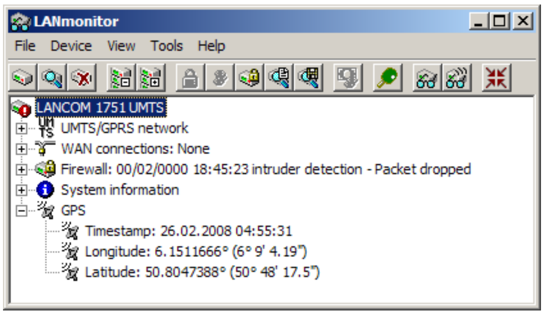
  - □ 'Self call' for a check via ISDN by means of a return call.
  - □ 'Call forwarding check' via ISDN by requesting the call number from the exchange. No call-back is necessary in this case.
  - □ 'GPS verification' for a check on the geographical coordinates.

For a location check by GPS an appropriate GPS antenna must be connected to the AUX connector on the device. Additionally, a SIM card for mobile telephone operation has to be inserted and the device must be logged on to a mobile phone network.

- For the location check enter 'Self call' or 'Call forwarding check' and enter the destination number as the telephone number to be used for the check.
- For location verification by GPS enter the necessary parameters:
  - □ Degrees latitude and longitude
  - □ Deviation from the intended position in meters

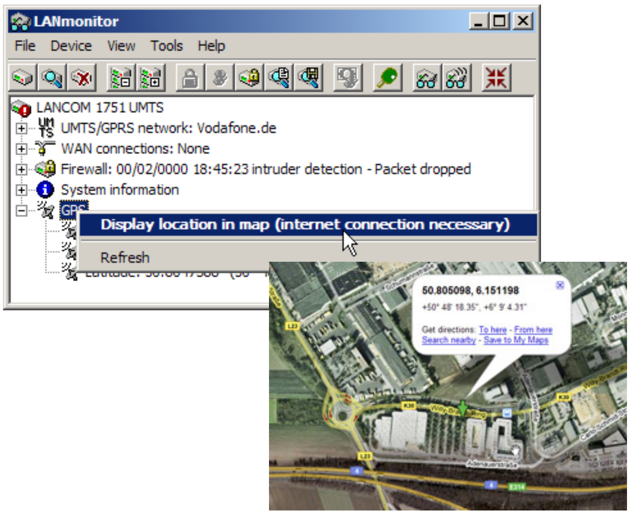
The device is itself able to determine the geographical coordinates for its current position by activating the 'Get reference coordinates via GPS' checkbox. Once the configuration is written back to the device, the current longitude and latitude are entered automatically, assuming that location verification is activated and a valid GPS position is available. Subsequently this option is automatically deactivated again.

As an alternative you can determine the geographical coordinates from tools such as Google Maps.



LANCOM 1751 UMTS
UMTS/GPRS network
WAN connections: None
Firewall: 00/02/0000 18:45:23 intruder detection - Packet dropped
System information
GPS
Timestamp: 26.02.2008 04:55:31
Longitude: 6.1511666° (6° 9' 4.19")
Latitude: 50.8047388° (50° 48' 17.5")

When the current geographical coordinates are displayed in LANmonitor, you can right-click with the mouse on the entry 'GPS' to call up that location in Google maps.


LANmonitor
File Device View Tools Help
Display location in map (internet connection necessary)
Refresh

LANCOM 1751 UMTS
UMTS/GPRS network: Vodafone.de
WAN connections: None
Firewall: 00/02/0000 18:45:23 intruder detection - Packet dropped
System information
GPS

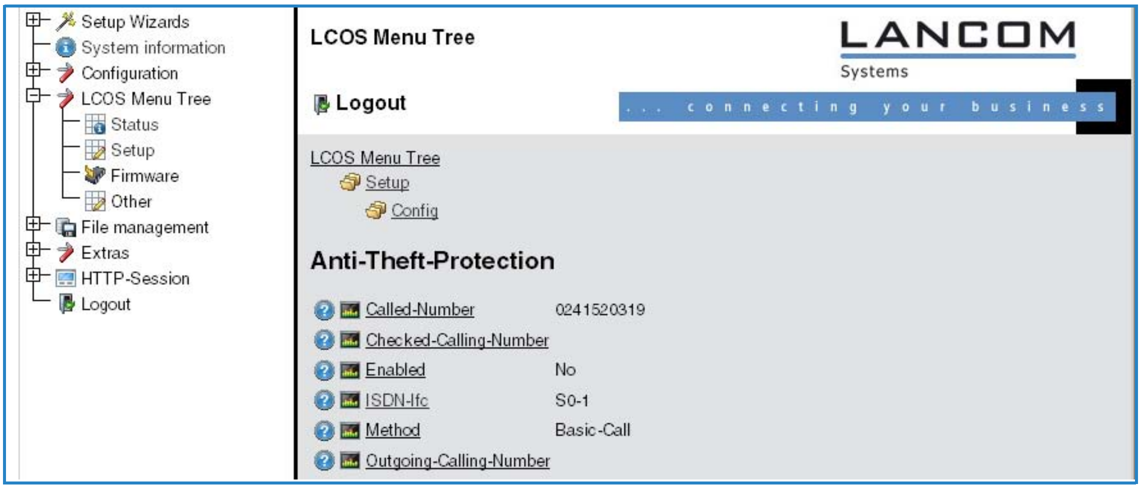
50.805098, 6.151198
+50° 48' 18.35", +6° 9' 4.31"
Get directions: To here - From here
Search nearby - Save to My Maps

WEBconfig, Telnet or terminal program

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

LANconfig: communication ▶ remote sites ▶ remote sites (ISDN/serial)

WEBconfig: LCOS menu tree ▶ Setup ▶ Config ▶ Location verification

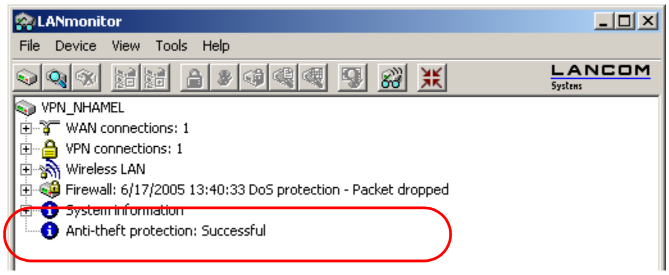


Anti-Theft-Protection

Called-Number	0241520319
Checked-Calling-Number	
Enabled	No
ISDN-Ifc	S0-1
Method	Basic-Call
Outgoing-Calling-Number	

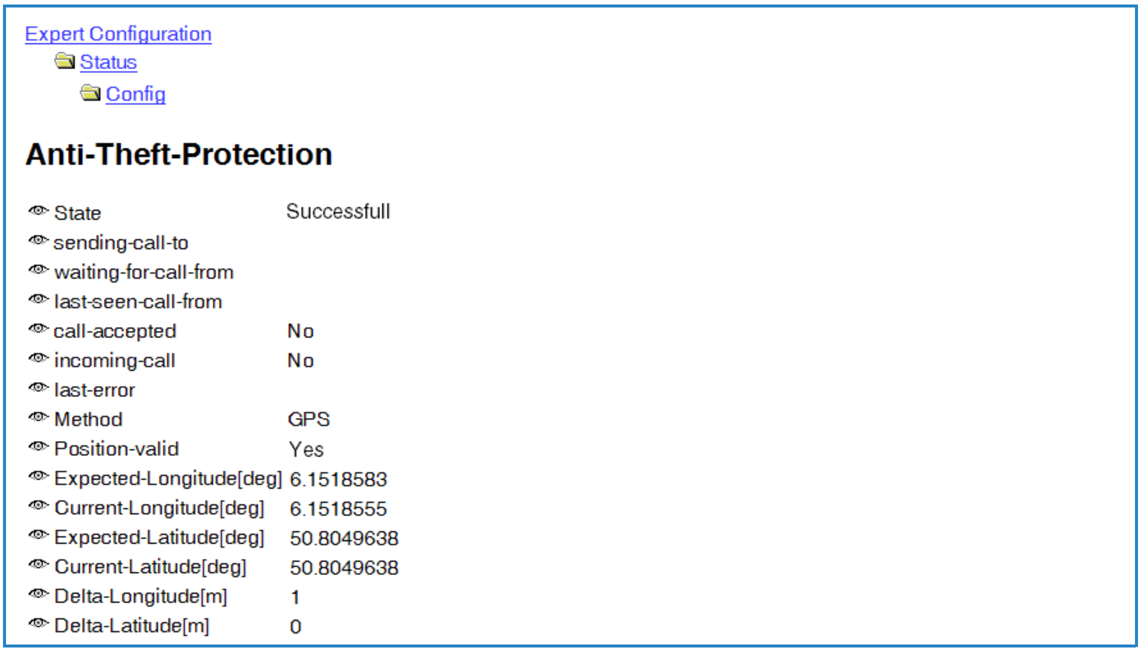
Location verification status request

The status of location verification can be viewed under LANmonitor:



VPN_NHAMEL
WAN connections: 1
VPN connections: 1
Wireless LAN
Firewall: 6/17/2005 13:40:33 DoS protection - Packet dropped
System information
Anti-theft protection: Successful

With WEBconfig (**LCOS menu tree ▶ Status ▶ Config ▶ Location verification**) or Telnet (`Status/Config/Location verification`) you can view the status of the location verification:



Anti-Theft-Protection

State	Successfull
sending-call-to	
waiting-for-call-from	
last-seen-call-from	
call-accepted	No
incoming-call	No
last-error	
Method	GPS
Position-valid	Yes
Expected-Longitude[deg]	6.1518583
Current-Longitude[deg]	6.1518555
Expected-Latitude[deg]	50.8049638
Current-Latitude[deg]	50.8049638
Delta-Longitude[m]	1
Delta-Latitude[m]	0

Only when the location verification has the status 'Successful' will the router data be transferred over the WAN interfaces.

- Location verification via ISDN is successful when the number 'Expect call from' agrees with the number 'Last call from'. This call is not picked up by the router. The status also displays whether a call was accepted at all.
- Location verification via GPS is successful when the GPS position is valid and within the tolerated range deviation from the known position.

6.4 The security checklist

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

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

- **Have you secured your wireless network with encryption and access control lists?**

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

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

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

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

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

- **Have you protected the configuration with a password?**

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

- **Have you permitted remote configuration?**

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

- **Have you allowed configuration from the wireless LAN?**

  If you do not need to configure the device from the wireless LAN, switch this function off. The field for disenabling configuration from the wireless LAN is to be found in LANconfig in the 'Management' configuration area on the 'Admin' tab. Under ‘Access rights – From the wireless LAN’ select the option ‘denied’ for all methods of configuration.

- **Have your password-protected the SNMP configuration?**

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

- **Have you activated the firewall?**

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

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

- **Are you using a 'deny all' firewall strategy?**

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

- **Have you activated IP masquerading?**

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

- **Have you used filters to close critical ports?**

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

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

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

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

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

- **Concerning the exchange of your particularly sensitive data via wireless LAN; have you set up the functions offered by IEEE 802.1x?**

  If you move especially sensitive data via wireless LAN you can provide even stronger security by using the IEEE 802.1x technology. To check or activate the IEEE 802.1x settings in LANconfig select the configuration area '802.1x'.

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

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

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

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

  GPS location verification enables a geographical position to be defined within the device. After being switched on the device automatically checks if it is located at the "correct" position. Only after a positive check is the router module activated.

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

  For self-sufficient operations, the configuration for a WLAN interface being managed by a LANCOM WLAN Controller is stored in flash memory for a certain time only, or even in the RAM only. This device configuration is deleted if contact to the WLAN-Controller is lost or if the power supply is interrupted for longer than the set time period.

- **Have you ensured that the reset button is safe from accidental configuration resets?**

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

LANCOM reference manual part 2

- Routing and WAN connections
- Firewall
- Quality of Service

Version: LCOS 7.6 with addendum 7.7 (see appendix)

(last update August 2009)

LANCOM
Systems

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

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

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen
Deutschland

www.lancom.de

Würselen, August 2009

110650/0809

Contents

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

WAN connections are used for the following applications.

- Internet access
- LAN to LAN coupling
- Remote access

7.1.1 Bridges for standard protocols

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

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

Which protocols are used for WAN connections?

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

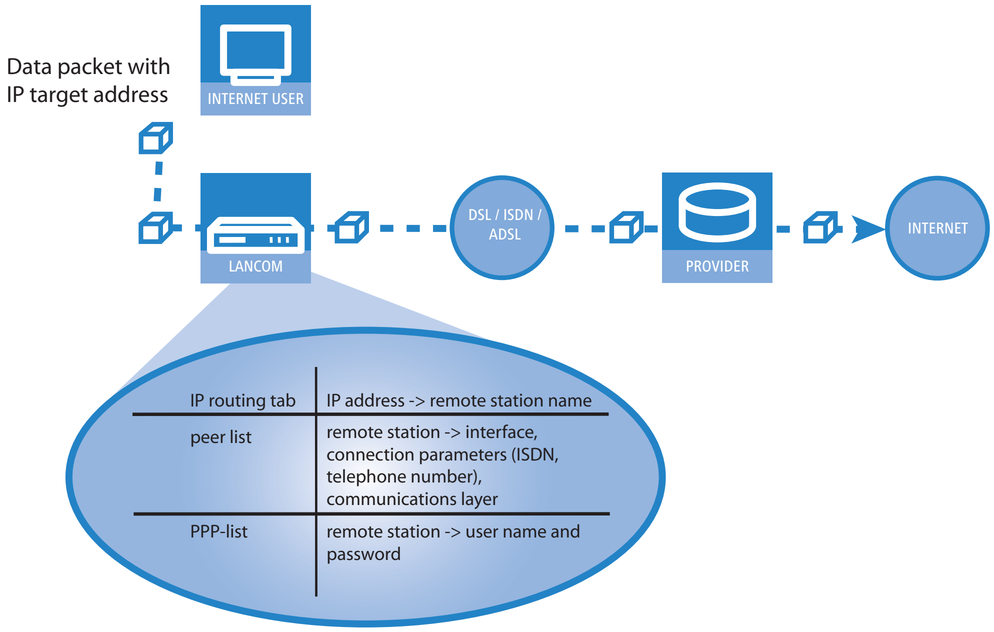
Close cooperation with router modules

Characteristic of WAN connections is the close cooperation with the router modules in the LANCOM. The router modules (IP and IPX) provide the connection to LAN and WAN. They make use of the WAN modules to respond 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 to. 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, whose interaction permits the correct conections.

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.



IP routing tab	IP address -> remote station name
peer list	remote station -> interface, connection parameters (ISDN, telephone number), communications layer
PPP-list	remote station -> user name and password

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 remote station list and finds the necessary connection data for the provider. 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 a provider via a WAN interface. It authenticates itself with a user name and password.

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

7.2 IP routing

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

7.2.1 The IP routing table

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

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

Configuration of the routing table

LANconfig: IP-Router ▶ Routing ▶ Routing-Table

WEBconfig: LCOS menu tree ▶ Setup ▶ IP-Router ▶ IP-Routing-Table

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

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

What do the various entries on the list mean?

- IP addresses and netmasks

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

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

- Routing Tag

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

- Router

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

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

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

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

- ■ Distance

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

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

- ■ Masquerading

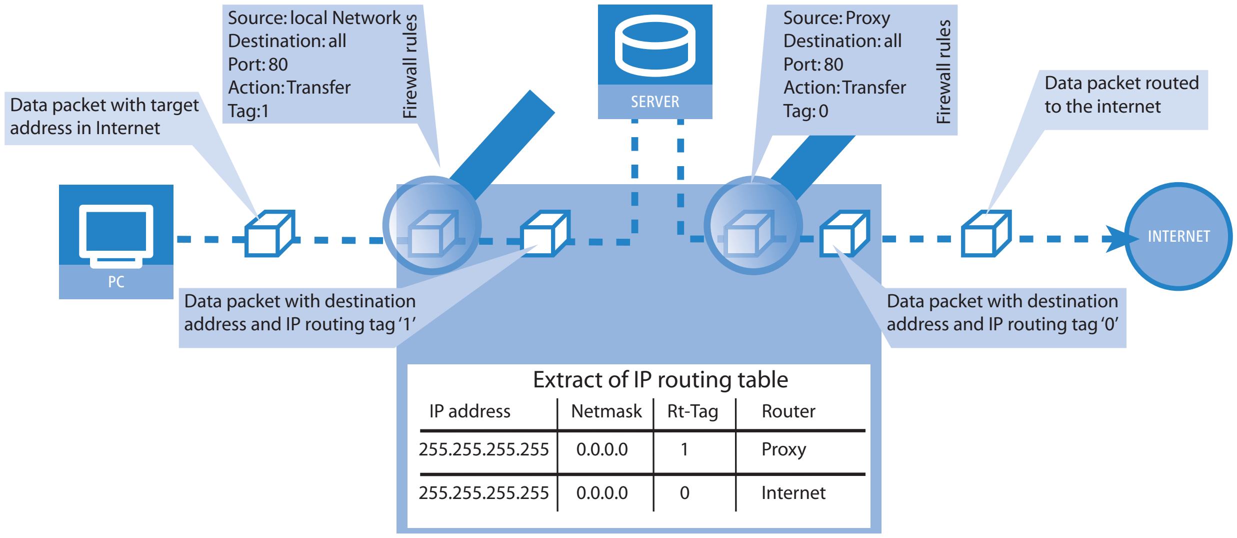
  Use the 'Masquerade' option in the routing table to inform the router which IP addresses to use when transferring packets from local networks.

  For further information see the section 'IP masquerading' → page 7-16.

7.2.2 Policy-based routing

Policy-based routing does not rely exclusively upon the destination IP address to define the destination route (meaning the remote device that is to be used to transfer the data). Further information can be used-such as the service or the protocol used, sender addresses or the destination for the data packets-for the selection of the destination route. Policy-based routing can be used to achieve a significantly finer-grained routing behavior, such as in the following application scenarios:

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


Source: local Network
Destination: all
Port: 80
Action: Transfer
Tag:1
Firewall rules
SERVER
Source: Proxy
Destination: all
Port: 80
Action: Transfer
Tag: 0
Firewall rules
Data packet with target address in Internet
Data packet routed to the internet
PC
INTERNET
Data packet with destination address and IP routing tag ‘1’
Data packet with destination address and IP routing tag ‘0’

Extract of IP routing table

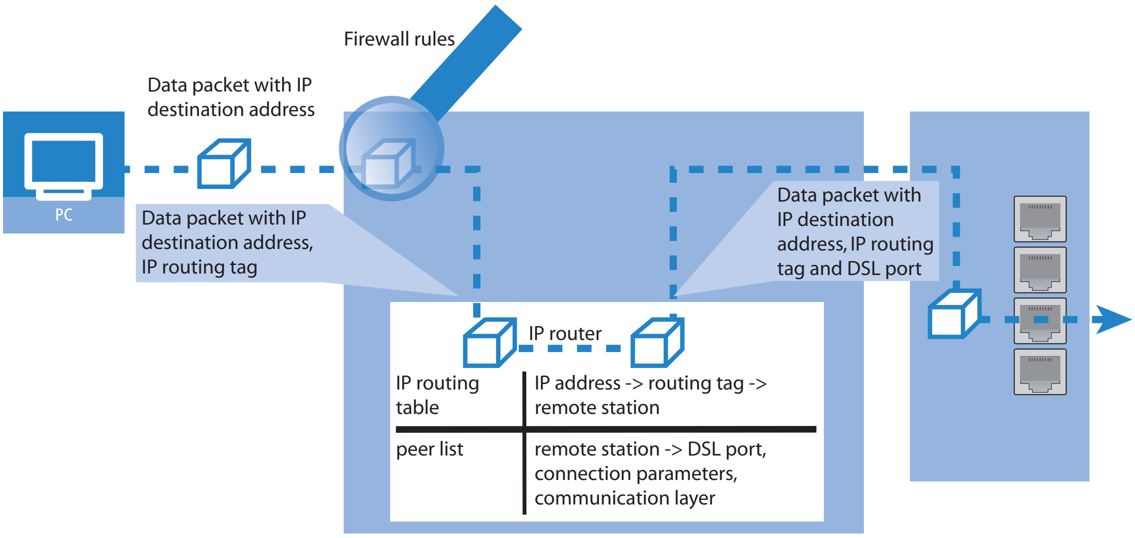
IP address	Netmask	Rt-Tag	Router
255.255.255.255	0.0.0.0	1	Proxy
255.255.255.255	0.0.0.0	0	Internet

- ■ With load balancing, the data traffic for selected protocols is diverted over a certain DSL port that uses an additional external ADSL modem.
- ■ A server in the local network is only supposed to be accessible from the WAN via a fixed IP address; this is routed via a certain WAN interface.

- VPN traffic is forwarded to a VPN tunnel with dynamic end points by using the routing tag '0'; the company's remaining Internet traffic is diverted to another firewall by means of another suitable routing tag.

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

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


Firewall rules
Data packet with IP destination address
PC
Data packet with IP destination address, IP routing tag
Data packet with IP destination address, IP routing tag and DSL port
IP router
IP routing table
IP address -> routing tag -> remote station
peer list
remote station -> DSL port, connection parameters, communication layer

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

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

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

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

Routing tags for VPN and PPTP connections

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

- Routing tags for VPN connections

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

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

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

- Routing tags for PPTP connections

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

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

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

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

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

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

7.2.3 Local routing

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

How can you assist the workstation computer now?

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

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

LANconfig: IP router ▶ General ▶ Forward packets within the local network

WEBconfig: LCOS menu tree ▶ Setup ▶ IP-router ▶ Loc.-routing

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

7.2.4 Dynamic routing with IP RIP

In addition to the static routing table, LANCOM Systems routers also have a dynamic routing table. 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 RIP. The '16' stands for "This route is not available at the moment". A router may be prevented from establishing a connection in addition to the present one may be due to one of the following causes:
  - Another connection has already been established on all the other channels (also via the LANCAPI).
  - Y connections for the S_0 port have been explicitly excluded in the interface table.
  - The existing connection is using all B channels (channel bundling).
  - The existing connection is a leased-line connection. Only a few ISDN providers enable a dial-up connection to be established on the second B channel in addition to a permanent connection on the first B channel.

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

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

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

What do the entries mean?

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

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

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

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

The interaction of static and dynamic tables

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

Scaling with IP RIP

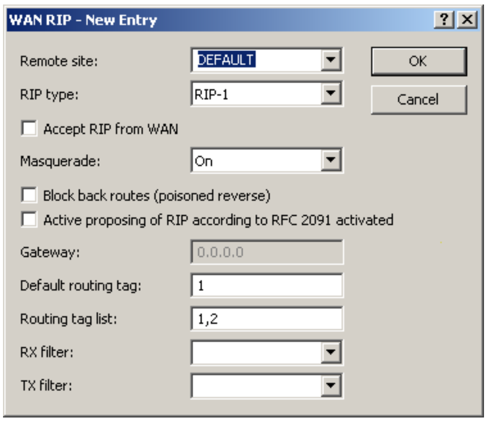
If you use several routers in a local network with IP RIP, you can represent the routers outwardly as one large router. This procedure is also known as “scaling”. As a result of the constant exchange of information between the routers, such a router theoretically has no limits to the transmission options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

Configuration of IP-RIP function

You can fill in the corresponding remote stations in the WAN-RIP-table, to declare the static defined routes over the WAN, which are learned over RIP, or to learn routes from the WAN.

WEBconfig: Setup ▶ IP-router ▶ RIP ▶ WAN table

LANconfig: IP-Router ▶ General ▶ WAN RIP



WAN RIP - New Entry

Remote site: DEFAULT

RIP type: RIP-1

□ Accept RIP from WAN

Masquerade: On

□ Block back routes (poisoned reverse)

□ Active proposing of RIP according to RFC 2091 activated

Gateway: 0.0.0.0

Default routing tag: 1

Routing tag list: 1,2

RX filter:

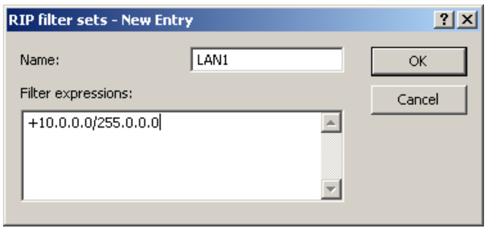
TX filter:

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.

RIP filter

Routes learned from RIP can be filtered by their routing tag according to the settings for LAN and WAN RIP. Routes can additionally be filtered by specifying network addresses (e. g. "Only learn routes in the network 192.168.0.0/255.255.0.0"). First of all a central table is used to define the filters that can then be used by entries in the LAN and WAN RIP table. Initially the filters are defined in a central table; these can then used by entries in the LAN and WAN RIP table.

LANconfig: IP-Router ▶ General▶ RIP filter sets



RIP filter sets - New Entry

Name: LAN1

Filter expressions:

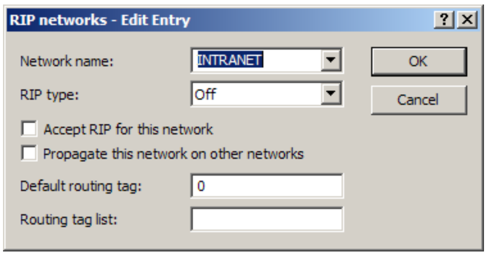
+10.0.0.0/255.0.0.0

WEBconfig: Setup ▶ IP-Router ▶ RIP ▶ filter

Set up RIP for separate networks

Most of the time it is not required (as well as for NetBIOS-Proxy), that the local network structure is propagated over RIP to the DMZ. Furthermore it is sometimes required, to propagate the known routes to a certain network, but not to learn routes from the network (eg. in the WAN). Therefore the RIP functionality can be set up for every network separately.

LANconfig: IP-Router ▶ General ▶ RIP networks



Network name: INTRANET

RIP type: Off

□ Accept RIP for this network

□ Propagate this network on other networks

Default routing tag: 0

Routing tag list:

WEBconfig: LCOS-menu tree ▶ Setup ▶ IP-Router ▶ RIP ▶ LAN-table

Timer settings

The Routing Information Protocol (RIP) regularly provides neighboring routers with updates on the available networks and the associated metrics (hops). RIP uses various timers to control the exchange of routing information.

- WEBconfig: Setup ▶ IP-router ▶ RIP ▶ Parameters

Triggered update in the LAN

With a triggered update, changes to the metrics are immediately reported to the neighboring router. The system does not wait until the next regular update. An update delay stops faulty configurations from causing excessive update messages.

- **Update delay**

  The update delay starts as soon as the routing table, or parts of it, are propagated. As long as this delay is running, new routing information is accepted and entered into the table but it is not reported any further. The router actively reports its current entries only after expiry of this delay.

  The value set here sets the upper limit for the delay—the actual delay is a random value between one second and the value set here.

Triggered update in the WAN

Other than in the LAN, WAN bandwidth limitations may make regular updates every 30 seconds undesirable. For this reason, RFC 2091 requires that routes are transmitted to the WAN once only when the connection is established. After this, updates only are transmitted.

Because updates are explicitly requested here, broadcasts or multicasts are not to be used for delivering RIP messages. Instead, the the subsidiary device must be statically configured with the IP address of the next available router at the central location. Due to these requests, the central router knows which subsidiary routers it has received update requests from; it then sends any messages on route changes directly to the subsidiary device.

The WAN-RIP table has been extended for configuring the triggered update in the WAN.

Poisoned reverse

Poisoned reverse prevents routing loops from forming. An update is sent back to the router that propagated the route to inform it that the network is unreachable at the associated interface.

However, this has a significant disadvantage over WAN connections: The central location transmits a high number of routes which would then suffer from route poisoning, so leading to a heavy load on the available bandwidth. For this reason, poisoned reverse can be manually activated for every LAN/WAN interface.

The LAN and WAN RIP tables have been extended for the configuration of poisoned reverse.

Static routes for constant propagation

Routers use RIP to propagate not only dynamic routes but statically configured routes as well. Some of these static routes may not be constantly available, for example when an Internet connection or dial-up access is temporarily unavailable.

For a static route, the setting for "Active" in the routing table defines whether it should be propagated constantly or only when it is actually reachable.

- WEBconfig: Setup ▶ IP-Router ▶ IP-Routing-Table

7.2.5 SYN/ACK speedup

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

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

The SYN/ACK speedup is activated at the factory.

Switching off in case of problems

Due to the preferred handling of individual packets, the original packet order is changed. Although TCP/IP does not ensure a certain packet order, problems may result in a few isolated applications. This only concerns applications that assume a certain order that differs from the protocol standard. In this case the SYN/ACK speedup can be deactivated:

LANconfig: IP router ▶ General ▶ Pass on TCP SYN and ACK packets preferentially

WEBconfig: LCOS menu tree ▶ Setup ▶ IP router ▶Routing method ▶ SYN/ACK speedup

7.3 Advanced Routing and Forwarding

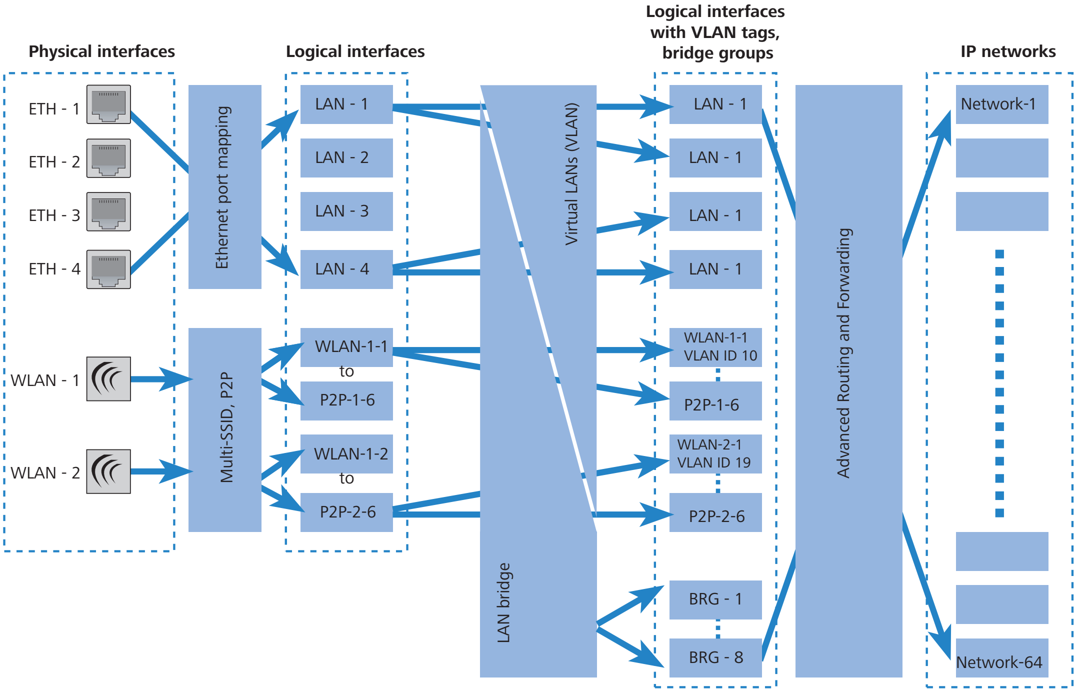
7.3.1 Introduction

Up until LCOS version 6.30, LANCOM Routers supported two local networks only: The intranet and the DMZ. For some applications, however, it may be desirable to realize more than one intranet and one DMZ with a LANCOM Router, for example to provide multiple IP networks with Internet access via a central router. As of LCOS version 7.00, LANCOM Routers support up to 64 different IP networks, depending on the model.

Various scenarios are possible when realizing multiple IP networks:

- One network per interface.
- Multiple networks per interface.
- Multiple VLANs per interface; one or more networks per VLAN (which corresponds with a combination of the first two scenarios).

The realization of these scenarios is facilitated by advanced routing and forwarding (ARF), which provides very flexible options in the definition of IP networks and the assignment of these networks to the interfaces. The diagram below illustrates the network/interface assignment at various levels. The configuration options applied here are described in the following chapters.



The assignment of IP networks to interfaces proceeds as follows:

- The various models have different numbers of physical interfaces, i.e. Ethernet ports or WLAN modules.
- The logical interface(s) is/are assigned to the physical interface:
  - □ For the Ethernet ports, Ethernet port mapping assigns the physical ETH-1 to ETH-4 to the logical LAN-1 to LAN-4.

For some but not all models, the number of logical LAN interfaces corresponds to the number of physically available Ethernet ports.

  - In the case of the WLAN modules, the establishment of point-to-point connections (P2P) and/or the use of Multi-SSID can mean that multiple WLAN interfaces are assigned to each physical WLAN module: Per module this may be up to eight WLAN networks and up to six P2P connections.
- These logical interfaces are further specified and grouped in the next stage:
  - For devices supporting VLAN, multiple VLANs can be defined for each logical interface simply by using VLAN-IDs. Although the data traffic for the various VLANs flows via a common logical interface, the VLAN-ID ensures that the different VLANs remain strictly separated. From the perspective of the LANCOM Router the VLANs are completely separate interfaces, meaning that a single logical interface becomes multiple logical interfaces for the LANCOM Router, and each of these interfaces can be addressed individually.
  - For devices with WLAN modules, the individual logical interfaces can be grouped together. This is handled by the LAN bridge which regulates data transfer between the LAN and WLAN interfaces. The formation of bridge groups (BRG) allows multiple logical interfaces to be addresses at once and they appear as a single interface to the LANCOM Router—in effect achieving the opposite of the VLAN method.
- In the final stage, the ARF forms a connection between the logical interfaces with VLAN tags and the bridge groups on the one side, and the IP networks on the other. For this reason, an IP network is configured with a reference to a logical network (with VLAN-ID, if applicable) or to a bridge group. Furthermore, for each IP network an interface tag can be set, with which the IP network can be separated from other networks without having to use firewall rules.

The definition of routing tags for IP networks as described above is one of the main advantages of Advanced Routing and Forwarding. This option allows "virtual routers" to be realized. A virtual router only takes up a portion of the rounting table by using interface tags for a IP-network and therefore configures routing individually for this particular IP-network. This method allows, for example, several default routes to be defined in the routing table, each of which is given a routing tag. Virtual routers in the IP networks use the tags to select the default route which applies to the IP network with the appropriate interface tag. The separation of IP networks via virtual routers even permits multiple IP networks with one and the same address range to be operated in parallel in just one LANCOM Router without problem.

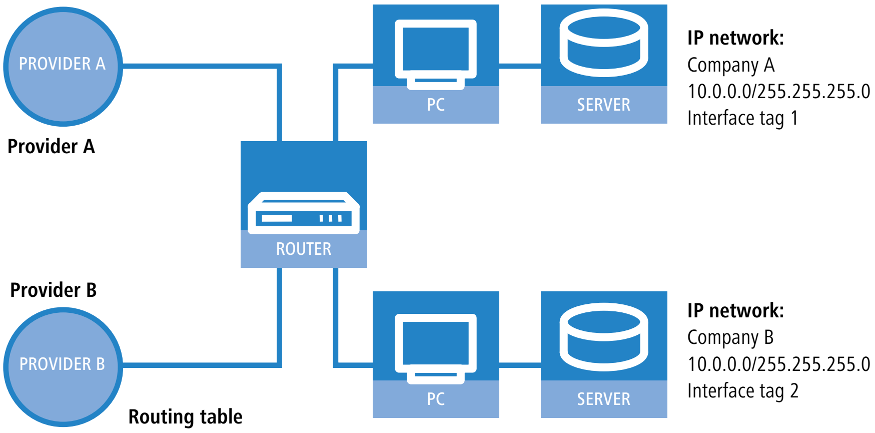
For example: Within an office building, a number of companies have to be connected to the Internet via a central LANCOM Router, even though each of these companies has its own Internet provider. All of the companies want to use the popular IP network '10.0.0.0' with the netmask '255.255.255.0'. To implement these requirements, each company is given an IP network '10.0.0.0/255.255.255.0' with a unique name and a unique interface tag. In the routing table, a default route with the corresponding routing tag is created for each Internet provider. This allows the clients in the different company networks, all of which use the same IP addresses, to access the Internet via their own provider. Employing VLANs enables logical networks to be separated from one another even though they use the same physical medium (Ethernet).

The differences between routing tags and interface tags

Routing tags as assigned by the firewall and interface tags as defined by the IP networks have a great deal in common, but also some important differences:

- The router interprets both tags in the same way. Packets with the interface tag '2' are valid for routes with the routing tag set to '2' in the routing table (and all routes with the default route tag '0'). The same routes apply for packets which the firewall has assigned with the routing tag '2'.

  Thus the interface tag is used in the same way as a routing tag.
- Interface tags have the additional ability to delimit the visibility (or accessibility) between different networks:
  - In principle, only networks with the same interface tag are "visible" to one another and thus able to interconnect.
  - Networks with the interface tag '0' have a special significance; they are in effect supervisor networks. The networks can see all of the other networks and can connect to them. Networks with an interface tag not equal to '0' cannot make connections to supervisor networks, however.
  - Networks of the ’DMZ’ type can be seen by all other networks independentlly of their interface tag - which makes sense, since the DMZ often contains servers which are open to the public, like webservers etc.. The DMZ-networks only see networks with the same interface tag (and of course all other DMZ-networks).
  - Networks of the ’DMZ’ type with the interface tag '0' have a special significance: As "supervisor networks" they can see all other networks, and they are also visible to all other networks.



Routing table

IP address	Netzmaske	Interface tag	Router
255.255.255.255	0.0.0.0	1	Provider A
255.255.255.255	0.0.0.0	2	Provider B

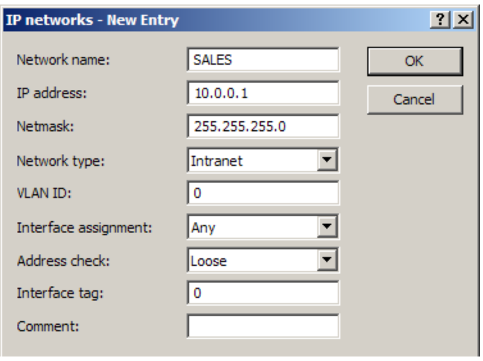
For cases which do not allow IP addresses to be uniquely assigned by interface tag, the Advanced Routing and Forwarding can be supported by firewall rules. In the above example, this would be the case if each of the networks were to support a public web or mail server, all of which use the same IP address.

7.3.2 Defining networks and assigning interfaces

When defining a network, the first setting is for the IP-address range which is to be valid for a certain local interface on the LANCOM Router. "Local interfaces" are logical interfaces which are assigned either to a physical Ethernet port (LAN) or a wireless port (WLAN). To realize the scenarios outlined above, it is possible for several networks to be active on one interface: Conversely, a network can also be active on multiple interfaces (via bridge groups or with the interface assignment 'Any').

The networks are defined in a table. A unique name for the networks is set along with definitions for the address range and interface assignment. The network name allows the identification of networks in other modules (DHCP server, RIP, NetBIOS, etc.) and to enable control over which services are available in which networks.

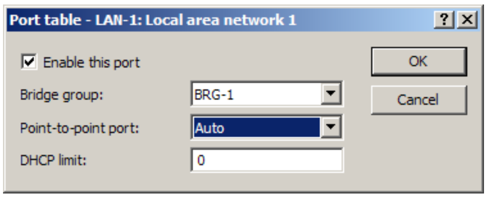
TCP/IP ▶ General ▶ IP networks



Network name:	SALES
IP address:	10.0.0.1
Netmask:	255.255.255.0
Network type:	Intranet
VLAN ID:	0
Interface assignment:	Any
Address check:	Loose
Interface tag:	0
Comment:	

7.3.3 Assigning logical interfaces to bridge groups

Particular properties of the logical interfaces are defined in the port table.



☑ Enable this port

Bridge group:	BRG-1
Point-to-point port:	Auto
DHCP limit:	0

LANconfig: Interfaces ▶ LAN ▶ Port table

WEBconfig: LCOS menu tree ▶ Setup ▶ LAN Bridge ▶ Port Data

- **Active**

  This option activates or deactivates the logical interface.

- **Bridge group**

  Assigns the logical interface to a bridge group to enable bridging from/to this logical interface via the LAN bridge. If assigned to a common bridge group, several logical interfaces can be addressed at once and they appear to the LANCOM Router to be a single interface. This can then be used for Advanced Routing and Forwarding, for example.

  If the interface is removed from all bridge groups by setting 'none', then there is no communication between the LAN and WLAN via the LAN bridge (isolated mode). With this setting, LAN/WLAN data transfers over this interface are only possible via the router.

A requirement for data transfer from/to a logical interface via the LAN bridge is the deactivation of the global "isolated mode" which applies to the whole of the LAN bridge. Furthermore, the logical interface must be assigned to a bridge group. With the setting 'none', no transfers can be made via the LAN bridge.

- **Priority**

  Sets the priority for the logical interface where the spanning-tree protocol is being used. Where multiple connections are available, the interface with the highest priority is used. The smaller the value, the higher the priority. If priorities are the same then the interface with lower transmission fees is chosen or, alternatively, the interface which is highest in the table.

- **DHCP limit**

  Number of clients which can be handled by DHCP. If the limit is exceeded, the oldest entry is dropped. This feature can be used in combination with the protocol filer table to limit access to just one logical interface.

7.3.4 Interfaces tags for remote sites

By defining interfaces tags, virtual routers can be used as part of Advanced Routing and Forwarding (ARF) that only use part of the overall routing table. For inbound data packets from the WAN, the assignment of interfaces tags can be regulated in different ways:

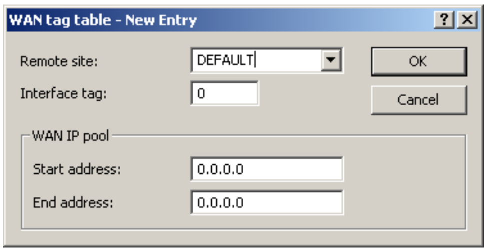
- By using appropriate firewall rules that only capture data packets from particular remote sites, IP addresses or ports
- Based on the routing table
- Via an explicit assignment of tags to remote sites.

This assignment of tags to the remote sites to separate ARF networks can also be conveniently used for packets received at the WAN-side (which by default contain Tag 0). Without controlling the assignment of tags explicitly with the firewall, the virtual router can be determined directly from the remote site or source route from the form of the interface tag. Inbound and outbound communication can thus be easily divided between virtual routers bidirectionally.

The interface tags determined via the tag table and on the basis of the routing table can be overwritten with an appropriate entry in the firewall.

Assignment of interface tags via the tag table

LANconfig: Communication ▶ Remote sites ▶ WAN tag table


WAN tag table - New Entry

Remote site: DEFAULT

Interface tag: 0

WAN IP pool

Start address: 0.0.0.0

End address: 0.0.0.0

WEBconfig: Setup ▶ IP router

- **WAN tag generation**

  WAN tag generation defines the source for the assignment of interfaces tags. Besides assignment via the firewall or direct assignment via the tag table, the interface tag can also be selected based on the source route in the effective routing table (static routing entries plus routes learned via RIP). The source IP and the name of the remote site used to establish the IP connection is compared with the routing information. The routing tag of this source route is assigned for further processing to the packets received at the WAN-side of this connection. If the effective routing table contains more than one entry for a remote site with the same network, the smallest tag is used.

Example: The following ARF networks have been defined:

Network	IP address	Rtg tag	Port
PRIVATE	192.168.1.1/24	1	LAN -1
HOME-OFFICE	192.168.10.1/24	10	LAN -2

PRIVATE is to have Internet access only, HOME-OFFICE is to have a VPN tunnel to the remote site VPN-COMPANY only. The corresponding effective routing table appears as follows:

IP address	IP netmask	Rtg tag	Remote site	Distanz	Masking
192.168.10.0	255.255.255.0	10	VPN-COMPANY	0	No
255.255.255.255	0.0.0.0	1	INTERNET	0	No

- □ Data packet coming from network 192.168.10.x: Tag = 10
- □ Data packet coming from network 192.168.1.x: Tag = 1
- □ Data packet coming from any other network: Tag = 0

Possible values:

- □ Manual: With this setting, the interface tags are determined solely by an entry in the tag table. The routing table has no significance in the assignment of interfaces tags.
- □ Auto: With this setting, the interface tags are determined initially by an entry in the tag table. If no matching entry is located there, the tag is determined based on the routing table.

! The interface tags determined via the tag table and on the basis of the routing table can be overwritten with an appropriate entry in the firewall.

7.3.5 Virtual routers

With interface-dependent filtering in combination with policy-based routing, virtual routers can be defined for every interface.

Example:

Two separate IP networks are used by the Development and Sales departments. Both networks are connected to different switch ports although they use the same network '10.1.1.0/255.255.255.0'. Sales should be able to enter the Internet only, whereas Development should also have access to a partner company's network ('192.168.1.0/255.255.255.0').

The result is the following routing table (where the Development dept. has tag 2, Sales has tag 1):

IP address	IP netmask	Rtg tag	Peer or IP	Distanz	Masking	Active
192.168.1.0	255.255.255.0	2	PARTNER	0	No	yes
192.168.0.0	255.255.0.0	0	0.0.0.0	0	No	yes
255.255.255.255	0.0.0.0	2	INTERNET	2	yes	yes
255.255.255.255	0.0.0.0	1	INTERNET	2	yes	yes

If Development and Sales were in IP networks with different address ranges, then it would be no problem to assign the routing tags with firewall rules. Since both departments are in the same IP network, the only available method of assignment is with network names.

Tag assignment can be carried out directly in the network definition

Network name	IP address	Netzmaske	VLAN ID	Interface	Source check	Type	Rtg tag
DEVELOPMENT	10.1.1.1	255.255.255.0	0	LAN -1	strict	Intranet	2
SALES	10.1.1.1	255.255.255.0	0	LAN -2	strict	Intranet	1

Alternatively the assignment of tags can be carried out with a combination of network definitions and firewall rules. The networks are defined as follows:

Network name	IP address	Netzmaske	VLAN ID	Interface	Source check	Type	Rtg tag
DEVELOPMENT	10.1.1.1	255.255.255.0	0	LAN -1	strict	Intranet	0
SALES	10.1.1.1	255.255.255.0	0	LAN -2	strict	Intranet	0

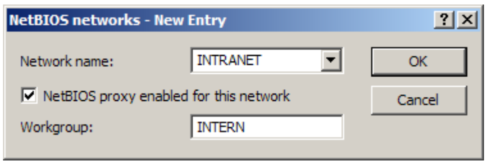
Routing tags can be used to define the following firewall rules:

Name	Protocol	Source	Destination	Action	Linked	Prio	(...)	Rtg tag
DEVELOPMENT	ANY	%Ldevelopment	ANYHOST	%a	yes	255		2
SALES	ANY	%Lsales	ANYHOST	%a	yes	255		1

Important for these rules is the maximum priority (255) so that these rules are always checked first. Since filtering is still possible by services, the option "Linked" has to be set in the firewall rule.

7.3.6 NetBIOS proxy

For security reasons, the behavior of the NetBIOS proxy has to be adjusted to the relevant networks, for example because it normally is not to be active within the DMZ. For this reason, the NetBIOS proxy can be configured separately for each network.


NetBIOS networks - New Entry

Network name: INTRANET

☑ NetBIOS proxy enabled for this network

Workgroup: INTERN

LANconfig: NetBIOS ▶ General ▶ NetBIOS networks

WEBconfig: LCOS menu tree ▶ Setup ▶ NetBIOS ▶ networks

- **Network name**

  Name of the network that the NetBIOS proxy is to be activated for.
- **NetBIOS proxy operating for the network**

  This option shows if the NetBIOS-proxy is activated for the selected network.
- **Workgroup**

  The workgroup or domain used by the network clients. With multiple workgroups, mentioning one workgroup suffices.

In the default setting 'Intranet' and 'DMZ' are entered into this table; the NetBIOS proxy is activated for the intranet and deactivated for the DMZ.

As soon as a network has an interface tag, then the only names (hosts and groups) visible from this network are those in a network with the same tag, or which are accessible via a suitably tagged (with the same tag) WAN route. An untagged network sees all names. Similarly, all names learned from untagged networks are visible to all networks.

The DNS server considers the interface tags when resolving names, i.e. the only names resolved by DNS are those learned from a network with the same tag. The special role played by untagged networks applies here too.

The workgroup/domain enables networks to be scanned for NetBIOS names when a device is started. The workgroup is different for every network and has to be defined everywhere. In networks without domains, the name of the largest workgroup should be defined here.

7.4 Configuration of remote stations

Remote stations are configured in two tables:

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

The configuration of the authentication (protocol, user name, password) is not covered in this section.Information on authentication is contained in the section 'Establishing connection with PPP' → page 7-33.

7.4.1 Peer list

The available remote stations are created in the peer list with a suitable name and additional parameters. For every WAN interface exists a separate peer list. The peer list reached as follows: For every WAN interface exists a separate peer list. The peer list reached as follows.LANconfig: Communication ▶ Remote sites ▶ Remote Sites (DSL)

WEBconfig: LCOS menu tree ▶ Setup ▶ WAN ▶ DSL-Broadband-Peers

For the remote stations following parameters are required:

Peer list	Parameter	Meaning
DSL	Name	With this name the remote stations are identified in the router modules. As soon as the router module has detected the remote station (using the IP address of the destination), the connection parameters are located in the peer list.
	Short hold	This time indicates how long the connection is kept if no data is being transmitted anymore. If zero is entered, the connection does not terminate automatically. If 9999 seconds are entered a broken off connection is rebuild automatically. (see 'Extended connection for flat rates—Keep-alive' → page 7-37)
	Access concentrator	The Access concentrator (AC) is a server, which can be accessed by the remote station. If several ADSL providers are listed, select the provider that is responsible for the remote station (using the name of the AC). The value for the AC is advised to you by your provider. If no value is entered for the AC, every AC is accepted that provides the demanded service.
	Service	Enter the service you would like to use from your provider. The service can be e.g. internet surfing or even video downstream. The value for the service is advised to you by your provider. If no value is entered, every Service is accepted that is provided by the AC.
	Layer name	Select the layer name for the connection. The configuration of this layer is described in the following section.
	VPI	Virtual Path Identifier.
	VCI	Virtual Channel Identifier. The value for VCI and VPI are advised to you by your provider. Standard values for the combination of VPI and VCI are: 0/35, 0/38, 1/32, 8/35, 8/48.
Dialup-Peers	Name	See DSL-Broadband-Peers
	Phonenumber	A Phonenumber is only then required, if the remote station must be called. This field can remain empty if only incoming calls should be accepted. Several phonenumbers for the same remote station can be entered in the RoundRobin list.
	Short hold	See DSL-Broadband-Peers
	Short hold 2	The second B channel is cut down, if it is not used for the set duration.
	Layer name	See DSL-Broadband-Peers
	Callback	The automatic callback provides a secure connection and decreases the costs for the caller. Further information can be found in the next section 'Callback functions' → page 7-38.

Please note following points when editing the peer list:

- □ If two identical peer lists (e.g. DSL-Broadband-Peers list and Dialup-Peers list) are entered, the LANCOM when connecting to the remote station uses the “faster” interface. The other interface is then used as a backup.
- □ If nor the access concentrator neither the service is specified the router connects to the first AC that answers the query.
- □ In the occasion of a DSLoL interface the same entries as for the DSL interface are valid. The entries are made in the Broadband-Peers list.

7.4.2 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:

LANconfig: Communication ▶ General ▶ Communication layers

WEBconfig: LCOS menu tree ▶ Setup ▶ WAN ▶ Layer-list

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

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

Parameter	Meaning	
Layer name	The layer is selected in the peer list under this name.	
Encapsulation	Additional encapsulations can be set for data packets.	
	'Transparent'	No additional encapsulations.
	'Ethernet'	Encapsulation in the form of ethernet frames.
	'LLC-MUX'	Multiplexing via ATM with LLC/SNAP encapsulation according to RFC 2684. Several protocols can be transmitted over the same VC (Virtual Channel).
	'VC-MUX'	Multiplexing with ATM by establishing additional VCs according to RFC 2684.
Layer-3	The following options are available for the switching layer or network layer:	
	'Transparent'	No additional header is inserted.
	'PPP'	The connection is established according to the PPP protocol (in the synchronous mode, i.e. bit-oriented). The configuration data are taken from the PPP table.
	'AsyncPPP'	Like 'PPP', only the asynchronous mode is used. This means that PPP functions character-oriented.
	'... with script'	All options can be run with their own script if desired. The script is specified in the script list.
	'DHCP'	Assignment of the network parameters via DHCP.
Layer-2	In this field the upper section of the security layer (Data Link Layer) is configured. The following options are available:	
	'Transparent'	No additional header is inserted.
	'PPPoE'	Encapsulation of the PPP protocol information in ethernet frames.
	'PPPoE'	The PPP negotiation runs via Ethernet. The PPP packets are encapsulated in Ethernet frames for this purpose. This process is frequently used for DSL connections.
Options	Here you can activate the compression of the data to be transmitted and the bundling of channels. The selected option only becomes active when it is supported by both the ports used and the selected Layer-2 and Layer-3 protocols. For further information see section 'ISDN Channel bundling with MLPPP' → page 7-40.	
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)

7.5 IP masquerading

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

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

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

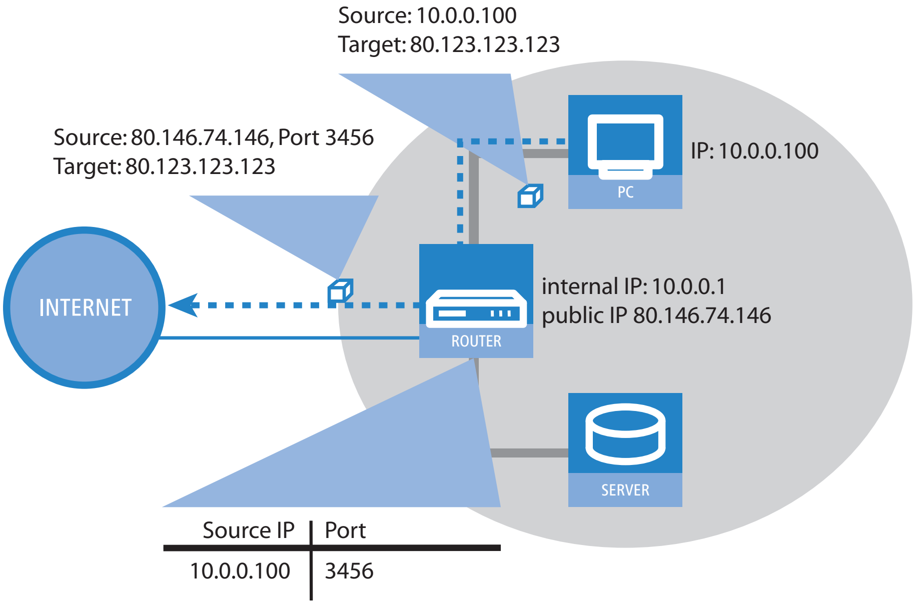
- the intranet IP address to communicate with computers in the LAN
- the public IP address to communicate with remote stations in the Internet

The computers in the LAN use the router as a gateway but are not recognizable themselves. The router divides the intranet from the internet.

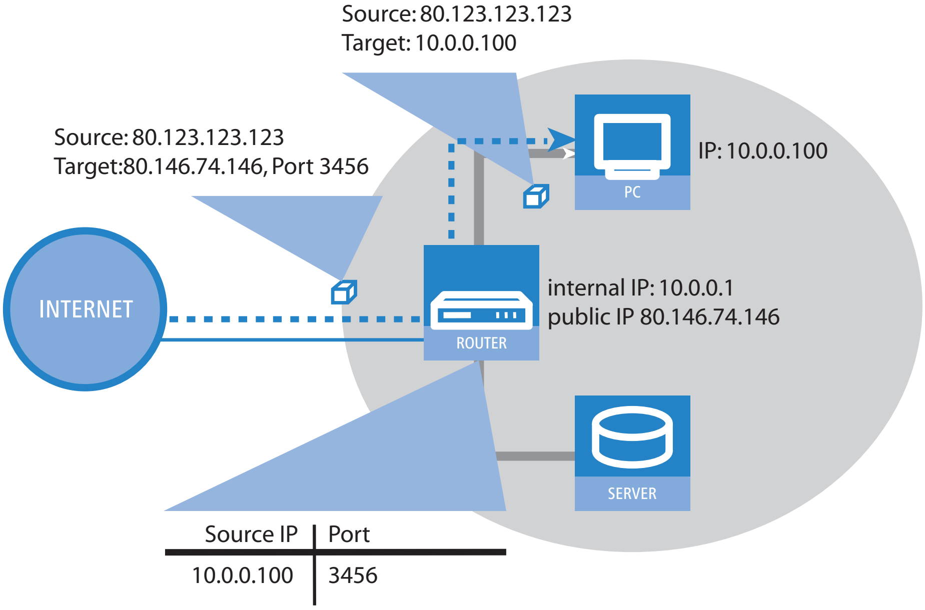
7.5.1 Simple masquerading

How does IP masquerading work?

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



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



Which protocols can be transmitted using IP masquerading?

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

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

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

- IPSec
- IRC

Configuration of IP masquerading

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

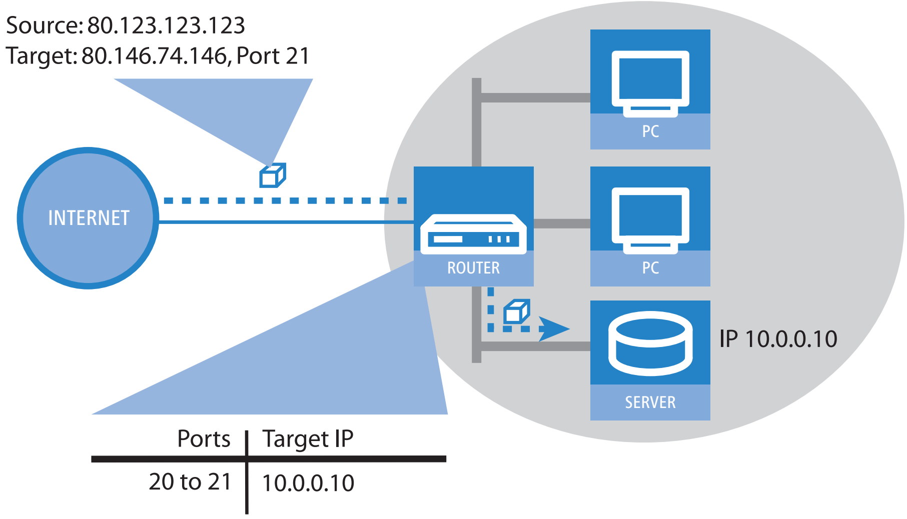
LANconfig: IP router ▶ Routing ▶ Routing table

WEBconfig: LCOS menu tree ▶ Setup ▶ IP-router ▶ IP-routing-table

7.5.2 Inverse masquerading

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

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



Ports	Target IP
20 to 21	10.0.0.10

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.

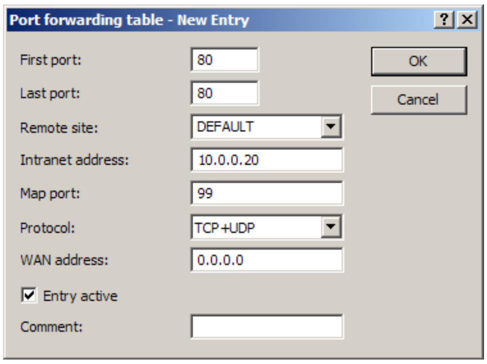
After a specified period of time, the router, however, assumes that the entry is no longer required and deletes it automatically from the table.

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.

On occasion it is desirable for the "exposed" host not to be contacted over this standard port, e.g. when security reasons demand the use of another port.

In this case not only the implementation of ports to an IP address is necessary, but as well the implementation to other ports (port mapping). Another example of use for this port implementation is the implementation of several ports of the WAN to a shared port in the LAN, which can be assigned to different IP addresses (N-IP-Mapping).

The configuration of port mapping involves the assignment of a port or port range (start port to end port) to an IP address from the LAN as the target and the port (map port) to be used in the LAN.



Port forwarding table - New Entry

First port: 80

Last port: 80

Remote site: DEFAULT

Intranet address: 10.0.0.20

Map port: 99

Protocol: TCP+UDP

WAN address: 0.0.0.0

☑ Entry active

Comment:

LANconfig: IP-Router ▶ Masquerading ▶ Port-Forwarding table

WEBconfig: LCOS-menu tree ▶ Setup ▶ IP-Router ▶ 1-N-NAT ▶ Service table

- **Start port**

  D-port from (start port)

- **End port**

  D-port to (end port)

- **Remote site**

  Remote site which applies for this entry.

  - The use of virtual routers requires for the port forwarding a specific selection of the remote station. If no peer is entered then the entry applies to all peers.

- **Intranet-Adresse**

  Internet address that a packet within the port range is forwarded to.

- **Map port**

  Port used for forwarding the packet.

If "0" is entered for the map port, the ports used in the LAN will be the same as those used in the WAN. If a port range is to be mapped, then the map port identifies the first LAN port to be used. For example, mapping the port range '1200' to '1205' to the internal map port '1000' means that the ports 1000 to 1005 will be used for data transfer in the LAN.

Port mapping is static, meaning that two ports or port ranges cannot be mapped to the same map port of a target computer in the LAN. The same port mapping can be used for different target computers.

- **Protocol**

  Protocol which applies for this entry.

- **WAN address**

  WAN address which applies for this entry. If the device has more than one static IP address, then this allows port forwarding to be limited to certain connections.

- **Entry active**

  Switches the entry on or off.

- **Comment**

  Comment on the defined entry (64 characters)

7.6 Demilitarized Zone (DMZ)

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

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

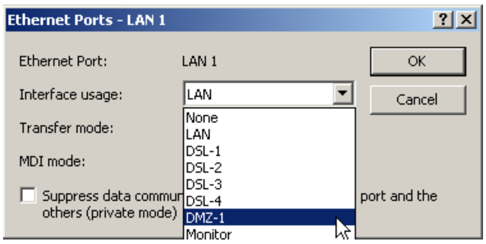
- LAN interface

- WAN interface
- DMZ interface

The 'Overview of functions by model and LCOS* version' → page 17-18 table lists which devices support this functionality.

7.6.1 Assigning interfaces to the DMZ

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


Ethernet Ports - LAN 1

Ethernet Port: LAN 1

Interface usage: LAN

Transfer mode:

MDI mode:

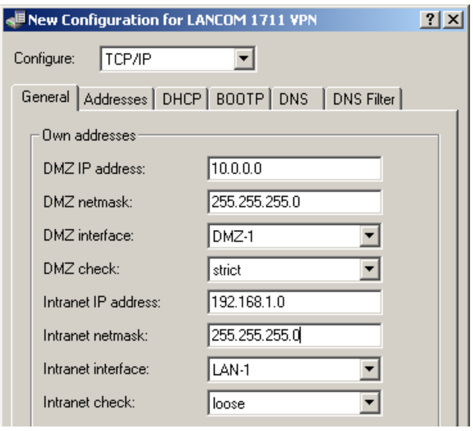
☐ Suppress data commur … port and the others (private mode)

LANconfig: Interfaces ▶ LAN ▶ Ethernet-Ports

WEBconfig: LCOS-menu tree ▶ Setup ▶ Interfaces ▶ LAN

7.6.2 Assigning network zones to the DMZ

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


New Configuration for LANCOM 1711 VPN

Configure: TCP/IP

Own addresses

DMZ IP address: 10.0.0.0

DMZ netmask: 255.255.255.0

DMZ interface: DMZ-1

DMZ check: strict

Intranet IP address: 192.168.1.0

Intranet netmask: 255.255.255.0

Intranet interface: LAN-1

Intranet check: loose

LANconfig: TCP/IP ▶ General

WEBconfig: LCOS-menu tree ▶ Setup ▶ TCP-IP

7.6.3 Address check with DMZ and intranet interfaces

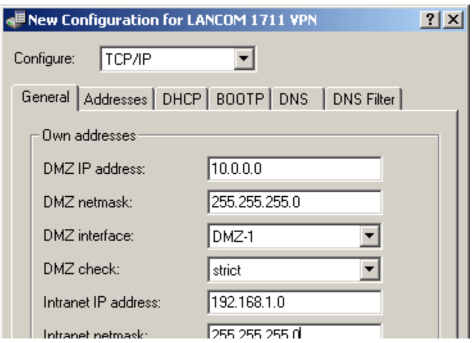
To shield the DMZ (demilitarized zone) and the Intranet from unauthorized attacks, you can activate an additional address check for each interface using the firewall's Intrusion Detection System (IDS).

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

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

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

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


New Configuration for LANCOM 1711 VPN
Configure: TCP/IP
General | Addresses | DHCP | BOOTP | DNS | DNS Filter
Own addresses

DMZ IP address: 10.0.0.0
DMZ netmask: 255.255.255.0
DMZ interface: DMZ-1
DMZ check: strict
Intranet IP address: 192.168.1.0
Intranet netmask: 255.255.255.0

LANconfig: TCP/IP ▶ General

WEBconfig: LCOS-menu tree ▶ Setup ▶ TCP-IP

7.6.4 Unmasked Internet access for server in the DMZ

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

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

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

Two local networks - operating servers in a DMZ

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

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

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

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

Separation of Intranet and DMZ

Although Intranet and DMZ may be already separated on a Ethernet level by distinct interfaces, an appropriate Firewall rule 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:

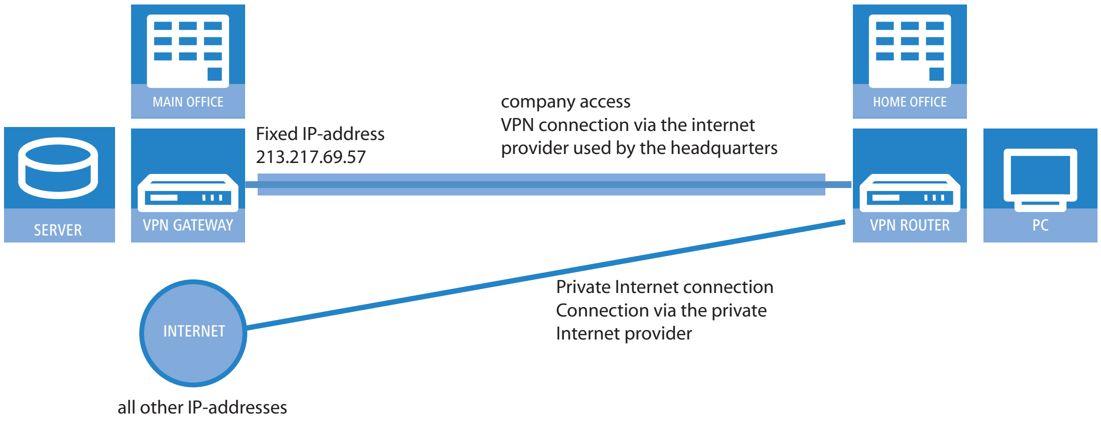
- With a 'Allow All' strategy (default): Deny access from 123.45.67.2 to “All stations in local network“
- With a 'Deny All' strategy (see 'Set-up of an explicit "Deny All" strategy' → page 8-20): Allow access from "All stations in local network" to 123.45.67.2

7.7 Multi-PPPoE

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

7.7.1 Example application: Home-Office with private Internet access

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



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

7.7.2 Configuration

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

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

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

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

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

Administrator rights for the employee in the home office: To avoid the employee making accidental changes to the settings for the Internet provider or VPN access, he should be assigned with the WEBconfig function rights for the "Internet connection" and "Selection of Internet provider" Wizards only. Information about the configuration of special user rights can be found in this addendum under ’Managing rights for different administrators’ → page 4-13.

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

7.8 Load balancing

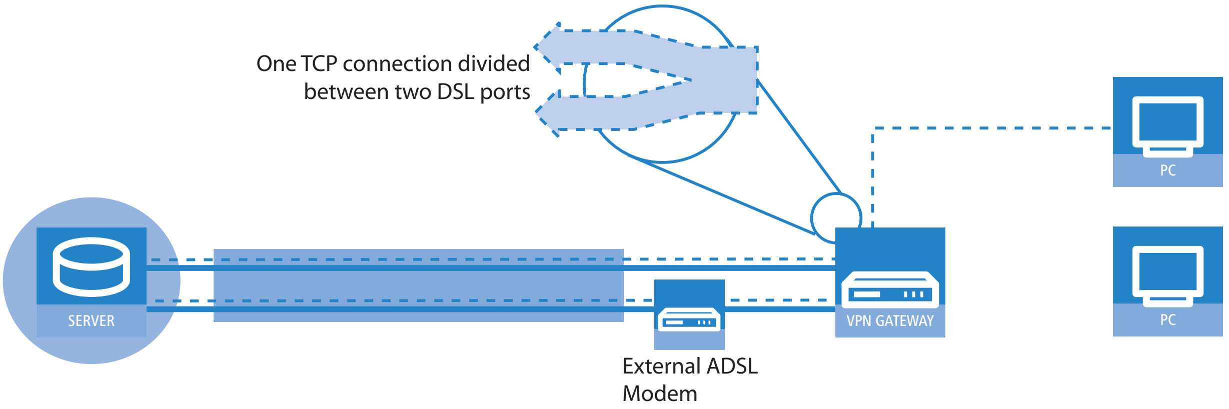
Despite the ever increasing bandwidth of DSL connections, these remain the communications bottle-neck. In some cases it can be advisable to combine multiple DSL connections. There are a number of possibilities to realize this, some of which need active support from the Internet provider:

- DSL channel bundling (Multilink-PPPoE – MLPPPoE)

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

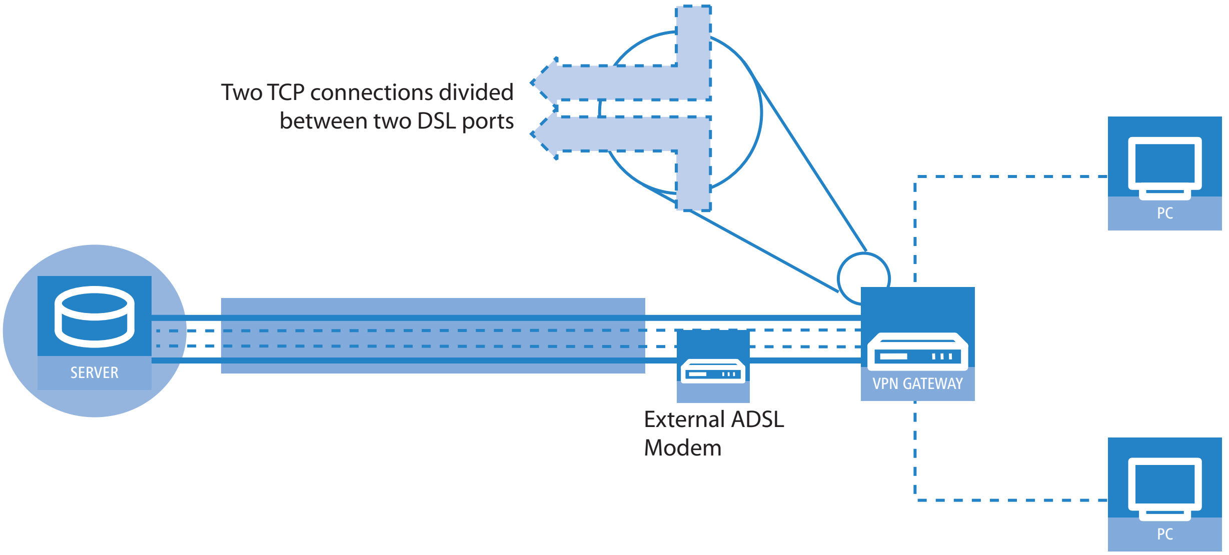
This version of channel bundling provides bandwidths that are a multiple of the smallest bundled channel. This means that it is especially efficient when channels are all of the same bandwidth. The direct bundling of different bandwidths means that the channels with the higher data rates suffer from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

When bundling MLPPPoE for DSL channels behaves in the same way as the well known MLPPP for ISDN channel bundling ('ISDN Channel bundling with MLPPP' → page 7-40).



- Load balancing

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



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

7.8.1 DSL port mapping

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

Please refer to the feature table in the appendix ('Overview of functions by model and LCOS* version' → page 17-18) to see if your device supports the connection of external DSL modems.

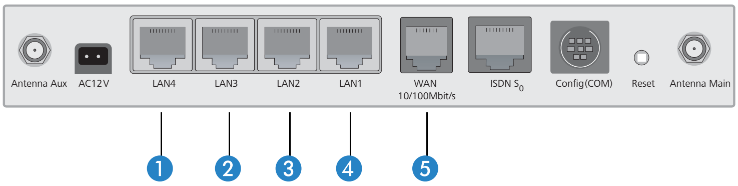
Allocation of switch ports to the DSL ports

Depending on the model ('Overview of functions by model and LCOS* version' → page 17-18), devices with an integrated switch can enable some of the LAN ports to be used as additional WAN ports for connecting to external DSL modems. These ports are listed in the interface table as separate DSL interfaces (DSL-1, DSL-2, etc.). The DSL ports are activated as DSL interfaces in teh WAN interfaces list, configured with the up- and downstream rates and allocated to the switch ports in the LAN interfaces list (example: LANCOM Wireless 1811DSL)

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

- The column 'Port' contains the description of the associated port as marked on the back cover of the device.
- The utilization of the port is listed In the column 'Allocation':
  - None: The port is deactivated
  - LAN-1: The port is allocated to the LAN
  - DSL-1, DSL-2, ... : The port is allocated to one of the DSL interfaces
  - Monitor: The port is a monitor port, i.e. everything received at the other ports is output via this port. A packet sniffer such as Ethereal can be connected to this port, for example.

The allocation of DSL ports to the Ethernet ports can be chosen freely. A well-arranged assignment can be achieved by assigning the DSL ports in reversed order to the ports on the switch (for example: LANCOM Wireless 1811 DSL):



1 LAN4 ▷ DSL-2

2 LAN3 ▷ DSL-3

3 LAN2 ▷ DSL-4

4 LAN1 ▷ LAN-1: This port remains reserved for the LAN.

5 WAN ▷ DSL-1: (dedicated WAN port for the device)

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

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

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

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

- □ The DSL ports have to be activated as DSL interfaces in the list of the WAN interfaces and need to be configurated with the correct up- and downstreams.
- □ In the layer used for the connection, a bundling method has to be activated that is also supported at the remote site.
- □ To configure channel bundling for an internal ADSL interface, the ADSL port '0' is entered into the list of ports **at the top of the list** (e.g. '0,1,2,3' as port list or '0-3' as port range). In the remote device, the communications layer must be set to Layer 1 'AAL-5'.

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

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

For Multi-PPPoE ('Multi-PPPoE' → page 7-22), multiple PPPoE connections share one physical DSL connection. With Multi-DSL, several PPPoE connection are divided between the available DSL interfaces. The maximum possible number of parallel connections is limited to 8 channels.

Allocation of MAC addresses to the DSL ports

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

The following options are available for setting the MAC address:

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

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

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

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

7.8.2 DSL-channel bundling (MLPPPoE)

The used DSL ports are registered in the list of the DSL broadband remote stations to bundle DSL links. Therefore the number of the DSL port is indicated, for several ports in a by comma seperated list (1,2,4) or as a region (1-4).

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

7.8.3 Dynamic load balancing

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

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

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

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

Connection establishment

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

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

Spreading the data load

Two basic methods are available for balancing the data load:

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

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

7.8.4 Static load balancing

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

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

Destination-based channel selection

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

Policy-based Routing

Suitable entries can be made in the firewall to select channels according to the destination port or the source address. These entries are supplemented with a special routing tag that is used to control the channel selection with the routing table. Please refer to 'Policy-based routing' → page 7-3 for further information.

7.8.5 Configuration of load balancing

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

Direct channel bundling via PPPoE

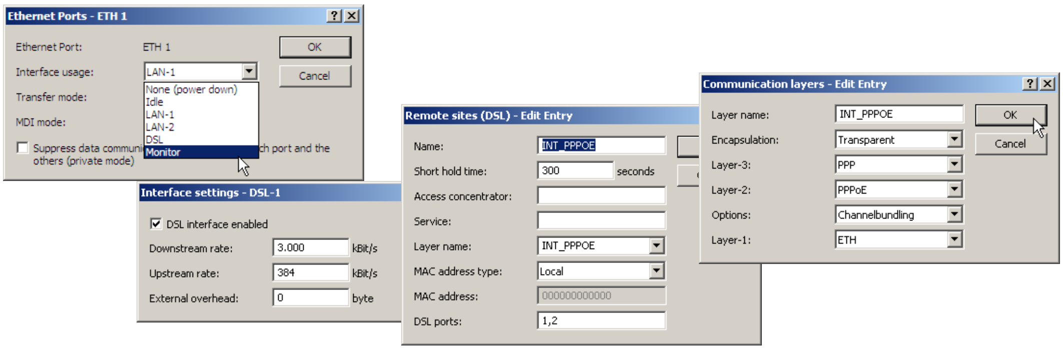
The following method is for the configuration of channel bundling via PPPoE:

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

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

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

④ Activate channel bundling for the relevant layers in LANconfig via **Communication ▶ General ▶ Communication layers**.
Telnet: `/Setup/WAN/Layer`
WEBconfig: **LCOS menu tree ▶ Setup ▶ WAN ▶ Layer**


Ethernet Ports - ETH 1
OK
Cancel
None (power down)
Idle
LAN-1
LAN-2
DSL
Monitor
Interface settings - DSL-1
Remote sites (DSL) - Edit Entry
Communication layers - Edit Entry
OK
Cancel

Ethernet Port: ETH 1
Interface usage: LAN-1
Transfer mode:
MDI mode:
□ Suppress data communi... ...ch port and the others (private mode)

☑ DSL interface enabled
Downstream rate: 3.000 kBit/s
Upstream rate: 384 kBit/s
External overhead: 0 byte

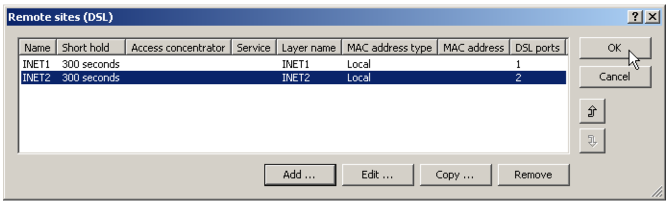
Name: INT_PPPOE
Short hold time: 300 seconds
Access concentrator:
Service:
Layer name: INT_PPPOE
MAC address type: Local
MAC address: 000000000000
DSL ports: 1,2

Layer name: INT_PPPOE
Encapsulation: Transparent
Layer-3: PPP
Layer-2: PPPoE
Options: Channelbundling
Layer-1: ETH

Dynamic load balancing with multiple DSL connections

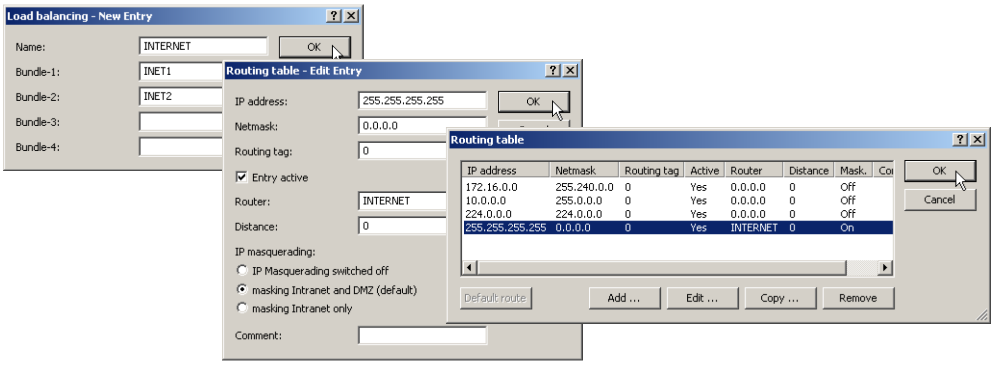
The first step in setting up dynamic load balancing is to define the Internet accesses, e.g. 'INET1' and 'INET2', with the aid of the LANconfig Wizard.

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



Name	Short hold	Access concentrator	Service	Layer name	MAC address type	MAC address	DSL ports
INET1	300 seconds			INET1	Local		1
INET2	300 seconds			INET2	Local		2

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



Name: INTERNET
Bundle-1: INET1
Bundle-2: INET2
Bundle-3:
Bundle-4:

IP address: 255.255.255.255
Netmask: 0.0.0.0
Routing tag: 0
☑ Entry active
Router: INTERNET
Distance: 0
IP masquerading:
○ IP Masquerading switched off
● masking Intranet and DMZ (default)
○ masking Intranet only
Comment:

IP address	Netmask	Routing tag	Active	Router	Distance	Mask.	Co
172.16.0.0	255.240.0.0	0	Yes	0.0.0.0	0	Off	
10.0.0.0	255.0.0.0	0	Yes	0.0.0.0	0	Off	
224.0.0.0	224.0.0.0	0	Yes	0.0.0.0	0	Off	
255.255.255.255	0.0.0.0	0	Yes	INTERNET	0	On	

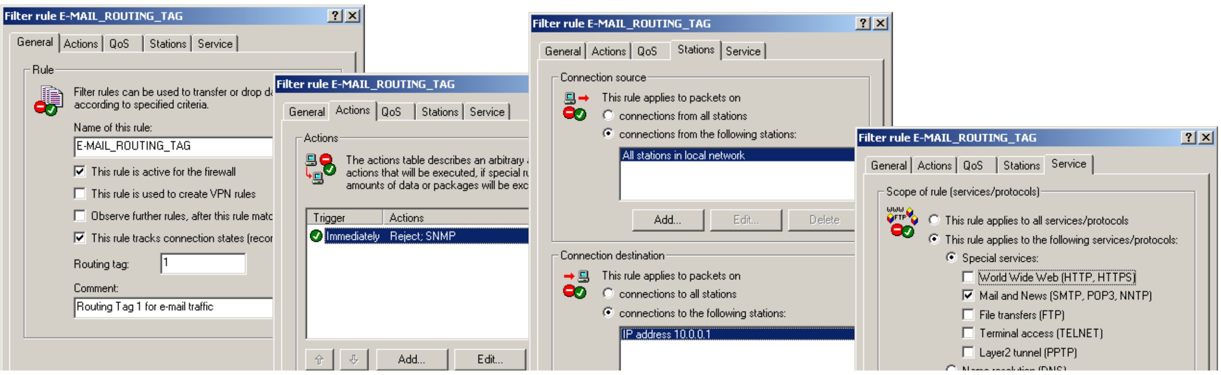
③ The virtual remote site is entered into the routing table as the router for the default route in LANconfig via **IP router ▶ Routing ▶ Routing table**.

Telnet: `/Setup/IP-router/IP-routing-table`
WEBconfig: **LCOS menu tree** ▶ **Setup** ▶ **IP router** ▶ **IP routing table**

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

Routing tags can be used for the application-dependent direction of data traffic to specific DSL ports. If i.e outbound E-Mail traffic ought to be routed via a particular DSL-interface with a particular IP-address, a fitting rule must be established via LANconfig under **Firewall/QoS** ▶ **Rules**, which reroutes all data traffic of all local station’s E-Mail services to the mail server and sets the routing tag ’1’.

Telnet: `/Setup/IP-router/Firewall/Rules`
WEBconfig: **LCOS menu tree** ▶ **Setup** ▶ **IP router** ▶ **Firewall**▶ **Rules**.



Rule
Filter rules can be used to transfer or drop d
according to specified criteria.
Name of this rule: E-MAIL_ROUTING_TAG
☑ This rule is active for the firewall
☐ This rule is used to create VPN rules
☐ Observe further rules, after this rule matc
☑ This rule tracks connection states (recor
Routing tag: 1
Comment: Routing Tag 1 for e-mail traffic

Actions
The actions table describes an arbitrary
actions that will be executed, if special r
amounts of data or packages will be exc

Trigger	Actions
✓ Immediately	Reject; SNMP

Connection source
This rule applies to packets on
○ connections from all stations
● connections from the following stations:
All stations in local network

Connection destination
This rule applies to packets on
○ connections to all stations
● connections to the following stations:
IP address 10.0.0.1

Scope of rule (services/protocols)
○ This rule applies to all services/protocols
● This rule applies to the following services/protocols:
● Special services:
☐ World Wide Web (HTTP, HTTPS)
☑ Mail and News (SMTP, POP3, NNTP)
☐ File transfers (FTP)
☐ Terminal access (TELNET)
☐ Layer2 tunnel (PPTP)
○ Name resolution (DNS)

7.9 N:N mapping

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

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

In the first application the so-called N:1 NAT, also known as IP masquerading (’IP masquerading’ → page 7-16) 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 7-18).

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.

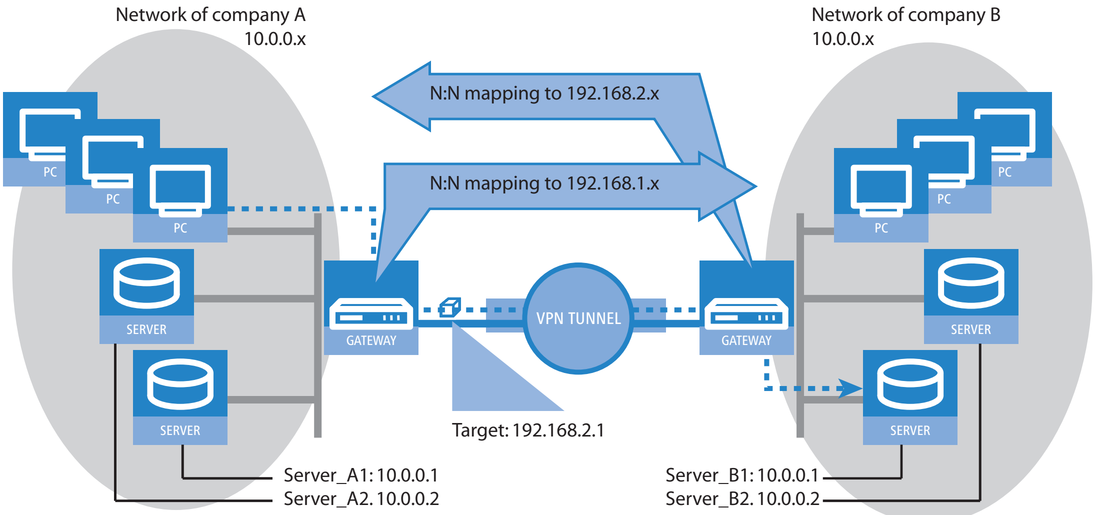
7.9.1 Application examples

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:

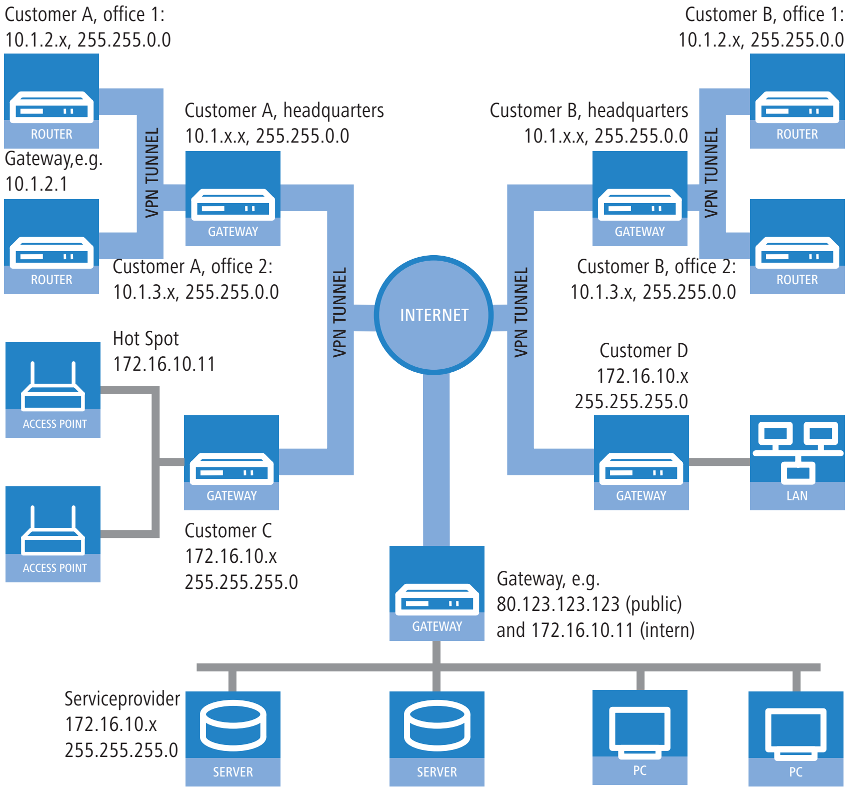


In this example network servers of company A and B should have access over a VPN tunnel to the respective other network. All stations of the LAN should have access to the server of the remote network. For the time being, there is no access possible to the other network, because both networks use the 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 important 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 17-10).

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

There are two different variants to resolve these address conflicts:

Loopback: decentralized 1:1 mapping

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

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

alternatively: central N:N mapping

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

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

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

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

7.9.2 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.

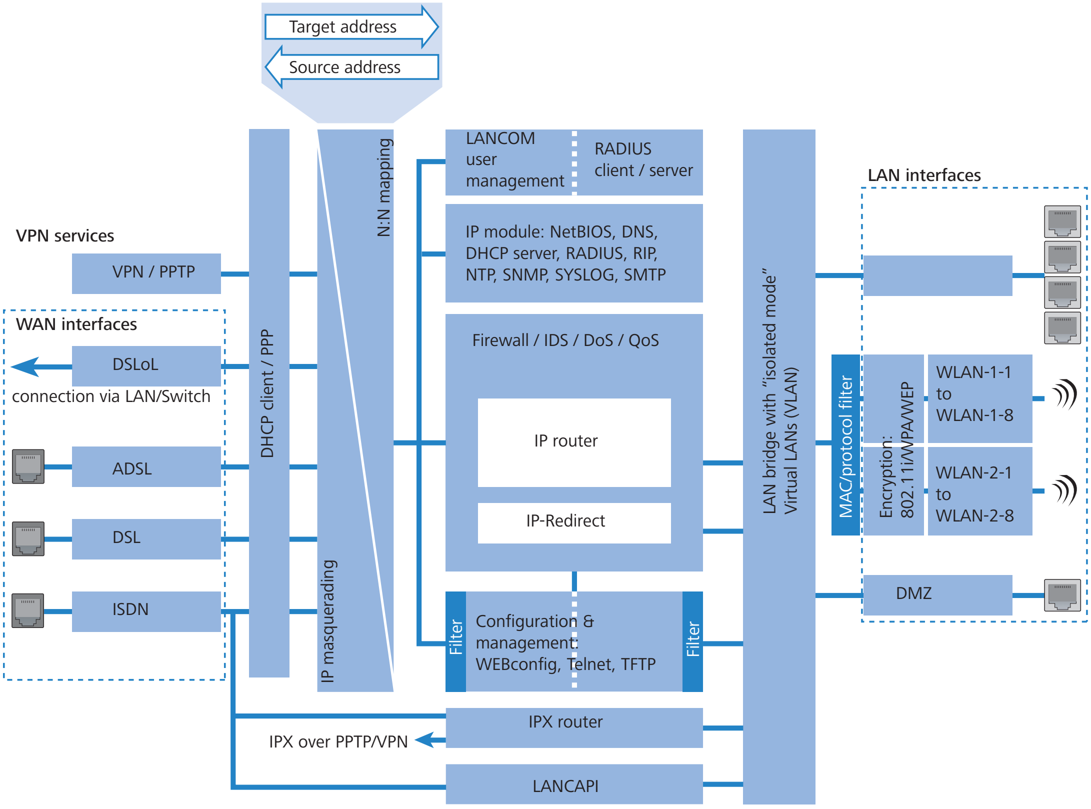
Please notice that the N:N mapping functions are only effective when the firewall has been activated ('General settings of the Firewall' → page 8-10).

Additional configuration hints

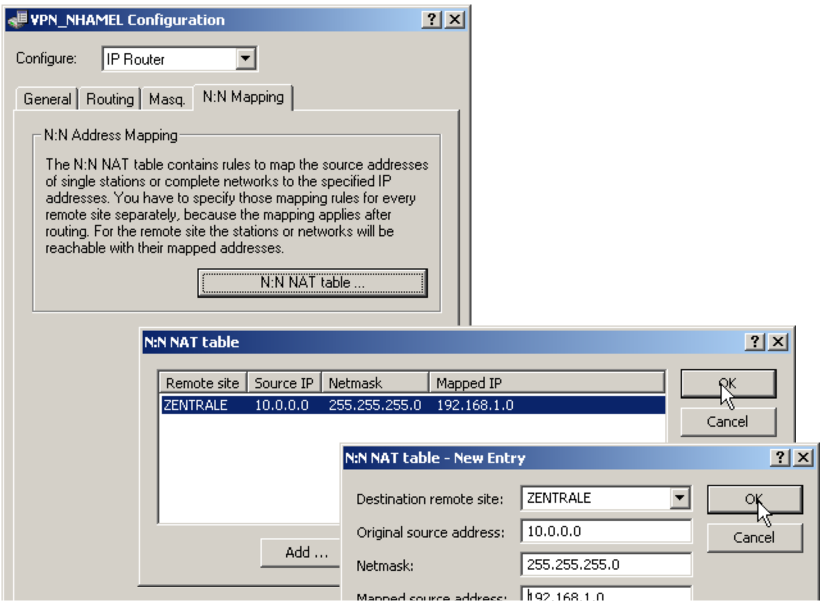
By setting up address translation in the NAT table, the networks and workstations become only visible under another address at first in the higher network compound. But for a seamless routing of data between the networks some further settings are still necessary:

- 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 16-11).
- 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



VPN_NHAMEL Configuration

Configure: IP Router

N:N Address Mapping

The N:N NAT table contains rules to map the source addresses of single stations or complete networks to the specified IP addresses. You have to specify those mapping rules for every remote site separately, because the mapping applies after routing. For the remote site the stations or networks will be reachable with their mapped addresses.

N:N NAT table

Remote site	Source IP	Netmask	Mapped IP
ZENTRALE	10.0.0.0	255.255.255.0	192.168.1.0

N:N NAT table - New Entry

Destination remote site: ZENTRALE

Original source address: 10.0.0.0

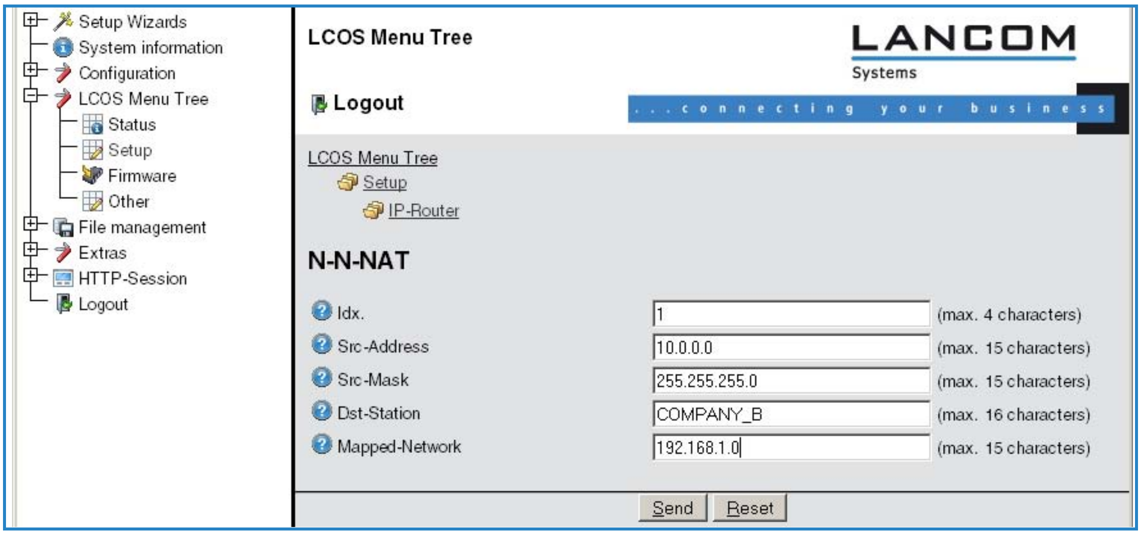
Netmask: 255.255.255.0

Mapped source address: 192.168.1.0

LANconfig: IP router ▶ N:N-Mapping

WEBconfig: LCOS menu tree ▶ Setup ▶ IP router ▶ NAT table

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



N-N-NAT

Idx.	1	(max. 4 characters)
Src-Address	10.0.0.0	(max. 15 characters)
Src-Mask	255.255.255.0	(max. 15 characters)
Dst-Station	COMPANY_B	(max. 16 characters)
Mapped-Network	192.168.1.0	(max. 15 characters)

7.10 Establishing connection with PPP

LANCOM Systems routers also support the point-to-point protocol (PPP). PPP is a generic term for a whole series of WAN protocols which enable the interaction of routers made by different manufacturers since this protocol is supported by practically all manufacturers.

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

7.10.1 The protocol

What is PPP?

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

- Password protection according to PAP, CHAP or MS CHAP
- Callback functions
- Negotiation of the network protocol to be used over the connection established (IP or IPX, for example). Included in this are any parameters necessary for these protocols, for example IP addresses. This process is carried out using IPCP (IP Control Protocol).
- Negotiation of the connection parameters, e.g. the MTU (Maximum Transmission Unit, 'Manual definition of the MTU' → page 7-45).
- Verification of the connection through the LCP (Link Control Protocol)
- Combining several ISDN or DSL channels (MultiLink PPP resp. MultiLink PPPoE)

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

What is PPP used for?

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

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

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

The phases of PPP negotiation

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

- Establish phase

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

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

- Authenticate phase

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

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

- Network phase

  LANCOM, supports the protocols IPCP and IPXCP.

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

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

- Terminate phase

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

PPP negotiation in the LANCOM

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

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

```
trace + ppp
```

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

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

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

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

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

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

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

7.10.3 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.

7.10.4 Settings in the PPP list

In the PPP list, you are able to specify you own definition of PPP negotiation for every remote site contacting your network.

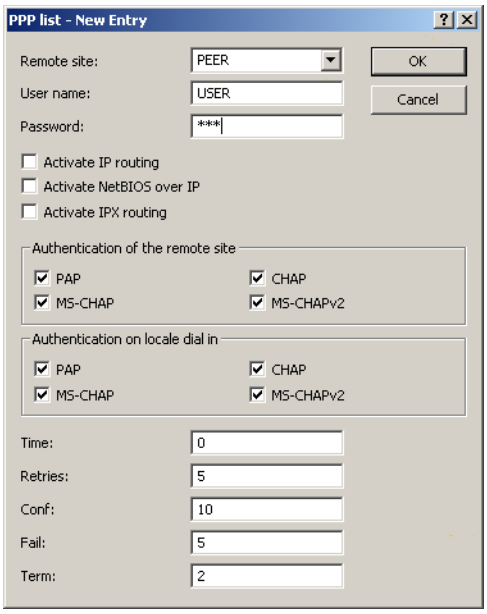
The authentication of point-to-point connections in the WAN commonly relies on one of the protocols PAP, CHAP, MSCHAP or MSCHAPv2. The protocols here have a "hierarchy" amongst themselves, i. e. MSCHAPv2 is a "higher-level" protocol than MSCHAP, CHAP and PAP (higher protocols provide higher security). Many dial-in routers at Internet providers allow up-front authentication using a higher-level protocol such as CHAP, but only support the use of PAP further down the line. If the setting for the protocol for authentication is fixed in the LANCOM, the connection may fail because no common authentication protocol can be negotiated.

In principle authentication can be repeated while the connection is being negotiated. Another protocol can be selected if, for example, it can only be recognized from the username at the earliest. However, this repeat negotiation is not supported in all scenarios. In particular when dialing in over UMTS, the LANCOM must explicity refuse the provider's request for CHAP to be able to provide PAP user data for requests to be forwarded by the provider.

A flexible setting for the authentication protocols in the LANCOM ensures that the PPP connection is established as required. In addition, one or more protocols can be defined that are accepted for authentication of remote sites in the LANCOM (inbound connections) and on login of the LANCOM into other remote sites (outbound connections).

- When establishing inbound connections, the LANCOM requires the lowest of the permitted protocols, but where possible it also permits the remote site to use one of the higher-level protocols (enabled in the LANCOM).
- When establishing outbound connections, the LANCOM offers all enabled protocols, but only permits a selection from precisely these protocols. It is not possible to negotiate one of the disabled, possibly higher-level, protocols.

The PPP authentication protocols are set in the PPP list.



PPP list - New Entry

Remote site: PEER

User name: USER

Password: ***

☐ Activate IP routing

☐ Activate NetBIOS over IP

☐ Activate IPX routing

Authentication of the remote site

☑ PAP ☑ CHAP

☑ MS-CHAP ☑ MS-CHAPv2

Authentication on locale dial in

☑ PAP ☑ CHAP

☑ MS-CHAP ☑ MS-CHAPv2

Time: 0

Retries: 5

Conf: 10

Fail: 5

Term: 2

LANconfig: Communication ▶ Protocols ▶ PPP list

WEBconfig: Setup ▶ WAN ▶ PPP

7.10.5 The meaning of the DEFAULT remote site

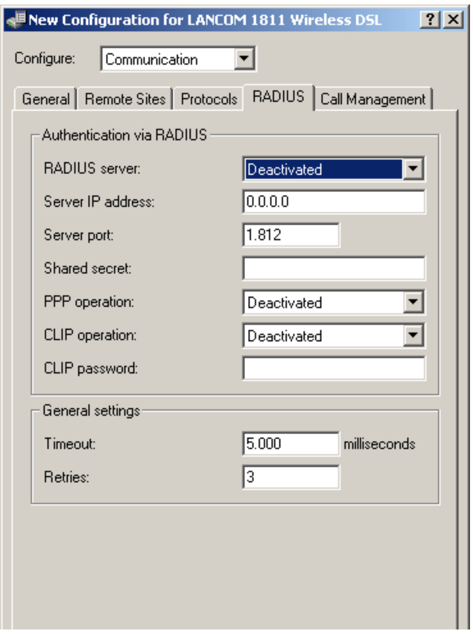
During PPP negotiations, a remote site dialing-in to the LANCOM logs on with its name. The LANCOM can use the name to retrieve the permitted values for authentication from the PPP table. At the start of the negotiation, the remote site occasionally cannot be identified by call number (ISDN dial-in), IP address (PPTP dial-in) or MAC address (PPPoE dial-in). It is thus not possible to determine the permitted protocols in this first step. In these cases, authentication is performed first with those protocols enabled for the remote site with name DEFAULT. If the remote site is authenticated successfully with these settings, the protocols permitted for the remote site can also be determined.

If authentication uses a protocol entered under DEFAULT, but which is not permitted for the remote site, then authentication is repeated with the permitted protocols.

7.10.6 RADIUS authentication of PPP connections

PPP connections can also be authenticated by an external RADIUS server. However, these external RADIUS servers do not necessarily support all available protocols. For this reason, the permitted protocols can also be selected in the configuration of the RADIUS authentication. LCP negotiation is restarted with the permitted protocols if the RADIUS server does not support the negotiated protocol.

WAN RADIUS table



New Configuration for LANCOM 1811 Wireless DSL

Configure: Communication

Authentication via RADIUS

RADIUS server: Deactivated

Server IP address: 0.0.0.0

Server port: 1.812

Shared secret:

PPP operation: Deactivated

CLIP operation: Deactivated

CLIP password:

General settings

Timeout: 5.000 milliseconds

Retries: 3

LANconfig: Communication ▶ RADIUS

WEBconfig: Setup ▶ WAN ▶ RADIUS

7.11 DSL dial-in over PPTP

Some DSL providers enable dial-in over PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) instead of PPPoE. PPTP is an extension of PPP, partly developed by Microsoft.

With PPTP it is possible to build up a “tunnel” over IP nets to a remote station. A tunnel is a logical shielded connection, that protects the transferred data from unauthorized access. For this purpose the encoding algorithm RC4 is used.

Configuration of PPTP

As soon as the internet access over PPTP is selected the LANCOM enquires all needed PPTP parameters with the Internet Access Wizard. Additionally to the entries for PPPoE access the IP address of the gateway must be specified. A PPTP gateway is often a DSL modem. Detailed information is available from your DSL provider.

The configuration can be changed in the PPTP list:

LANconfig: communication ▶ protocols ▶ PPTP list

WEBconfig: LCOS menu tree ▶ Setup ▶ WAN ▶ PPTP list

The PPTP configuration consists of three parameters:

- 'Remote site'—the entry from the DSL-Broadband-Peers list.
- 'IP address'—IP address of the PPTP gateway, often the address of the DSL modem.
- 'Port'—IP port the PPTP protocol runs on. For conformity with the protocol standard enter the port '1.723'.

7.12 Extended connection for flat rates—Keep-alive

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

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

Configuration of Keep-alive function

The keep alive procedure is configured in the peer list.

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

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

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

7.13 Callback functions

LANCOM models with ISDN interface support the automatic callback function.

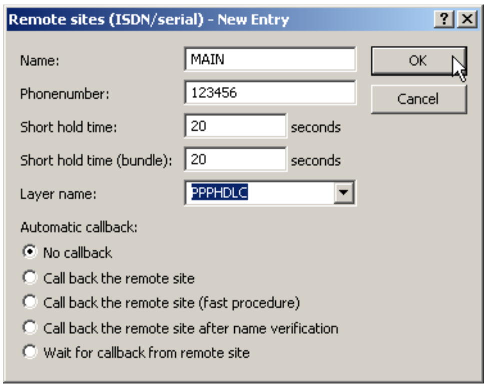
In addition to callback via the D channel, the CBCP (**C**allback **C**ontrol **P**rotocol) specified by Microsoft and callback via PPP as per RFC 1570 (PPP LCP extensions) are also offered. There is also the option of a particularly fast callback using a process developed by LANCOM. PCs with Windows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

7.13.1 Callback for Microsoft CBCP

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

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

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



Name: MAIN
Phonenumber: 123456
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

No callback

For this setting, the callback entry must be set to 'off' when configuring via WEBconfig or in the console.

Callback number specified by caller

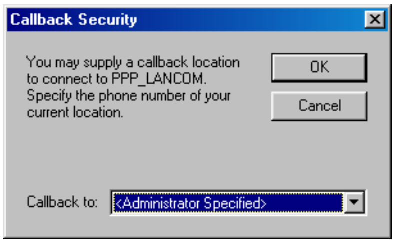
For this setting the callback entry must be set to 'Call back the remote site after name verification' (or must have the value 'Name' in WEBconfig or in the console). In the peer list **no** telephone number may be specified.

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

The calling number is determined in the LANCOM

For this setting the callback entry must be set to 'Call back the remote site after name verification' (or must be set to the value 'Name' in WEBconfig or in the console). In the peer list **one** telephone number must be specified.

Some Windows versions (especially Windows 98) prompt the user to confirm the callback to the telephone number stored in the LANCOM ('Administrator Specified') with an input window. Other Windows versions only inform the user that the PC is waiting for the callback from the LANCOM.



You may supply a callback location to connect to PPP_LANCOM. Specify the phone number of your current location.

Callback to: <Administrator Specified>

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.

7.13.2 Fast callback

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

- The caller who may wish to be called back can activate the function 'Wait for callback from remote site' in the peer list (or 'Looser' when configuring via WEBconfig, terminal program or Telnet).
- The callback party selects 'Call back the remote site (fast procedure)' in the peer list and enters the calling number ('fast' when configuring via WEBconfig, terminal program or Telnet).

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

7.13.3 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.

7.13.4 Overview of configuration of callback function

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

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

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

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

7.14 ISDN Channel bundling with MLPPP

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

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

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

Bundling over MLPPPoE can also be arranged for DSL channels (’DSL-channel bundling (MLPPPoE)’ → page 7-25).

Two methods of channel bundling

- Static channel bundling

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

- Dynamic channel bundling

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

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

Here's how to configure your system to combine channels

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

① Select a communication layer for the remote station from the layer list that has bundling activated in the Layer-2 options. Select from the following Layer-2 options:

- □ **compr.** according to the LZS data compression procedure (Stac) reduces the amount of data if the data hasn't already been compressed. This procedure is also supported by routers of other manufacturers and by ISDN adapters under Windows operating systems.
- □ **bundle** uses two B channels per connection.
- □ **bnd+cmpr** uses both (compression and channel bundling) and provides the maximum possible data transmission performance.

② Now create a new entry in the peer list. When doing so, watch the holding times for the connection. Please observe the following rules:

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

③ Use the entry for the Y connection in the Router interface list to determine what should happen if a second connection to a different remote station is requested during an existing connection using channel bundling.

WEBconfig: LCOS menu tree ▶ Setup ▶ WAN ▶ Router-interface-list

- □ Y connection **On**: The router interrupts the bundled connection to establish a connection to the other remote station. When the second channel is free again, the originally bundled connection automatically takes the channel back (always in the case of static bundling, only as required when using dynamic bundling).
- □ Y connection **Off**: The router maintains the existing bundled connection; the establishment of the new connection must wait.

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

7.15 Operating a modem over the serial interface

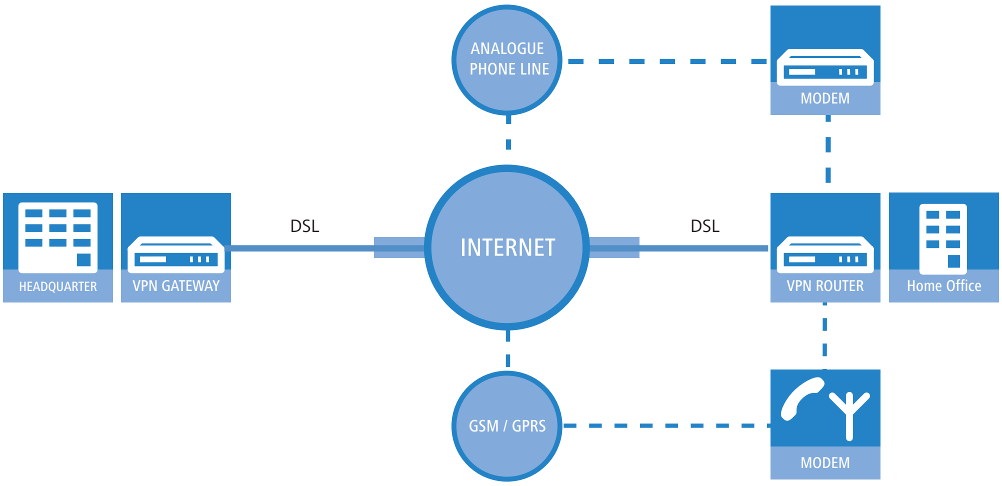
This section refers only to devices with a serial configuration interface.

7.15.1 Introduction

Internationally, analog telephone connections are just as common in the business world as the predominant ISDN connections in Germany. The operation of international networks thus places particular demands on remote maintenance options and for high-availability of the gateways and thus requires different interfaces than the ISDN common in Germany. Apart from conventional analog telephone lines, mobile telephone networks such as GSM or GPRS may, in certain cases, represent the only way of providing remote maintenance without broadband or other cabled access.

In response to these requirements, most LANCOM models with a serial interface can be extended with an additional WAN interface with the use of analog modems, GSM or GPRS. The following functions are available with a suitable modem in combination with the LANCOM Modem Adapter Kit:

- Internet access via modem with all of the router functions such as firewall, automatic connection establishment and termination, etc.
- Remote maintenance (e.g. dial-in to international sites)
- Backup connection (e.g. high-availability through GSM/GPRS modem connection)



7.15.2 System requirements

The following are required to set up a backup connection over the serial interface:

- LANCOM with serial configuration interface and support for LANCOM modem adapter kit. For devices with serial configuration interface please refer to the table 'Overview of functions by model and LCOS* version' → page 17-18 to see, whether your model supports the modem operation at serial interface.
- LANconfig or alternatively a web browser or Telnet
- Serial configuration cable (supplied with the device)
- Analog modem, Hayes compatible, with access to a suitable analog telephone connection (D-sub9 or D-sub25 connector)
- LANCOM modem adapter kit to connect the modem over the serial configuration cable

7.15.3 Installation

The installation simply involves the connection of the modem with the LANCOM Modem Adapter Kit with the serial configuration interface of the LANCOM.

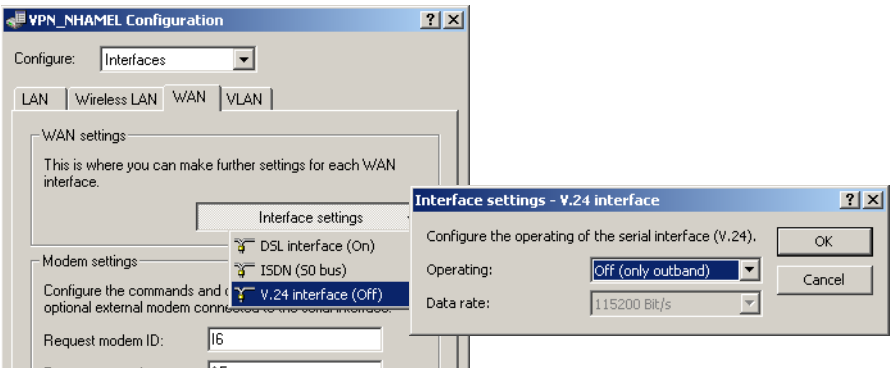
Please do not use any other adapters than the original LANCOM Modem Adapter Kit! The contact assignment of the LANCOM Modem Adapter Kit differs from other commercial adapters like “null modem cables” or the like. The use of uncompliant accessories will cause serious damage on the LANCOM and/or the modem. For further details please refer to the 'Contact assignment of modem adapter kit' → page 7-45.

7.15.4 Set the serial interface to modem operation

The operation of the serial interface requires the operating mode and bitrate to be set.

- Operating mode [default: outband]
  - Outband: In this mode, the serial interface is only used for configuration with a terminal program.
  - Modem: In the 'Modem' setting, the device attempts to find a modem connected to the serial interface. If this is successful then the modem can be used as an additional WAN interface. If a computer running a terminal program is detected, then the device automatically switches the interface into outband mode.
  - Interlink: Direct connection between two LANCOM devices
- Bitrate [default: 115,200 bps.]

  Set the maximum bitrate supported by your modem. The serial interfaces of LANCOM devices support data rates of 19,200 bps, 38,400 bps, 57,600 bps up to a maximum of 115,200 bps.



VPN_NHAMEL Configuration

Configure: Interfaces

WAN settings

This is where you can make further settings for each WAN interface.

Modem settings

Configure the commands and optional external modem conn

Request modem ID: I6

Interface settings - V.24 interface

Configure the operating of the serial interface (V.24).

Operating: Off (only outband)

Data rate: 115200 Bit/s

LANconfig: Interfaces ▶ WAN ▶ V.24-Interface

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ V.24-Interface

As long as the LANCOM is set to modem mode, a terminal program operating over the serial interface will display the AT commands that the LANCOM device transmits while attempting to identify a connected modem. In the terminal program, press the return key repeatedly until the modem identification is interrupted and start the configuration session.

7.15.5 Configuration of modem parameters

The operation of a modem at the serial interface requires the following settings:

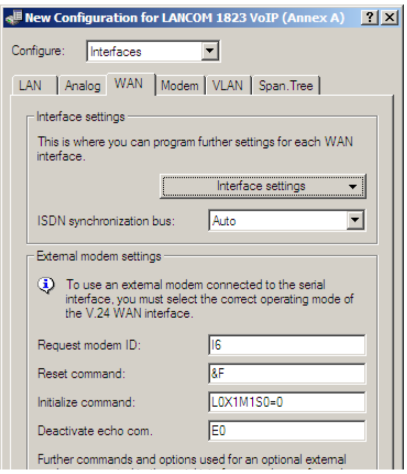
- Request modem ID [Default: `ATI6`]
- Reset command [default: `AT&F`]
- Initialize command [default: `ATL0M1X1S0=0`]
  - `L0`: Loudspeaker quiet
  - `M1`: Loudspeaker on while connecting
  - `X1`: Operation at an extension
  - `S0=0`: Disable auto answering
- Deactivate modem echo [default: `ATE0`]
- AT polling cycle time [Default: `1` in seconds]
- AT polling count [Default: `5`]
- Ring count [Default: `1`]
- Initialize answer command
- Answer command [Default: `ATA`]
- Initialize dial command
- Dial command [default: `ATDT`]
- Escape sequence to terminate data phase resp. to return to command phase [Default: `+++`]
- Hold time after escape sequence [Default: `1000` in milliseconds]
- Disconnect: command to hang up during data phase [Default: `ATH`]

The modem parameters are set with values that should suit most modems. Thus changes are generally not necessary. Refer to the documentation for your modem for settings that vary from these.

Setting up a GPRS backup connection

If the connection is to use a GPRS-capable modem at the serial interface, you will need the APN name and the dial-up telephone number. The following init-strings for the configuration apply to T-Mobile and Vodafone:

- T-Mobile
  - Init-string: `L0X1M1S0=0+CGDCONT=1, "IP", "internet.t-d1.de"`
  - Dial-up number: `*99#`
- Vodafone
  - Init-string: `L0X1M1S0=0+CGDCONT=1, "IP", "web.vodafone.de"`
  - Dial-up number: `*99#` or `*99***1#`



Configure: Interfaces

This is where you can program further settings for each WAN interface.

ISDN synchronization bus: Auto

To use an external modem connected to the serial interface, you must select the correct operating mode of the V.24 WAN interface.

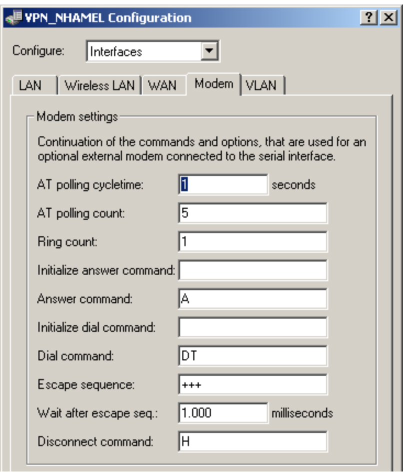
Request modem ID: I6

Reset command: &F

Initialize command: L0X1M1S0=0

Deactivate echo com. E0

Further commands and options used for an optional external



Configure: Interfaces

Continuation of the commands and options, that are used for an optional external modem connected to the serial interface.

AT polling cycletime: 1 seconds

AT polling count: 5

Ring count: 1

Initialize answer command:

Answer command: A

Initialize dial command:

Dial command: DT

Escape sequence: +++

Wait after escape seq.: 1.000 milliseconds

Disconnect command: H

LANconfig: Interfaces ▶ WAN or ▶ Modem

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ Modem-Parameters

Entering special characters in the console

For a GPRS dial-up, the initialisation strings require the entry of inverted commas and equal signs. Certain special characters can be correspondingly marked with a leading backslash:

- *
- "
- =
- space
- **Example:** `+cgdcont\=1,\"IP\",\"internet.t-d1.de\"`

As an alternative, the entire command sequence can be enclosed within inverted commas. In this case, those inverted commas which are inside the surrounding inverted commas must be preceded by a backslash.

- **Example:** `"+cgdcont=1,\"IP\",\"internet.t-d1.de\""`

7.15.6 Direct entry of AT commands

The command

- `sendserial "AT..."`

allows you to use Telnet to send a character string directly to a modem that is connected to the LANCOM. This function allows you to send any AT commands to the modem.

Sending AT commands ist possible in the internal modem state 'idle' or 'Modem ready' only. The responses can be found in the serial trace ('Trace output' → page 7-44).

7.15.7 Statistics

Statistics about activities of the serial interface can be accessed with a terminal program or Telnet under:

`Status/Modem-Status`

The statistics show the following states:

- the type of modem identified
- the status of its last connection, e.g. the transfer rate, the transfer protocol used or the error-detection method used
- internal state of modem management, e.g.
  - □ device detection
  - □ interface deactivated
  - □ modem initialization
  - □ modem ready
  - □ connection establishment
  - □ modem in data mode

  These messages may be very helpful for debugging purposes.

7.15.8 Trace output

The command

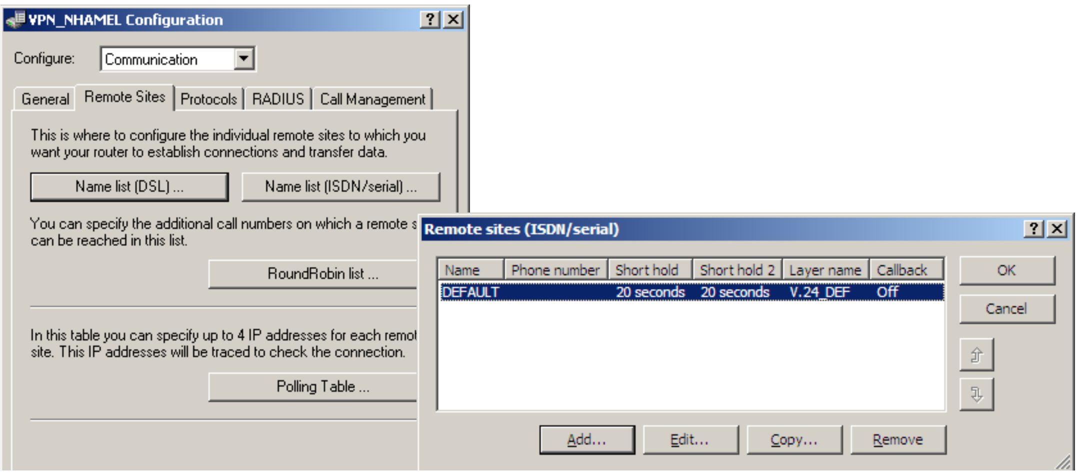
- `trace + serial`

allows you to start the trace output for the serial interface in a Telnet session when a LANCOM has a modem connected. The output shows all messages exchanged up until the establishment of data transfer between the modem and the LANCOM.

7.15.9 Configuration of remote sites for V.24 WAN interfaces

To establish a connection to a remote station via the modem connected to the serial interface, a corresponding entry in the remote site list (ISDN/serial) must be generated. The remote sites list (ISDN/serial) contains the following information:

- Name: Name of the remote site
- Telephone number: Telephone number that reaches the remote site. The field can be left empty if calls are to be received only.
- Hold time: This time defines how long a connection is kept active even if no more data is being transferred. If a zero is entered, the connection will not be interrupted automatically. A hold time of "9999" means that the connection is permanently held open. If it is interrupted, then the connection will be actively opened up again. This behavior is known as **keep alive**.
- 2. Hold time: Is ignored.
- Layer name: The layer 'V.24_DEF' is selected for the connection over the serial WAN interface. The layer is preset and does not need further configuration. The layer 'V.24_DEF' uses the following settings:
  - □ Encapsulation: Transparent
  - □ Layer 3: APPP (asynchronous PPP)
  - □ Layer 2: Transparent
  - □ Options: none
  - □ Layer 1: SERIAL (shows that the serial interface is being used for connections via the layer 'V.24_DEF')



This is where to configure the individual remote sites to which you want your router to establish connections and transfer data.

You can specify the additional call numbers on which a remote s can be reached in this list.

In this table you can specify up to 4 IP addresses for each remot site. This IP addresses will be traced to check the connection.

Name	Phone number	Short hold	Short hold 2	Layer name	Callback
DEFAULT		20 seconds	20 seconds	V.24_DEF	Off

The remote site list with the remote sites for the modem at the serial interface can be found under the following paths:

LANconfig: Communication ▶ Remote sites ▶ Remote sites (ISDN/serial)

WEBconfig: LCOS menu tree ▶ Setup ▶ WAN ▶ Dialup-Peers

Once an entry in the remote site list has been generated for the WAN interface, this remote station can be used just like any other for routing and WAN connections.

7.15.10 Configuration of a backup connection on the serial interface

The configuration of a backup connection via a modem at the serial interface requires first of all an entry in the Dialup-Peers list so that the required remote site can be reached. The following entries will also be required for the configuration of the LANCOM:

- Entry in the backup table

  In the backup table, generate an entry for the remote site that is to be used for the backup connection. This remote site is to be allocated to the remote site that is to be called by the modem at the serial interface.

  The backup table is to be found under the following paths:

LANconfig: Communication ▶ Call Management ▶ Backup Table

WEBconfig: LCOS menu tree ▶ Setup ▶ WAN ▶ Backup table

- Entry in the polling table

  If the link to the remote station that is to be backed up cannot be checked by LCP polling (with PPP only) then an additional entry in the polling table is required. This involves assigning the remote site with an IP address that can be regularly tested with a ping command. The IP address should typically be a computer directly at the opposite end of the connection being tested, e.g. a DNS server in your provider's network.

  The polling table is to be found under the following paths:

LANconfig: Communication ▶ Remote Sites ▶ Polling Table

WEBconfig: LCOS menu tree ▶ Setup ▶ WAN ▶ Polling table

7.15.11 Contact assignment of modem adapter kit

Device signal	D-Sub9 plug	Device or modem signal	D-Sub9 plug
TxD	3	RxD	2
RxD	2	TxD	3
RTS	7	CTS	8
CTS	8	RTS	7
DTR	4	DCD	1
DCD	1	DTR	4
GND	5	GND	5

7.16 Manual definition of the MTU

Many Internet providers operate their own backbone; however, their customers dial in to the network over the access nodes provided by third-party telecommunications providers. The two-stage dail-in procedure can lead to problems with the realized data rate:

- When dialing into the nodes of Deutsche Telekom, for example, a LANCOM negotiates a permissible maximum transmission unit (MTU), which defines the greatest possible size of unfragmented data packet. This MTU is then used by the LANCOM.
- When the data packets are forwarded to the actual provider, an additional header is added which increases the size of the data packets again. For the data packets to meet with the permitted size, they must now be fragmented into smaller units. This additional fragmentation can cause losses in the data-transfer speeds.

This problem can be avoided by entering a fixed MTU for each remote site.

7.16.1 Configuration

WEBconfig: LCOS-menu tree ▶ Setup ▶ WAN ▶ MTU list

The table contains the following entries:

- Device name: Name of the remote device. It can be a physical or a virtual (PPTP/VPN) remote site
- MTU: MTU to be used for the connection

7.16.2 Statistics

Under **Status** ▶ **WAN-statistics** you will find the MTU statistics recorded for all current connections. The table is partially dynamic and begins with 16 entries. Like the MTU-list under **Setup** ▶ **WAN** it includes two columns in which the device name and the MTU are stored.

Remote site	MTU	Remark
INET	1200	The INET remote site is the Internet connection and a forced MTU of 1200 bytes.
MULTI	1492	MULTI is a PPPoE connection, for which the MTU was negotiated (and is consequently 1492 bytes).
TESTVPN	1100	TESTVPN is a VPN connection established via the Internet. An assumed overhead of 100 bytes is taken for VPN connections, and consequently the MTU here is 1100 bytes.
TESTVPN-PPTP	1060	TESTVPN-PPTP is a PPTP connection established over the VPN connnection TESTVPN. The overhead for PPTP connections is 40 bytes, and consequently the MTU here is 1060 bytes.

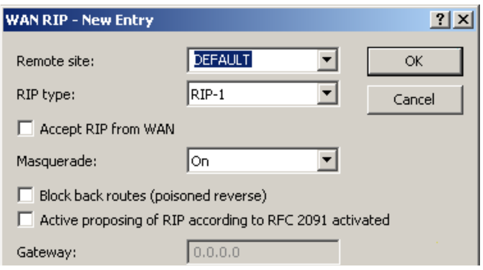
MTU lists and MTU statistics are only available for devices with a DSL or ADSL interface.

7.17 WAN RIP

In order for routes learned from RIP to be broadcast across the WAN, the respective remote sites can be entered into the WAN RIP table. The WAN RIP table contains the following values:

- **Remote site**: The name of the remote site is listed in the 'Remote site' column
- **RIP type**: The column RIP type details the RIP version with which the local routes are propagated
- **RIP accept**: The column RIP accept lists whether RIP from the WAN is to be accepted. The RIP type must be set for this.
- **Masquerade**: The column Masquerade lists whether or not masquerading is performed on the connection and how it is carried out. This entry makes it possible to start WAN RIP even with an empty routing table. The following values are possible:
  - **Auto**: The masquerade type is taken from the routing table (value: 0). If there is no routing entry for the remote site, then masquerading is not performed.
  - **On**: All connections are masqueraded (value: 1).
  - **Intranet**: IP masquerading is used for connections from the intranet, connections from the DMZ pass through transparently (value: 2).
- **Default tag**: The column Default tag lists the valid "Default routing tag" for the WAN connection. All untagged routes are tagged with this tag when sent on the WAN.
- **Routing tags list**: The column Routing tags list details a comma-separated list of the tags that are accepted on the interface. If this list is empty, then all tags are accepted. If at least one tag is in the list, then only the tags in this list are accepted. When sending tagged routes on the WAN, only routes with valid tags are propagated.

  All learned routes from the WAN are treated internally as untagged routes and propagated on the LAN with the default tag (0). In the WAN, they are propagated with the tag with which they were learned.


WAN RIP - New Entry

Remote site: DEFAULT

RIP type: RIP-1

□ Accept RIP from WAN

Masquerade: On

□ Block back routes (poisoned reverse)

□ Active proposing of RIP according to RFC 2091 activated

Gateway: 0.0.0.0

LANconfig: IP-Router ▶ General

WEBconfig: LCOS-menu tree ▶ Setup ▶ IP-Router ▶ RIP ▶ WAN-Sites

7.18 The rapid spanning tree protocol

In networks with many switches and bridges, many physical connections can exist between two stations that are connected to the network. These redundant data paths are desirable because they can offer alternative paths to the desired destination in case individual network paths fail. On the other hand, these multiple connections can also lead to loops or cause network stations to receive multiple frames. Both occurrences negatively impact free data traffic performance in the network.

The Spanning Tree Protocol (STP) enables an analysis of the network at the layer 2 level and, as such, offers solutions for intelligent path selection between two network stations below the routing layer. By discovering redundant paths between network stations, STP builds a unique structure in which loops and double packets can be avoided. To this end, so-called Bridge Protocol Data Units (BPDUs) are sent as a multicast to a specific MAC address. The BPDUs allow redundant paths to be discovered as well as the distance and the data rate available on this connection. Using these values, the Spanning Tree Protocol calculates a priority (also called route or path costs) with which the various connections are to be treated. The low-priority connections are disabled and are therefore no longer available for clients. Through the reduction of non-redundant connections between the clients, the protocol builds a tree which unambiguously defines all of the connections that arise from a central switch (root bridge).

The BPDUs are sent regularly in the network in order to check the availability of the connections. If a connection fails, then the network analysis is triggered again; the possible paths and the corresponding priorities are redefined.

After initialisation all ports will initially be in the "blocking" state, in which only BPDUs are transmitted. The ports subsequently switch to the states of "listening" and then "learning" before reaching "forwarding" which allows payload data to be exchanged via the ports.

7.18.1 Classic and rapid spanning tree

The early version of the spanning-tree protocol compliant with IEEE 802.1D, here referred to as classic spanning tree, had the problem that changes to topology after a connection failure were implemented very slowly: Depending on the complexity of the network, the classic spanning tree takes between 20 seconds and a minute to establish new routes. For many network services a failure of this length of time is unacceptable.

The spanning tree protocol was improved and published as the "Rapid Spanning Tree Protocol" (RSTP), initially as the IEE 802.1t/w standard and later as a part of the newly published IEEE 802.1D. Even though the classic spanning tree protocol was thus withdrawn, it continues to be supported by LCOS.

7.18.2 Improvements from rapid spanning tree

As mentioned above, the primary aim of RSTP is to accelerate the activation of network paths once an active connection has failed. RSTP achieves this by dispensing with the states "blocking" and "listening" to reduce the time required to update the network paths to just a few seconds. In case of a network path failure, not all of the links are blocked until the new topology has been calculated; instead, only the failed connections are unavailable for use.

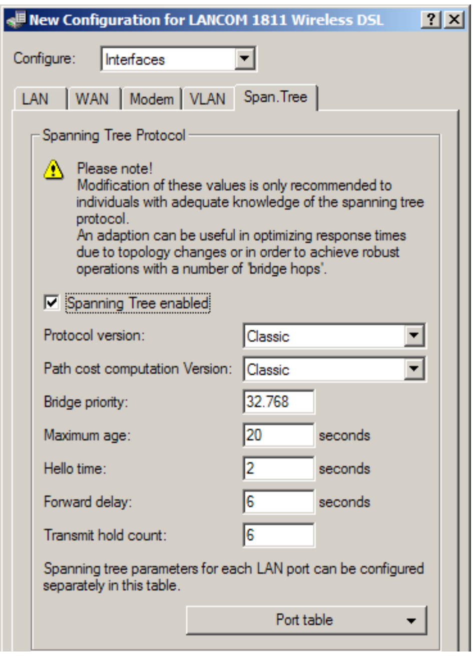
RSTP also enables the administrator to configure information on network topology.

- A bridge port can be defined as an edge port. An edge port is the only bridge port leading to the connected LAN segment, i.e. no other bridges are connected to the LAN segment, but workstations or servers only, for example. As these ports cannot lead to loops, they change immediately into the forwarding state without waiting for the network topology to be determined. However, RSTP continues to monitor these ports. Should BPDUs be unexpectedly received at an edge port due to another bridge being connected to the LAN, the ports automatically return to their normal state.
- A bridge port can also operate as a point-to-point link. In this case the port is directly connected with an additional bridge. Since no additional stations can occur between the two bridges, the switch into the forwarding state can take place faster.

In the ideal case, RSTP immediately resorts to familiar alternative network paths in case of connection failure.

7.18.3 Configuring the Spanning Tree Protocol

The following parameters are available for configuring RSTP or STP functionality in LANCOM:



Configure: Interfaces

Spanning Tree Protocol

Please note!
Modification of these values is only recommended to individuals with adequate knowledge of the spanning tree protocol.
An adaption can be useful in optimizing response times due to topology changes or in order to achieve robust operations with a number of 'bridge hops'.

☑ Spanning Tree enabled

Protocol version: Classic

Path cost computation Version: Classic

Bridge priority: 32.768

Maximum age: 20 seconds

Hello time: 2 seconds

Forward delay: 6 seconds

Transmit hold count: 6

Spanning tree parameters for each LAN port can be configured separately in this table.

LANconfig: Interfaces ▶ Span. Tree

WEBconfig: LCOS-menu tree ▶ Setup ▶ LAN-Bridge ▶ Spanning-Tree

General parameters

- **Spanning tree operating**

  When Spanning Tree is turned off, a LANCOM does not send any Spanning Tree packets and passes received packets along instead of processing them itself.

- **Protocol version**
  - □ Classic: Uses the classical STP to determine network topology.
  - □ Rapid: Uses the RSTP method to determine network topology.

RSTP is compatible with STP. Network components which only support classical STP continue to be supported where RSTP is operational.

- **Path Cost Computation**
  - □ Classic: Uses the classical STP method to compute path costs.
  - □ Rapid: Uses the RSTP method to compute path costs.

- **Bridge priority**

  Defines the priority of the bridge in the LAN. This can influence which bridge should preferably be made root bridge by the Spanning Tree Protocol.

So as to maintain compatibility with RSTP, this value should only be adjusted in steps of 4096 owing to the fact that RSTP uses the lower 12-bits of this 16-bit value for other purposes.

- **Maximum Age**

  This value defines the time (in seconds) after which a bridge drops messages received through Spanning Tree as 'outdated'. This parameter defines how quickly the Spanning Tree algorithm reacts to changes, for example due to failed bridges.

- **Hello Time**

  This parameter defines (in seconds) in which intervals a device selected to be the root bridge sends Spanning Tree information into the LAN.

- **Forward-Delay**

  This time (in seconds) determines how much time must pass at a minimum before a Spanning Tree port can change the status (listening, learning, forwarding).

When using RSTP the forwarding delay often has no effect because RSTP has suitable mechanisms of its own to prompt a rapid switching into the forwarding state.

ⓘ Modifying any of these three time values is only recommended for those with exact knowledge of the Spanning Tree protocol.

- **Transmit-Hold-Count**

  Number of BPDUs which can be transmitted by RSTP before a one second pause commences.

ⓘ When using classical STP the transmit-hold count has no effect.

Port table

The port table can be used to set the following values separately for all available ports (LAN, wireless LAN, point-to-point connections).

- **Mark as edge port**

  Marks the port as an edge port which is not connected to any further bridges but to workstations or servers only. Edge ports switch immediately into the forwarding state.

ⓘ Edge ports continue to be monitored by RSTP. If a port of this type receives BPDUs, then its status as an edge port is removed.

- **Priority**

  Defines the priority of the port. In the case of multiple network paths with identical path costs, the priority value decides which port is used. If priority values are identical then the port to be taken is the first in the list.

ⓘ So as to maintain compatibility with RSTP, this value may only be adjusted in steps of 16 owing to the fact that RSTP uses only the upper 4-bits of this 16-bit value.

- **Path-Cost-Override**

  This parameter controls the priority of paths with equal value. The value set here is used to make the selection instead of the computed path costs.

  - Special values: 0 switches path-cost override off.
  - Default: 0

7.18.4 Status reports via the Spanning Tree Protocol

The current STP values can be viewed via Telnet or WEBconfig in the LAN Bridge Status.

WEBconfig: LCOS-menu tree ▶ Status ▶ LAN-Bridge ▶ Spanning-Tree

General status information

- **Bridge ID**

  This is the ID for the device that is being used by the Spanning Tree algorithm. It is composed of the user-defined priority (upper 16 bits) and the device MAC address (lower 48 bits).

- **Root Bridge**

  The ID for the device that is currently elected root bridge.

- **Root Port**

  The port that can be used to reach the root bridge from this device. If the device itself is the root bridge, it is displayed with the special value '255'.

- **Root Path Cost**

  The path costs of all hops added together in order to reach the root bridge from this device.

- **Protocol version**

  The protocol version currently set for determining network topology.

- **Path Cost Computation**

  The protocol version currently set for computing path cost.

- **Bridge priority**

  Current setting for bridge priority.

Information in the port table

The port table can be used to inspect the following values for all available ports (LAN, wireless LAN, point-to-point connections).

- **Priority**

  The priority of this port taken from the port configuration

- **Status**

  The current status of the port:

  - □ Disabled: no packets can be sent or received through this port. This occurs when the port has either been disabled manually or when it has a negative link status.
  - □ Listening: Intermediate state on the way to enabling. Only Spanning Tree packets are listened to, data packets are ignored and are also not forwarded to this port.
  - □ Learning: Further intermediate state. As opposed to 'listening' additional MAC addresses from data packets entering this port are learned but data packets are still not forwarded.
  - □ Forwarding: the port is completely active, data packets are received and forwarded in both directions.
  - □ Blocking: Spanning Tree has identified this port to be redundant and disabled it for data traffic.

- **Root**

  The ID of the root bridge that can be reached through this port.

- **Bridge**

  This is the ID of the bridge through which the root bridge can be reached.

- **Costs**

  This value defines the 'costs' for this port. The value is determined by the port technology (Ethernet, WLAN, etc.) and the bandwidth. Examples of values used are:

Transfer technology	Costs of Classic Spanning Tree	Costs of Rapid Spanning Tree
Ethernet 10 MBit	100	2000000
Ethernet 100 MBit	19	200000
Ethernet 1000 MBit	4	200000
WLAN 2 MBit	500	12500000
WLAN 11 MBit	140	4000000
WLAN 54 MBit	35	900000
WLAN 108 MBit	25	450000

If path costs for a port were manually entered, then the configured value appears in this column.

Information in the RSTP port statistics

The RSTP port table can be used to inspect the following values for all available ports (LAN, wireless LAN, point-to-point connections).

- **Role**

  Root or Non-root bridge

- **Learning**

  Port in learning state.

- **Forwarding**

  Port in forwarding state.

- **Edge port**

  Port defined as an edge port.

- **Protocol version**

  Classic or Rapid

- **Costs**

  Setting for this port's cost

7.19 The Action table

7.19.1 Introduction

The action table controls actions triggered when there is a change in status of WAN connections. WAN connections include direct connections to an Internet provider, and also VPN connections based on this, such as those used to connect a branch office to a main office. Every action is linked with a condition that describes the change in status of the WAN connection (establishment, termination, failure or establish failure). Actions can be any of the commands available at the Telnet console. Furthermore, actions can transmit messages by e-mail or SYSLOG, send an HTTP request, or transmit a DNS request. Different variables allow information such as the current IP address, the name of the device, or an error message to be integrated into the action.

7.19.2 Actions for Dynamic DNS

Systems with dynamic IP addresses can be made available for access via the WAN, for example via the Internet, by using the services of commercially available dynamic DNS servers. Servers offering these services can assign the current IP address of a device to its FQDN name (Fully Qualified Domain Name, e. g. “http://MyLANCOM.dynDNS.org”).

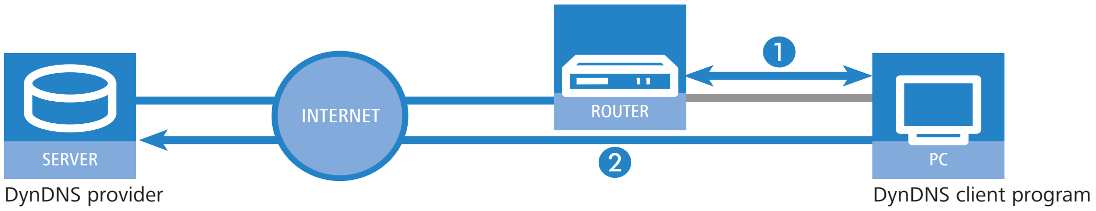
The advantage is obvious: If you wish to carry out remote maintenance via WEBconfig/HTTP, the only information you need is the dynamic DNS name. Also, a DynDNS name can be used to establish VPN connections between remote stations that have changing IP addresses.

In order for the current IP address to match with the DynDNS name at all times, the IP address recorded on the DynDNS server must be constantly updated. This change is triggered by a dynamic DNS client.

- The DynDNS server, maintained by a DynDNS service provider on the Internet, is in contact with the Internet DNS servers.
- The Dynamic DNS client can run on a workstation as a separate client program. As an alternative, a dynamic DNS client is integrated into the LANCOM. 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.

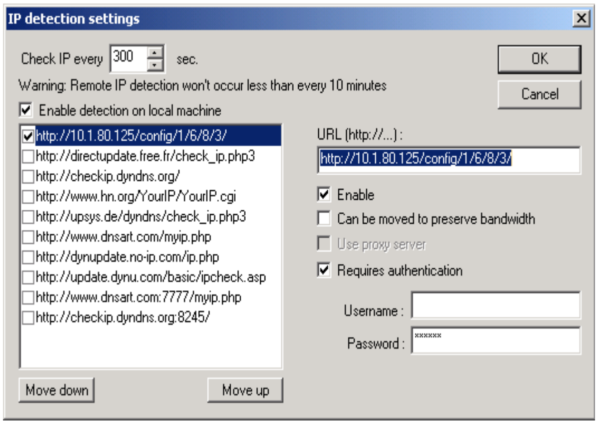
Dynamic DNS client on the workstation

Dynamic DNS providers support a range of PC client programs that use various methods to determine the IP address currently assigned to a LANCOM ①. A change in IP address is communicated to the appropriate dynamic DNS server ②.



The current WAN-side IP address of a LANCOM can be read from the following address and entered into a client program:

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



IP detection settings

Check IP every 300 sec.

Warning: Remote IP detection won't occur less than every 10 minutes

☑ Enable detection on local machine

☑ http://10.1.80.125/config/1/6/8/3/
□ http://directupdate.free.fr/check_ip.php3
□ http://checkip.dyndns.org/
□ http://www.hn.org/YourIP/YourIP.cgi
□ http://upsys.de/dyndns/check_ip.php3
□ http://www.dnsart.com/myip.php
□ http://dynupdate.no-ip.com/ip.php
□ http://update.dynu.com/basic/ipcheck.asp
□ http://www.dnsart.com:7777/myip.php
□ http://checkip.dyndns.org:8245/

URL (http://...) : http://10.1.80.125/config/1/6/8/3/

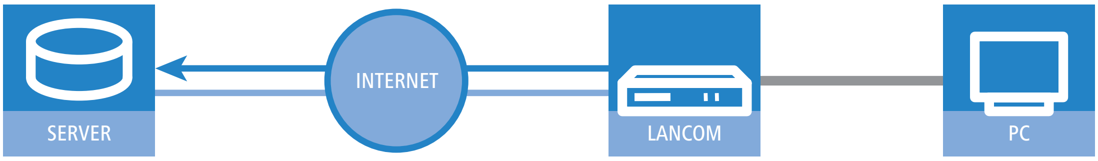
☑ Enable
□ Can be moved to preserve bandwidth
□ Use proxy server
☑ Requires authentication

Username :

Password : xxxxxx

Dynamic-DNS client in the LANCOM via HTTP

Alternatively the LANCOM can transmit the current WAN IP to the DynDNS provider directly:



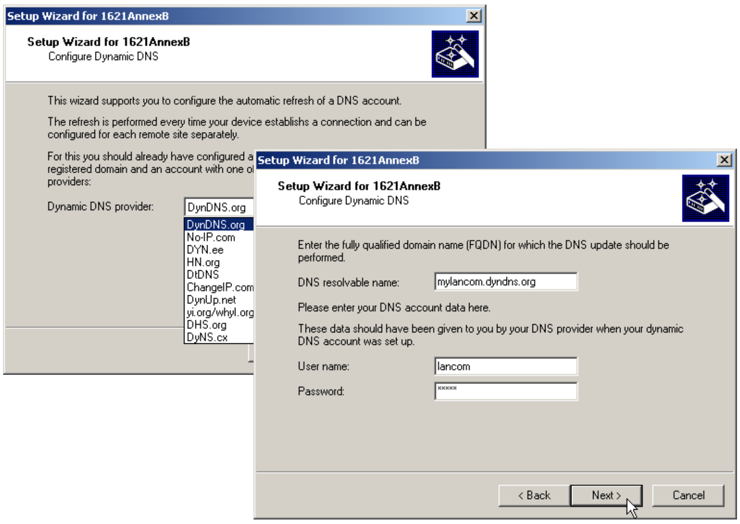
DynDNS provider

An action is defined for this which, for example, automatically sends an HTTP request to the DynDNS server each time a connection is established. The necessary information is transferred via the DynDNS account, so triggering an update of the registration. An HTTP request of this type from DynDNS.org appears as follows:

- http://Username:Password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a

The host name of the action and the LANCOM's current IP address are sent to an account at DynDNS.org as specified by a username and password, and the appropriate entry is updated.

The settings necessary for this can be adjusted easily by using the Setup Wizards in LANconfig:



Setup Wizard for 1621AnnexB

Setup Wizard for 1621AnnexB
Configure Dynamic DNS

This wizard supports you to configure the automatic refresh of a DNS account.

The refresh is performed every time your device establishs a connection and can be configured for each remote site separately.

For this you should already have configured a registered domain and an account with one o providers:

Dynamic DNS provider: DynDNS.org

Setup Wizard for 1621AnnexB

Setup Wizard for 1621AnnexB
Configure Dynamic DNS

Enter the fully qualified domain name (FQDN) for which the DNS update should be performed.

DNS resolvable name: mylancom.dyndns.org

Please enter your DNS account data here.

These data should have been given to you by your DNS provider when your dynamic DNS account was set up.

User name: lancom

Password: *****

The Setup Wizard supplements the basic action with further provider-specific parameters, which are not described here. Apart from that, the Setup Wizard creates additional actions that control the LANCOM in case the update does not success the first time.

Dynamic-DNS client in the LANCOM via GnuDIP

As an alternative to using a simple HTTP request to update DynDNS information, some services make use of the GnuDIP protocol. The GnuDIP protocol is based on a challenge-response mechanism:

① The client opens the connection to the GnuDIP server.

② The server responds with a random value calculated for the session.

③ The client uses the random value and the password to create a hash value, which is returned to the server.

④ The server checks this hash value and reports its result by sending a number back to the client.

The GnuDIP protocol can exchange the messages between the client and server either via a simple TCP connection (standard port 3495) or as a CGI script running on an Internet server. The version using an HTTP request from a CGI script has the advantage that no additional ports have to be opened on the GnuDIP, and also that HTTP offers protection from passive interception and offline dictionary attacks.

Requests to a GnuDIP server are triggered by the LANCOM with an action in the following form:

- gnudip://<srv>[:port][/path]?<parameter>
  - □ <srv> – The GnuDIP server address.
  - □ [:port] – Specifiying the port is optional. If it is not defined, default values are taken instead (3945 for TCP, 80 or 443 for HTTP/HTTPS).
  - □ [/path] – Path information is only required by HTTP/HTTPS to define the location where the CGI script is stored.

  The following parameters are extensions to the request:

  - □ method=<tcp|http|https> – Selects the protocol to be used for the transmission between the GnuDIP server and client. Only one protocol can be selected here.

- user=<username> – Specifies the user name for the account on the GnuDIP server.
- pass=<password> – Specifies the password for the account on the GnuDIP server.
- domn=<domain> – Specifies the DNS domain containing the DynDNS entry.
- reqc=<0|1|2> – Defines the action that is triggered by the request. Action <0> sends the server a dedicated IP address that is to be used for the update. Action <1> deletes a DynDNS entry. Action <2> triggers an update, although no IP address is transmitted to the server. Instead, the server carries out the update with the IP address of the GnuDIP client.
- addr=<address> – Specifies the IP address that an action with the parameter <0> is to use for updating the DynDNS entry. If this is unspecified in a <0> action, the request is treated as a <2> action.

With the GnuDIP protocol, the host name that is to be registered corresponds to the user name sent to the server. If, for example, the username is "myserver" and the DNS domain is "mydomain.org", then the DNS name "myserver.mydomain.org" is registered.

For example, the following action executed via the GnuDIP protocol updates the DynDNS entry at a DynDNS provider with the current IP address of the LANCOM (%a) as soon as a connection is established:

- gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org
  &pass=password&reqc=0&addr=%a

Use the following action to delete a DynDNS entry, for example once the connection has been terminated:

- gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org
  &pass=password&reqc=1

The line-break is for legibility only and is not to be entered into the action.

In response ot the request, the GnuDIP server returns one of the following values to the GnuDIP client (assuming that the connection between server and client was established):

- 0 – The DynDNS entry was updated successfully.
- 0:address – The DynDNS entry was successfully updated with the specified address.
- 1 – Authentication at the GnuDIP server failed.
- 2 – The DynDNS entry was deleted successfully.

These responses can be processed by the LANCOM's actions to trigger further actions if necessary.

7.19.3 Further example actions

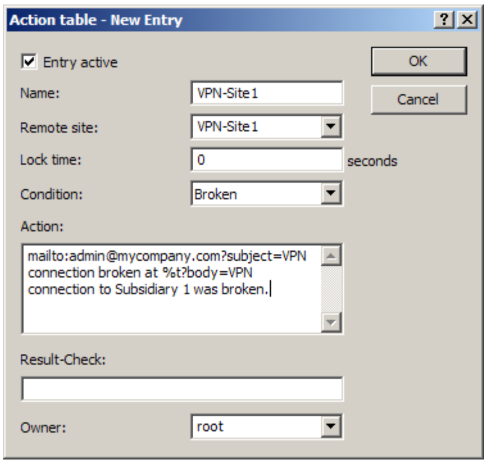
Broken connection alert as an SMS to a mobile telephone

The placeholder %t allows the current time of an event to be incorporated into a message. For example, an alert about the interruption of an important VPN connection can be sent by e-mail or as an SMS to a system administrator's mobile telephone.

The following requirements have to be met for messaging:

- The status of the VPN connection must be monitored, for example by means of "dead-peer-detection" (DPD).
- The LANCOM has to be configured as an NTP client in order to have the current system time.
- An SMTP account must be set up for transmitting e-mails.

Once these requirements are fulfilled, messaging can be set up. This is done with a new entry in the action table; e. g. with LANconfig under **Communication ▶ General ▶ Action table**.



☑ Entry active
Name: VPN-Site1
Remote site: VPN-Site1
Lock time: 0 seconds
Condition: Broken
Action: mailto:admin@mycompany.com?subject=VPN connection broken at %t?body=VPN connection to Subsidiary 1 was broken.
Result-Check:
Owner: root

Select the remote site for the relevant connection. As Condition select 'Broken' and enter the action as the transmission of an e-mail.

`mailto:admin@mycompany.com?subject=VPN connection broken at %t?body=VPN connection to Subsidiary 1 was broken.`

If the connection is broken, this action sends an e-mail to the administrator with the time of the event in the subject line.

If the mail is sent to an appropriate Mail2SMS gateway the alert can be sent directly to a mobile telephone.

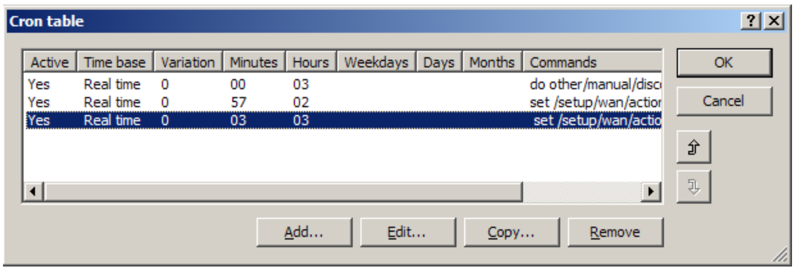
For complex scenarios with several subsidiaries, each of the remote sites is given a corresponding entry in the central LANCOM. For monitoring the central device itself, an action is entered into a device at one of the subsidiaries. In this way the administrator receives an alert even if the VPN gateway at the central location fails, which could potentially prevent any messages from being transmitted.

Example: Suppress messaging in case of re-connects with a DSL connection

Some providers interrupt the DSL connection used for the VPN connections once every 24 hours. To avoid informing the administrator of these regular interruptions, messaging can be disabled at the time when the re-connect occurs.

First of all an action is required to force the re-connect to occur at a fixed time; generally at night when the Internet connection is not in use. The entry defines, for example, 03:00h and the Internet connection is broken with the command `do other/manual/disconnect internet`.

With two more cron commands `set /setup/wan/action-table/1 yes/no` the corresponding entry in the action table is switched off three minutes before 03:00h and switched on again three minutes after 03:00h. The number 1 following the path to the action table is an index that stands for the first entry in the table.



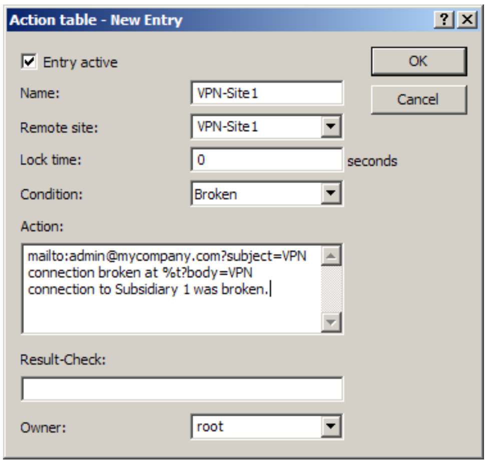
Active	Time base	Variation	Minutes	Hours	Weekdays	Days	Months	Commands
Yes	Real time	0	00	03				do other/manual/disc
Yes	Real time	0	57	02				set /setup/wan/actior
Yes	Real time	0	03	03				set /setup/wan/actio

7.19.4 Configuration

Changes with LCOS 7.6:

- "Failure" as a condition for a change in status of the WAN connection
- "Establish failure" as a condition for a change in status of the WAN connection
- GnuDIP protocol support

With the action table you can define actions that are executed when the status of a WAN connection changes.



☑ Entry active

Name: VPN-Site1

Remote site: VPN-Site1

Lock time: 0 seconds

Condition: Broken

Action:

mailto:admin@mycompany.com?subject=VPN connection broken at %t?body=VPN connection to Subsidiary 1 was broken.

Result-Check:

Owner: root

LANconfig: Communication ▶ General ▶ Action table

WEBconfig: Setup ▶ WAN ▶ Action table

- **Index**

  The index gives the position of the entry in the table, and thus it must be unique. Entries in the action table are executed consecutively as soon as there is a corresponding change in status of the WAN connection. The entry in the field "Check for" can be used to skip lines depending on the result of the action. The index sets the position of the entries in the table (in ascending order) and thus significantly influences the behavior of actions when the option "Check for" is used. The index can also be used to actuate an entry in the action table via a cron job, for example to activate or deactivate an entry at certain times.

- **Active**

  Activates or deactivates this entry.

- **Host name**

  Action name. This name can be referenced in the fields "Action" and "Check for" with the place holder %h (host name).

- **Remote site**

  A change in status of this remote site triggers the action defined in this entry.

- **Lock time (max. 10 characters)**

  Prevents this action from being repeated within the period defined here in seconds.

- **Condition**

  The action is triggered when the change in WAN-connection status set here occurs.

  Possible values:

  - Establish – The action is triggered when the connection has been established successfully.
  - Disconnect – The action is triggered when the device itself terminates the connection (e.g. by manual disconnection or when the hold time expires).
  - End – The action is triggered on disconnection (whatever the reason for this).
  - Failure – This action is triggered on disconnects that were not initiated or expected by the device.
  - Establish failure – This action is triggered when a connection establishment was started but not successfully concluded.

- **Action (max. 250 characters)**

  Here you describe the action that should be executed when there is a change in the status of the WAN connection. Only one action can be triggered per entry.

  Possible values for the actions (max. 250 characters):

  - exec: – This prefix initiates any command as it would be entered at the Telnet console. For example, the action “exec:do /o/m/d” terminates all current connections.
  - dnscheck: – This prefix initiates a DSN name resolution. For example, the action “dnscheck:myserver.dyndns.org” requests the IP address of the indicated server.
  - http: – This prefix initiates an HTTP-get request. For example, you can use the following action to execute a DynDNS update at dyndns.org:
    http://username:password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a
    The meaning of the place holders %h and %a is described below.
  - https: – Like “http:”, except that the connection is encrypted.
  - gnudip: – This prefix initiates a request to the corresponding DynDNS server via the GnuDIP protocol. For example, you can use the following action to use the the GnuDIP protocol to execute a DynDNS update at a DynDNS provider:
    gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org
    &pass=password&reqc=0&addr=%a
    The line-break is for legibility only and is not to be entered into the action. The meaning of the place holder %a is described below.
  - repeat: – This prefix together with a time in seconds repeats all actions with the condition "Establish" as soon as the connection has been established. For example, the action "repeat:300" causes all of the establish actions to be repeated every 5 minutes.
  - mailto: – This prefix causes an e-mail to be sent. For example, you can use the following action to send an e-mail to the system administrator when a connection is terminated:
    mailto:admin@mycompany.de?subject=VPN connection broken at %t?body=VPN connection to Branch Office 1 was terminated.

  Optional variables for the actions:

  - %a – WAN IP address of the WAN connection relating to the action.

- %H – Host name of the WAN connection relating to the action.
- %h – Like %H, except the hostname is in small letters
- %c – Connection name of the WAN connection relating to the action.
- %n – Device name
- %s – Device serial number
- %m – Device MAC address (as in Sysinfo)
- %t – Time and date in the format YYYY-MM-DD hh:mm:ss
- %e – Description of the error that was reported when connection establishment failed.

The result of the actions can be evaluated in the "Check for" field.

Default:

- Blank

- **Check for**

  The result of the action can be evaluated here to determine the number of lines to be skipped in the processing of the action table.

  Possible values for the actions (max. 50 characters):

  - contains= – This prefix checks if the result of the action contains the defined string.
  - isequal= – This prefix checks if the result of the action is exactly equal to the defined string.
  - ?skipiftrue= – This suffix skips the defined number of lines in the list of actions if the result of the "contains" or "isequal" query is TRUE.
  - ?skipiffalse= – This suffix skips the defined number of lines in the list of actions if the result of the "contains" or "isequal" query is FALSE.

  Optional variables for the actions:

  - As with the definition of the action.

  Example:

  - A DNS check queries the IP address of an address in the form "myserver.dyndns.org". The check “contains=%a?skipiftrue=2” allows the two following entries in the action table to be skipped if the IP address found by the DNS check agrees with the current IP address (%a) of the device.

- **Owner**

  Owner of the action. The exec actions are executed with the rights of the owner. If the owner does not have the necessary rights (e.g. administrators with write access) then the action will not be carried out.

7.20 Using the serial interface in the LAN

7.20.1 Introduction

In the IT field, COM port servers (also known as serial port servers) are devices that transport data between TCP and serial connections. There are many applications.

- Networking of devices with a serial interface but without a network interface.
- Remote maintenance of devices that can only be configured via a serial interface.
- Virtual extension of a serial connection between two devices with serial interfaces over a network.

Most LANCOM devices feature a serial interface that can be used to carry out configurations or to connect to a modem. In some cases the interface is used for neither of these scenarios, and yet a COM port server is required in the vicinity of the device. In such cases the LANCOM can use its serial interface as a COM port server, thus saving the costs for an external COM port server. If this application focuses on the serial configuration interfaces of these devices, additional serial interfaces can be provided by some models in combination with suitable CardBus or USB adapters. This enables multiple instances of the COM port server to be operated in one device.

7.20.2 Operating modes

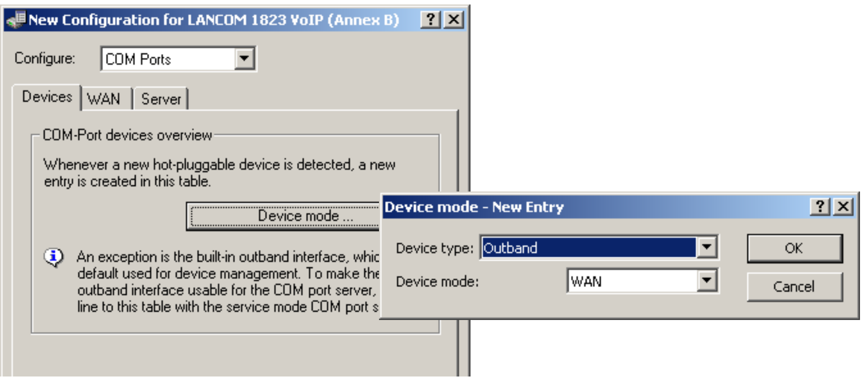
A COM port server has two operating modes:

- Server mode: The COM port server waits for requests from a defined TCP port to establish TCP connections. The mode is used for remote maintenance, for example.
- Client mode: As soon as a device connected to the serial interface becomes active, the COM port client opens a TCP connection to a preset remote site. This operating mode is used, for example, for devices that have just one serial interface but requiring network access.

In both of these cases a transparent connection is set up between the serial interface and the TCP connection. Data packets received at the serial interface are forwarded to the TCP connection, and vice versa. A common server-mode application is to install a virtual COM port driver at the remote site which connects to the COM port server. Drivers of this type allow applications running at the remote site to use the TCP connection as if it were an additional COM port. The IETF RFC 2217 standard sets down the Telnet WILL/DO protocol extensions, which transmit the negotiations for the serial connection (bitrate, data and stop bits, handshake) to the COM port server. The use of this protocol is optional, so practical default values can be set in the COM port server.

7.20.3 Serial interface configuration

The serial interfaces in the LANCOM can be used for various applications, for example for the COM port server or as a WAN interface. The Devices table allows individual serial devices to be assigned to certain applications. As soon as a HotPlug-capable USB adapter is detected, a new entry for the serial interface provided by this USB adapter is created automatically in this table. This automation simplifies the configuration of the serial devices. An exception is the built-in serial interface, which is used for configuration purposes as standard. Entries can be added to the Devices table manually to use this interface for the COM port server or WAN applications.


New Configuration for LANCOM 1823 VoIP (Annex B)
Devices
WAN
Server
COM-Port devices overview
Device mode ...
Device mode - New Entry
OK
Cancel

Configure: COM Ports

Whenever a new hot-pluggable device is detected, a new entry is created in this table.

An exception is the built-in outband interface, whic default used for device management. To make the outband interface usable for the COM port server, line to this table with the service mode COM port s

Device type: Outband

Device mode: WAN

LANconfig: COM ports ▶ Devices ▶ Device operating mode

WEBconfig: Setup ▶ COM-Ports ▶ Devices

- **Device type**

  Selects a serial interface from the list of those available in the device.

- **Service**

  Activation of the port in the COM port server.

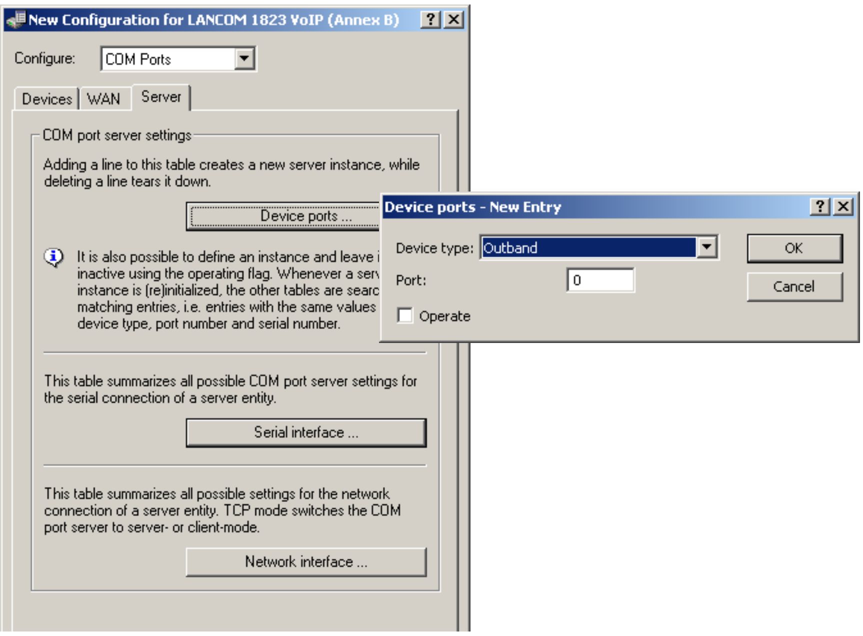
7.20.4 Configuring the COM port server

Configuring the COM port server involves three tables. What all three tables have in common is that a certain port at a serial interface is identified by the values for device type and port number. Because some serial devices such as a CardBus card have multiple ports, the port to be used must be specified explicitly. For a device with just one port, such as with the serial configuration interface, the port number is set to zero.

Operational settings

This table activates the COM port server at a port of a certain serial interface. Add an entry to this table to start a new instance of the COM port server. Delete an entry to stop the corresponding server instance. The switch Operating can be used to deactivate a server instance in the table.

When a server instance is created or activated, the other tables in the COM port configuration are searched for matching device type and port number values. If no suitable entry is found, the server instance takes workable default values.



New Configuration for LANCOM 1823 VoIP (Annex B)

Configure: COM Ports

COM port server settings

Adding a line to this table creates a new server instance, while deleting a line tears it down.

It is also possible to define an instance and leave i inactive using the operating flag. Whenever a serv instance is (re)initialized, the other tables are searc matching entries, i.e. entries with the same values device type, port number and serial number.

This table summarizes all possible COM port server settings for the serial connection of a server entity.

This table summarizes all possible settings for the network connection of a server entity. TCP mode switches the COM port server to server- or client-mode.

Device ports - New Entry

Device type: Outband

Port: 0

☐ Operate

LANconfig: COM ports ▶ Server ▶ Device ports

WEBconfig: Setup ▶ COM-Ports ▶ COM-Port-Server ▶ Devices

- **Device type**

  Selects a serial interface from the list of those available in the device.

- **Port number**

  Some serial devices such as the CardBus have more than one serial port. Enter the number of the port on the serial interface that is to be used for the COM-port server.

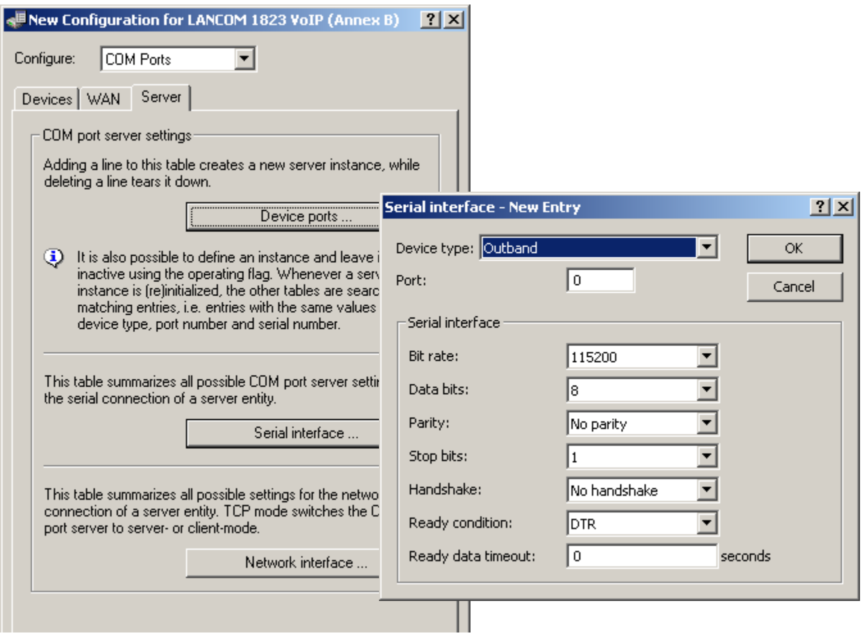
- **Operating**

  Activates the COM port server on the selected port of the selected interface.

COM-port settings

This table contains the settings for data transmission over the serial interface.

Please note that all of these parameters can be overwritten by the remote site if the RFC2217 negotiation is active. Current settings can be viewed in the status menu.



New Configuration for LANCOM 1823 VoIP (Annex B)

Configure: COM Ports

COM port server settings

Adding a line to this table creates a new server instance, while deleting a line tears it down.

It is also possible to define an instance and leave i inactive using the operating flag. Whenever a serv instance is (re)initialized, the other tables are searc matching entries, i.e. entries with the same values device type, port number and serial number.

This table summarizes all possible COM port server setti the serial connection of a server entity.

This table summarizes all possible settings for the netwo connection of a server entity. TCP mode switches the C port server to server- or client-mode.

Serial interface - New Entry

Device type: Outband

Port: 0

Serial interface

Bit rate: 115200

Data bits: 8

Parity: No parity

Stop bits: 1

Handshake: No handshake

Ready condition: DTR

Ready data timeout: 0 seconds

LANconfig: COM ports ▶ Server ▶ Serial interface

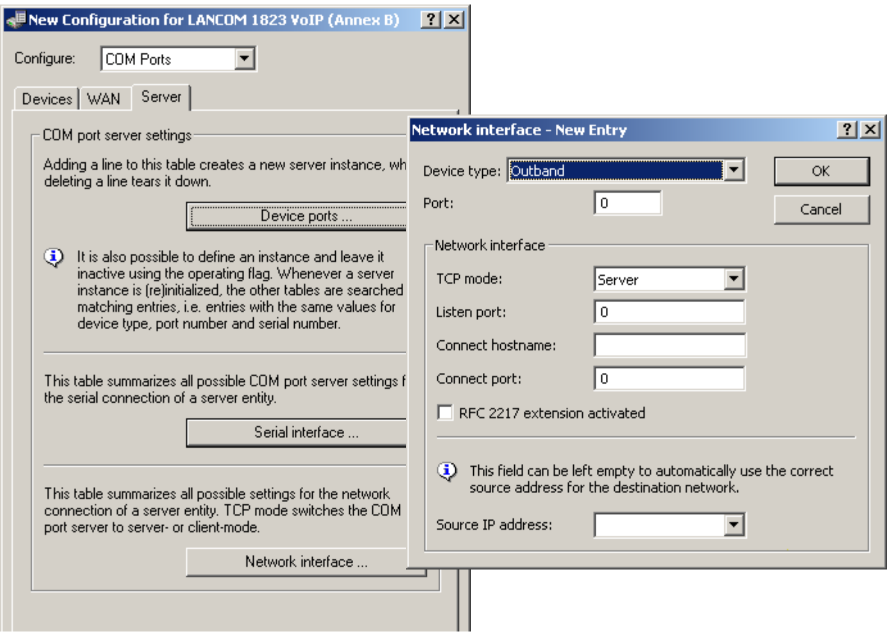
WEBconfig: Setup ▶ COM-Ports ▶ COM-Port-Server ▶ COM-Port-Settings

- **Device type**
  Selects a serial interface from the list of those available in the device.
- **Port number**
  Some serial devices such as the CardBus have more than one serial port. Enter the number of the port on the serial interface that is to be used for the COM-port server.
- **Bitrate**
  Bitrate used on the COM port
- **Data bits:**
  Number of data bits.
- **Parity**
  The checking technique used on the COM port.
- **Stop bits**
  Number of stop bits.
- **Handshake**
  The data-flow control used on the COM port.
- **Ready condition**
  The ready condition is an important property of any serial port. The COM port server transmits no data between the serial port and the network if the status is not "ready". Moreover, the transition from the "ready" to the "not ready" states is used to establish and cancel TCP connections in client mode. There are two ways of determining whether the port is ready or not. In DTR mode (default) only the DTR handshake is monitored. The serial interface is considered to be ready for as long as the DTR line is active. In data mode, the serial interface is considered to be active for as long as it receives data. If no data is received during the timeout period, the port reverts to its not-ready status.
- **Ready-Data-Timeout**
  The timeout switches the port back to the not-ready status if not data is received. This function is deactivated when timeout is set to zero. In this case the port is always ready if the data mode is selected.

Network settings

This table contains all settings that define the behavior of the COM port in the network.

Please note that all of these parameters can be overwritten by the remote site if the RFC2217 negotiation is active. Current settings can be viewed in the status menu.



New Configuration for LANCOM 1823 VoIP (Annex B)

Configure: COM Ports

Devices | WAN | Server

COM port server settings

Adding a line to this table creates a new server instance, wh
deleting a line tears it down.

Device ports ...

It is also possible to define an instance and leave it inactive using the operating flag. Whenever a server instance is (re)initialized, the other tables are searched matching entries, i.e. entries with the same values for device type, port number and serial number.

This table summarizes all possible COM port server settings f
the serial connection of a server entity.

Serial interface ...

This table summarizes all possible settings for the network connection of a server entity. TCP mode switches the COM port server to server- or client-mode.

Network interface ...

Network interface - New Entry

Device type: Outband

Port: 0

OK

Cancel

Network interface

TCP mode: Server

Listen port: 0

Connect hostname:

Connect port: 0

□ RFC 2217 extension activated

This field can be left empty to automatically use the correct source address for the destination network.

Source IP address:

LANconfig: COM ports ▶ Server ▶ Network interface

WEBconfig: Setup ▶ COM-Ports ▶ COM-Port-Server ▶ Network settings

- **Device type**
  Selects a serial interface from the list of those available in the device.

- **Port number**

  Some serial devices such as the CardBus have more than one serial port. Enter the number of the port on the serial interface that is to be used for the COM-port server.

- **TCP mode**

  Each instance of the COM port server in server mode monitors the specified listen port for incoming TCP connections. Just one active connection is permitted per instance. All other connection requests are refused. In client mode, the instance attempts to establish a TCP connection via a defined port to the specified remote site, as soon as the port is ready. The TCP connection is closed again as soon as the port becomes unavailable. In both cases a LANCOM closes any open connections when the device is restarted.

- **Listen port**

  The TCP port where the COM port in TCP server mode expects incoming connections.

- **Connect host name**

  The COM port in TCP client mode establishes a connection to this host as soon as the port is in "Ready" status.

- **Connect port**

  The COM port in TCP client mode uses this TCP port to establish a connection as soon as the port is in "Ready" state.

- **Loopback address**

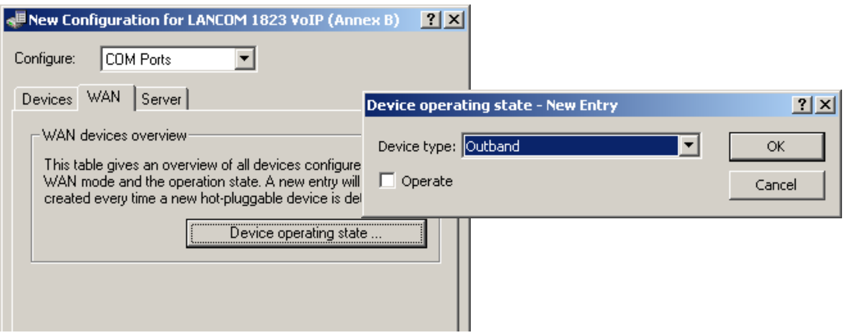
  The COM port can be reached at this address. This is its own IP address that is given as the source address when establishing connections. This is used to define the IP route to be used for the connection.

- **RFC2217 extensions**

  The RFC2217 extensions can be activated for both TCP modes. With these extensions activated, the LANCOM uses the IAC DO COM-PORT-OPTION sequence to signal that it will accept Telnet control sequences. The COM port subsequently works with the corresponding options; the configured default values are overwritten. The port also attempts to negotiate the local echo and line mode for Telnet. Using the RFC2217 extensions with incompatible remote sites is not critical. Unexpected characters may be displayed at the remote site. A side effect of using the FRC2217 extensions may be that the port regularly carries out an alive check as Telnet NOPs are transmitted to the remote site.

7.20.5 WAN device configuration

The table with WAN devices is a status table only. All Hotplug devices (connected via USB or CardBus) enter themselves into this table.


New Configuration for LANCOM 1823 VoIP (Annex B)
Devices
WAN
Server
WAN devices overview
Device operating state ...
Device operating state - New Entry
OK
Cancel

Configure: COM Ports

This table gives an overview of all devices configure WAN mode and the operation state. A new entry will created every time a new hot-pluggable device is de

Device type: Outband

□ Operate

LANconfig: COM ports ▶ WAN ▶ Device operating state

WEBconfig: Setup ▶ COM ports ▶ WAN ▶ Devices

- **Device type**

  List of serial interfaces available in the device.

- **Active**

  Status of connected device:

7.20.6 Serial connection status information

Various statistics and status values are recorded for every instance of the COM-port server. The serial port using the instance is indicated in the first two columns of the table—the values for device type and port number as entered during the configuration are displayed here.

Network status

Telnet: Status ▶ COM-Ports ▶ COM-Port-Server ▶ Network status

This table contains information on current and recent TCP connections.

- **Device type**

  List of serial interfaces available in the device.
- **Port number**

  The port number used for the COM port server on the serial interface.
- **Connection status**

  Possible values:

  - Connected: An active connection exists (server or client mode).
  - Listening: This instance is working in server mode; no TCP connection is currently active.
  - Not listening: In server mode, the specified TCP port could not be reserved for inbound connections, e.g. because it is already occupied by another application.
  - Blank: This instance is working in client mode and the port is not ready. No TCP connection will be established now.
  - Transfer: The port has reached the "ready" state; a connection is being established.
- **Last error**

  In client mode this displays the reason for the last connection error. In server mode this value has no significance.
- **Remote address:**

  Displays the IP address of the remote site for a successful TCP connection.
- **Local port**

  Displays the local TCP port used for a successful TCP connection.
- **Remote port**

  Displays the remote TCP port used for a successful TCP connection.

COM-port status

This table displays the serial port status and the settings currently used by this port.

- **Device type**

  List of serial interfaces available in the device.
- **Port number**

  The port number used for the COM port server on the serial interface.
- **Port status**

  - Possible values:
    Not available: The serial port is currently not available to the COM port server, for example because the USB or CardBus adapter has been removed or because it is being used by other functions in the LANCOM.
    Not ready: The serial port is available to the COM port server but is currently not ready for data transfer, for example because the DTR line is inactive. In the client state, no attempt is made to establish a connection as long as the port is in this state.
    Ready: The serial port is available and ready for data transfer. In the client state, an attempt is made to establish a TCP connection as soon as the port is in this state.

Please note that the port status is relevant in server mode, too. All TCP connection requests are accepted, although the COM port instance will only transfer data between the serial port and the network when the serial port has reached the "ready" state. The following columns display the settings that are currently in use on the serial port. These are either the values as configured or as set by the negotiations via the RFC2217 extensions.

- **Bitrate**

  Bitrate used on the COM port
- **Data bits:**

  Number of data bits.
- **Parity**

  The checking technique used on the COM port.
- **Stop bits**

  Number of stop bits.
- **Handshake**

  The data-flow control used on the COM port.

Byte counters

This table displays the inbound and outbound data packets at the serial port and on the network side.

These values are not reset when the connection is opened or closed.

- **Device type**
  List of serial interfaces available in the device.
- **Port number**
  The port number used for the COM port server on the serial interface.
- **Serial-Tx**
  Number of bytes sent over the serial interface.
- **Serial- Rx**
  Number of bytes received over the serial interface.
- **Network-Tx**
  Number of bytes sent to the network.
- **Network- Rx**
  Number of bytes received from the network.

Port- Errors

This table displays the serial port errors. These errors may indicate a faulty cable or errors in the configuration.

- **Device type**
  List of serial interfaces available in the device.
- **Port number**
  The port number used for the COM port server on the serial interface.
- **Parity errors**
  Number of errors due to a checksum mismatch.
- **Framing errors**
  Number of erroneous data packets.

Connections

This table displays successful and failed TCP connections in both server mode and client mode.

- **Device type**
  List of serial interfaces available in the device.
- **Port number**
  The port number used for the COM port server on the serial interface.
- **Server granted**
  Number of connections granted by the COM port server.
- **Server rejected**
  Number of connections rejected by the COM port server.
- **Client succeeded**
  Number of connections successfully established by the COM port client.
- **Client DNS error**
  Number of connections that the COM port client could not establish due to DNS errors.
- **Client TCP error**
  Number of connections that the COM port client could not establish due to TCP errors.
- **Client- remote disconnects**
  Number of connections where the COM port was disconnected from the remote site.

Delete values

This action deletes all values in the status tables.

7.20.7 COM-port adapters

Devices with serial interfaces can be connected to a LANCOM in the following ways:

Adapter	LANCOM devices
COM-port adapters	All those with a serial configuration interface
USB serial adapter	All those with a USB interface
CardBus serial adapter	All those with a CardBus slot
LANCOM modem adapter kit	All those with a serial configuration interface

The COM port adapter must be a two-way D-sub plug with the following PIN assignment:

Pin	Signal	Signal	Pin
2	RxD	TxD	3
3	TxD	RxD	2
4	DTR	DSR	6
5	GND	GND	5
6	DSR	DTR	4
7	RTS	CTS	8
8	CTS	RTS	7

8 Firewall

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

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

8.1 Threat analysis

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

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

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

8.1.1 The dangers

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

Regardless of the individual motivation, the intention of the perpetrators mostly leads to the following aims:

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

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

8.1.2 The ways of the perpetrators

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

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

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

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

8.1.3 The methods

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

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

If the access via e-mail or www is not possible, the attacker can also look out for certain services of servers in the LAN, which are useful for his purposes. Because services of the servers are identified over certain ports of the TCP/IP protocol, the search for open ports is also called “port scanning”. On the occasion, the attacker starts an inquiry for particular services with a certain program, either generally from the Internet, or, only on certain networks and unprotected workstations, which in turn will give the according answer.

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

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

8.1.4 The victims

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

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

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

All things considered, we can resume that the statistical probability for an attack to the network of a global player of the industry may be higher than to a midget network of the home office. But probably it is only a matter of time that a defenceless workstation installed in the Internet will - perhaps even accidentally - become the victim of attacks.

8.2 What is a Firewall?

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

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

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

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

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

ⓘ The functions “Intrusion Detection” and “DoS protection” are part of the content of a Firewall in some applications. The LANCOM contains these functions also, but they are realised as separate modules beside the Firewall. Further information can be found in the section ’Protection against break-in attempts: Intrusion Detection’ → page 8-32 and ’Protection against “Denial of Service” attacks’ → page 8-33.

8.2.1 Tasks of a Firewall

Checking data packets

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

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

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

Logging and alerting

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

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

8.2.2 Different types of Firewalls

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

Packet filters

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

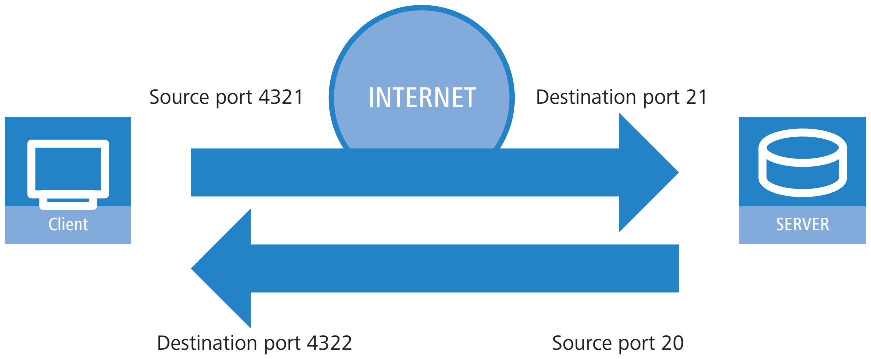
- IP address of source and destination
- Transfer protocol (TCP, UDP or ICMP)
- Port numbers of source and destination
- MAC address

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

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

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

One example for a process, which is quite problematical for simple packet filters, is the establishing of a FTP connection from a workstation of the own LAN to a FTP server in the Internet. By the generally used active FTP, the client (of the protected LAN) sends an inquiry from a port of the upper range (>1023) to port 21 of the server. The client informs the server, over which port it is expecting the connection. The server will establish as a result from its port 20 a connection to the desired port of the client.



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

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

Stateful Packet Inspection

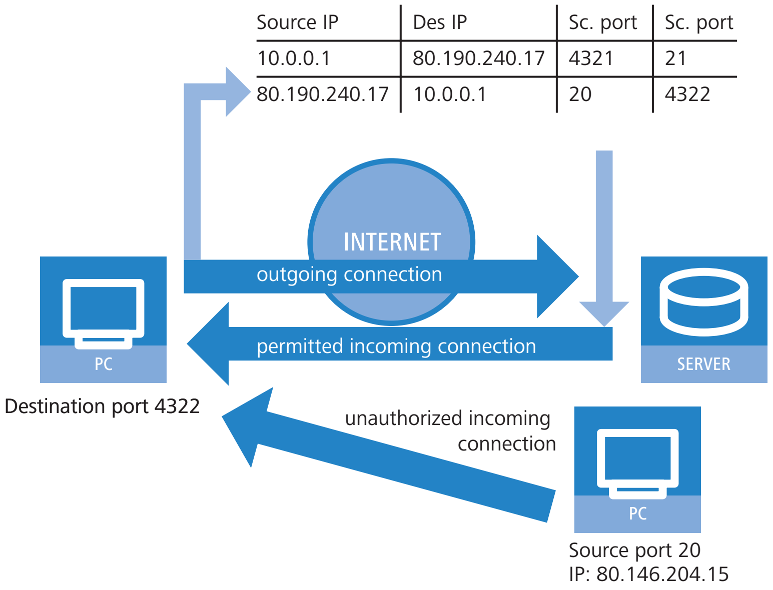
Stateful Packet Inspection (SPI), or briefly Stateful Inspection, enhances the packet filter approach by checking further connection state information. Beside the more static table with the permitted ports and address ranges, a dynamic table will be kept up in this variant, in which information about the connection state of the individual connections is held. This dynamic table enables to first block all endangered ports, and to selectively open only if required a port for a permitted connection (adjusted by source and destination address). The opening of ports is always made from the protected network to the unprotected one, that means mostly from LAN to WAN (Internet). Data packets that do not belong to one of the tracked session of the connection state table will be automatically discarded

Stateful Inspection: direction-dependent checking

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

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

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



Source IP	Des IP	Sc. port	Sc. port
10.0.0.1	80.190.240.17	4321	21
80.190.240.17	10.0.0.1	20	4322

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

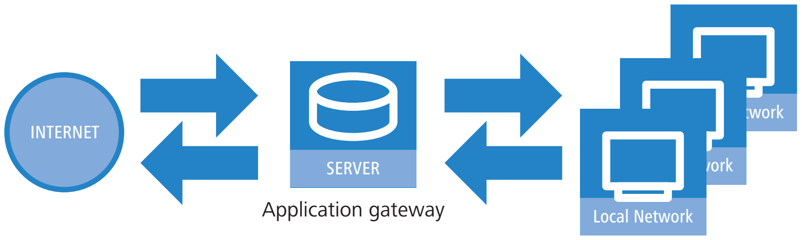
After the successful data transfer, the entries disappear automatically from the dynamic table and the ports will be closed again.

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

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

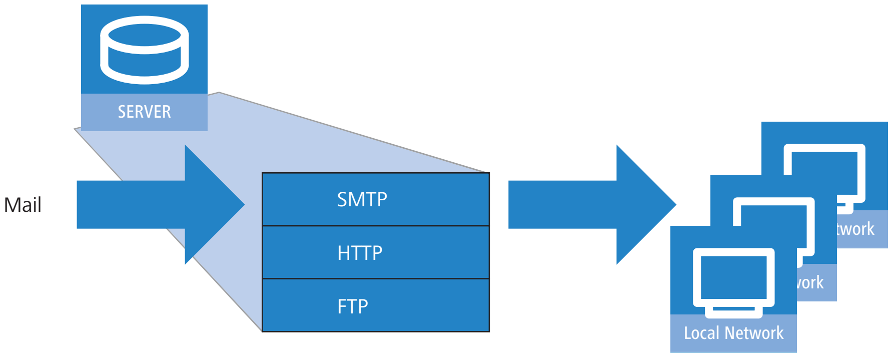
Application Gateway

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



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

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



This service accepts data received by either one of the two sides and depicts it to the respective other side. What seems to be at first sight a needless mirroring of existing data, is on closer examination the far-reaching concept of Application Gateways: It never exists a direct connection e.g. between a client of the local network and a server of the Internet. The LAN workstations only see the proxy, the workstations of the Internet likewise. This physical separation of LAN and WAN, makes it quite difficult for attackers to intrude into the protected network.

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

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

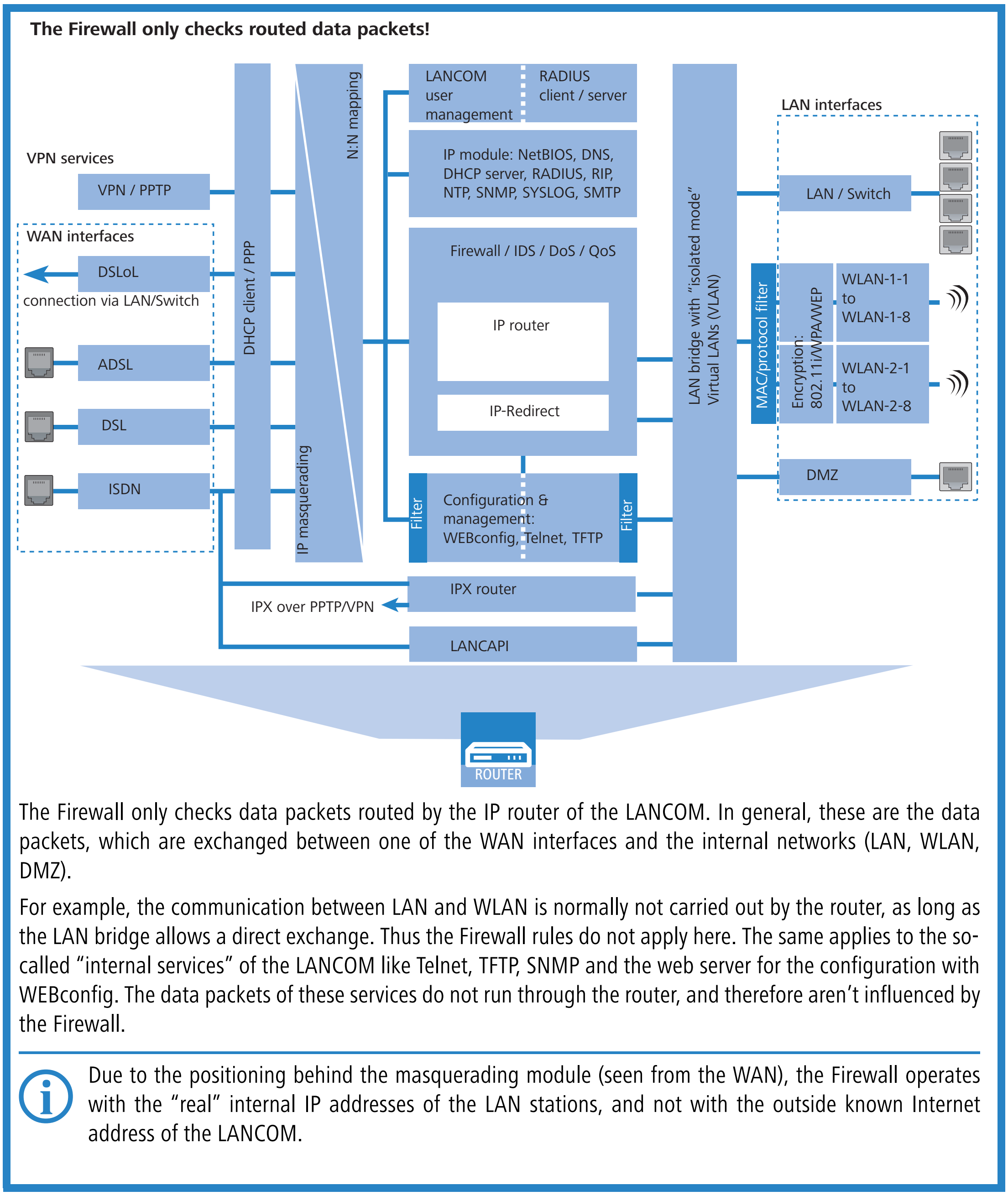
8.3 The LANCOM Firewall

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

For LANCOM devices with VoIP functions that were already integrated or added in with a software option, the ports required for voice connections are activated automatically.

8.3.1 How the LANCOM Firewall inspects data packets

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



The Firewall only checks routed data packets!

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

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

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

The 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

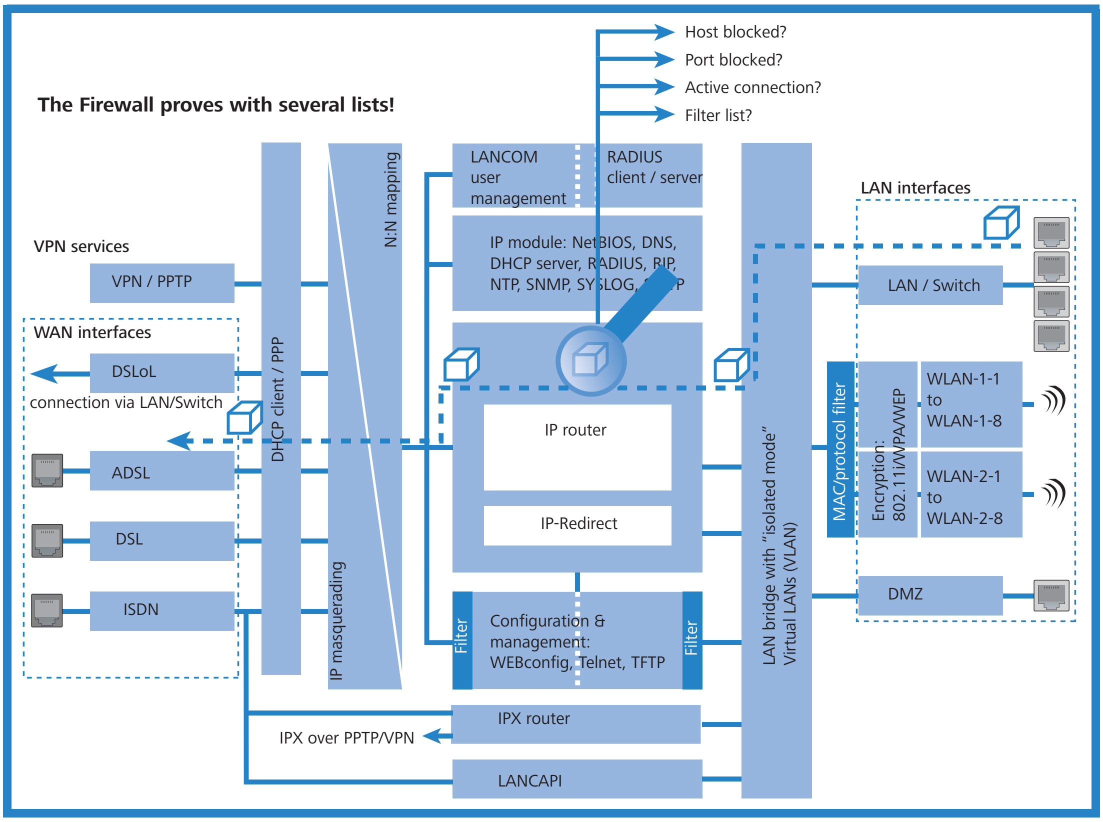
When a data packet should be routed via the IP router, the Firewall uses the lists as follows:

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 8-20.

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 8-12).

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 8-3.

UDP connections

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

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

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

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

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

TCP connections

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

ICMP connections

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

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

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

Connections of other protocols

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

8.3.3 General settings of the Firewall

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

- Firewall/QoS enabled
- Administrator email
- Fragments
- Re-establishing of the session
- Ping blocking
- Stealth mode
- Mask authentication port

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 7-28) are only active when the Firewall has been switched on!

Administrator email

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

Fragments

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

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

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

Session recovery

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

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

The parameter “Session recovery” determines the behavior of the Firewall for packets that indicate a former connection:

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

The function of the virtual routers is based on the analysis of the interface-tag, that is why in addition to the untagged default routes, as well other routes are included as default routes:

- When a packet is received at a **WAN interface**, then the WAN interface is considered by the firewall to be a default route if either a tagged or an untagged default route refers to this WAN interface.
- If a packet is received at a **LAN interface** and is to be routed to a WAN interface, then this WAN interface is considered to be a default route if either the untagged default route or if a default route tagged with the interface tag refers to this WAN interface.

Default route filter are as well effective if the default route is in the LAN. Here it applies that the filter takes effect when:

- A packet was received over a tagged LAN interface and is to be sent over a default route tagged with the interface, or
- A packet from another router was received at a tagged LAN interface and there is a default route with the interface tag to the packet's source address, or
- A packet was received from the WAN and is to be sent to the LAN via a default route with any tag

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).

The hints for the chapter Session recovery consider as well the choice of the default routes.

TCP Stealth mode

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

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

Possible settings are:

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

Mask authentication port

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

Also when the TCP Stealth mode is activated, the Firewall detects the intention of a station in the LAN to establish a connection to a mail server. As a result, the needed port will be opened for a short time (20 seconds) solely for the authentication inquiry.

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

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

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

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

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

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

8.3.4 Parameters of Firewall rules

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

Information regarding definition of Firewall rules with the different kinds of configuration tools (LANconfig, WEBconfig or Telnet) can be found in chapter 'Configuring the firewall with LANconfig' → page 8-21 and 'Configuring firewall rules with WEBconfig or Telnet' → page 8-26.

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?
- **Observe further rules**: Should further Firewall rules be observed when this rule applies to a data packet?
- **Create VPN rule**: Is this Firewall rule also used to create a VPN rule?
- **Routing Tag**: When applying the routing tag further information about for instance the used service or protocol can be used for selecting the target route. With this so called policy based routing a much better control of the routing behaviour is possible ('Policy-based Routing' → page 7-26).

Priority

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

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

For complex rule types please check the filter list as described in section 'Firewall diagnosis' → page 8-27.

Observe further rules

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

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

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

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

- either a rule applies to the packet, for which observe further rules is not activated.

- or the list of the Firewall rules has been completely worked through without applying a further rule to the packet.

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

VPN rules

A VPN rule can receive its information about source and destination network from Firewall rules.

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

If more than one local network is used (see ARF), the automatic extraction of the VPN rules has to be set up individually for every network. The definition of networks with automatically generated VPN rules uses the interface tag which is given for every network. This tag enables the allocation of local network to VPN route: Every packet received at a local interface is marked with the interface tag and forwarded along a route with the same tag or with the default tag (0).

For automatic VPN rule generation, all networks are taken up that

- Have the tag '0' or
- Fulfill the two conditions as follow:
  - The network has the same interface tag as the IP-routing-table entry for the VPN connection (not to be confused with the routing tag for the remote gateway).
  - The network is of the type 'Intranet'.

VPN rules for a DMZ also have to be manually created just as for networks with an interface tag which does not fit to the routing tag of the VPN route.

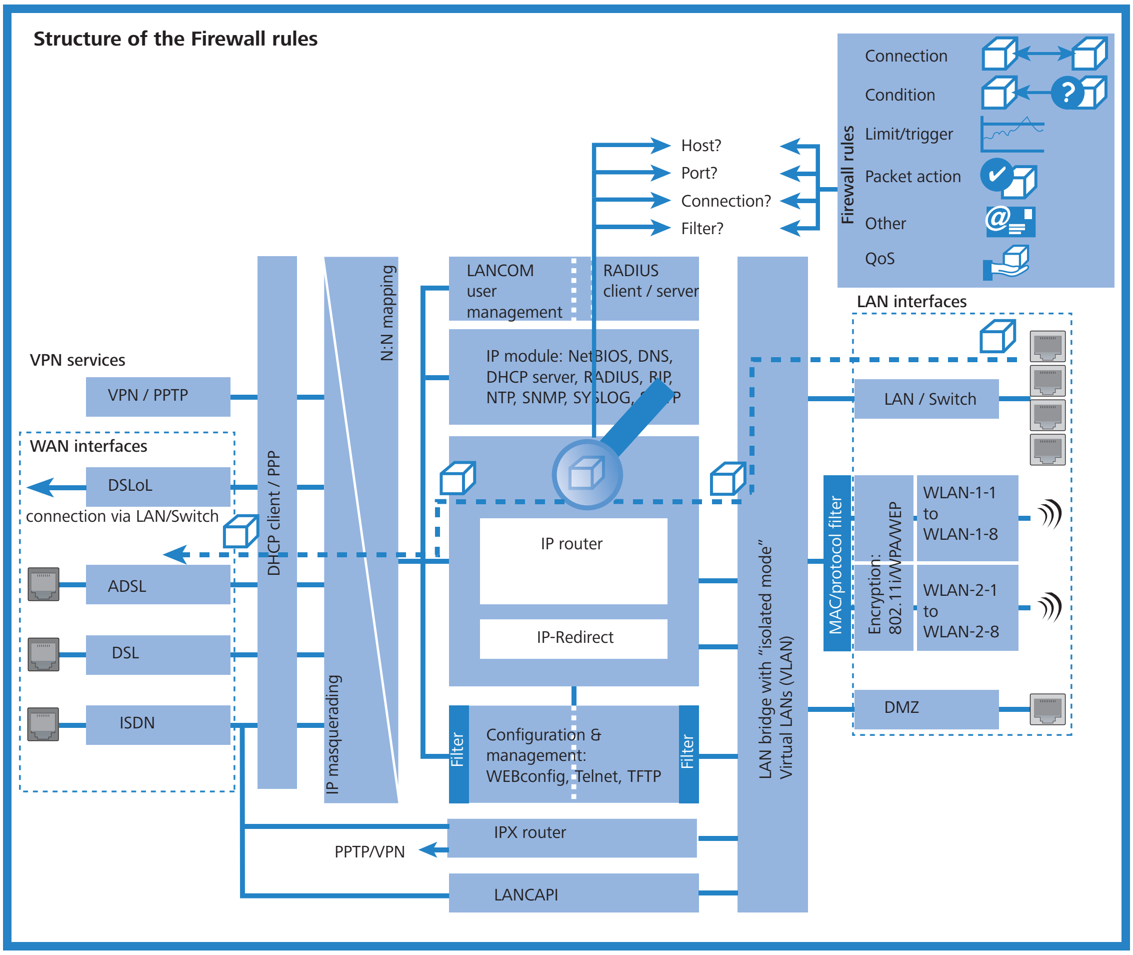
Application of the firewall rules

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?
- **Conditions**: Is the effectiveness of the rule reduced by other conditions?
- **Trigger**: On exceeding of which threshold shall the rule being triggered?
- **Action**: What should happen to the data packets when the condition applies and the limit is reached?
- **Further measures**: Should further measures be initiated apart from the packet action?
- **Quality of Service (QoS)**: Are data packets of certain applications or with the corresponding markings transferred preferentially by assurance of special Quality of Services?

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 8-6 we have already described that in the end the lists for checking data packets are created from Firewall rules. Thus the extension of the block diagram looks like as follows:



Connection

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

- All stations
- The entire local network (LAN)
- Certain remote stations (described by the name of the remote site list)
- Certain stations of the LAN described by the host name)
- Certain MAC[1] addresses
- Ranges of IP addresses
- Complete IP networks

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

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

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

Condition

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

- Only packets with certain ToS and/or DiffServ markings.

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

- Only, if the connection does not yet exist.
- Only for default route (Internet).
- Only for VPN routes.

Limit / Trigger

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

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

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

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

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 9-1.

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:

LANconfig: Log & Trace ▶ SMTP Account ▶ SNMP ▶ SYSLOG

WEBconfig: LCOS menu tree ▶ Setup ▶ SMTP ▶ SNMP Module 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 'SYSLOG' → page 5-9) as follows:

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

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

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

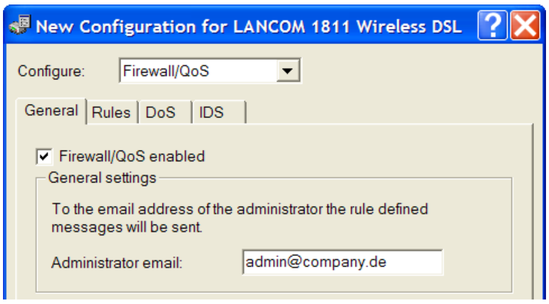
```
PACKET_ALERT: Dst: 192.168.200.10:80 {}, Src: 10.0.0.37:4353 {} (TCP): port filter

PACKET_INFO:

matched filter: BLOCKHTTP
exceeded limit: more than 0 packets transmitted or received on a connection
actions: drop; block source address for 1 minutes; send syslog message;
```

Notification by email

If the email system of the LANCOM is activated, then you can use the comfortable notification by email. The device sends an email to the administrator as soon as the firewall executes the appropriate action:

```
FROM: LANCOM_Firewall@MyCompany.com
TO: Administrator@MyCompany.com
SUBJECT: packet filtered

Date: 9/24/2002 15:06:46

The packet below

Src: 10.0.0.37:4353 {cs2} Dst: 192.168.200.10:80 {ntserver} (TCP)

45 00 00 2c ed 50 40 00 80 06 7a a3 0a 00 00 25 | E..,.P@. ..z....%
c0 a8 c8 0a 11 01 00 50 00 77 5e d4 00 00 00 00 | .......P .w^.....
60 02 20 00 74 b2 00 00 02 04 05 b4 | `. .t... ....

matched this filter rule: BLOCKHTTP
and exceeded this limit: more than 0 packets transmitted or received on a connection

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

Sending the email from the LANCOM to the administrator only works if the right email address is entered.



New Configuration for LANCOM 1811 Wireless DSL

Configure: Firewall/QoS

☑ Firewall/QoS enabled

General settings

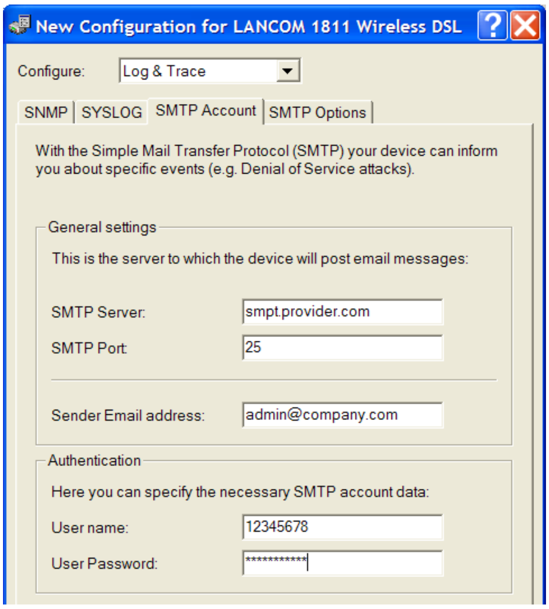
To the email address of the administrator the rule defined messages will be sent.

Administrator email: admin@company.de

LANconfig: Firewall/QoS ▶ General

WEBconfig: LCOS menu tree ▶ Setup ▶ IP Router ▶ Firewall

For sending an email there needs to be set up an email account.



New Configuration for LANCOM 1811 Wireless DSL

Configure: Log & Trace

With the Simple Mail Transfer Protocol (SMTP) your device can inform you about specific events (e.g. Denial of Service attacks).

General settings

This is the server to which the device will post email messages:

SMTP Server: smpt.provider.com

SMTP Port: 25

Sender Email address: admin@company.com

Authentication

Here you can specify the necessary SMTP account data:

User name: 12345678

User Password: ***********

LANconfig: Log & Trace ▶ SMTP Account

WEBconfig: LCOS menu tree ▶ Setup ▶ SMTP

Notification by SNMP trap

If as notification method dispatching SNMP traps was activated (see also 'SNMP' → page 3-37), then the first line of the logging table is sent away as enterprise specific trap 26. This trap contains additionally the system descriptor and the system name from the MIB-2.

For the example the following trap is thus produced:

```
SNMP: SNMPv1; community = public; SNMPv1 Trap; Length = 443 (0x1BB)
SNMP: Message type = SNMPv1
SNMP: Version = 1 (0x0)
SNMP: Community = public
SNMP: PDU type = SNMPv1 Trap
SNMP: Enterprise = 1.3.6.1.4.1.2356.400.1.6021
SNMP: Agent IP address = 10.0.0.43
SNMP: Generic trap = enterpriseSpecific (6)
SNMP: Specific trap = 26 (0x1A)
SNMP: Time stamp = 1442 (0x5A2)
```

System descriptor

```
SNMP: OID = 1.3.6.1.2.1.1.1.0 1.
SNMP: String Value = LANCOM Business 6021 2.80.0001 / 23.09.2002 8699.000.036
```

Device string

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

Time stamp	`SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.2.1 3.`
	`SNMP: String Value = 9/23/2002 17:56:57`

Source address	`SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.3.1 3.`
	`SNMP: IP Address = 10.0.0.37`

Destination address	`SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.4.1 4.`
	`SNMP: IP Address = 192.168.200.10`

Protocol (6 = TCP)	`SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.5.1 5.`
	`SNMP: Integer Value = 6 (0x6) TCP`

Source port	`SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.6.1 6.`
	`SNMP: Integer Value = 4353 (0x1101)`

Destination port (80 = HTTP)	`SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.7.1 7.`
	`SNMP: Integer Value = 80 (0x50)`

Name of the filter rule	`SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.8.1 8.`
	`SNMP: String Value = BLOCKHTTP`

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

8.3.6 Strategies for Firewall settings

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

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

Allow All

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

Deny All

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

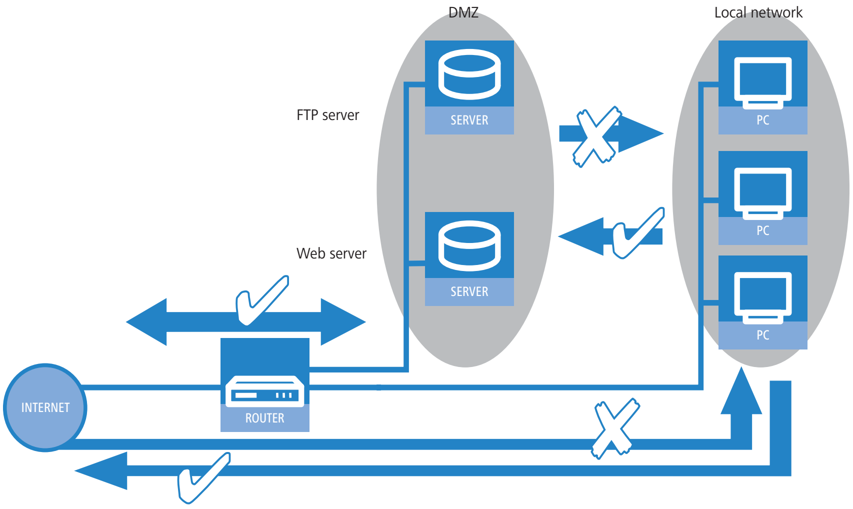
This approach ensures superior security for the LAN security compared to the Allow All strategy, but may lead especially in its initial stages to difficulties for the users. After activation of the Deny All strategy, some things just may behave differently than before, some stations may not reached any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

Firewall with DMZ

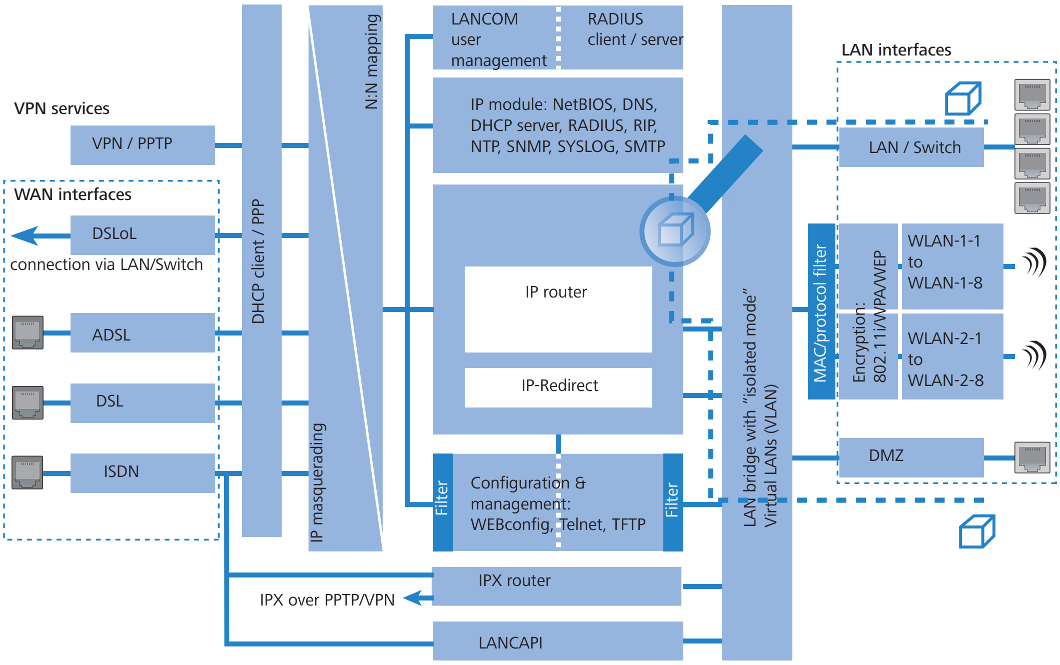
The demilitarized zone (DMZ) is a special range of the local network, which is shielded by a Firewall both against the Internet and against the normal LAN. All stations or servers that should be accessible from the unsecured network (Internet) should be placed into this network. These include for example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

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

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



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



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

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

8.3.7 Hints for setting the Firewall

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

For LANCOM devices with VoIP functions that were already integrated or added in with a software option, the ports required for voice connections are activated automatically.

The default settings of the Firewall

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

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

Security by NAT and Stateful Inspection

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

Transmitting firewall rules with scripts

With the help of scripts firewall rules can easily be transmitted to device and software ('Scripting' → page 4-1). Example scripts are saved in the LANCOM KnowledgeBase under www.lancom.de/support.

If you operate a web server in your LAN, that has been permitted access to this service from the outside (see 'IP masquerading' → page 7-16), 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	Local network	IP address of LANOM (or: Local network)	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 7-14):

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

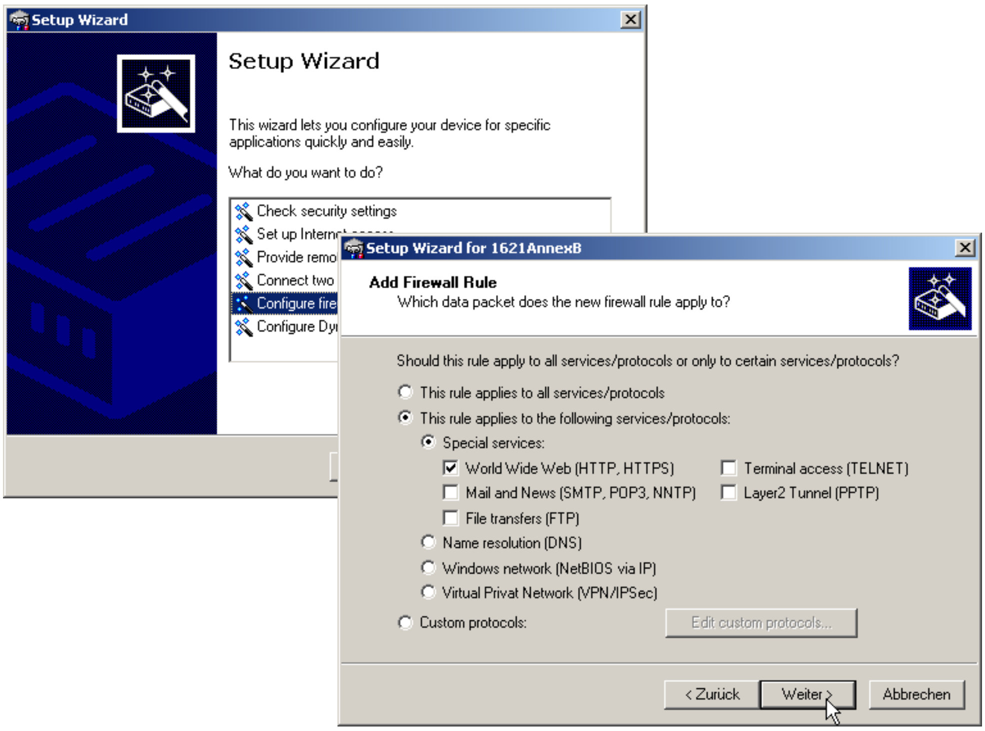
These rules can now be refined as needed - e.g. by the indication of minimum and maximum bandwidths for the server access, or by a finer restriction on certain services, stations or remote sites.

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.

8.4 Configuring the firewall with LANconfig

8.4.1 Firewall wizard

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



Setup Wizard

Setup Wizard

This wizard lets you configure your device for specific applications quickly and easily.

What do you want to do?

- Check security settings
- Set up Interne
- Provide remo
- Connect two
- Configure fire
- Configure Dy

Setup Wizard for 1621AnnexB

Add Firewall Rule

Which data packet does the new firewall rule apply to?

Should this rule apply to all services/protocols or only to certain services/protocols?

○ This rule applies to all services/protocols

● This rule applies to the following services/protocols:

● Special services:

☑ World Wide Web (HTTP, HTTPS) □ Terminal access (TELNET)

□ Mail and News (SMTP, POP3, NNTP) □ Layer2 Tunnel (PPTP)

□ File transfers (FTP)

○ Name resolution (DNS)

○ Windows network (NetBIOS via IP)

○ Virtual Privat Network (VPN/IPSec)

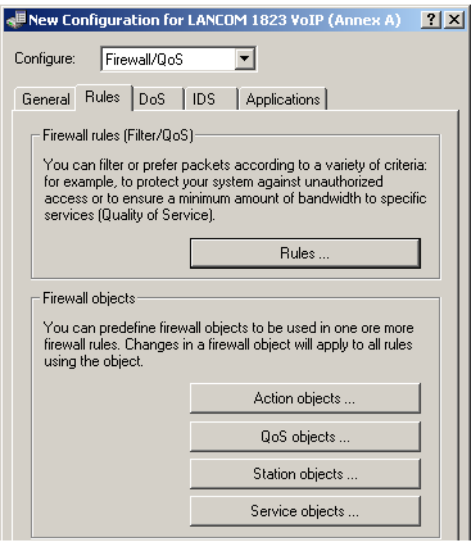
○ Custom protocols:

8.4.2 Definition of firewall objects

When configuring the firewall with LANconfig, various objects can be defined that are used in the firewall rules. This means that frequently used definitions (such as a particular action) do not need to be re-entered for every rule. Instead they can be stored once at a central location.

Please note that a change to firewall objects affects all of the firewall rules that use this object. For this reason, all firewall rules that also use these objects are displayed when you make changes to firewall objects.

Existing firewalls (in the % notation) are not automatically converted to the object-orientated form when the configuration is opened in LANconfig. The LANCOM KnowledgeBase contains the pre-defined firewall settings used by the new objects.



New Configuration for LANCOM 1823 VoIP (Annex A)

Configure: Firewall/QoS

Firewall rules (Filter/QoS)

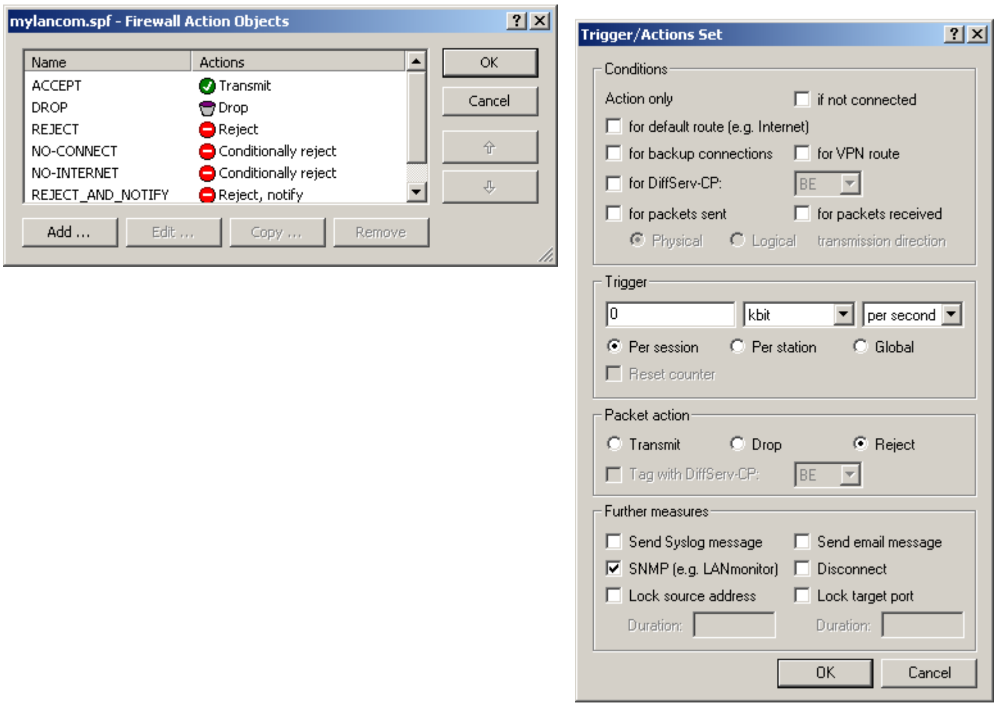
You can filter or prefer packets according to a variety of criteria: for example, to protect your system against unauthorized access or to ensure a minimum amount of bandwidth to specific services (Quality of Service).

Firewall objects

You can predefine firewall objects to be used in one ore more firewall rules. Changes in a firewall object will apply to all rules using the object.

Action objects

Here you specify here the firewall action, which is comprised of condition, limit, packet action and other measures to be used by the firewall rules.



mylancom.spf - Firewall Action Objects

Name	Actions
ACCEPT	Transmit
DROP	Drop
REJECT	Reject
NO-CONNECT	Conditionally reject
NO-INTERNET	Conditionally reject
REJECT_AND_NOTIFY	Reject, notify

Trigger/Actions Set

Conditions

Action only □ if not connected

□ for default route (e.g. Internet)

□ for backup connections □ for VPN route

□ for DiffServ-CP: BE

□ for packets sent □ for packets received

● Physical ○ Logical transmission direction

Trigger

0 kbit per second

● Per session ○ Per station ○ Global

□ Reset counter

Packet action

○ Transmit ○ Drop ● Reject

□ Tag with DiffServ-CP: BE

Further measures

□ Send Syslog message □ Send email message

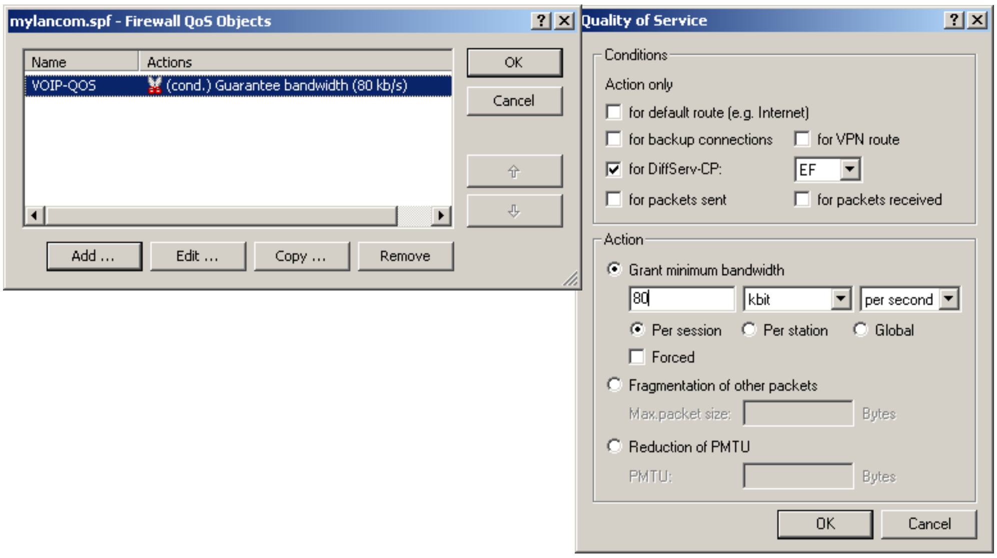
☑ SNMP (e.g. LANmonitor) □ Disconnect

□ Lock source address □ Lock target port

Duration: Duration:

QoS objects

Here you set the minimum bandwidths that the firewall rules allocate to data packets.



mylancom.spf - Firewall QoS Objects

Name	Actions
VOIP-QOS	(cond.) Guarantee bandwidth (80 kb/s)

Quality of Service

Conditions

Action only

□ for default route (e.g. Internet)

□ for backup connections □ for VPN route

☑ for DiffServ-CP: EF

□ for packets sent □ for packets received

Action

● Grant minimum bandwidth

80 kbit per second

● Per session ○ Per station ○ Global

□ Forced

○ Fragmentation of other packets

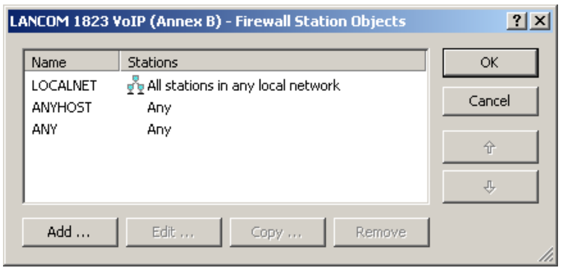
Max.packet size: Bytes

○ Reduction of PMTU

PMTU: Bytes

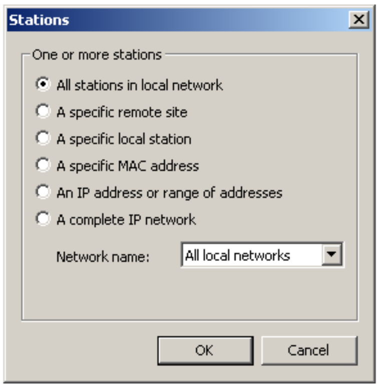
Station objects

This is where the stations are defined that the firewall rules are to use as packet sender or addressee. The station objects are not restricted to any particular source or destination, but can be used as required by the firewall rules. In the context of Advanced Routing and Forwarding (ARF) you can specify a certain IP network as station object ('Advanced Routing and Forwarding' → page 7-9).



LANCOM 1823 VoIP (Annex B) - Firewall Station Objects

Name	Stations
LOCALNET	All stations in any local network
ANYHOST	Any
ANY	Any



Stations

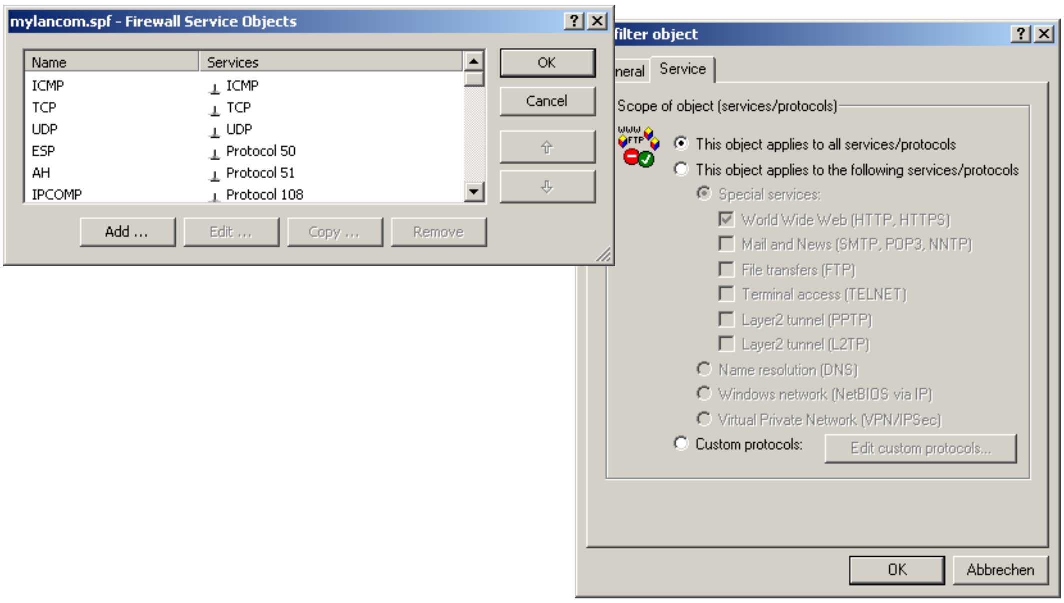
One or more stations

● All stations in local network
○ A specific remote site
○ A specific local station
○ A specific MAC address
○ An IP address or range of addresses
○ A complete IP network

Network name: All local networks

Service objects

The IP protocols and the source/destination ports to be used by the firewall rules are defined here.



mylancom.spf - Firewall Service Objects

Name	Services
ICMP	ICMP
TCP	TCP
UDP	UDP
ESP	Protocol 50
AH	Protocol 51
IPCOMP	Protocol 108

filter object

neral | Service

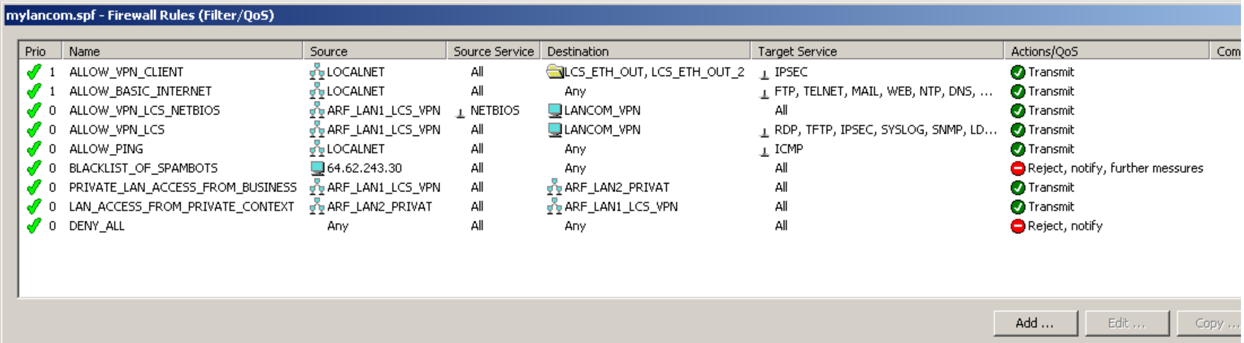
Scope of object (services/protocols)

● This object applies to all services/protocols
○ This object applies to the following services/protocols
● Special services:
☑ World Wide Web (HTTP, HTTPS)
□ Mail and News (SMTP, POP3, NNTP)
□ File transfers (FTP)
□ Terminal access (TELNET)
□ Layer2 tunnel (PPTP)
□ Layer2 tunnel (L2TP)
○ Name resolution (DNS)
○ Windows network (NetBIOS via IP)
○ Virtual Private Network (VPN/IPSec)
○ Custom protocols: Edit custom protocols...

8.4.3 Defining firewall rules

The firewall rules are shown in a clearly laid-out table containing the following information:

- In the left-most column, icons indicate the status of the firewall rule:
  - Green check-mark: Firewall rule is enabled.
  - Red cross: Firewall rule is disabled.
  - Lock: Firewall rule is used to create VPN rules manually.
  - Two interlinked arrows: If this firewall rule applies, please observe other rules.
- Name of firewall rule
- Source
- Destination
- Source and destination service
- Action/QoS
- Comment

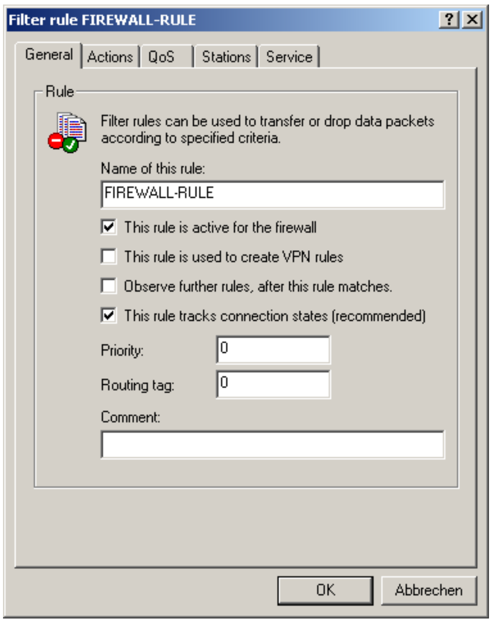


mylancom.spf - Firewall Rules (Filter/QoS)

Prio	Name	Source	Source Service	Destination	Target Service	Actions/QoS	Com
✓ 1	ALLOW_VPN_CLIENT	LOCALNET	All	LCS_ETH_OUT, LCS_ETH_OUT_2	IPSEC	Transmit	
✓ 1	ALLOW_BASIC_INTERNET	LOCALNET	All	Any	FTP, TELNET, MAIL, WEB, NTP, DNS, ...	Transmit	
✓ 0	ALLOW_VPN_LCS_NETBIOS	ARF_LAN1_LCS_VPN	NETBIOS	LANCOM_VPN	All	Transmit	
✓ 0	ALLOW_VPN_LCS	ARF_LAN1_LCS_VPN	All	LANCOM_VPN	RDP, TFTP, IPSEC, SYSLOG, SNMP, LD...	Transmit	
✓ 0	ALLOW_PING	LOCALNET	All	Any	ICMP	Transmit	
✓ 0	BLACKLIST_OF_SPAMBOTS	64.62.243.30	All	Any	All	Reject, notify, further messures	
✓ 0	PRIVATE_LAN_ACCESS_FROM_BUSINESS	ARF_LAN1_LCS_VPN	All	ARF_LAN2_PRIVAT	All	Transmit	
✓ 0	LAN_ACCESS_FROM_PRIVATE_CONTEXT	ARF_LAN2_PRIVAT	All	ARF_LAN1_LCS_VPN	All	Transmit	
✓ 0	DENY_ALL	Any	All	Any	All	Reject, notify	

Adding a new firewall rule

When creating a new firewall rule, the general data is entered first. Objects already defined can be selected directly from the tabs for Actions, QoS, Stations and Services. New objects that can also be used in other rules can be created here, as user-defined entries that are only to be used in the active firewall rule.



Filter rule FIREWALL-RULE

Filter rules can be used to transfer or drop data packets according to specified criteria.

Name of this rule: FIREWALL-RULE

☑ This rule is active for the firewall

☐ This rule is used to create VPN rules

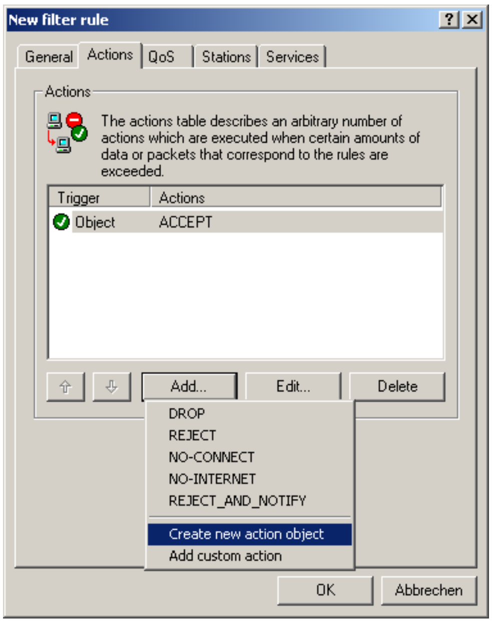
☐ Observe further rules, after this rule matches.

☑ This rule tracks connection states (recommended)

Priority: 0

Routing tag: 0

Comment:



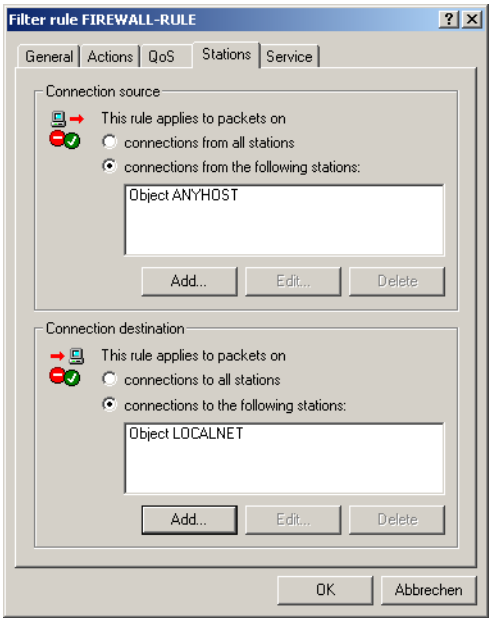
New filter rule

The actions table describes an arbitrary number of actions which are executed when certain amounts of data or packets that correspond to the rules are exceeded.

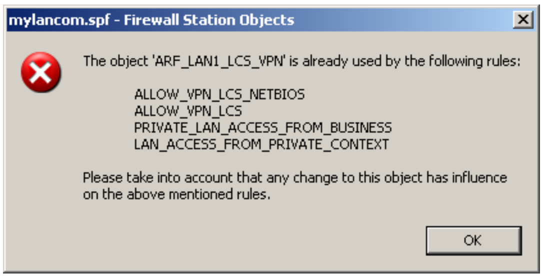
Trigger	Actions
Object	ACCEPT

Editing firewall rules

When editing an existing firewall rule, the user is shown whether actions, QoS, stations or services have been added as pre-defined objects. A message is displayed if you try to edit a referenced object that is already used by another firewall.



Filter rule FIREWALL-RULE
General
Actions
QoS
Stations
Service
Connection source
This rule applies to packets on
○ connections from all stations
● connections from the following stations:
Object ANYHOST
Add...
Edit...
Delete
Connection destination
This rule applies to packets on
○ connections to all stations
● connections to the following stations:
Object LOCALNET
Add...
Edit...
Delete
OK
Abbrechen



mylancom.spf - Firewall Station Objects

The object 'ARF_LAN1_LCS_VPN' is already used by the following rules:

ALLOW_VPN_LCS_NETBIOS
ALLOW_VPN_LCS
PRIVATE_LAN_ACCESS_FROM_BUSINESS
LAN_ACCESS_FROM_PRIVATE_CONTEXT

Please take into account that any change to this object has influence on the above mentioned rules.

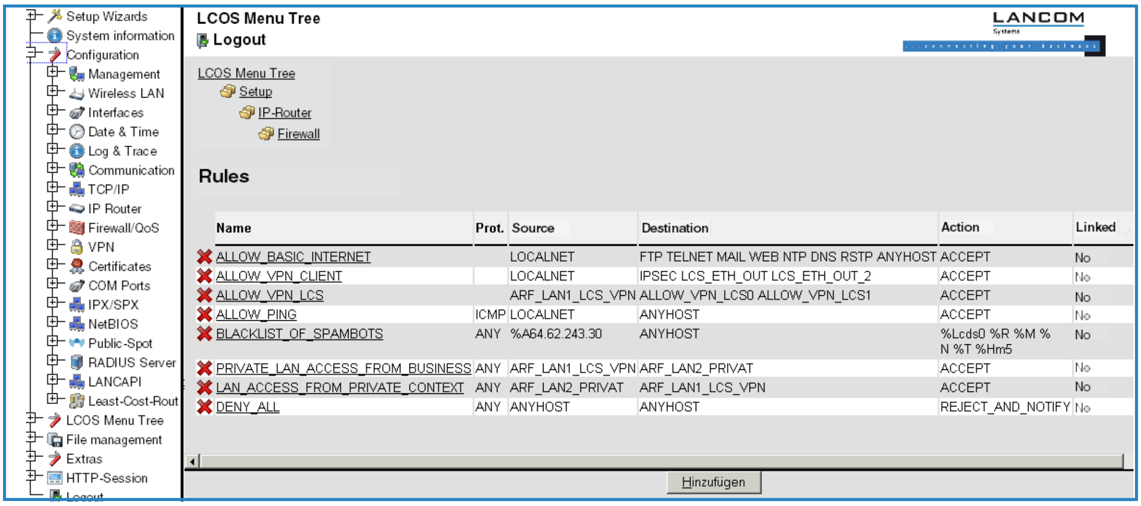
8.5 Configuring firewall rules with WEBconfig or Telnet

8.5.1 Rule table

- WEBconfig: Setup ▶ IP router ▶ Firewall ▶ Rules

The rules table links various pieces of information on a firewall rule. The rule contains the protocol to be filtered, the source, the destination and the firewall action to be executed. For every firewall rule there is also an on/off switch, a priority, the option to link with other rules, and activation of the rule for VPN connections.

Just as with LANconfig, WEBconfig can be used to configure the firewall with the help of objects. The % notation described as follows is only necessary for defining objects or actions.



Rules

Name	Prot.	Source	Destination	Action	Linked
ALLOW_BASIC_INTERNET		LOCALNET	FTP TELNET MAIL WEB NTP DNS RSTP ANYHOST	ACCEPT	No
ALLOW_VPN_CLIENT		LOCALNET	IPSEC LCS_ETH_OUT LCS_ETH_OUT_2	ACCEPT	No
ALLOW_VPN_LCS		ARF_LAN1_LCS_VPN	ALLOW_VPN_LCS0 ALLOW_VPN_LCS1	ACCEPT	No
ALLOW_PING	ICMP	LOCALNET	ANYHOST	ACCEPT	No
BLACKLIST_OF_SPAMBOTS	ANY	%A64.62.243.30	ANYHOST	%Lcds0 %R %M % N %T %Hm5	No
PRIVATE_LAN_ACCESS_FROM_BUSINESS	ANY	ARF_LAN1_LCS_VPN	ARF_LAN2_PRIVAT	ACCEPT	No
LAN_ACCESS_FROM_PRIVATE_CONTEXT	ANY	ARF_LAN2_PRIVAT	ARF_LAN1_LCS_VPN	ACCEPT	No
DENY_ALL	ANY	ANYHOST	ANYHOST	REJECT_AND_NOTIFY	No

Existing firewalls in the % notation are not automatically converted to the object-orientated form. However, the LANCOM KnowledgeBase contains the pre-defined firewall settings used by the new objects.

Devices with LCOS version 7.6 or later are automatically pre-defined with the main firewall objects. When processing older configurations with LANconfig, the firewall's standard objects are added automatically.

LCOS has a special syntax to define firewall rules. This syntax enables the representation of complex interrelationships for the testing and handling of data packets in the firewall with just a few characters. The rules are defined in the rules table. Pre-defined objects can be stored in two further tables so that frequently used objects do not have to be entered into the LCOS syntax every time:

- The firewall actions are stored in the action table
- The object table holds the stations and services

The objects from these tables can be used for rule definition, although this is not compulsory. They merely simplify the use of frequently used objects.

The definition of firewall rules can contain entries in the object table for protocols, services, stations and the action table for firewall actions, and also direct definitions in the appropriate LCOS syntax (e.g. %P6 for TCP).

For direct input of level parameters in the LCOS syntax, the same rules apply as specified in the following sections for protocols, source/destination and firewall actions.

8.5.2 Object table

- WEBconfig: Setup ▶ IP router ▶ Firewall ▶ Objects

Elements/objects that are to be used in the firewall rules table are defined in the objects table. Objects can be:

- Individual computers (MAC or IP address , hostname)
- Complete networks
- Protocols
- Services (ports or port areas, e.g. HTTP, Mail&News, FTP, ...)

These elements can be combined and hierarchically structured in any way. For example, objects for the TCP and UDP protocols can be defined first. Building upon this, objects can subsequently be created, for example, for FTP (= TCP + ports 20 and 21), HTTP (= TCP + port 80) and DNS (= TCP, UDP + port 53). These can in turn be combined into one object that contains all the definitions of the individual objects.

8.5.3 Action table

- WEBconfig: Setup ▶ IP Router ▶ Firewall ▶ Actions

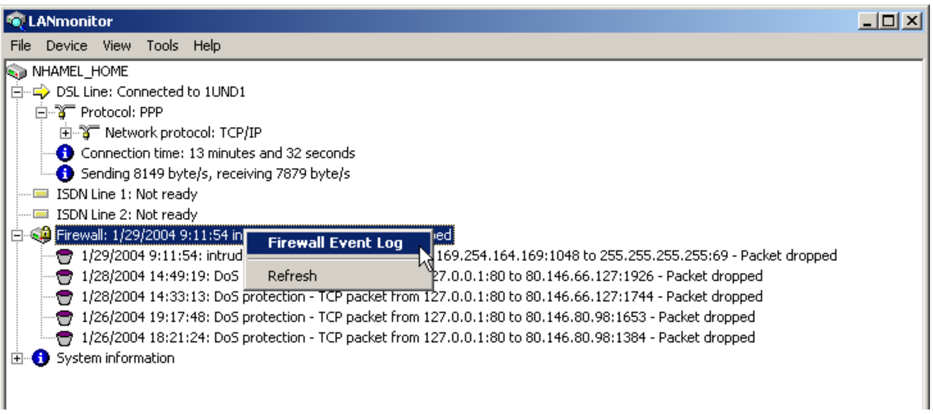
A firewall action comprises of a condition, a limit, a packet action and other measures.

As with the elements of the object table, firewall actions can be given a name and be combined with each other in any way recursively. The maximum recursion depth is limited to 16. They can also be entered into the actions field of the rules table directly.

8.6 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.



```
NHAMEL_HOME
  DSL Line: Connected to 1UND1
    Protocol: PPP
      Network protocol: TCP/IP
    Connection time: 13 minutes and 32 seconds
    Sending 8149 byte/s, receiving 7879 byte/s
  ISDN Line 1: Not ready
  ISDN Line 2: Not ready
  Firewall: 1/29/2004 9:11:54 in                ed
    1/29/2004 9:11:54: intrud                 169.254.164.169:1048 to 255.255.255.255:69 - Packet dropped
    1/28/2004 14:49:19: DoS                   27.0.0.1:80 to 80.146.66.127:1926 - Packet dropped
    1/28/2004 14:33:13: DoS protection - TCP packet from 127.0.0.1:80 to 80.146.66.127:1744 - Packet dropped
    1/26/2004 19:17:48: DoS protection - TCP packet from 127.0.0.1:80 to 80.146.80.98:1653 - Packet dropped
    1/26/2004 18:21:24: DoS protection - TCP packet from 127.0.0.1:80 to 80.146.80.98:1384 - Packet dropped
  System information
```

A new window with the complete logging table opens by clicking the right mouse button in the **Firewall Event Log** context menu.

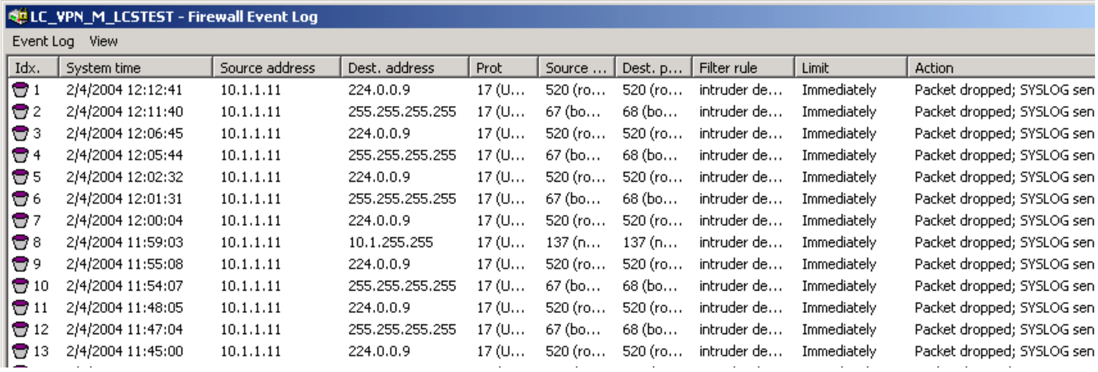
All lists and tables described in this section can be found under the following menu options:

WEBconfig: LCOS menu tree ▶ 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.

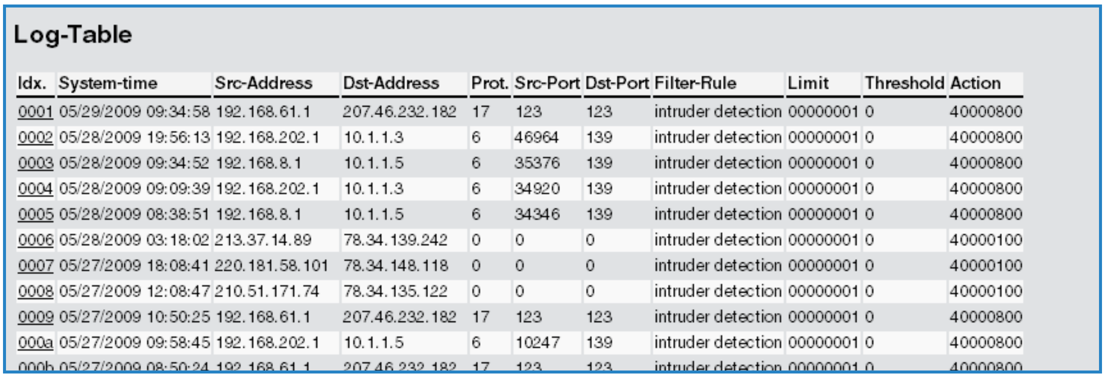
If you call up the logging table via LANmonitor, it looks like the following depiction:



LC_VPN_M_LCSTEST - Firewall Event Log

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

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



Log-Table

Idx.	System-time	Src-Address	Dst-Address	Prot.	Src-Port	Dst-Port	Filter-Rule	Limit	Threshold	Action
0001	05/29/2009 09:34:58	192.168.61.1	207.46.232.182	17	123	123	intruder detection	00000001	0	40000800
0002	05/28/2009 19:56:13	192.168.202.1	10.1.1.3	6	46964	139	intruder detection	00000001	0	40000800
0003	05/28/2009 09:34:52	192.168.8.1	10.1.1.5	6	35376	139	intruder detection	00000001	0	40000800
0004	05/28/2009 09:09:39	192.168.202.1	10.1.1.3	6	34920	139	intruder detection	00000001	0	40000800
0005	05/28/2009 08:38:51	192.168.8.1	10.1.1.5	6	34346	139	intruder detection	00000001	0	40000800
0006	05/28/2009 03:18:02	213.37.14.89	78.34.139.242	0	0	0	intruder detection	00000001	0	40000100
0007	05/27/2009 18:08:41	220.181.58.101	78.34.148.118	0	0	0	intruder detection	00000001	0	40000100
0008	05/27/2009 12:08:47	210.51.171.74	78.34.135.122	0	0	0	intruder detection	00000001	0	40000100
0009	05/27/2009 10:50:25	192.168.61.1	207.46.232.182	17	123	123	intruder detection	00000001	0	40000800
000a	05/27/2009 09:58:45	192.168.202.1	10.1.1.5	6	10247	139	intruder detection	00000001	0	40000800
000b	05/27/2009 08:50:24	192.168.61.1	207.46.232.182	17	123	123	intruder detection	00000001	0	40000800

The table contains the following values:

Element	Element meaning
Idx.	Current index (so that the table can be polled also via SNMP)
System time	System time in UTC codification (will be transformed on displaying of the table into clear text)
Src address	Source address of the filtered packet
Dst address	Destination address of the filtered packet
Prot.	Protocol (TCP, UDP etc.) of the filtered packet
Src-p	Source port of the filtered packet (only with port-related protocols)
Dst-p	Destination port of the filtered packet (only with port-related protocols)
Filter-Rule	Name of the rule, which has raised the entry.
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

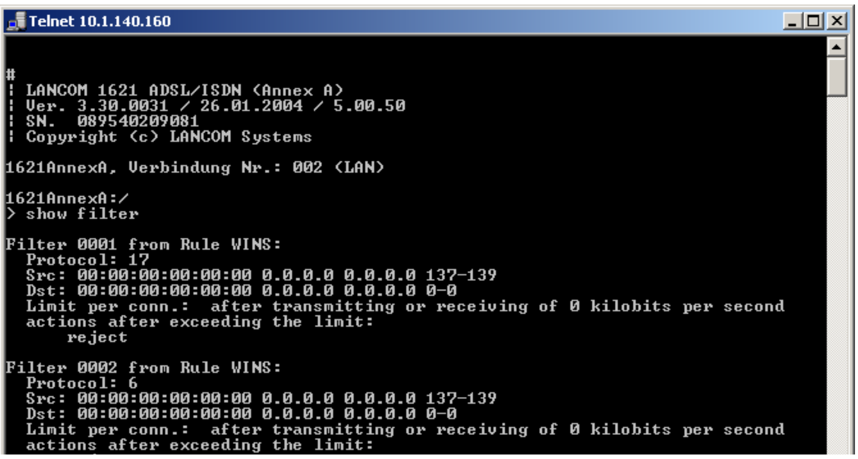
All Firewall actions are likewise displayed within the IP router trace ('How to start a trace' → page 5-1). Furthermore, some LANCOM models have a Firewall LED, which signals each filtered packet.

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.

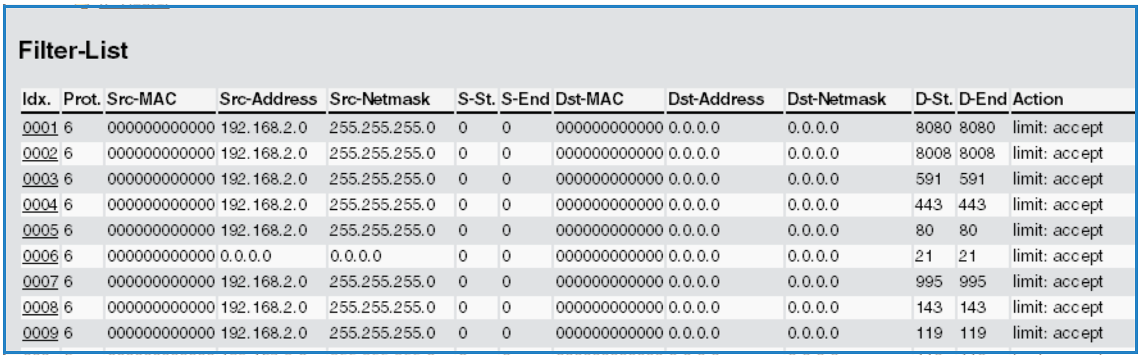
On Telnet level, the content of the filter list can be displayed with the command `show filter`:



Telnet 10.1.140.160

```
#
| LANCOM 1621 ADSL/ISDN (Annex A)
| Ver. 3.30.0031 / 26.01.2004 / 5.00.50
| SN.  089540209081
| Copyright (c) LANCOM Systems

1621AnnexA, Verbindung Nr.: 002 (LAN)

1621AnnexA:/
> 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
  Limit per conn.:  after transmitting or receiving of 0 kilobits per second
  actions after exceeding the limit:
      reject

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
  Limit per conn.:  after transmitting or receiving of 0 kilobits per second
  actions after exceeding the limit:
```

Under WEBconfig the filter list has the following structure:



Filter-List

Idx.	Prot.	Src-MAC	Src-Address	Src-Netmask	S-St.	S-End	Dst-MAC	Dst-Address	Dst-Netmask	D-St.	D-End	Action
0001	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	8080	8080	limit: accept
0002	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	8008	8008	limit: accept
0003	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	591	591	limit: accept
0004	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	443	443	limit: accept
0005	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	80	80	limit: accept
0006	6	000000000000	0.0.0.0	0.0.0.0	0	0	000000000000	0.0.0.0	0.0.0.0	21	21	limit: accept
0007	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	995	995	limit: accept
0008	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	143	143	limit: accept
0009	6	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	119	119	limit: accept

The individual fields in the filter list have the following meaning:

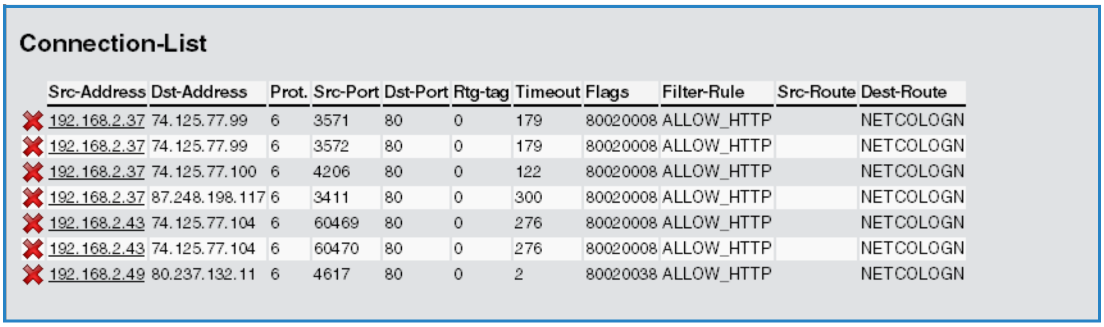
Entry	Description
Idx.	Current index
Prot	Protocol to be filtered, e.g. 6 for TCP or 17 for UDP.
Src MAC	Ethernet source address of the packet to be filtered or 000000000000, if the filter should apply to all packets.
Src address	Source IP address or 0.0.0.0, if the filter should apply to all packets.
Source mask	Source network mask, which determinates the source network together with the source IP address, or 0.0.0.0, if the filter should apply to packets from all networks.
Q start	Start source port of the packets to be filtered.
Q end	End source port of the packets to be filtered. Makes up the port range together with the start source port, in which the filter takes effect. If start and end port are 0, then the filter is valid for all source ports.
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.

Entry	Description
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:



Connection-List

	Src-Address	Dst-Address	Prot.	Src-Port	Dst-Port	Rtg-tag	Timeout	Flags	Filter-Rule	Src-Route	Dest-Route
✗	192.168.2.37	74.125.77.99	6	3571	80	0	179	80020008	ALLOW_HTTP		NETCOLOGN
✗	192.168.2.37	74.125.77.99	6	3572	80	0	179	80020008	ALLOW_HTTP		NETCOLOGN
✗	192.168.2.37	74.125.77.100	6	4206	80	0	122	80020008	ALLOW_HTTP		NETCOLOGN
✗	192.168.2.37	87.248.198.117	6	3411	80	0	300	80020008	ALLOW_HTTP		NETCOLOGN
✗	192.168.2.43	74.125.77.104	6	60469	80	0	276	80020008	ALLOW_HTTP		NETCOLOGN
✗	192.168.2.43	74.125.77.104	6	60470	80	0	276	80020008	ALLOW_HTTP		NETCOLOGN
✗	192.168.2.49	80.237.132.11	6	4617	80	0	2	80020038	ALLOW_HTTP		NETCOLOGN

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. As conditions the following values are possible: **new, establish, open, closing, closed, rejected** (corresponding to the TCP flags: SYN, SYN ACK, ACK, FIN, FIN ACK and RST). UDP connections know the conditions **new, open** and **closing** (the last one only, if the UDP connection is linked with a condition-afflicted control path. This is e.g. the case with protocol H.323.).
Src route	Name of the remote station, over which the first packet has been received.
Dst route	Name of the remote station, where the first packet will be sent to.
Filter rule	Name of the rule, which has generated the entry (determines also the actions to be executed), when a suitable packet is received.

Meaning of the flags of the connection list

Flag	Flag meaning
00000001	TCP: SYN sent
00000002	TCP: SYN/ACK received
00000004	TCP: waiting for ACK of the server
00000008	all: open connection
00000010	TCP: FIN received
00000020	TCP: FIN sent
00000040	TCP: RST sent or received

Flag	Flag meaning
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.

8.7 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.

8.8 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.

8.8.1 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.

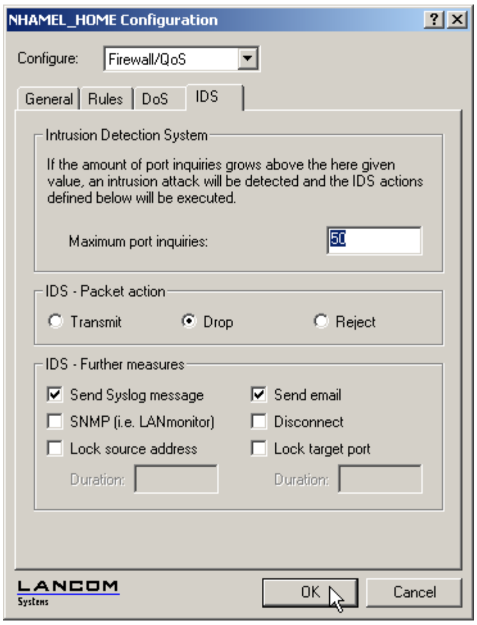
Portscan Detection

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: 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.

8.8.2 Configuration of the IDS



Configure: Firewall/QoS

Intrusion Detection System

If the amount of port inquiries grows above the here given value, an intrusion attack will be detected and the IDS actions defined below will be executed.

Maximum port inquiries: 50

IDS - Packet action

○ Transmit ● Drop ○ Reject

IDS - Further measures

☑ Send Syslog message ☑ Send email
□ SNMP (i.e. LANmonitor) □ Disconnect
□ Lock source address □ Lock target port
Duration: Duration:

LANconfig: Firewall/QoS ▶ IDS

WEBconfig: LCOS menu tree ▶ Setup ▶ IP-Router ▶ Firewall

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.

8.9 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.

8.9.1 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.

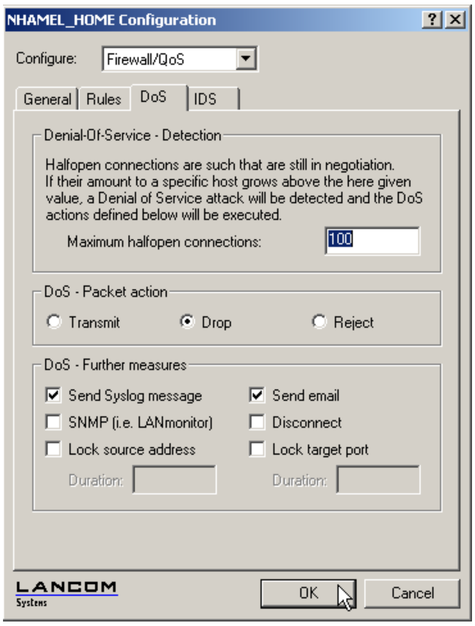
Bonk/Fragrouter

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.

8.9.2 Configuration of DoS blocking



Configure: Firewall/QoS

Denial-Of-Service - Detection

Halfopen connections are such that are still in negotiation. If their amount to a specific host grows above the here given value, a Denial of Service attack will be detected and the DoS actions defined below will be executed.

Maximum halfopen connections: 100

DoS - Packet action

○ Transmit ● Drop ○ Reject

DoS - Further measures

☑ Send Syslog message ☑ Send email
☐ SNMP (i.e. LANmonitor) ☐ Disconnect
☐ Lock source address ☐ Lock target port
Duration: Duration:

LANconfig: Firewall/QoS ▶ DoS

WEBconfig: LCOS menu tree ▶ Setup ▶ IP-Router ▶ Firewall

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.

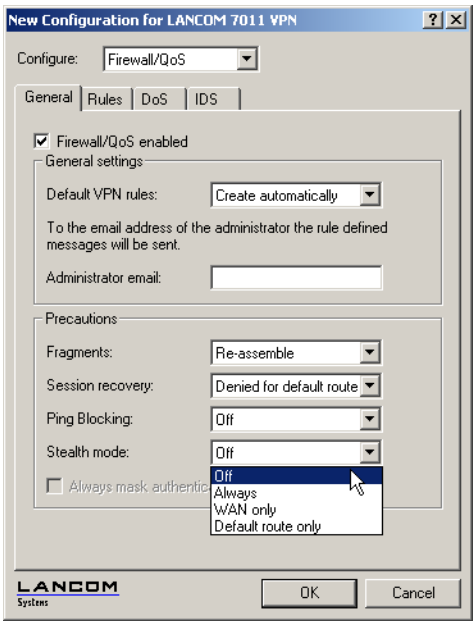
This part is configured centrally in order not to open a gate for DoS attacks by incorrect configuration of the Firewall. Apart from specifying the maximum number of half-open connections, fragment action and possible notification mechanisms, also these more extensive possibilities of reaction exist:

- 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.

However, always active are the following protection mechanisms:

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

8.9.3 Configuration of ping blocking and Stealth mode



Configure: Firewall/QoS

☑ Firewall/QoS enabled

General settings

Default VPN rules: Create automatically

To the email address of the administrator the rule defined messages will be sent.

Administrator email:

Precautions

Fragments: Re-assemble

Session recovery: Denied for default route

Ping Blocking: Off

Stealth mode: Off

□ Always mask authentic

WEBconfig, Telnet

LANconfig: Firewall/QoS ▶ General

WEBconfig: LCOS menu tree ▶ Setup ▶ IP-Router ▶ Firewall

9 Quality of Service

This chapter dedicates itself to quality: Under the generic term Quality of Service (short: QoS) those LCOS functions are summarized, which are concerned with the guarantee of certain service availabilities.

9.1 Why QoS?

The main objective of Quality of Service is to transfer certain data packets either particularly safe or as immediately as possible:

- It may happen during a data transfer that data packets are not delivered to the addressee. But for some applications it is very important that all sent packets really do arrive. An e-mail, for example, divided into several small data packets, can only be assembled together again, when all parts have arrived completely. Whether one or an other packet arrives with little time delay does not make any difference. These applications often count on the connection-orientated Transmission Control Protocol (TCP). This protocol ensures that data will be transferred correctly and chronologically via the net. It automatically adjusts the sending rate downwards if the confirmation of sent data packets is outstanding for longer times, and also takes care of repeated transmission in case of packet losses.
- In other applications, e.g. telephony via the Internet (Voice-over-IP, VoIP), it is - differently to the case above - very important that the data packets arrive at the addressee with only little time delay. But it really doesn't matter if once a data packet gets lost in this case. The participant at the other end of the connection will understand the caller, even if small parts of the speech got lost. This application aims at the fastest sending of data packets as possible. The connectionless User Datagram Protocol (UDP) is often used for this kind of application. Also this protocol has very little administrative overhead. But chronological delivery of packets is not guaranteed, data packets are simply sent out. Because no confirmation receipt exists, lost packets never get delivered again.

9.2 Which data packets to prefer?

The necessity of a QoS concept results only from the fact that the available bandwidth is not always sufficient for transferring all pending data packets reliably and on time. Load peaks result easily from running simultaneously large FTP downloads, while exchanging e-mails and using IP telephones over the data line. In order to meet also in these situations the demands of the desired data transfer, certain data packets must be treated preferentially. It is necessary for this, that at first a LANCOM recognizes which data packets should be preferred at all.

There are two possibilities to signal the need for a preferential treatment of data packets in the LANCOM:

- The application, as e.g. the software of certain IP telephones, is itself able to mark the data packets appropriately. This marking, the "tag", is set within the header of the IP packets. The two different variants of this marking "ToS" and "DiffServ" can simply described assume the following states:
  - ToS "Low Delay"
  - ToS "High Reliability"
  - DiffServ "Expedited Forwarding"
  - DiffServ "Assured Forwarding"

ⓘ The IP header bits of the ToS resp. DiffServ field are copied in case of a VPN route also into the enclosing IP header of the IPSec VPN packet. Thus QoS is available also for VPN routes over the Internet, as long as your provider treats according packets preferentially also in the WAN.

- When the application itself has no possibility to mark the data packets appropriately, the LANCOM can ensure the correct treatment. For this, it uses the existing functions of the firewall, which can classify e.g. data packets according to subnets or services (applications). Due to these functions it is e. g. possible to treat individually data packets of a FTP connection or those of a certain department (in a separate subnet).

  For treatment of data packets classified by the firewall the following two possibilities can be chosen:
  - Guaranteed minimum bandwidth
  - Limited maximum bandwidth

What is DiffServ?

DiffServ stands for "Differentiated Services" and is a quite recent model to signal the priority of data packets. DiffServ is based on the known Type-of-Service (ToS) field and uses the same byte within the IP header.

ToS is using the first three bits to describe the priorities (precedence) 0 to 7, as well as four further bits (the ToS bits) to optimize the data stream (e.g. "Low Delay" and "High Reliability"). This model is rather inflexible, and this is why it has been used quite rarely in the past.

The DiffServ model uses the first 6 bits to make distinctions of different classes. Up to 64 gradings are thus possible (Differentiated Services Code Point, DSCP) which enable a finer priorisation of the data stream:

- To ensure downward compatibility with ToS implementations, the previous precedence levels can be depicted with the “Class Selectors” (CS0 to CS7). Thereby, the level “CS0” denotes so-called “Best Effort” (BE) and stands for usual transfer of data packets without special treatment.
- The “Assured Forwarding” classes are used for a secured transfer of data packets. The first digit of the AF class describes each the priority of the transfer (1 to 4), the second digit the “drop probability” (1 to 3). Packets with AFxx marking are transferred in a secured way, and thus not dropped.

Finally, the class “Expedited Forwarding” marks those packets, that shall be transferred preferentially, before all other packets.

Code point	DSCP bits	Dec.
CS0 (BE)	000000	0
CS1	001000	8
CS2	010000	16
CS3	011000	24
CS4	100000	32
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.

For LANCOM devices with VoIP functions that were already integrated or added in with a software option, the QoS settings for SIP calls are defined automatically.

Full dynamic bandwidth management for sending

Concerning the sending direction, the bandwidth management takes place dynamically. This means that e.g. a guaranteed minimum bandwidth is only available, as long as the corresponding data transfer really exists.

An example:

For the transmission of VoIP data of an appropriate VoIP gateway, a bandwidth of 256 Kbps is to be guaranteed always. Thereby, each individual VoIP connection consumes 32 Kbps.

As long as nobody telephones, the entire bandwidth is at the disposal to other services. Per adjacent VoIP connection 32 Kbps less is available to other applications, until 8 VoIP connections are active. As soon as a VoIP connection is terminated, the corresponding bandwidth is available again to all other applications.

For correct functioning of this mechanism, the sum of the configured minimum bandwidth must not exceed the effectively available transmission bandwidth.

Dynamic bandwidth management also for reception

For receiving bandwidth control, packets can be buffered and only belatedly confirmed. Thus TCP/IP connections regulate themselves automatically on a smaller bandwidth.

Each WAN interface is assigned a maximum reception bandwidth. This bandwidth will be accordingly degraded by every QoS rule that guarantees a minimum bandwidth of reception on this interface.

- If the QoS rule has been defined connection-related, the reserved bandwidth will be unblocked immediately after releasing the connection and the maximum available bandwidth will increase accordingly on the WAN interface.
- If the QoS rule has been defined globally, then the reserved bandwidth will be unblocked only after the ending of the last connection.

9.2.2 Limited maximum bandwidths

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

An example:

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

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

Combination possible

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

9.3 The queue concept

9.3.1 Queues in transmission direction

Quality of Service requirements are realized in LCOS by using different queues for the data packets. For the transmission side, the following queues are utilized:

- Urgent queue I

  This queue is always processed at first before all others. The following data packets are handled here:

  - Packets with ToS “Low Delay“
  - Packets with DiffServ “Expedited Forwarding“
  - All packets that have been assigned a certain minimum bandwidth, as long as the guaranteed minimum bandwidth is not exceeded.
  - TCP control packets can be likewise dispatched by this queue preferentially (see ’SYN/ACK speedup’ → page 7-8).

- Urgent queue II

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

  As long as the interval for the minimum bandwidth is not exceeded (i.e. up to the end of the current second), all packets in this queue are treated without further special priority. All packets of this queue, of the "secured queue" and the "standard queue" share now the existing bandwidth. The packets are taken in order from the queues when sending in exactly the same sequence, in which they have been placed into these queues. If the interval runs off, all blocks, which are at this time still in the "Urgent queue II" up to the exceeding of the in each case assigned minimum bandwidth, are placed again into the "Urgent queue I". The rest remains in the "Urgent queue II".

  With this procedure it is guaranteed that prioritized connections do not crush the remaining data traffic.

- Secured queue

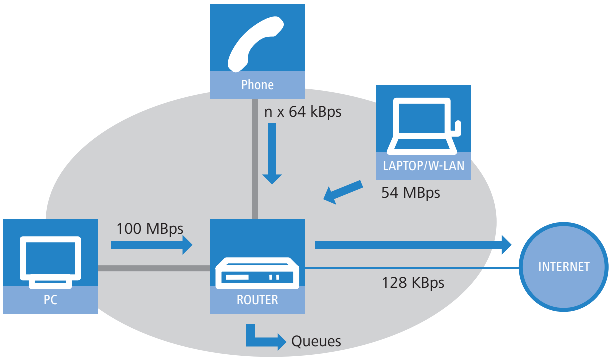
  This queue does not have a separate priority. However, packets in this queue are never dropped (transmission guaranteed).

  - Packets with ToS “High Reliability“
  - Packets with DiffServ “Assured Forwarding“

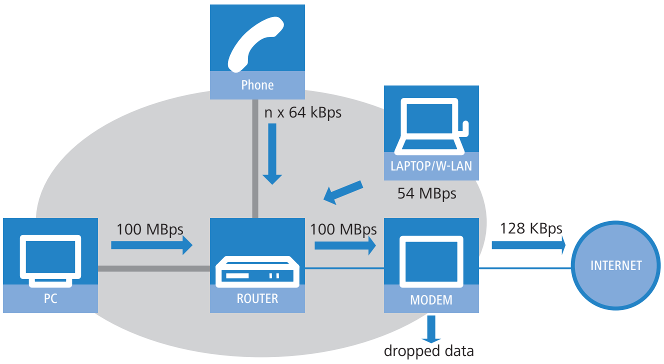
- Standard queue

  The standard queue contains all not classified data traffic. Packets in this queue are dropped at first when packets cannot be delivered fast enough.

The queue concept can, however, only work out when a “traffic congestion“ of data packets has been accumulated at the interface from LAN to the WAN. Such a congestion is created when the interface within the LANCOM can submit fewer data to the WAN than data are delivered in peak periods from the LAN. This is e.g. the case, if the interface to the WAN is an integrated ADSL interface with comparatively low transmission speed (“upstream”). The integrated ADSL modem automatically reports back to the LANCOM how many data packets it is still able to receive, and thus brakes the data stream already within the router. As a result, the queues will automatically fill up.



Different is the case, if an Ethernet interface represents the connection to the WAN. From the LANCOM's point of view, the connection to the Internet via an external broadband modem looks like an Ethernet segment. On the distance from the LANCOM to the DSL modem, data will be transferred with full LAN speed of 10 or 100 Mbps. Because of an equal input and output speed, no natural congestion will be produced then. Furthermore, the Ethernet between the LANCOM and the broadband modem does not report anything about the capacity of the connection. The consequence: a congestion will only be happen within the broadband modem. But because no queues are deployed therein, surplus data will be lost. Thus a prioritization of "preferred" data is not possible!



To solve this problem, the transfer rate of the LANCOM's WAN interface will be reduced artificially. This interface will thereby be adjusted to the transfer rate that is available for the actual data transport towards the WAN. For a standard DSL connection, the DSL interface is thus adjusted in the LANCOM to the appropriate upstream rate (e.g. 128 kbps).

Data rates indicated by providers are mostly likely net rates. The gross data rate, which is available for the interface is a little bit higher than the net data rate guaranteed by the provider. If you know the gross data rate of your provider, you can enter this value for the interface and slightly increase in this way the data throughput. However, with entering the net data rate you play safe in any case!

9.3.2 Queues for receiving direction

Apart from the data transfer rate in transmission direction, the same consideration applies also to the receiving direction. Due to its 10 or 100 Mbps Ethernet interface, the LANCOM's WAN interface is fed by clearly fewer data from the broadband modem than would actually be receivable. All data packets received on the WAN interface are transferred to the LAN with equal rights.

In order to be able to prioritize incoming data as well, thus an artificial "brake" must be added also in this direction. Like already incorporated for the upstream direction, the data transfer rate of the interface is therefore adapted to the provider's offer in the downstream direction. For a standard DSL connection thus e.g. a downstream rate of 768 kbps applies. Again, the gross data rate can be entered here, if known.

Reducing the receiving bandwidth makes possible to treat received data packets suitably. Preferred data packets will be directly passed on to the LAN up to the guaranteed minimum bandwidth, all remaining data packets are running into congestion. This congestion produces generally a delayed confirmation of the packets. For a TCP connection, the sending server will react to this delay by reducing its sending frequency and adapting itself to the available bandwidth.

The following queues operate on the receiving side:

- Deferred Acknowledge Queue

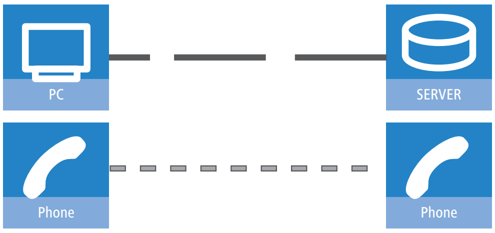
  Each WAN interface contains additionally a QoS reception queue, which takes up those packets that should be „slowed down". The storage period of each individual packet depends on its length and on the actual permitted reception bandwidth on the receiving side. Packets with a minimum reception bandwidth assigned by a QoS rule are passing through without any further delay, as long as the minimum bandwidth is not exceeded.

- Standard reception queue

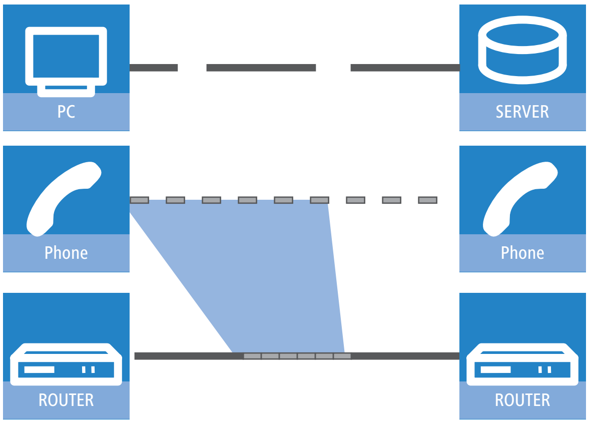
  All packets that do not need special treatment because of an active QoS rule on the receiving side end up here. Packets of this queue are directly passed on resp. confirmed without consideration of maximum bandwidths.

9.4 Reducing the packet length

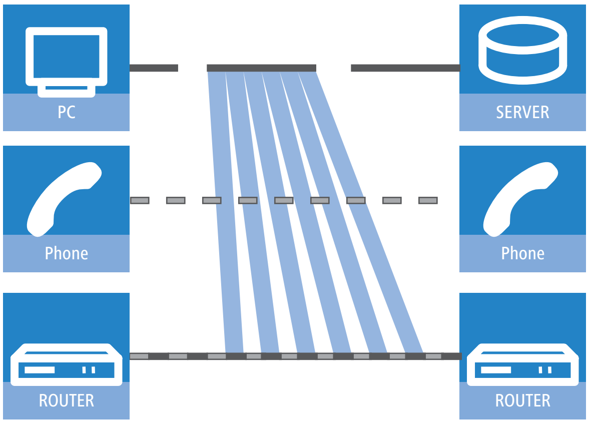
The preferential treatment of data packets belonging to important applications can be endangered - depending on the situation - by very long data packets of other applications. This is the case e.g. when IP telephony and a FTP data transfer are simultaneously active on the WAN connection.



The FTP transfer uses quite large data packets of 1500 byte, whereas, the Voice over IP connection sends packets of e.g. 24 byte net in relatively short intervals. If FTP packets are in the sending queue of the LANCOM just at the moment when a VoIP packet is to be transferred, then the VoIP packet can only be sent after the line is free again. Depending on the transfer rate of the connection, this may cause a noticeable delay of the speech transmission.



This annoying behavior can be compensated if all data packets, which are not belonging to the connection preferred by QoS, do not exceed a certain packet length. While doing so, the data packets of the FTP connection will be divided into such small sections that the time-critical VoIP connection is able to deliver the packets without noticeable delay within the required time slots. A resulting delay has no disadvantageous effect to the TCP-secured FTP transfer.



Two different procedures exist to influence the packet length:

- The LANCOM can inform the peers of a data connection that they should only send data packets up to a certain length. Thereby, an appropriate PMTU (Path Maximum Transmission Unit) is enforced on the sending side. This procedure is called PMTU reduction".

The PMTU reduction can be used for sending as well as for receiving direction. For the sending direction, the data source of the own LAN is adjusted with the PMTU reduction to a smaller packet size, for the receiving direction the data source of the WAN, e.g. web or FTP servers in the Internet.

Provided that the data connection already exists when the VoIP connection is started, the senders regulate packet lengths very quickly to the permitted value. When setting up new data connections while a VoIP connection is already established, the maximum permitted packet length is negotiated directly during the connection phase.

The reduced packet length on the data connection still remains also after terminating the VoIP connection, as long as the sender checks the PMTU value again.

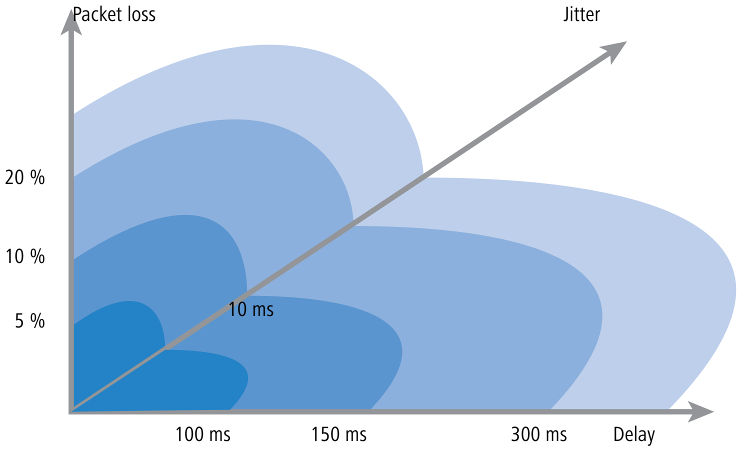
- The LANCOM is able to split packets to be sent above an adjustable maximum size (e.g. 256 byte) into smaller units itself. But such a procedure called "fragmentation" is not supported by all servers of the Internet, because dealing with fragmented packets is considered as a security risk, and therefore is turned off by many servers. That's why disturbances can occur e.g. while downloading or while transmitting web pages.

  Thus, this procedure is recommended only for connections without involving unknown servers, e.g. for a direct connection of branches to their head office via VPN connection, over which the Internet traffic is not running simultaneously.

9.5 QoS parameters for Voice over IP applications

An important task when configuring VoIP systems is to guarantee a sufficient voice quality. Two factors considerably influence the voice quality of a VoIP connection: The voice delay on its way from sender to addressee, as well as the loss of data packets, which do not arrive or do not arrive in time at the addressee. The "International Telecommunications Union" (ITU) has examined in extensive tests, what human beings perceive as sufficient voice quality, and has published as the result in the ITU G.114 recommendation.

For LANCOM devices with VoIP functions that were already integrated or added in with a software option, the QoS settings for SIP calls are defined automatically.



In case of a delay of not more than 100 ms, and a packet loss of less than 5%, the quality is felt like a "normal" telephone connection. In case of more than 150 ms delay and less than 10% packet loss, the telephone user perceives still a very good quality. Up to 300 ms and 20%, some listeners feel this quality like still suitable, beyond that the connection is considered as no more suitable for voice transmission.

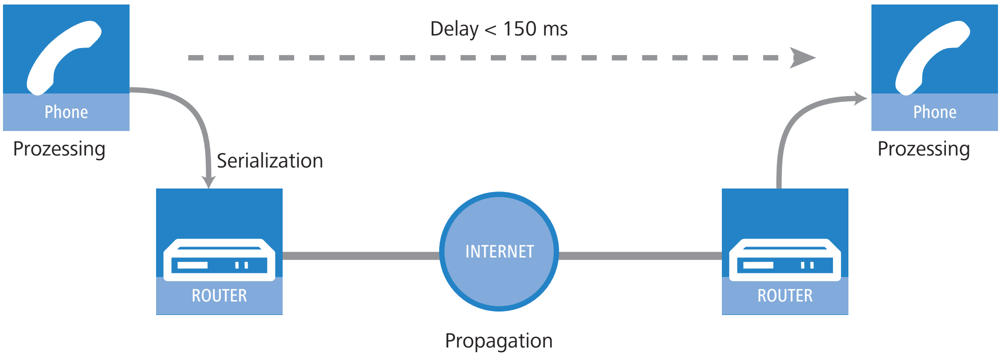
Apart from the average delay time, also a variation in this delay is perceived by the human ear. Delay differences of the voice information from sender to addressee (jitter) are still tolerated up to 10 ms, and values beyond considered as irritating.

Accordingly, a VoIP connection should be configured such that the criteria for good speech quality are met: Packet loss up to 10%, delay up to 150 ms and jitter up to 10ms.

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

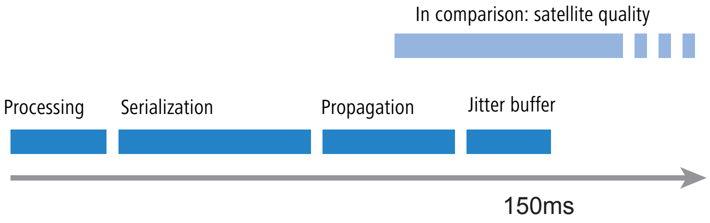
- □ Time of processing (packeting, coding and compression by the sender and the addressee), duration of handing over the packet from application to the interface (serialization), and the time for transmitting via the WAN distance (propagation) contribute to the fixed part of delay.
- □ The variable part is determined by the jitter resp. by the setting of the jitter buffer.

These two parts together compose a delay, which should ideally not exceed 150 ms.



- ■ Apart from the general loss by network transmission, the packet loss is significantly influenced by the jitter buffer. If packets arrive with a larger delay than it can be balanced by the jitter buffer, the packets will be discarded and will increase the packet loss. The larger the jitter buffer, the smaller is the loss. Conversely, the entire delay will increase with the jitter buffer size. That means for configuration, that the jitter buffer should be selected as small as the quality can be considered still as sufficient.

In detail, delay is determined especially by the codec used, the resulting packet size and the available bandwidth:



- ■ The time for processing is determined by the used codec. For a sampling time of 20 ms, exactly each 20 ms a new packet is generated. Times for compression can mostly be neglected.

The time for handing over the packet to the interface is defined by the quotient of packet size and available bandwidth

	Packet size in bytes						
	1	64	128	256	512	1024	1500
56 Kbps	0,14	9	18	36	73	146	215
64 Kbps	0,13	8	16	32	64	128	187
128 Kbps	0,06	4	8	16	32	64	93
256 Kbps	0,03	2	4	8	16	32	47
512 Kbps	0,016	1	2	4	8	16	23
768 Kbps	0,010	0,6	1,3	2,6	5	11	16
1536 Kbps	0,005	0,3	0,6	1,3	3	5	8

A 512 byte packet of an FTP connection occupies the line at 128 Kbps upstream cablefor 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).

Without IPSec	Payload	IP-Payload	Ethernet/ PPPoE	ATMNetto Bps	ATMBrutto Bps
Code	20ms	20ms	20ms	20ms	20ms
G711-64	160	200	222	96000,0	106000,0
G722-64	160	200	222	96000,0	106000,0
G726-40	100	140	162	76800,0	84800,0
G726-32	80	120	142	76800,0	84800,0
G726-24	60	100	122	57600,0	63600,0
G726-16	40	80	102	57600,0	63600,0
G729-8	20	60	82	57600,0	63600,0
G723-6,3	16	56	78	38400,0	42400,0

Without IPSec	Payload	IP-Payload	Ethernet/ PPPoE	ATMNetto Bps	ATMBrutto Bps
Code	30ms	30ms	30ms	30ms	30ms
G711-64	240	280	302	89510,4	98834,4
G722-64	240	280	302	89510,4	98834,4
G726-40	150	190	212	63936,0	70596,0
G726-32	120	160	182	63936,0	70596,0
G726-24	90	130	152	51148,8	56476,8
G726-16	60	100	122	38361,6	42357,6
G729-8	30	70	92	38361,6	42357,6
G723-6,3	24	64	86	38361,6	42357,6

With IPSec	Payload	IP-Payload	IPSEC-Payload	Ethernet/ PPPoE	ATMNetto Bps	ATMBrutto Bps
Code	20ms	20ms	20ms	20ms	20ms	20ms
G711-64	160	200	260	282	134400,0	148400,0
G722-64	160	200	260	282	134400,0	148400,0
G726-40	100	140	200	222	96000,0	106000,0
G726-32	80	120	180	202	96000,0	106000,0
G726-24	60	100	160	182	96000,0	106000,0
G726-16	40	80	140	162	76800,0	84800,0
G729-8	20	60	120	142	76800,0	84800,0
G723-6,3	16	56	116	138	76800,0	84800,0

With IPSec	Payload	IP-Payload	IPSEC-Payload	Ethernet/ PPPoE	ATMNetto Bps	ATMBrutto Bps
Code	30ms	30ms	30ms	30ms	30ms	30ms
G711-64	240	280	340	362	102297,6	112953,6
G722-64	240	280	340	362	102297,6	112953,6
G726-40	150	190	250	272	76723,2	84715,2
G726-32	120	160	220	242	76723,2	84715,2
G726-24	90	130	190	212	63936,0	70596,0
G726-16	60	100	160	182	63936,0	70596,0
G729-8	30	70	130	152	51148,8	56476,8
G723-6,3	24	64	124	146	51148,8	56476,8

- IP payload: Voice payload + 40 byte header (12 byte RTP; 8 byte UDP; 20 byte IP header)

- IPSec payload: IP paket + padding + 2 byte (padding length & next header) = multiple of the IPSec initialization vector

The values in the table apply to the use of AES. With other encryption methods the resulting package may vary on a minor degree.

Further information on bandwidth requirements for Voice over IP with IPSec is available in the LANCOM techpaper Performance Analysis of LANCOM Routers.

- 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	Serialization	Propagation	Jitter buffer	Sum
G.723.1	30 ms	32 ms	50 ms	60 ms	172 ms
G.711	20 ms	32 ms	50 ms	40 ms	142 ms

The transfer time of the packets to the interface (serialization) assumes a PMTU of 512 bytes on a 128 Kbps connection. Therefore, for slower interfaces or other codecs it is eventually necessary to adjust jitter buffers and/or PMTU values.

Please notice that the bandwidths are required in the sending and receiving direction, as well as just for one single connection.

9.6 QoS in sending or receiving direction

For controlling data transfer by means of QoS one can select whether the according rule applies to the sending or to the receiving direction. But which direction refers to sending and receiving for a given a data transfer depends on the particular point of view. The following two variants apply:

- The direction corresponds to the logical connection setup
- The direction corresponds to the physical data transfer over the appropriate interface

The differences are unveiled by looking at a FTP transfer. A client of the LAN is connected to the Internet through a LANCOM.

- During an active FTP session, the client sends by the PORT command the information to the server, on which port the DATA connection is expected. As the result, the server establishes the connection to the client and sends the data in the same direction. In this case, the logical connection as well as the real data stream over the interface go from the server to the client, and the LANCOM takes both as the receiving direction.
- Different is the case of a passive FTP session. Here the client itself establishes the connection to the server. The logical connection setup thus is from client to server, but the data transmission over the physical interface flows in the reverse direction from server to client.

With standard settings, a LANCOM assumes the sending or receiving direction depending on the logical connection setup. Because such a point of view may not be easy to follow in certain application scenarios, the point of view can alternatively be changed to the flow of the physical data stream.

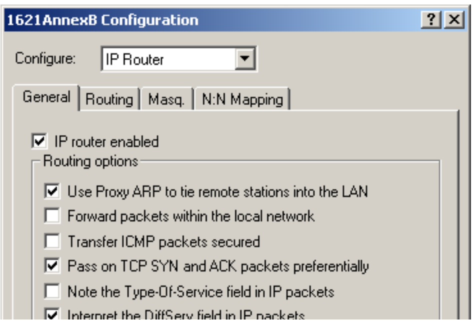
The differentiation between sending and receiving direction applies only to the installation of maximum bandwidths. For a guaranteed minimum bandwidth, as well as for fragmentation and PMTU reduction always the physical data transfer via the respective interface applies as the direction!

9.7 QoS configuration

9.7.1 Evaluating ToS and DiffServ fields

ToS or DiffServ?

For configuration with LANconfig adjust on index card 'General' whether the 'Type of service field' or alternatively the 'DiffServ field' is to be observed for prioritization of data packets. When both options are turned off, the ToS/DiffServ field will be ignored.



1621AnnexB Configuration

Configure: IP Router

☑ IP router enabled

Routing options

☑ Use Proxy ARP to tie remote stations into the LAN
☐ Forward packets within the local network
☐ Transfer ICMP packets secured
☑ Pass on TCP SYN and ACK packets preferentially
☐ Note the Type-Of-Service field in IP packets
☑ Interpret the DiffServ field in IP packets

LANconfig: IP router ▶ general ▶ routing methods

WEBconfig: Setup ▶ IP router ▶ Routing method

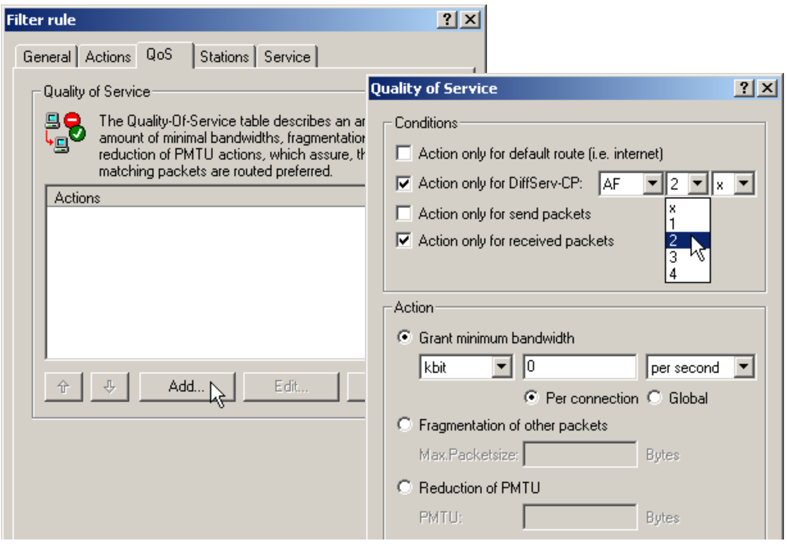
Feature settings for routing method values are the following:

- **Standard**: The ToS/DiffServ field is ignored.
- **TOS**: The ToS/DiffServ field is considered as ToS field, the bits “Low delay” and “High reliability” will be evaluated.
- **DiffServ**: The ToS/DiffServ field is interpreted as DiffServ field and evaluated as follows:

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

DiffServ in Firewall rules

The code points from the DiffServ field can be evaluated by Firewall rules for further control of QoS parameters such as minimum bandwidth or PMTU reduction.



Filter rule

Quality of Service

The Quality-Of-Service table describes an ar amount of minimal bandwidths, fragmentatio reduction of PMTU actions, which assure, th matching packets are routed preferred.

Quality of Service

Conditions

☐ Action only for default route (i.e. internet)
☑ Action only for DiffServ-CP: AF 2 x
☐ Action only for send packets
☑ Action only for received packets

Action

● Grant minimum bandwidth
kbit 0 per second
● Per connection ○ Global
○ Fragmentation of other packets
Max.Packetsize: Bytes
○ Reduction of PMTU
PMTU: Bytes

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 9-1.

LANconfig: Firewall/QoS ▶ Rules ▶ Filter rules ▶ Quality of Service

WEBconfig: Setup ▶ IP router ▶ Firewall ▶ Rule list

The Firewall rule is extended by condition “@d” and the DSCP (Differentiated Services Code Point). The code point can either be indicated with its name (CS0 - CS7, AF11 to AF 43, EF or BE) or its decimal resp. hexadecimal depiction. “Expedited Forwarding” can therefore be indicated as “@dEF”, “@d46” or “@d0x2e”. Furthermore, collective names (CSx resp. AFxx) are possible.

Examples:

- **%Lcds0 @dAFxx %A**: Accept (secured transmission) on DiffServ “AF”, limit “0”
- **%Qcds32 @dEF**: Minimum bandwidth for DiffServ “EF” of 32 kbps
- **%Fprw256 @dEF**: PMTU reduction for reception for DiffServ “EF” to 256 bytes

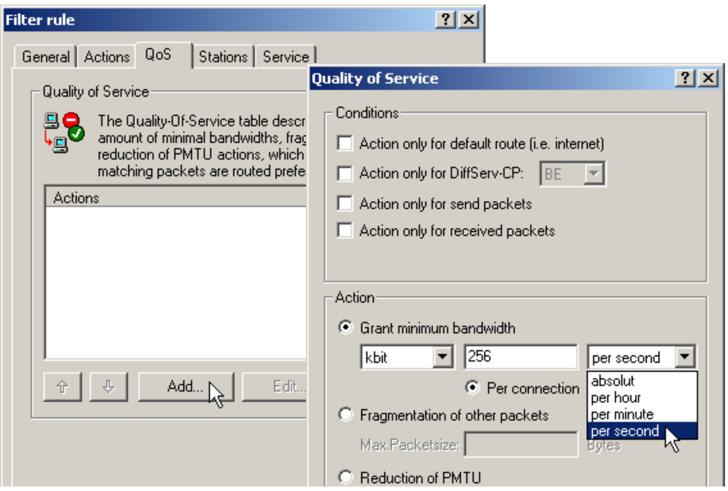
These examples reserve a desired bandwidth for Voice over IP phone calls. The first element “%Lcds0 @dAFxx %A” accepts DSCP “AFxx” marked packets of signalling calls. Voice data marked with “EF” is transferred preferentially by the entry “%Qcds32 @dEF”, and a bandwidth of 32 Kbps is guaranteed thereby as well. In parallel, the PMTU is reduced to 256 byte by “%Fprw256 @dEF”, which enables ensuring the required bandwidth in receiving direction at all.

ⓘ Further information about defining Firewall rules can be found in chapter ’Firewall’ → page 8-1.

9.7.2 Defining minimum and maximum bandwidths

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'.



Filter rule

General | Actions | QoS | Stations | Service

Quality of Service

The Quality-Of-Service table descr
amount of minimal bandwidths, frag
reduction of PMTU actions, which
matching packets are routed prefe

Actions

⇧ ⇩ Add... Edit...

Quality of Service

Conditions

□ Action only for default route (i.e. internet)

□ Action only for DiffServ-CP: BE

□ Action only for send packets

□ Action only for received packets

Action

● Grant minimum bandwidth

kbit | 256 | per second

● Per connection

absolut
per hour
per minute
per second

○ Fragmentation of other packets

Max.Packetsize: Bytes

○ Reduction of PMTU

  - The option 'Action only for default route' limits the rule to those packets, which are sent or received via default route.
  - The option 'Action only for VPN route' limits the rule to those packets, which are sent or received via VPN tunnel.
  - The option 'Forced' defines a static reservation of bandwidth. Bandwidth reserved in this way cannot be used for any other connections, even while the preferred connection is inactive.
  - The option 'Per connection' resp. 'Globally' specifies, whether the minimum bandwidth set here is valid for each single connection corresponding to this rule (’per connection’), or, if this should be the upper limit for the sum of all connections together (’globally’).
- Like for other Firewall rules, index cards 'Stations' and 'Services' determine for which stations in the LAN / WAN and for which protocols this rule applies.

LANconfig: Firewall/QoS ▶ Rules ▶ Filter rules ▶ Quality of Service

WEBconfig: Setup ▶ IP router ▶ Firewall ▶ Rule list

A required minimum bandwidth is introduced by “%Q”. Here it is implicitly assumed that the respective rule is an “Accept” action, and that the packets will thus be transmitted.

A maximum bandwidth is simply defined by a limit rule, which discards by a “Drop” action all packets, which exceed the defined bandwidth.

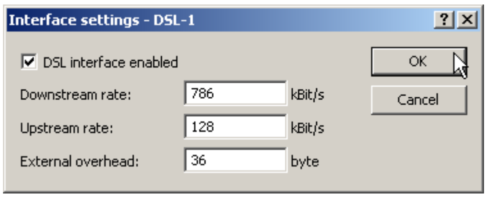
Examples:

- **%Qcds32**: Minimum bandwidth of 32 kbps for each connection
- **%Lgds256 %d**: Maximum bandwidth of 256 kbps for all connections (globally)

Further information about defining Firewall rules can be found in chapter 'Firewall' → page 8-1.

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.


Interface settings - DSL-1

☑ DSL interface enabled

Downstream rate: 786 kBit/s

Upstream rate: 128 kBit/s

External overhead: 36 byte

- An Ethernet WAN (DSL/cable) interface can be switched off completely in this dialogue.
- As upstream and downstream rate the gross data rates are entered, which are usually a little bit higher than the net data rates indicated by the provider as the guaranteed data rate (see also 'The queue concept' → page 9-3).
- 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:

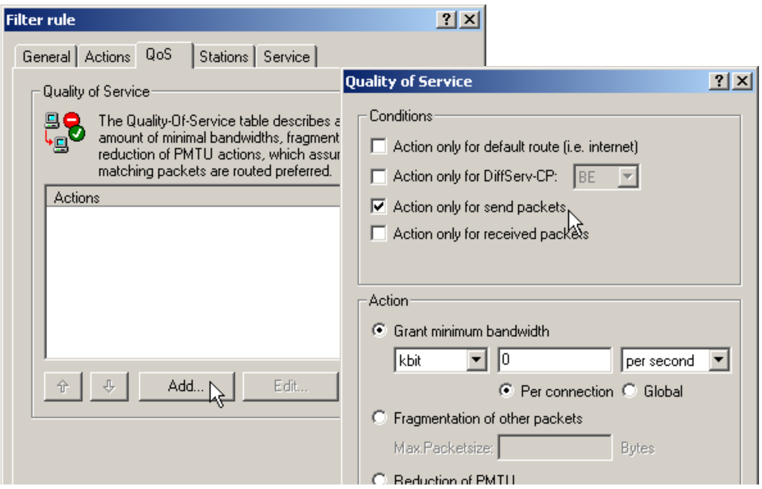
Transfer	External overhead	Note
PPPoEoA	36 bytes	additional headers, loss by not completely used ATM cells
PPTP	24 bytes	additional headers, loss by not completely used ATM cells
IPoA (LLC)	22 bytes	additional headers, loss by not completely used ATM cells
IPoA (VC-MUX)	18 bytes	additional headers, loss by not completely used ATM cells
Cable modem	0	direct transfer of Ethernet packets

LANconfig: Interfaces ▶ WAN

WEBconfig: 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


Filter rule

Quality of Service

The Quality-Of-Service table describes a amount of minimal bandwidths, fragment reduction of PMTU actions, which assur matching packets are routed preferred.

Quality of Service

Conditions

☐ Action only for default route (i.e. internet)

☐ Action only for DiffServ-CP: BE

☑ Action only for send packets

☐ Action only for received packets

Action

● Grant minimum bandwidth

kbit 0 per second

● Per connection ○ Global

○ Fragmentation of other packets

Max.Packetsize: Bytes

○ Reduction of PMTU

For configuration with WEBconfig or Telnet, the interpretation of the data transfer direction is specified in a new Firewall rule by parameters "R" for receive, "T" for transmit (send) and "W" for reference to the WAN interface:

LANconfig: Firewall/QoS ▶ Rules ▶ Filter rules ▶ Quality of Service

WEBconfig: Setup ▶ IP router ▶ Firewall ▶ Rule list

A restriction of data transfer to 16 Kbps in sending direction applying to the physical WAN interface is e.g. made by the following Firewall rule:

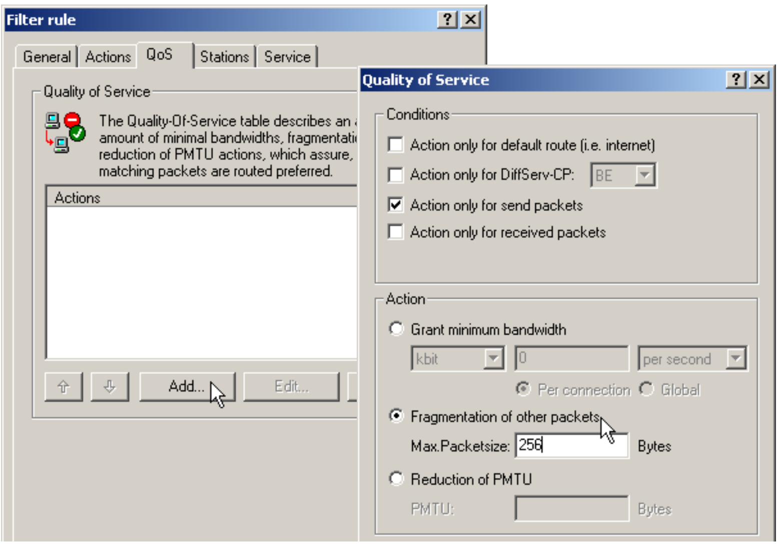
- %Lcdstw16%d

9.7.5 Reducing the packet length

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

- The reduction refers to **all** packets, which will be sent to the interface and which do **not** correspond to the rule.
- Not packets of certain protocols are reduced, rather than all packets globally on that interface

> For LANCOM devices with VoIP functions that were already integrated or added in with a software option, fragmentation and PMTU reduction can be set separately for SIP calls.



Filter rule

General | Actions | QoS | Stations | Service

Quality of Service

The Quality-Of-Service table describes an amount of minimal bandwidths, fragmentati reduction of PMTU actions, which assure, matching packets are routed preferred.

Actions

Quality of Service

Conditions

☐ Action only for default route (i.e. internet)

☐ Action only for DiffServ-CP: BE

☑ Action only for send packets

☐ Action only for received packets

Action

○ Grant minimum bandwidth

kbit | 0 | per second

● Per connection ○ Global

● Fragmentation of other packets

Max.Packetsize: 256 Bytes

○ Reduction of PMTU

PMTU: Bytes

For configuration with WEBconfig or Telnet, the reduction is entered in a new Firewall rule by parameter “P” for PMTU reduction (Path MTU, MTU = Maximum Transmission Unit) and “F” for the fragment size.

LANconfig: Firewall/QoS ▶ Rules ▶ Filter rules ▶ Quality of Service

WEBconfig: Setup ▶ IP router ▶ Firewall ▶ Rule list

> PMTU reduction and fragmentation refer always to the physical connection. Indicating parameter “W” for WAN sending direction is not required here and hence will be ignored if existing.

The following example shows a setting for Voice over IP telephony:

Rule	Source	Destination	Action	Protocol
VOIP	IP addresses of IP telephones in the LAN, all ports	IP addresses of IP telephones in the LAN, all ports	%Qcds32 %Prt256	UDP

This rule defines the minimum bandwidth for sending and receiving to 32 Kbps, forces and reduces the PMTU while sending and receiving to packets of 256 byte size. For the TCP connection, the maximum segment size of the local workstation is determined to 216, so that the server will send packets of maximum 256 byte (reduction of the PMTU in sending and receiving direction).

9.8 QoS for WLANs according to IEEE 802.11e (WMM/WME)

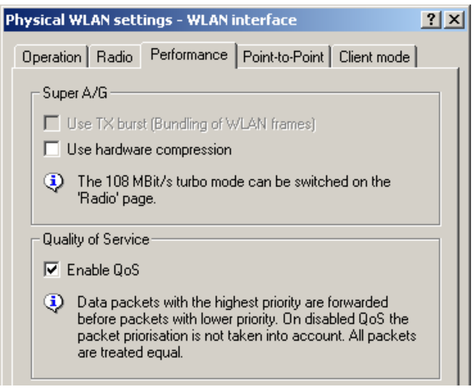
With the extension to the 802.11 standard, 802.11e, Quality of Service can be provided for transfers via WLAN. Among others, 802.11e supports the prioritization of certain data-packet types. This extension is an important basis for the use of voice applications in WLANs (Voice over WLAN, VoWLAN).

The WiFi alliance certifies products that support Quality of Service according to 802.11e, and refer to WMM (WiFi Multimedia, formerly known as WME or Wireless Multimedia Extension). WMM defines four categories (voice, video, best effort and background) which make up separate queues to be used for prioritization.

The 802.11e standard sets priorities by referring to the VLAN tags or, in the absence of these, by the DiffServ fields of IP packets. Delay times (jitter) are kept below 2 milliseconds, a magnitude which is inaudible to the human ear. 802.11e controls access to the transfer medium with EDCF, the Enhanced Distributed Coordination Function.

Priorities can only be set if the WLAN client and the access point both support 802.11e or WMM, and also if the applications are able to mark the data packets with the corresponding priorities.

A LANCOM access point can activate 802.11e for each of its physical WLAN networks separately.



Physical WLAN settings - WLAN interface

Operation | Radio | Performance | Point-to-Point | Client mode

Super A/G

□ Use TX burst (Bundling of WLAN frames)

□ Use hardware compression

The 108 MBit/s turbo mode can be switched on the 'Radio' page.

Quality of Service

☑ Enable QoS

Data packets with the highest priority are forwarded before packets with lower priority. On disabled QoS the packet priorisation is not taken into account. All packets are treated equal.

LANconfig: Interfaces ▶ Wireless LAN ▶ Physical WLAN settings ▶ Performance

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ Performance

LANCOM reference manual part 3

- Virtual Private Networks - VPN

Version: LCOS 7.6 with addendum 7.7 (see appendix)
(last update August 2009)

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

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

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen
Deutschland

www.lancom.de

Würselen, August 2009

110650/0809

Contents

10 Virtual Private Networks—VPN

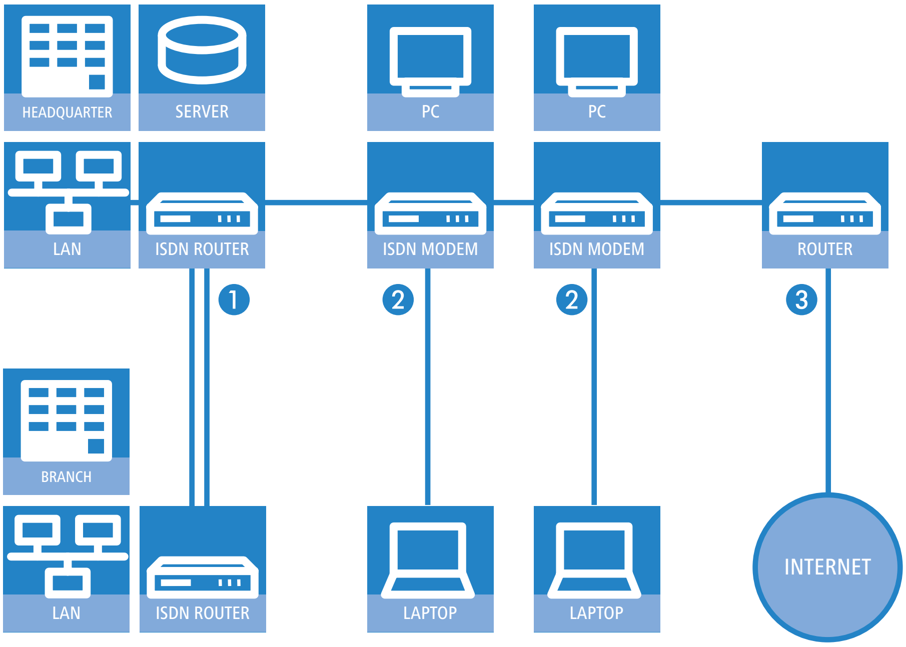
10.1 What does VPN offer?

A VPN (**V**irtual **P**rivate **N**etwork can be used to set up cost-effective, public IP networks, for example via the Internet.

While this may sound unspectacular at first, in practice it has profound effects. To illustrate this, let's first look at a typical corporate network without VPN technology. In the second step, we will see how this network can be optimized by the deployment of VPN.

Conventional network infrastructure

First, let's have a look at a typical network structure that can be found in this form or similar forms in many companies:



Computers using remote access, e.g. home working

The corporate network is based on the internal network (LAN) in the headquarters. This LAN is connected to the outside world in three ways:

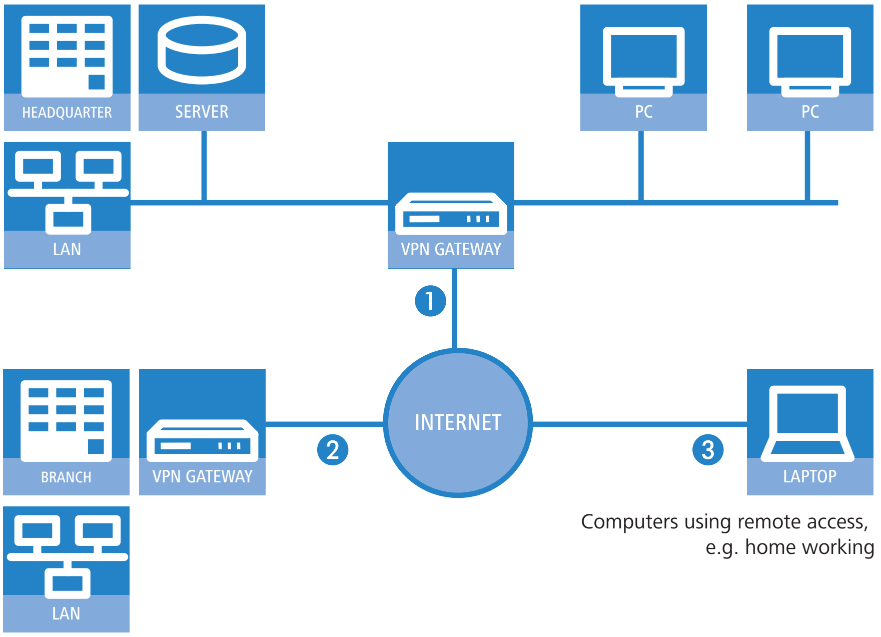
1. A subsidiary is connected to the LAN, typically using a leased line.
2. PCs dial into the central network via modem or ISDN connections (Remote Access Service – RAS).
3. The central LAN has a connection to the Internet so that its users can access the Web, and send and receive e-mail.

All connections to the outside world are based on dedicated lines, i. e. switched or leased lines. Dedicated lines are very reliable and secure. On the other hand, they involve high costs. In general, the costs for dedicated lines are dependent on the distance. Especially in the case of long-distance connections, keeping an eye out of cost-effective alternatives can be worthwhile.

The appropriate hardware must be available in the headquarters for every type of required connection (analog dial-up, ISDN, leased lines). In addition to the original investment costs, ongoing costs are also incurred for the administration and maintenance of this equipment.

Networking via the Internet

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



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

1. All that is required is the Internet connection of the LAN in the headquarters. Special switching devices or routers for dedicated lines to individual participants are superfluous.

2. The subsidiary also has its own connection to the Internet.

3. The RAS PCs connect to the headquarters LAN via the Internet.

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

The physical connection no longer exists directly between two participants; instead, the participants rely on their connection to the Internet. The access technology used is not relevant in this case: ideal is the use of broadband technologies such as DSL (Digital Subscriber Line) in combination with flatrate contracts. But also a conventional ISDN line can be used.

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

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

Two technical properties of the IP standard speak against using the Internet as a part of a corporate network, however:

- The necessity of public IP addresses for all participants
- The lack of data security of unprotected data transfers

10.1.1 Private IP addresses on the Internet?

The IP standard defines two types of IP addresses: public and private. A public IP address is valid worldwide, while a private IP address only applies within a closed LAN.

Public IP addresses must be unique on a worldwide basis. Private IP addresses can occur any number of times worldwide; they must only be unique within their own closed network.

Normally, PCs in a LAN only have private IP addresses, while the router to the Internet also has a public address. All PCs behind this router have access to the Internet via its public IP address (IP masquerading). In such a case, only the router itself is responsive via the Internet. PCs behind the router are not responsive to the Internet without intervention by the router.

Routing at the IP level with VPN

IP connections must be established between routers with public IP addresses in order to link networks via the Internet. These routers provide the connections between multiple subnetworks. When a computer sends a packet to a private IP address in a remote network segment, the local router forwards the packet to the router of the remote network segment via the Internet.

The VPN gateway handles the conversion between private and public IP addresses. Without VPN, computers without public IP addresses would not be able to communicate with one another via the Internet.

10.1.2 Secure communications via the Internet?

The idea of using the Internet for corporate communications has been met with skepticism. The reason for this is that the Internet lies beyond a company's field of influence. Unlike dedicated connections, data on the Internet travels through the network structures of third parties that are frequently unknown to the company.

In addition, the Internet is based on a simple form of data transfer using unencrypted data packets. Third parties can monitor and perhaps even manipulate the contents of these packets. Anyone can access the Internet. As a result, third parties may gain unauthorized access to the transferred data.

VPN – Security through encryption

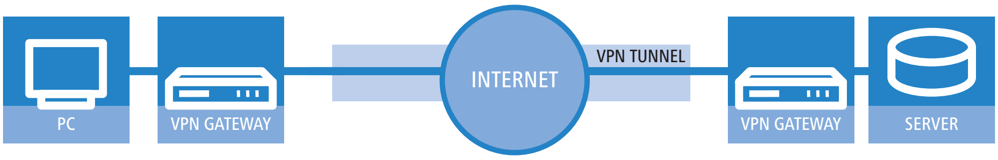
VPN was developed as a solution to this security problem. If necessary, it can encrypt the complete data communications between two participants. The packets are then unreadable for third parties.

The latest and most secure encryption technologies can be used for VPN. A very high level of security can thus be reached. VPN-protected data traffic via the Internet offers a degree of security that at least corresponds to that of dedicated lines.

Codes usually referred to as "keys" are agreed upon between the participants and used for data encryption. Only the participants in the VPN know these keys. Without a valid key, it is not possible to decrypt the data. They thus remain "private", inaccessible to unauthorized parties.

Send your data through the tunnel – for security’s sake

This also explains the nature of a virtual private network: A fixed, physical connection between the devices of the type required for a direct connection does not exist at any time. Rather, the data flows via suitable routes through the Internet. With the proper technology, third parties can monitor and even record data traffic. As the packets are encrypted by VPN, the actual content of the packets is inaccessible. Experts compare this state to a tunnel: it's open at either end, but perfectly shielded in between. Secure connections within public IP networks are thus also referred to as "tunnels".

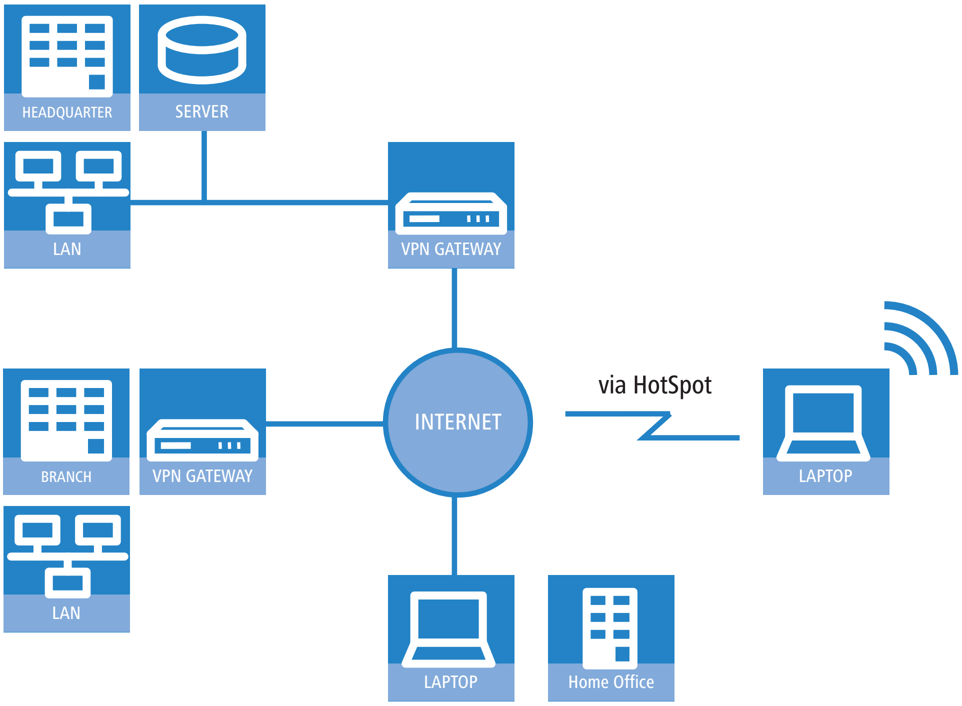


The goal of modern network structures has thus been achieved: secure connections via the largest and most low-cost public IP network: the Internet.

10.2 LANCOM VPN: an overview

10.2.1 VPN example application

VPN connections are used in many different fields of application. In most cases, a variety of communications technologies is used for transferring both data and audio, and VPN unites these systems into an integrated network. The following example illustrates a typical application that is often used in practice.



The principal components and features of these applications:

- The coupling of networks, for example between headquarters and a branch office
- Connecting external locations without fixed IP addresses via VPN router
- Connecting home offices without fixed IPs via ISDN or analog modems
- Connecting to Voice-over-IP telephone exchanges
- Connecting mobile users, for example when using public WLAN access

10.2.2 LANCOM VPN functions

This section lists all of the functions and properties of LANCOM VPN. This overview will provide a great deal of information for VPN experts. It is very compact, but contains a lot of complex, specialized terminology. Knowledge of the technical basics of VPN are required to understand this section. Don't worry: it's no problem if you skip this section. The information contained here is not required to set up and use LANCOM VPN.

- VPN in accordance with IPSec standard
- VPN tunnel via leased lines, switched connections and IP networks
- IPSec main and aggressive mode
- LANCOM Dynamic VPN: Public IP addresses can be static or dynamic (initiation of a connection towards remote sites with dynamic IP addresses requires ISDN)
- IPSec protocols AH, ESP and IPCOMP in transport and tunnel mode
- Hash algorithms:
  - HMAC-MD5-96, Hash length 128 bit
  - HMAC-SHA-1-96, Hash length 160 bit
- Symmetrical encryption methods
  - AES, key length 128, 192 and 256 bit
  - Triple-DES, key length 168 bit
  - Blowfish, key length 128 - 448 bit
  - CAST, key length 128 bit
  - DES, key length 56 bit
- IKE Config Mode
- IKE key exchange with Preshared Keys
- IKE with RSA signature and digital certificates (X.509)
- Key exchange via Oakley, Diffie-Hellman algorithm with key lengths 768 bit, 1024 bit or 1536 bit, well-known groups 1, 2 and 5
- Key management in accordance with ISAKMP

- Apart from conventional IPSec implementations, LANCOM devices offer extended functionality, such as the LANCOM Dynamic VPN that allows the use of the high-security IKE Main Mode even with dynamic IP addresses.
- In combination with the LANCOM Advanced VPN Client, a separate pre-shared key can be used for each connection even when using IKE Aggressive Mode connections.

10.3 VPN connections in detail

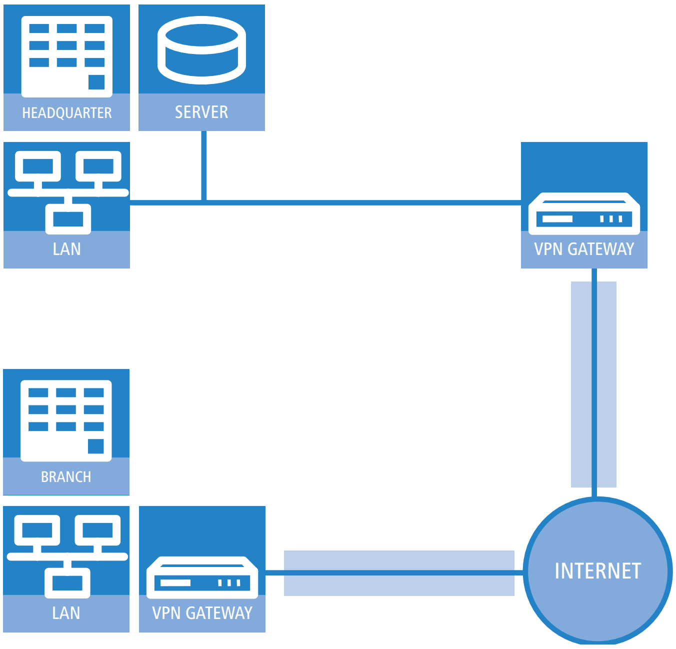
Two types of VPN connections are available:

- VPN connections linking two local networks. This type of connection is also known as a "LAN-LAN coupling".
- The connection of an individual computer with a network, generally via a dial-in connection (Remote Access Service – RAS).

10.3.1 LAN-LAN coupling

The coupling of two remote networks is known as a LAN-LAN coupling. With such a connection, the devices in one LAN can access those of the remote LAN (assuming they have the necessary access rights).

In practice, LAN-LAN couplings are frequently used between company headquarters and subsidiaries, or for connections to partner companies.



A VPN-enabled router (VPN gateway) is located at either end of the tunnel. The configuration of both VPN gateways must be matched to one another.

The connections are transparent for the remaining devices in the local networks, i.e., they appear to have a direct connection. Only the two gateways must be configured for the VPN connection.

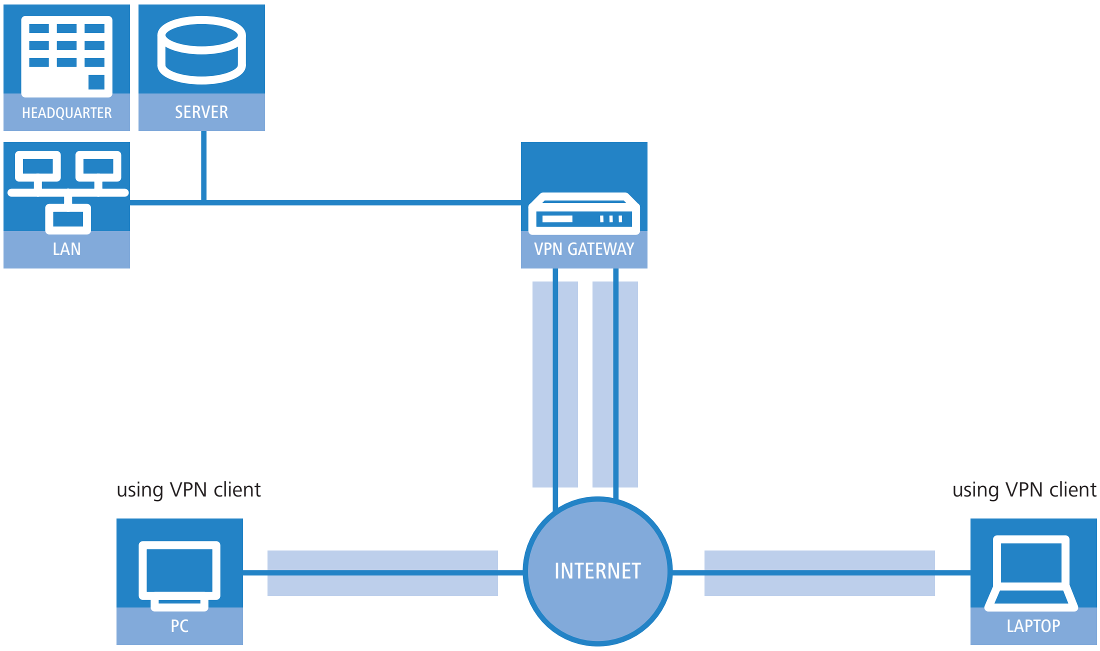
Internet access in parallel

The Internet access for VPN can be used simultaneously for other Internet applications, such as web-browsing or e-mail. For security reasons, the parallel Internet access may be unwanted in some cases. For instance, if a branch office should be enforced to access the Internet only via a central firewall. For such applications the parallel Internet access can be disabled as well.

10.3.2 Dial-in connections (Remote Access Service)

Individual remote computers (hosts) can access the resources of the LAN via dial-up connections. Practical examples of this are employees working from home or field staff that dial into the company network.

If the dial-up connection of an individual computer to a LAN is to be realized via VPN, that computer first connects to the Internet. A special VPN client software then sets up a tunnel to the VPN gateway of the LAN using this Internet connection.



The VPN gateway of the LAN must support the establishment of VPN tunnels with the VPN client software of the remote PC.

10.4 What is LANCOM Dynamic VPN?

LANCOM Dynamic VPN is a LANCOM Systems technology which permits VPN tunnels to be connected **to** remote stations that do not have a static, but only a dynamic IP address.

Who needs LANCOM Dynamic VPN and how does it work? We will answer this question in two steps: First, a look at the basics of IP addressing will show the problem of static IP addresses. The second step shows the solution thereof with LANCOM Dynamic VPN.

10.4.1 A look at IP addressing

Every participant on the Internet needs an IP address. Participants even need a special kind of IP address - a public one. The administration of public IP addresses is handled from central locations in the Internet. Each public IP address may only occur once on the entire Internet.

Local IP-based networks do not use public, but private IP addresses. For this reason, a number of address ranges within the entire IP address range have been reserved for private IP addresses.

A computer connected to both a local network and directly to the Internet therefore has two IP addresses: a public one for communication with the rest of the Internet and a private one by which the computer can be reached within the local network.

Static and dynamic IP addresses

Public IP addresses must be applied for and managed, which involves costs. There is also only a limited number of public IP addresses. For this reason, not every Internet user has his or her own fixed (static) IP address.

The alternative to static IP addresses are the so-called dynamic IP addresses. A dynamic IP address is assigned to an Internet user by the Internet Service Provider (ISP) upon dialling-in, and remains valid for the duration of the connection. The ISP takes an unused address selected at random from their pool of IP addresses. This IP address is only temporarily assigned to the user for the duration of a given connection. When the connection is ended, the IP address is once again free and the ISP can assign it to another user.

Many flatrate connections, too, are realised with via dynamic IP addresses. Every 24 hours or so, the connection is forcibly interrupted. The new connection is generally assigned with a new and different IP address.

Advantages and disadvantages of dynamic IP addresses

This process has a very important advantage for ISPs: they only need relatively small pools of IP addresses. Dynamic IP addresses are also favorable for users: it's not necessary for them to apply for static IP addresses in advance - they can connect to the Internet immediately. It's also not necessary for them to manage IP addresses. This saves trouble and costs. The other side of the coin: A user without a static IP address cannot be addressed directly from the Internet.

This is a major problem when setting up VPNs. If, for example, Computer A would like to communicate with Computer B using a VPN tunnel on the Internet, Computer A needs the remote computer's IP address. If B only has a dynamic address, A cannot know that address and therefore cannot contact B.

The LANCOM Dynamic VPN offers the answer here.

10.4.2 This is how LANCOM Dynamic VPN works

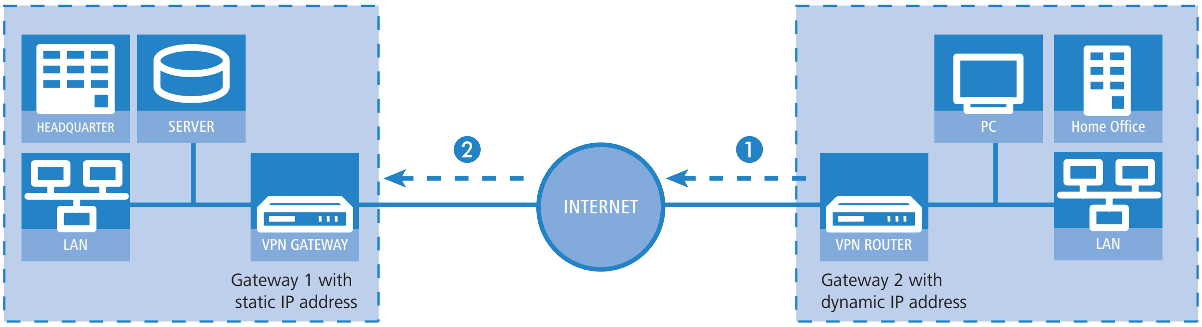
Let's use two examples to explain how LANCOM Dynamic VPN works (designations refer to the IP addressing type of the two VPN gateways):

- dynamic – static
- static – dynamic
- dynamic – dynamic

Dynamic – static

If a user on computer B in LAN 2 wishes to connect to computer A in LAN 1, then gateway 2 receives a request and tries to establish a VPN tunnel to gateway 1. Gateway 1 has a static IP address and can be directly contacted over the Internet.

A problem arises in that the IP address from gateway 2 is assigned dynamically, and gateway 2 must communicate its current IP address to gateway 1 when attempting to connect. In this case, LANCOM Dynamic VPN takes care of transmitting the IP address during connection establishment.



① Gateway 2 connects to the Internet and is assigned a dynamic IP address.

② Gateway 2 contacts Gateway 1 via its known public IP address. LANCOM Dynamic VPN enables the identification and transmission of the actual IP address of Gateway 2. Gateway 1 initiates the VPN tunnel then.

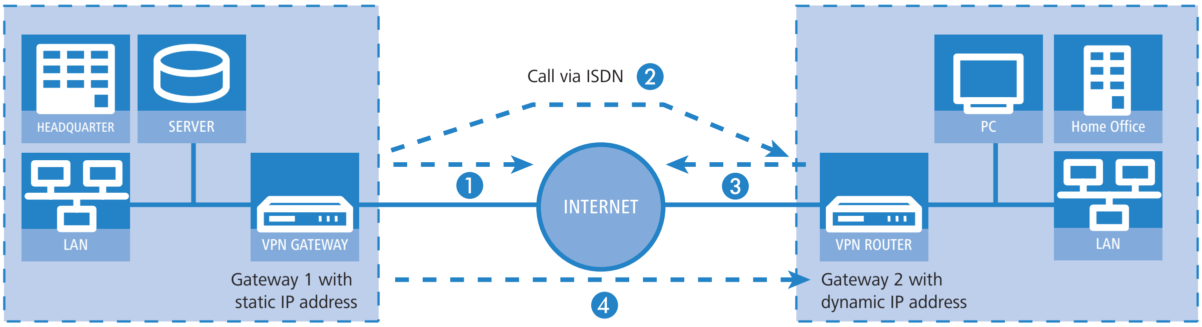
The great advantage of LANCOM devices with this application: Instead of the “Aggressive Mode” that is normally used when connecting VPN clients to the headquarters, the far more secure “Main Mode” can be applied. Although with Main Mode more unencrypted messages can be exchanged during the IKE handshake, the method is overall more secure than Aggressive Mode.

An ISDN line is not necessary for establishing this type of connection. The dynamic end communicates its IP address encrypted via the Internet protocol ICMP (or alternatively via UDP).

Static – dynamic

If, on the other hand, computer A in LAN 1 requires a connection to computer B in LAN 2, for example when headquarters carries out remote maintenance at the external locations, then gateway 1 receives the request and attempts to establish a VPN tunnel to gateway 2. Gateway 2 only has a dynamic IP address and cannot be directly contacted over the Internet.

With LANCOM Dynamic VPN, the VPN tunnel can be set up nevertheless. The connection is established in three steps:



① Gateway 1 calls Gateway 2 via ISDN. It takes advantage of the ISDN functionality of sending its own subscriber number via the D-channel free of charge. Gateway 2 determines the IP address of Gateway 1 from the preconfigured VPN remote stations using the received subscriber number.

If Gateway 2 does not receive a subscriber number via the D-channel (if that particular ISDN service feature is not available, for example) or an unknown number is transferred, the authentication will be performed via the B-channel. Once the negotiation was successful, Gateway 1 sends its IP address and closes the connection on the B-channel immediately.

② Now its Gateway 2's turn: It first connects to its ISP and is assigned a dynamic IP address.

③ Gateway 2 authenticates itself at Gateway 1. The static IP address of gateway 1 is known, of course.

④ Gateway 1 now knows the address of Gateway 2 and sets up the VPN tunnel to Gateway 2.

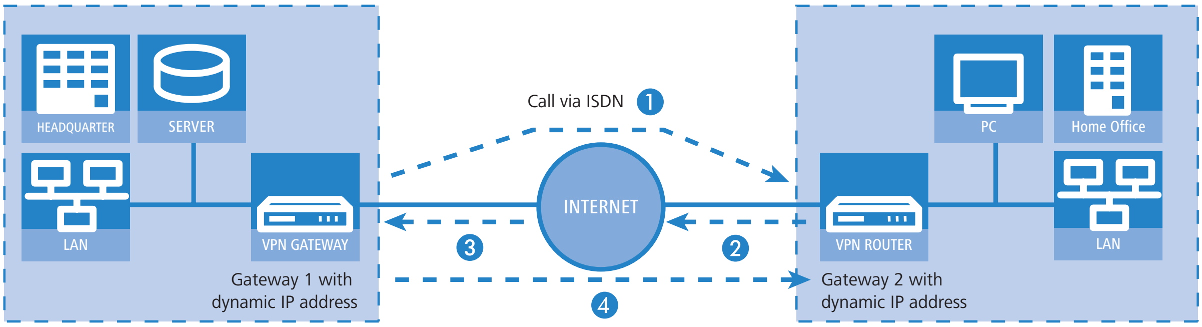
The advantage of LANCOM devices, for example when connecting from the headquarters to branch offices: The functions in LANCOM Dynamic VPN also allows access to networks without a flatrate, i.e. networks that are not always online. The ISDN connection and an associated MSN act to substitute the another address, such as a static IP address or the dynamic address translation via dynamic DNS services, a solution often used with flatrate connections.

ⓘ The described connection set up requires an ISDN connection for both VPN gateways. But usually no charges will arise for this procedure.

ⓘ Please note 'Information to the Dynamic VPN registration' → page 10-10.

Dynamic – dynamic

With LANCOM Dynamic VPN, VPN tunnels can also be set up between two gateways that both only have dynamic IP addresses. Let's modify the previous example so that in this case Gateway 1 also has a dynamic IP address. Once again, Computer A would like to connect to Computer B:



① Gateway 1 connects to its ISP and is assigned a public, dynamic IP address.

② It then calls Gateway 2 via ISDN to send this dynamic address. Three procedures are used to send the address:

- □ **As information in the LLC element of the D-channel.** In the D-channel protocol of Euro-ISDN (DSS-1), the so-called LLC (**L**ower **L**ayer **C**ompatibility) element can be used to send additional information to the remote station. This transfer takes place before the B-channel connection is established. Once the address has been sent successfully, the remote station rejects the call. Charges are thus not incurred for a B-channel connection. The IP address is sent nevertheless for free in this case.

The LLC element is generally available as a standard feature in Euro-ISDN that does not require registration or activation. It may be disabled by telephone companies or individual exchanges, however. The LLC element is not available in 1TR6, the German national ISDN. The procedure described above thus will not work with 1TR6.

- □ **As a subaddress via the D-channel.** If it is not possible to send the address via the LLC element, Gateway 1 will attempt to send the address as a so-called subaddress. Like the LLC element, the subaddress is an information element of the D-channel protocol that permits short items of information to be sent free of charge. In this case, the telephone company must enable the 'subaddressing' feature first; this is generally subject to a charge. As with the LLC element, the call is rejected by the remote station once the IP address has been transferred successfully. The connection thus remains free of charge.
- □ **Via the B-channel.** If both attempts to send the IP address via the D-channel fail, then a conventional connection via the B-channel must be established to send the IP address. The connection is dropped immediately after the IP address has been sent. This connection is subject to the usual charges.

③ Gateway 2 connects to the ISP and receives a dynamic IP address.

④ Gateway 2 authenticates itself at Gateway 1. The static IP address of gateway 1 is known, of course.

⑤ Gateway 1 now knows the address of Gateway 2 and sets up the VPN tunnel to Gateway 2.

Dynamic VPN works only between LANCOM that each feature at least one ISDN port that can be used for the ISDN connection.

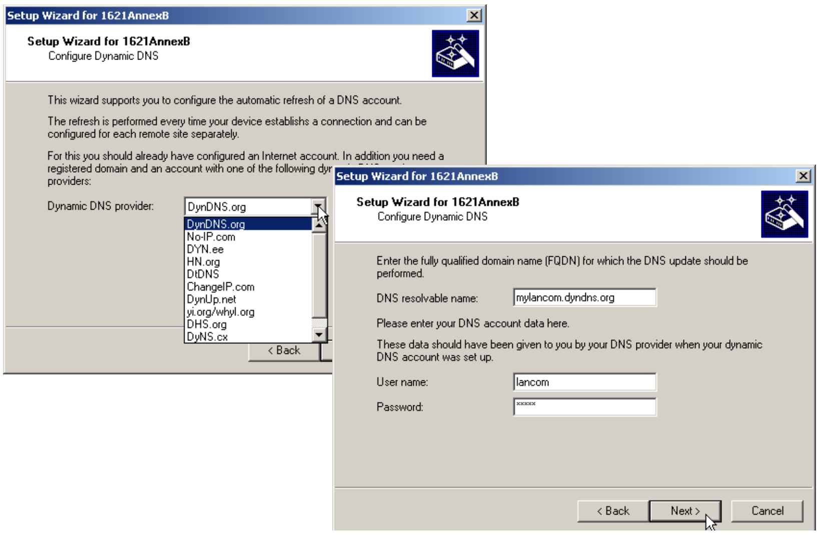
Please note 'Information to the Dynamic VPN registration' → page 10-10..

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):



Setup Wizard for 1621AnnexB

Setup Wizard for 1621AnnexB
Configure Dynamic DNS

This wizard supports you to configure the automatic refresh of a DNS account.

The refresh is performed every time your device establishs a connection and can be configured for each remote site separately.

For this you should already have configured an Internet account. In addition you need a registered domain and an account with one of the following dyr
providers:

Dynamic DNS provider: DynDNS.org

DynDNS.org
No-IP.com
DYN.ee
HN.org
DtDNS
ChangeIP.com
DynUp.net
yi.org/whyl.org
DHS.org
DyNS.cx

Setup Wizard for 1621AnnexB

Setup Wizard for 1621AnnexB
Configure Dynamic DNS

Enter the fully qualified domain name (FQDN) for which the DNS update should be performed.

DNS resolvable name: mylancom.dyndns.org

Please enter your DNS account data here.

These data should have been given to you by your DNS provider when your dynamic DNS account was set up.

User name: lancom

Password: *****

For reasons of security and availability, LANCOM Systems recommends the use of Dynamic VPN in preference to dynamic DNS-based VPN solutions. Dynamic VPN is based on direct connections via the ISDN network and ensures a higher degree of availability than dynamic DNS services in the Internet.

10.4.3 Information to the Dynamic VPN registration

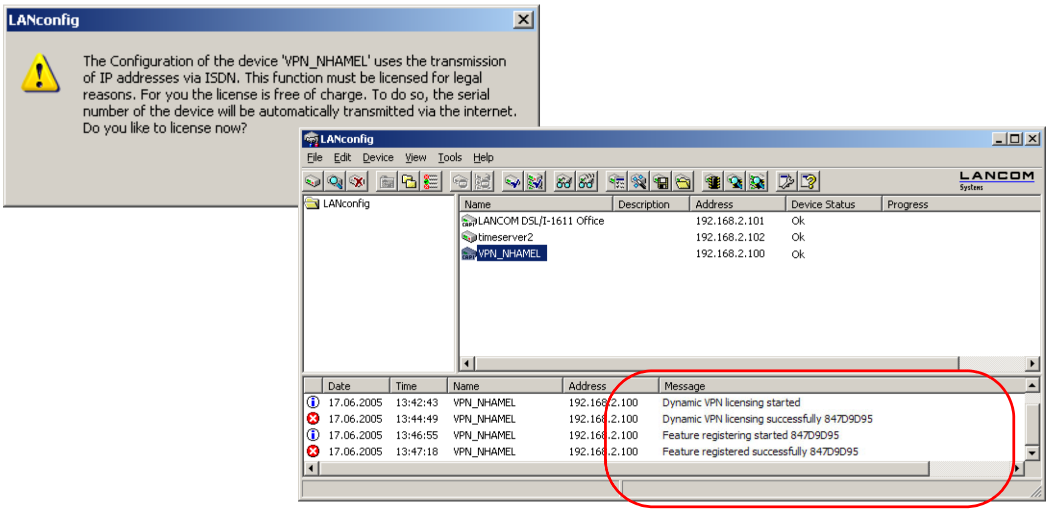
When using dynamic VPN with IP address transmission over ISDN you must activate this feature. This operating mode is usually then required, when you configure a VPN tunnel with dynamic IP addresses on both sides without dynamic DNS services. All other operation modes of dynamic VPN (for transmitting the IP address by ICMP, to provoke a callback etc.) do **not** require a registration.

The registration is anonymous, i.e. no personal or firm data is transmitted.

The registration of the dynamic VPN option requires administrator rights.

Registration with LANconfig

When scanning the device for instance right after the program start LANconfig automatically recognizes if the device must be activated. After confirming the arising hint the LANconfig automatically transmits the required data of the device to the registration server of LANCOM Systems. The release code ist automatically transmitted back to the device and activated. The state of this procedure is visible in LANconfig.



LANconfig

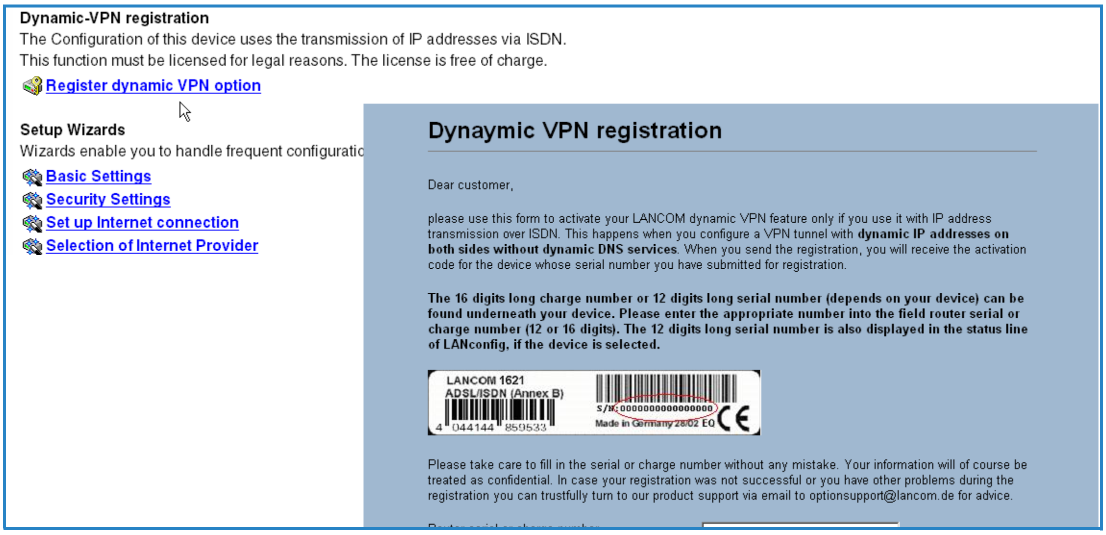
The Configuration of the device 'VPN_NHAMEL' uses the transmission of IP addresses via ISDN. This function must be licensed for legal reasons. For you the license is free of charge. To do so, the serial number of the device will be automatically transmitted via the internet. Do you like to license now?

```
Name                      Description  Address         Device Status  Progress
LANCOM DSL/I-1611 Office               192.168.2.101   Ok
timeserver2                            192.168.2.102   Ok
VPN_NHAMEL                             192.168.2.100   Ok
```

```
Date        Time      Name        Address         Message
17.06.2005  13:42:43  VPN_NHAMEL  192.168.2.100   Dynamic VPN licensing started
17.06.2005  13:44:49  VPN_NHAMEL  192.168.2.100   Dynamic VPN licensing successfully 847D9D95
17.06.2005  13:46:55  VPN_NHAMEL  192.168.2.100   Feature registering started 847D9D95
17.06.2005  13:47:18  VPN_NHAMEL  192.168.2.100   Feature registered successfully 847D9D95
```

Registration with WEBconfig

For the registration with WEBconfig the serial number of the device ist required. You can find this information on the bottom side of your device.



Dynamic-VPN registration

The Configuration of this device uses the transmission of IP addresses via ISDN.
This function must be licensed for legal reasons. The license is free of charge.

Register dynamic VPN option

Setup Wizards

Wizards enable you to handle frequent configuratic

Dynaymic VPN registration

Dear customer,

please use this form to activate your LANCOM dynamic VPN feature only if you use it with IP address transmission over ISDN. This happens when you configure a VPN tunnel with **dynamic IP addresses on both sides without dynamic DNS services**. When you send the registration, you will receive the activation code for the device whose serial number you have submitted for registration.

The 16 digits long charge number or 12 digits long serial number (depends on your device) can be found underneath your device. Please enter the appropriate number into the field router serial or charge number (12 or 16 digits). The 12 digits long serial number is also displayed in the status line of LANconfig, if the device is selected.

Please take care to fill in the serial or charge number without any mistake. Your information will of course be treated as confidential. In case your registration was not successful or you have other problems during the registration you can trustfully turn to our product support via email to optionsupport@lancom.de for advice.

When using WEBconfig you can find a link on the first page which leads you to the registrating server of LANCOM Systems. There you must enter the serial number of your device and your e-mail address. After transmitting the data you receive a release code for the device.

To load this release code into your router, please proceed as follows:

Log on with administrator rights on WEBconfig. Select **Enable Software Option**, which is placed on the entry page. On the following page enter the release code and confirm by clicking on **Apply**.

10.5 Configuration of VPN connections

Three questions are answered in the configuration of VPN connections:

- Between which VPN gateways (remote stations) is the connection established?
- What security parameters are used to secure the VPN tunnel between the two gateways?
- Which networks or computers can intercommunicate via these tunnels?

This section introduces the basic considerations for configuring VPN connections. Considered first of all is the simple connection of two local networks. Special cases such as dialling in to LANs with individual computers (RAS) or the connection of structured networks will be covered subsequently.

10.5.1 VPN tunnel: Connections between VPN gateways

Virtual Private Networks (VPNs) are used to interconnect local networks over the Internet. This involves the routing of the private LAN IP addresses via an Internet connection between two gateways with public IP addresses.

For the secure routing of private IP addresses over the Internet, a VPN connection, also known as a VPN tunnel, is established between the two LANs.

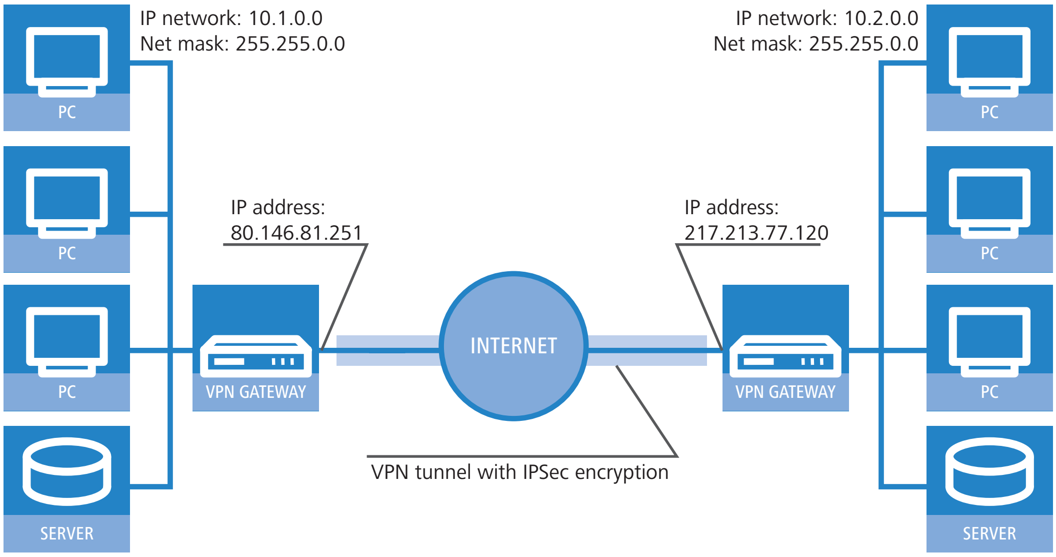
The VPN tunnel has two important tasks:

- To shield the transported data from unauthorized access
- To route private IP addresses via an Internet connection that can normally only be used to route public IP addresses.

The VPN connection between the two gateways is defined by the following parameters:

- The end-points of the tunnel, the VPN gateways, each of which are accessible via public IP addresses (static or dynamic)
- The IP connection between the two gateways
- The private IP address range that are to be routed between the VPN gateways
- Setting relevant to security, such as passwords, IPSec keys etc. to shield the VPN tunnel

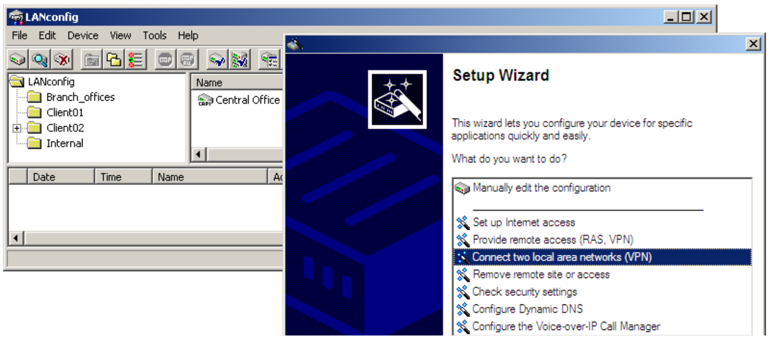
This information is contained in the so-called VPN rules.



10.5.2 Set up VPN connections with the Setup Wizard

If possible, make use of the Setup Wizard within LANconfig to set up VPN connections between local networks. The Wizard guides you through the configuration and makes all the necessary settings for you. Carry out the configuration on both routers, one after the other.

① Choose your device from the selection window in LANconfig and select the **Setup Wizard** button or use the menu bar **Tools** ▶ **Setup Wizard**.


LANconfig
File Edit Device View Tools Help
LANconfig
Branch_offices
Client01
Client02
Internal
Name
Central Office
Date
Time
Name
Setup Wizard
Manually edit the configuration
Set up Internet access
Provide remote access (RAS, VPN)
Connect two local area networks (VPN)
Remove remote site or access
Check security settings
Configure Dynamic DNS
Configure the Voice-over-IP Call Manager

This wizard lets you configure your device for specific applications quickly and easily.

What do you want to do?

② Follow the Wizard's instructions and enter the necessary data. The Wizard will inform you when the required information is complete. You can then close the Wizard with **Finish**.

③ Once you have completed the set-up of both routers, you can start testing the network connection. Try to communicate with a computer in the remote LAN (e.g. with `ping`). The device should automatically connect to the remote station and make contact to the requested computer.

This Wizard automatically sets up the VPN connections essential for typical LAN-LAN coupling. In the following situations, the VPN connections will have to be configured manually:

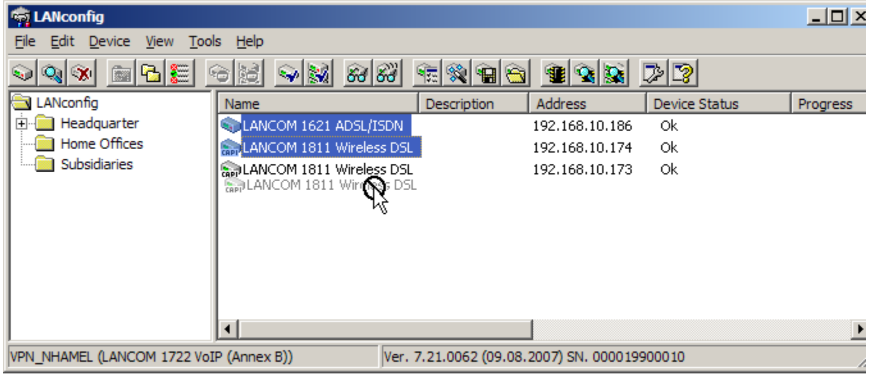
- Where no Windows computer with LANconfig is available. In this case, the necessary parameters are set with WEBconfig or via the Telnet console.
- Where only selected portions of the LAN (intranet) are to communicate with other computers via the VPN connection. This is the case where, for example, the intranet is connected to further subnets with routers, or when only selected portions of the intranet should have access to the VPN connection. In such cases, additional parameters are defined supplementary to those entered in the Setup Wizard.
- Configuring VPN connections to third-party devices.

10.5.3 1-Click-VPN for networks (site-to-site)

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

① In LANconfig, mark the routers at branch offices which are to be coupled to a central router via VPN.

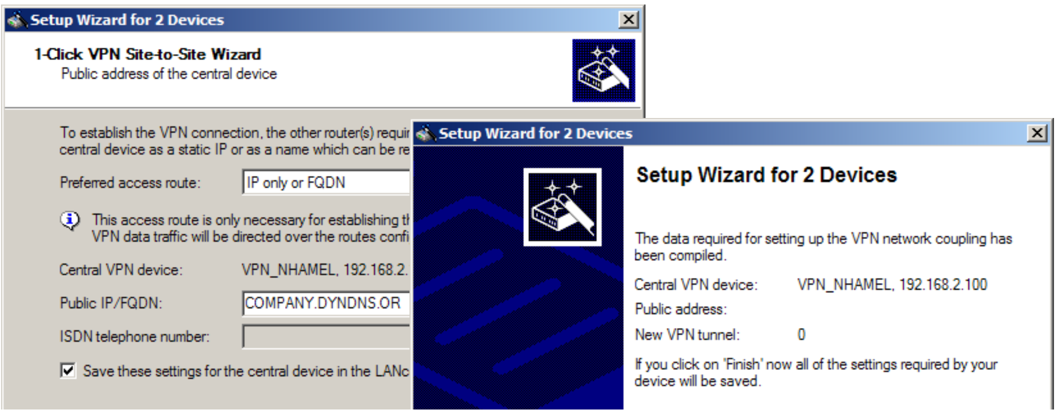
② Use drag&drop by mouse to place the devices onto the entry for the central router.



Name	Description	Address	Device Status	Progress
LANCOM 1621 ADSL/ISDN		192.168.10.186	Ok	
LANCOM 1811 Wireless DSL		192.168.10.174	Ok	
LANCOM 1811 Wireless DSL		192.168.10.173	Ok	

VPN_NHAMEL (LANCOM 1722 VoIP (Annex B)) Ver. 7.21.0062 (09.08.2007) SN. 000019900010

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



Setup Wizard for 2 Devices

1-Click VPN Site-to-Site Wizard
Public address of the central device

To establish the VPN connection, the other router(s) requir
central device as a static IP or as a name which can be re

Preferred access route: IP only or FQDN

This access route is only necessary for establishing th
VPN data traffic will be directed over the routes confi

Central VPN device: VPN_NHAMEL, 192.168.2.

Public IP/FQDN: COMPANY.DYNDNS.OR

ISDN telephone number:

☑ Save these settings for the central device in the LANc

Setup Wizard for 2 Devices

Setup Wizard for 2 Devices

The data required for setting up the VPN network coupling has been compiled.

Central VPN device: VPN_NHAMEL, 192.168.2.100
Public address:
New VPN tunnel: 0

If you click on 'Finish' now all of the settings required by your device will be saved.

④ Select whether connection establishment is to take place via the name or IP address of the central router, or via an ISDN connection. Enter the address or name of the central router, or its ISDN number.

⑤ The final step is to define how the networks are to intercommunicate:

- The INTRANET at headquarters only is to be provided to the branch offices.
- All private networks at the branch offices can also be connected to one another via headquarters.

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

10.5.4 1-Click-VPN for LANCOM Advanced VPN Client

VPN accesses for employees who dial into the network with the LANCOM Advanced VPN Client are very easy to set up with the Setup Wizard and exported to a file. This file can then be imported as a profile by the LANCOM Advanced VPN Client. All of the information about the LANCOM VPN Router's configuration is also included, and then supplemented with randomly generated values (e.g. for the preshared key).

① Use LANconfig to start the 'Set up a RAS Account' wizard and select the 'VPN connection'.

② Activate the options 'LANCOM Advanced VPN Client' and 'Speed up configuration with 1-Click-VPN'.

③ Enter a name for this access and select the address under which the router is accessible from the Internet.

④ In the final step you can select how the access data is to be entered:

- Save profile as an import file for the LANCOM Advanced VPN Client
- Send profile via e-mail
- Print out profile

Sending a profile via e-mail could be a security risk should the e-mail be intercepted en route!

To send the profile via e-mail, the device configuration must be set up with an SMTP account with the necessary access data. Further, the configuration computer requires an e-mail program that is set up as the standard e-mail application and that can be used by other applications to send e-mails.

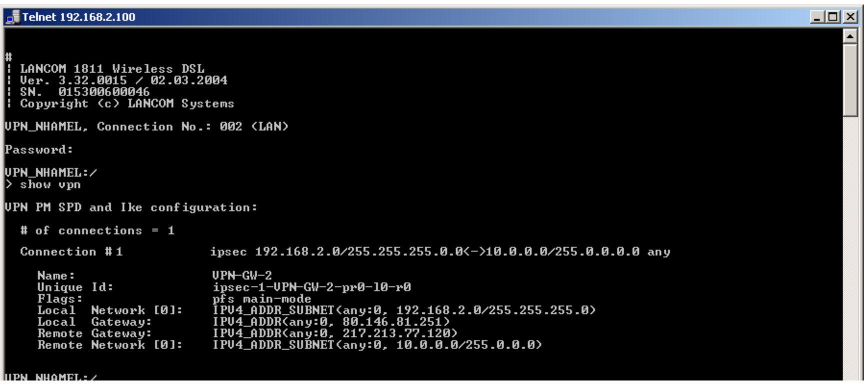
When setting up the VPN access, certain settings are made to optimize operations with the LANCOM Advanced VPN Client, including:

- Gateway: If defined in the LANCOM VPN Router, a DynDNS name is used here, or alternatively the IP address
- FQUN: Combination of the name of the connection, a sequential number and the internal domain in the LANCOM VPN Router.
- Domain: If defined in the LANCOM VPN Router, the internal domain is used here, or alternatively a a DynDNS name or IP address
- VPN IP networks: All IP networks defined in the device as type 'Intranet'.
- Preshared key: Randomly generated key 16 ASCII characters long.
- Connection medium: The LAN is used to establish connections.
- VoIP prioritization: VoIP prioritization is activated as standard.
- Exchange mode: The exchange mode to be used is 'Aggressive Mode'.
- IKE config mode: The IKE config mode is activated, the IP address information for the LANCOM Advanced VPN Client is automatically assigned by the LANCOM VPN Router.

10.5.5 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:



```
#
¦ LANCOM 1811 Wireless DSL
¦ Ver. 3.32.0015 / 02.03.2004
¦ SN.  015300600046
¦ Copyright (c) LANCOM Systems

VPN_NHAMEL, Connection No.: 002 (LAN)

Password:

VPN_NHAMEL:/
> show vpn

VPN PM SPD and Ike configuration:

  # of connections = 1

  Connection #1           ipsec 192.168.2.0/255.255.255.0<->10.0.0.0/255.0.0.0.0 any

    Name:                 VPN-GW-2
    Unique Id:            ipsec-1-VPN-GW-2-pr0-10-r0
    Flags:                pfs 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)

VPN_NHAMEL:/
```

The output informs you of the network relationships that are relevant to VPN connections to other networks.

In this example, the local network at a branch office (network 192.168.2.0, netmask 255.255.255.0) is connected to the network at the headquarters (network 10.0.0.0, netmask 255.255.255.0). The public IP address of the local gateway is 80.146.81.251, and that of the remote VPN gateway is 217.213.77.120.

Entering “any:0” displays the protocols and ports that can be used over the connection.

Further output is displayed by the command “show vpn long”. The information displayed here covers network relationships and also the parameters that are relevant to security, such as IKE and IPSec proposals.

10.5.6 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 28.
- When coupling Windows networks (NetBIOS/IP): Without WINS servers at both ends of the VPN connection (such as when linking a home office), the LANCOM can take over the necessary NetBIOS proxy functions. To this end, the NetBIOS module in the LANCOM must be activated, and the corresponding VPN remote site must be entered into the NetBIOS module as the remote site. Should WINS servers be present in both of the coupled networks, then the NetBIOS module should be deactivated so that the LANCOM does not perform NetBIOS proxy functions.

To use the LANCOM NetBIOX proxy either LANCOM Dynamic VPN must be applied, because it transmits the required addresses, or the IP address of the remote station as a primary NBNS must be entered in the IP parameter list (*LANconfig*: Communication / Protocols).

- When using LANCOM Dynamic VPN: Entry for the corresponding remote site in the PPP list with a suitable password for the Dynamic VPN handshake. The username entered here must correspond with the name entered in the remote device that describes the VPN connection to this local device. Activate "IP routing". If Windows networks are also to be coupled, then the NetBIOS entry should be activated here.

The tunnel endpoints, i.e. the local VPN gateway and each of the VPN remote stations, are entered into the VPN connection list.

Manually configuring the VPN connection involves the following steps:

① Create an entry for the remote VPN gateway in the connection list and enter its public IP address.

② The security parameters for the VPN connection are normally taken from the prepared list, and all that is required here is to define an IKE key.

③ For a Dynamic VPN connection, create a new entry in the PPP list with the name of the remote VPN gateway as the remote station, with the name of the local VPN gateway as the User Name, and set a suitable password. Be sure to activate the IP routing for this PPP connection and, if required, the routing of “NetBIOS over IP” as well. The remaining PPP parameters, such as the procedure for checking the remote station, can be defined in the same way as for other PPP connections.

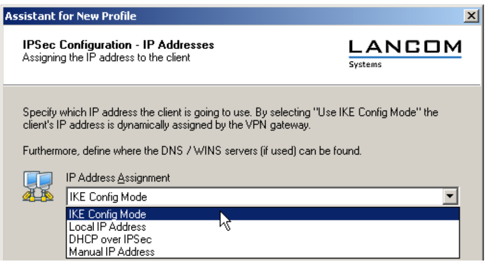
④ The main task in setting up VPN connections is in defining the network relationships. Which IP address ranges at each end of the VPN tunnel should be included in the secured connection?

10.5.7 IKE config mode

When configuring VPN dial-in connections, there is as an alternative to fixed IP addresses for the remote stations that dial in, in that a pool of IP addresses can be made available to them. To this end, the "IKE-CFG" mode is additionally added to the entries in the connection list. This can assume the following values:

- **Server**: With this setting, the device functions as the server for this VPN connection. The assignment of an IP address to the client can take place in two ways:
  - If the remote site is entered in the routing table, the IP address defined here will be assigned to the client.
  - If the remote site is not entered in the routing table, an IP address which is available from the IP pool will be taken for the dial-in connections.

The remote site must be configured as IKE-CFG client in this case, and thus has to request an IP address from the server. To dial in with a LANCOM Advanced VPN Client, the option **Use IKE Config Mode** has to be activated in the connection profile.



Assistant for New Profile

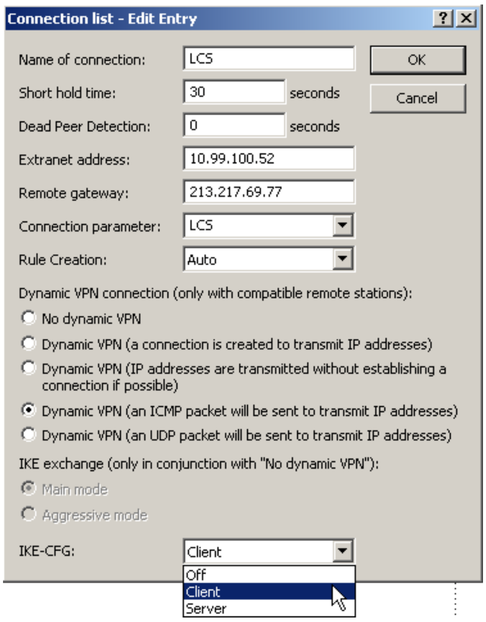
IPSec Configuration - IP Addresses
Assigning the IP address to the client

Specify which IP address the client is going to use. By selecting "Use IKE Config Mode" the client's IP address is dynamically assigned by the VPN gateway.

Furthermore, define where the DNS / WINS servers (if used) can be found.

IP Address Assignment: IKE Config Mode

- **Client**: With this setting, the device functions as the client for this VPN connection and requests an IP address from the remote site (server). The device acts in a similar manner to a VPN client.
- **Off**: If the IKE-CFG mode is switched off, no IP addresses will be assigned for the connection. Fixed IP addresses must be defined for both ends of the connection.



Connection list - Edit Entry

Name of connection: LCS
Short hold time: 30 seconds
Dead Peer Detection: 0 seconds
Extranet address: 10.99.100.52
Remote gateway: 213.217.69.77
Connection parameter: LCS
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

IKE-CFG: Client

LANconfig: VPN ▶ General ▶ Connection list

WEBconfig: LCOS menu tree ▶ Setup ▶ VPN ▶ VPN-Peers

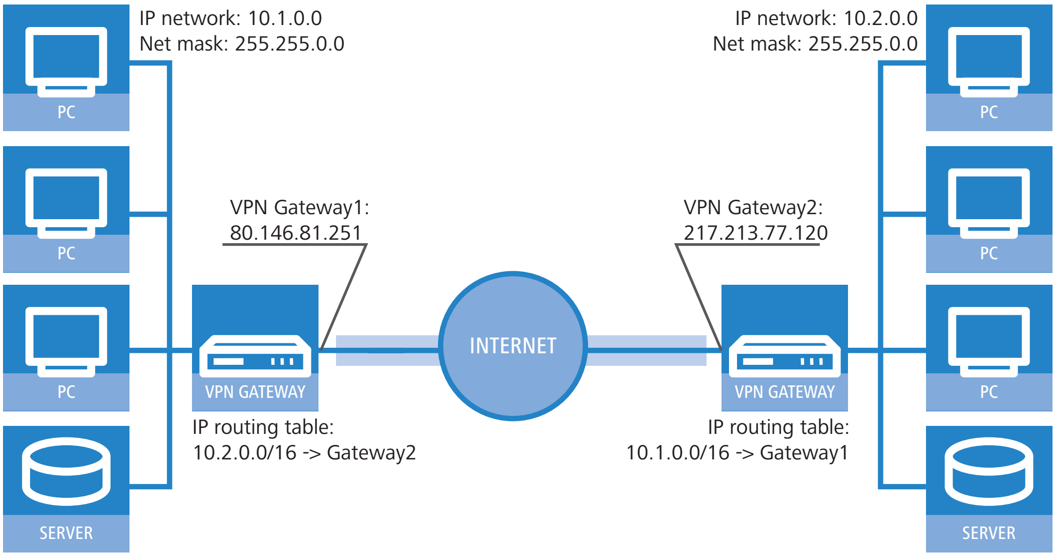
10.5.8 Prepare VPN network relationships

The firewall integrated into LANCOM routers is a powerful instrument for defining source and target address ranges between which data transfer (and limitations to it) can be enabled or prohibited. These functions are also used for setting up the network relationships for the VPN rules.

In the simplest case, the firewall can generate the VPN rules automatically.

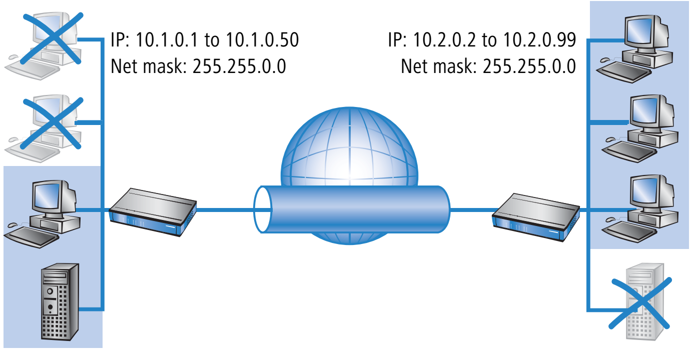
- The local intranet serves as the source network, i.e. the same private IP address range that the local VPN gateway itself belongs to.
- For automatically generated VPN rules, the target networks are those network ranges that have a remote VPN gateway set as their router.

To activate the automated rule generation, simply switch on the corresponding option in the firewall[1]. When coupling two simple local networks, the automatic VPN can interpret the necessary network relationships from the IP address range in its own LAN and from the entry for the remote LAN in the IP routing table.



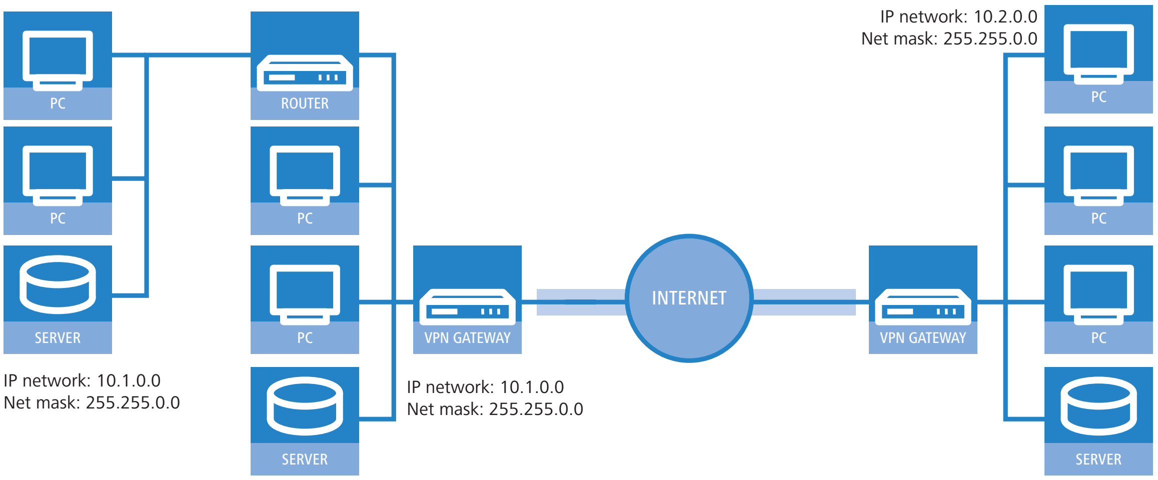
The description of the network relationships is more complicated if the source and target networks are not only represented by the intranet address ranges of the connected LANs:

- When only a portion of the local intranet is to be available to the remote network, then the automatic method is unsuited as the IP address range that is open to the VPN connection is too large.



- In many network structures, the local network is connected by further routers to sections of other networks with their own IP address ranges. Additional settings are required to include these address ranges in the network relationship.

[1] automatic when using the VPN installation Wizard under LANconfig



In these cases, the network relationships that describe the source and target networks must be entered manually. Depending on the situation, the scope of the automatically generated VPN rules may be extended, although sometimes it is better to deactivate the automatic VPN system to prevent unwanted network relationships.

The necessary network relationships are defined by the appropriate firewall rules under the following circumstances:

- In the firewall rules, the option “Consider this rule when generating VPN rules” must be activated.

The firewall rules for generating VPN rules are active even when the actual firewall function in the LANCOM device is not required and is switched off!

- Make sure that the firewall action is set to “Transfer”.
- Sources and targets for the connection can be entered as individual stations, certain IP address ranges, or whole IP networks.

It is vital that target networks are defined in the IP routing table so that the router in the LANCOM devices can forward the appropriate data packets to the other network. You can make use of the entries that already exist there and simply enter a higher-level network as the target. The intersecting portion of the target network defined by the firewall and the subordinate entries in the IP routing table is integrated into the network relationships for the VPN rules.

Example: The target networks 10.2.1.0/24, 10.2.2.0/24 and 10.2.3.0/24 are entered into the IP routing table and can be accessed via the router VPN-GW 2. An entry for the target network 10.2.0.0/16 is sufficient for these three subnets to be included in the VPN rules.

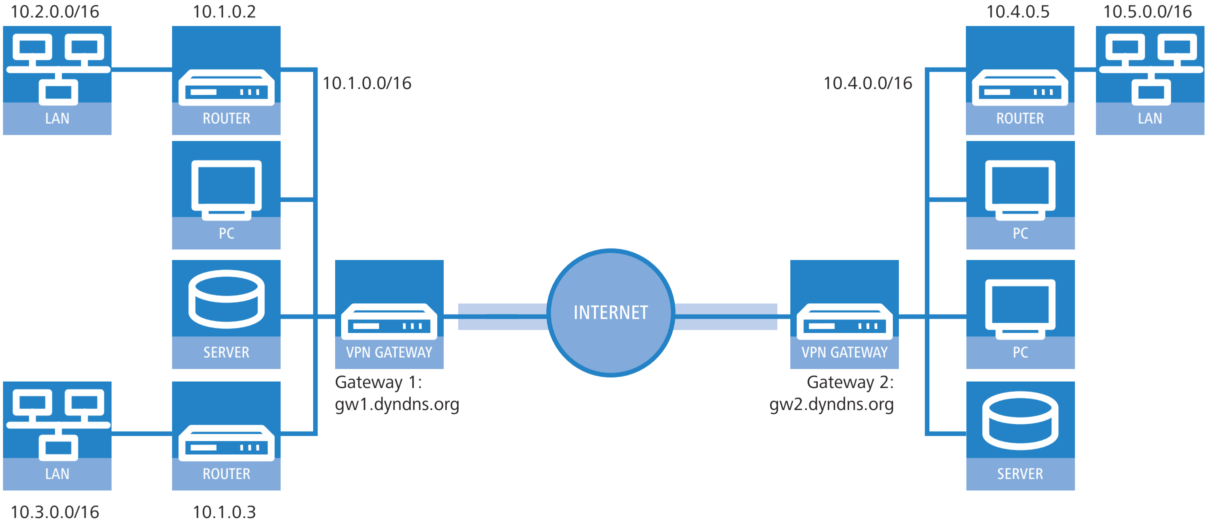
The definition of source and target networks must agree at both ends of the VPN connection. It is not possible, for example, to map a larger target address range to a smaller source address range at the opposite end. Decisive here are the IP address ranges allowed by the VPN rules and not the networks defined in the firewall rules. These can be very different from the network relationships in the VPN rules because of the intersecting ranges.

- VPN connections can also be limited to certain services or protocols according to your requirements. This means that the VPN connection can be limited to use only with a Windows network, for example.

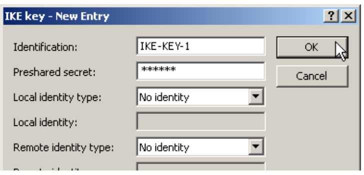
These limitation should be defined by a separate set of rules that applies only to the firewall and that will not be used in generating VPN rules. Combined firewall/VPN rules can very quickly become highly complex and difficult to comprehend.

10.5.9 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:



Identification: IKE-KEY-1

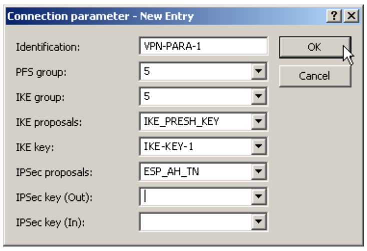
Preshared secret: ******

Local identity type: No identity

Local identity:

Remote identity type: No identity

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.



Identification: VPN-PARA-1

PFS group: 5

IKE group: 5

IKE proposals: IKE_PRESH_KEY

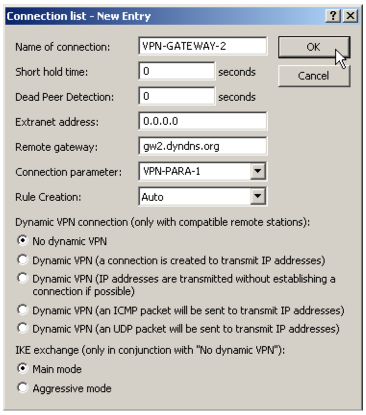
IKE key: IKE-KEY-1

IPSec proposals: ESP_AH_TN

IPSec key (Out):

IPSec key (In):

③ You should then generate a new entry in the Connection list with the name of the remote gateway as "name for the connection". For LANCOM Dynamic VPN connections the entry "Remote gateway" must remain empty. Otherwise enter the public address of the remote station: either the fixed IP address or the name for translation by DNS.



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)

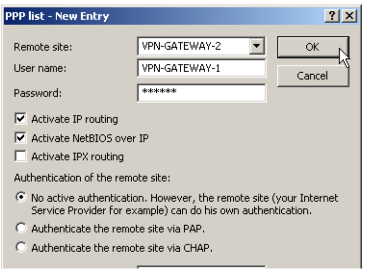
○ Dynamic VPN (an UDP packet will be sent to transmit IP addresses)

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, but for safety reasons should not be identical to the pre-shared key.



PPP list - New Entry

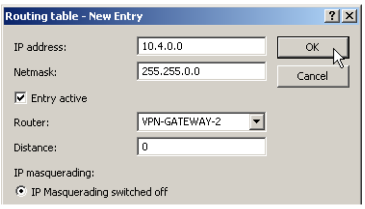
Remote site: VPN-GATEWAY-2
User name: VPN-GATEWAY-1
Password: ******

☑ 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".

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.



Routing table - New Entry

IP address: 10.4.0.0
Netmask: 255.255.0.0
☑ Entry active
Router: VPN-GATEWAY-2
Distance: 0
IP masquerading:
● IP Masquerading switched off

For the “VPN gateway 1”, the following entries are necessary so that the remote network sections can be reached.

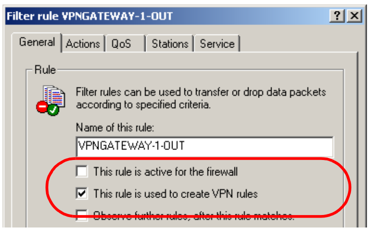
IP address	Net mask	Router	IP masquerading
10.4.00.0	255.255.0.0	VPN gateway 2	No
10.5.0.0	255.255.0.0	VPN gateway 2	No

For those subnetworks connected to your own LAN, define the router as the IP address for the appropriate LAN router.

IP address	Net mask	Router	IP masquerading
10.2.0.0	255.255.0.0	10.1.0.2	No
10.3.0.0	255.255.0.0	10.1.0.3	No

These entries enable VPN gateway 1 to forward packets arriving from the remote network to the correct sections of the local network.

⑥ Change to the “Firewall/QoS” configuration area. On the “Rules” tab, add a new firewall rule with the name “VPN GATEWAY 1 OUT” and activate the option “This rule is used to create VPN rules”. This ensures that IP networks described in this rule will be used in establishing VPN network relationships.



Filter rule VPNGATEWAY-1-OUT

Rule

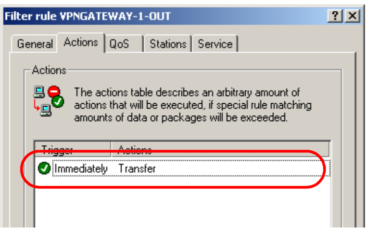
Filter rules can be used to transfer or drop data packets according to specified criteria.

Name of this rule: VPNGATEWAY-1-OUT

☐ This rule is active for the firewall
☑ This rule is used to create VPN rules
☐ Observe further rules, after this rule matches

It is recommended to keep the rules used for making network relationships (source and target IP) separate from those firewall rules that for instance affect the services used in communications. Combining both aspects can leed to a higher number of internal managed VPN relationships and therefore to a loss of performance in the VPN tunnels.

⑦ On the “Actions” tab for these firewall rules, set the “Packet Action” to “Transmit”.

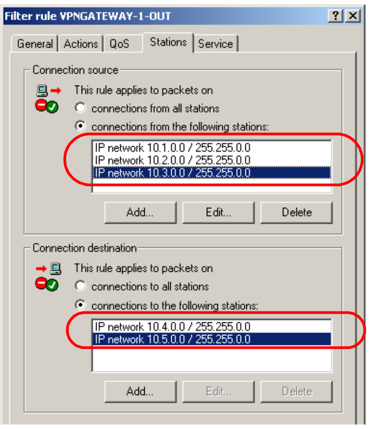


Filter rule VPNGATEWAY-1-OUT

The actions table describes an arbitrary amount of actions that will be executed, if special rule matching amounts of data or packages will be exceeded.

Trigger	Actions
✓ Immediately	Transfer

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.



Filter rule VPNGATEWAY-1-OUT

Connection source

This rule applies to packets on

○ connections from all stations

● connections from the following stations:

IP network 10.1.0.0 / 255.255.0.0
IP network 10.2.0.0 / 255.255.0.0
IP network 10.3.0.0 / 255.255.0.0

Connection destination

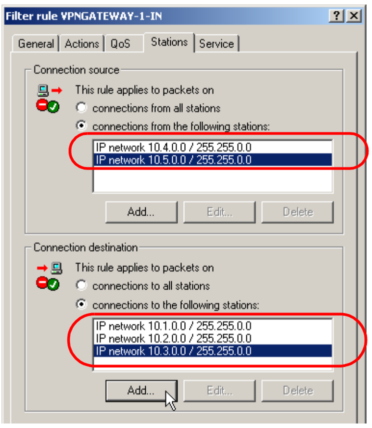
This rule applies to packets on

○ connections to all stations

● connections to the following stations:

IP network 10.4.0.0 / 255.255.0.0
IP network 10.5.0.0 / 255.255.0.0

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.



Filter rule VPNGATEWAY-1-IN

Connection source

This rule applies to packets on

○ connections from all stations

● connections from the following stations:

IP network 10.4.0.0 / 255.255.0.0
IP network 10.5.0.0 / 255.255.0.0

Connection destination

This rule applies to packets on

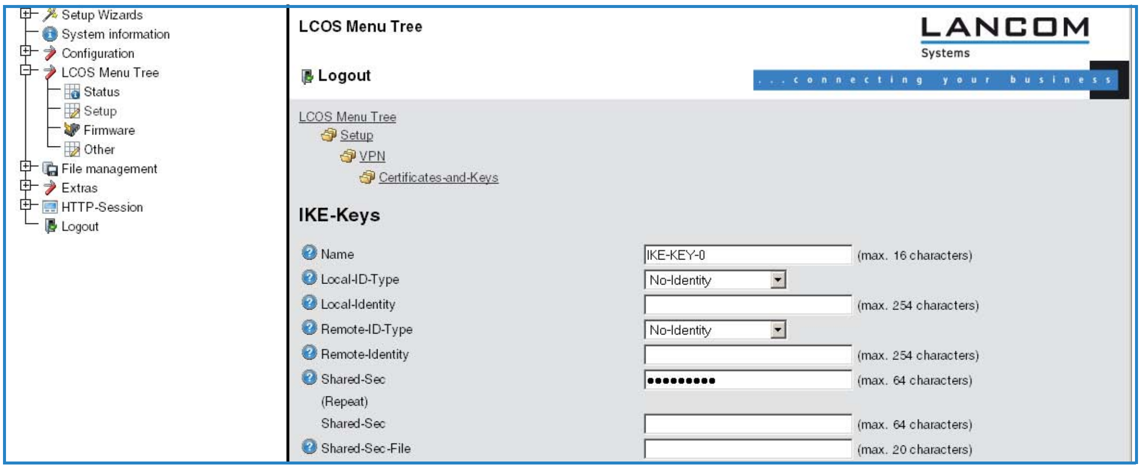
○ connections to all stations

● connections to the following stations:

IP network 10.1.0.0 / 255.255.0.0
IP network 10.2.0.0 / 255.255.0.0
IP network 10.3.0.0 / 255.255.0.0

10.5.10 Configuration with WEBconfig

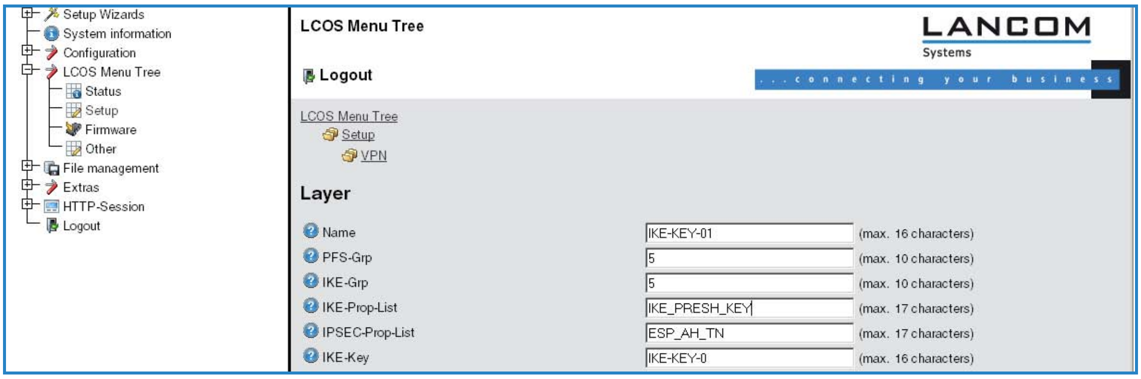
① Under **Configuration ▶ VPN ▶ IKE-Param. ▶ IKE key** set a new IKE key for the connection:



IKE-Keys

Name	IKE-KEY-0	(max. 16 characters)
Local-ID-Type	No-Identity	
Local-Identity		(max. 254 characters)
Remote-ID-Type	No-Identity	
Remote-Identity		(max. 254 characters)
Shared-Sec	●●●●●●●●●	(max. 64 characters)
(Repeat) Shared-Sec		(max. 64 characters)
Shared-Sec-File		(max. 20 characters)

② Under **Configuration ▶ VPN ▶ General ▶ Connection parameters** define a new “VPN layer” for the connection parameters. Select the IKE key created earlier for this.



LCOS Menu Tree

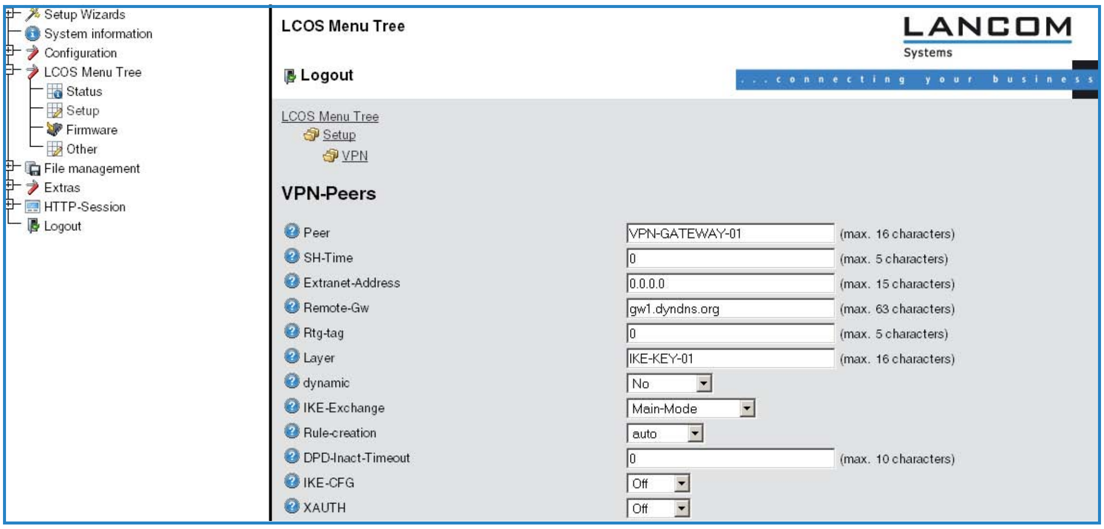
Logout

LCOS Menu Tree
Setup
VPN

Layer

Name	IKE-KEY-01	(max. 16 characters)
PFS-Grp	5	(max. 10 characters)
IKE-Grp	5	(max. 10 characters)
IKE-Prop-List	IKE_PRESH_KEY	(max. 17 characters)
IPSEC-Prop-List	ESP_AH_TN	(max. 17 characters)
IKE-Key	IKE-KEY-0	(max. 16 characters)

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.



LCOS Menu Tree

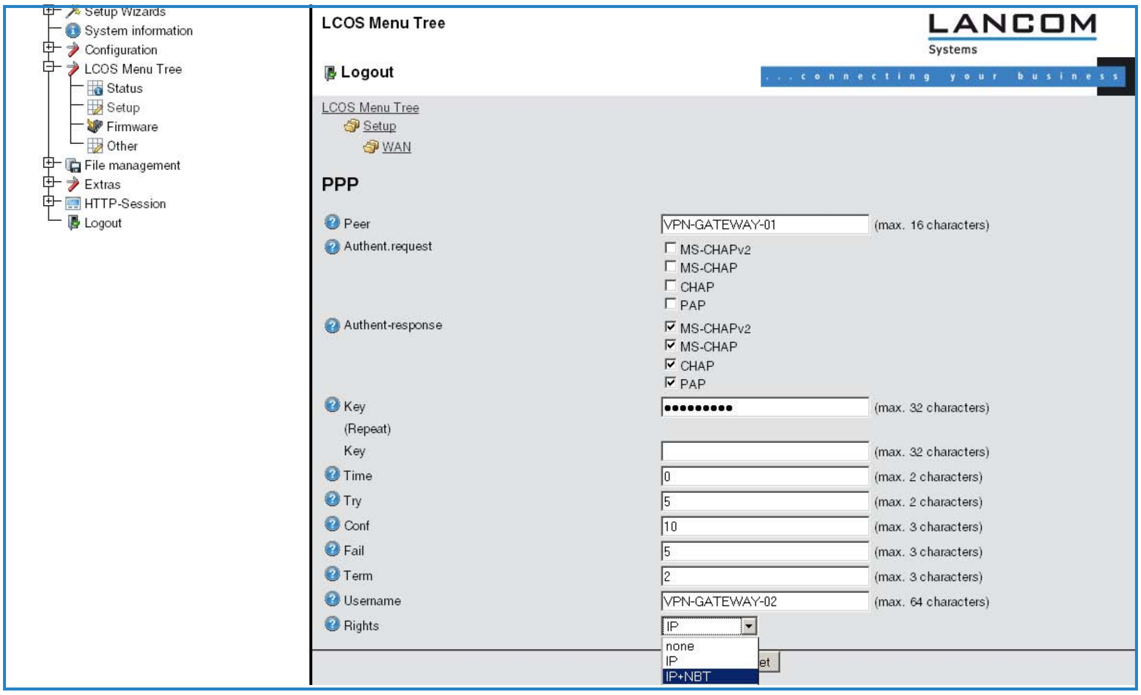
Logout

LCOS Menu Tree
Setup
VPN

VPN-Peers

Peer	VPN-GATEWAY-01	(max. 16 characters)
SH-Time	0	(max. 5 characters)
Extranet-Address	0.0.0.0	(max. 15 characters)
Remote-Gw	gw1.dyndns.org	(max. 63 characters)
Rtg-tag	0	(max. 5 characters)
Layer	IKE-KEY-01	(max. 16 characters)
dynamic	No	
IKE-Exchange	Main-Mode	
Rule-creation	auto	
DPD-Inact-Timeout	0	(max. 10 characters)
IKE-CFG	Off	
XAUTH	Off	

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.



LCOS Menu Tree

Logout

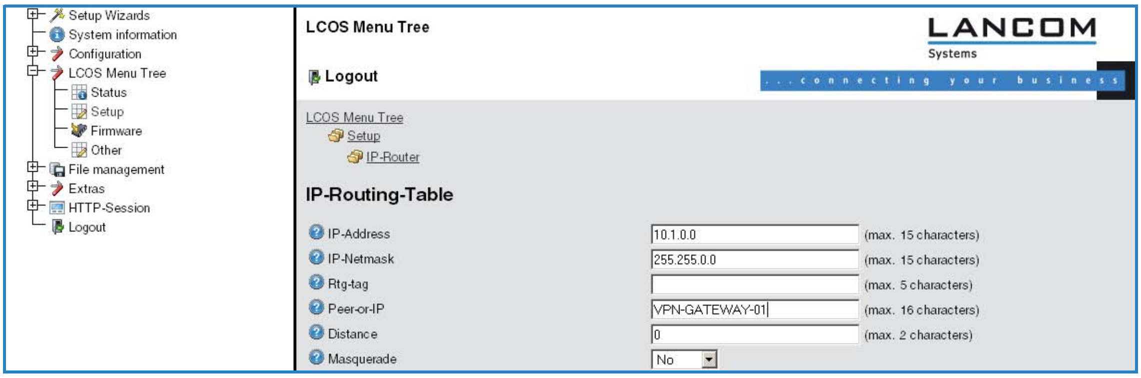
LCOS Menu Tree
Setup
WAN

PPP

Peer	VPN-GATEWAY-01	(max. 16 characters)
Authent.request	□ MS-CHAPv2 □ MS-CHAP □ CHAP □ PAP	
Authent-response	☑ MS-CHAPv2 ☑ MS-CHAP ☑ CHAP ☑ PAP	
Key	●●●●●●●●●	(max. 32 characters)
(Repeat) Key		(max. 32 characters)
Time	0	(max. 2 characters)
Try	5	(max. 2 characters)
Conf	10	(max. 3 characters)
Fail	5	(max. 3 characters)
Term	2	(max. 3 characters)
Username	VPN-GATEWAY-02	(max. 64 characters)
Rights	IP	

Be sure to activate "IP routing" and, if required, "NetBIOS over IP".

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.



IP-Routing-Table

IP-Address	10.1.0.0	(max. 15 characters)
IP-Netmask	255.255.0.0	(max. 15 characters)
Rtg-tag		(max. 5 characters)
Peer-or-IP	VPN-GATEWAY-01	(max. 16 characters)
Distance	0	(max. 2 characters)
Masquerade	No	

For the “VPN gateway 2”, the following entries are necessary so that the remote network sections can be reached.

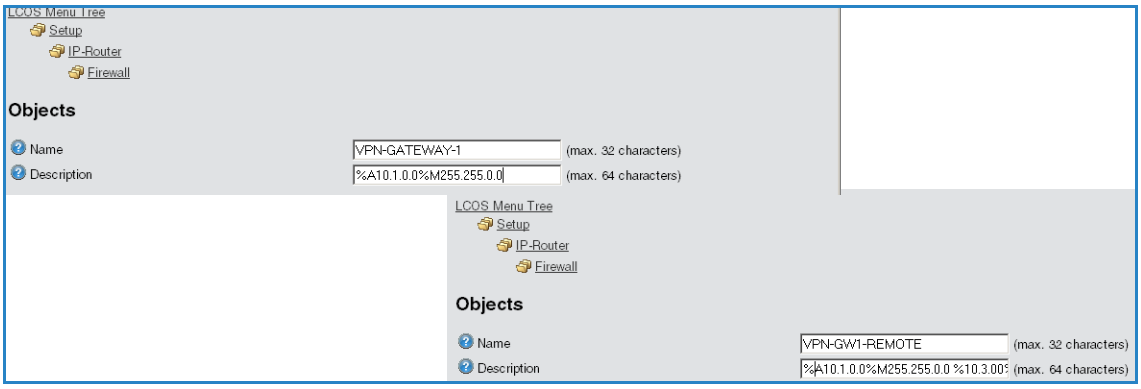
IP address	Net mask	Router	IP masquerading
10.1.0.0	255.255.0.0	VPN gateway 1	No
10.2.0.0	255.255.0.0	VPN gateway 1	No
10.3.0.0	255.255.0.0	VPN gateway 1	No

For those subnetworks connected to your own LAN, define the router as the IP address for the appropriate LAN router.

IP address	Net mask	Router	IP masquerading
10.5.0.0	255.255.0.0	10.4.00.5	No

These entries enable VPN gateway 2 to forward packets arriving from the remote network to the correct sections of the local network.

⑥ Under **Configuration ▶ Firewall/QoS ▶ Object table** make an entry for each part of the network that should be used as a source or destination for the VPN connection via “VPN GATEWAY 1” (“VPN-GW1-LOCAL” and “VPN-GW1-REMOTE”). Enter each subnet in the form “%A10.1.0.0 %M255.255.0.0”.



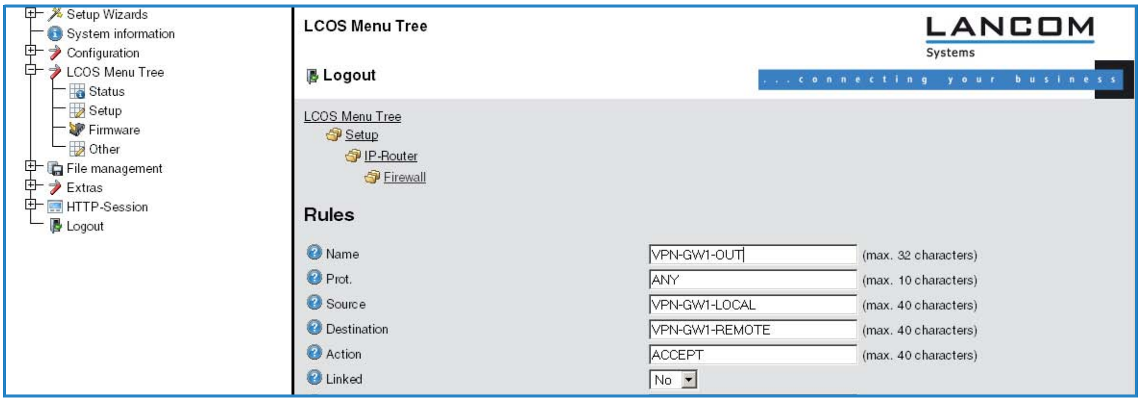
Objects

Name	VPN-GATEWAY-1	(max. 32 characters)
Description	%A10.1.0.0%M255.255.0.0	(max. 64 characters)

Objects

Name	VPN-GW1-REMOTE	(max. 32 characters)
Description	%A10.1.0.0%M255.255.0.0 %10.3.00	(max. 64 characters)

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.



LCOS Menu Tree

Logout

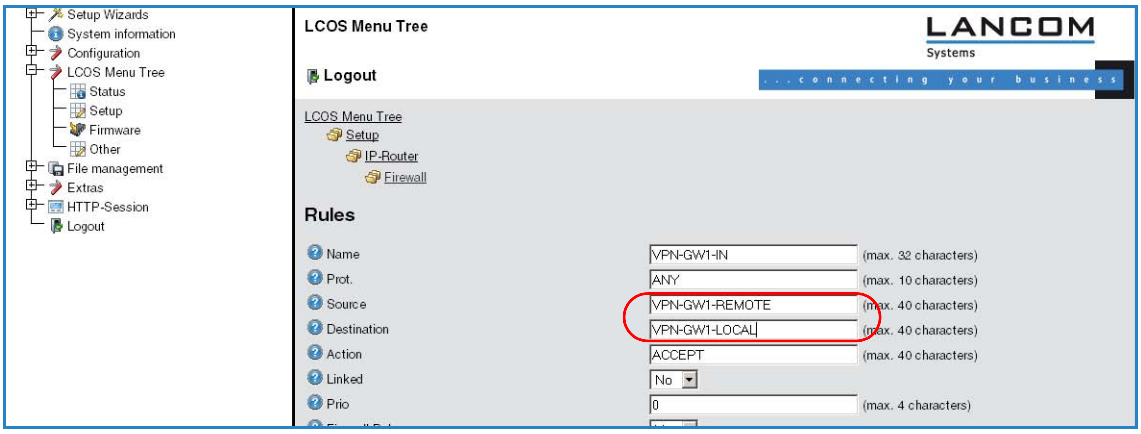
LCOS Menu Tree > Setup > IP-Router > Firewall

Rules

Name	VPN-GW1-OUT	(max. 32 characters)
Prot.	ANY	(max. 10 characters)
Source	VPN-GW1-LOCAL	(max. 40 characters)
Destination	VPN-GW1-REMOTE	(max. 40 characters)
Action	ACCEPT	(max. 40 characters)
Linked	No	

As a rule, it is recommended that you keep the rules used for making network relationships separate from those firewall rules that affect the services used in communications, for example.

⑧ Now for the incoming data transmissions, generate a firewall rule named “VPN-GWY1-IN” with the same parameters as the rule just described. The only difference is that the source and the destination networks are swapped.



LCOS Menu Tree

Logout

LCOS Menu Tree > Setup > IP-Router > Firewall

Rules

Name	VPN-GW1-IN	(max. 32 characters)
Prot.	ANY	(max. 10 characters)
Source	VPN-GW1-REMOTE	(max. 40 characters)
Destination	VPN-GW1-LOCAL	(max. 40 characters)
Action	ACCEPT	(max. 40 characters)
Linked	No	
Prio	0	(max. 4 characters)

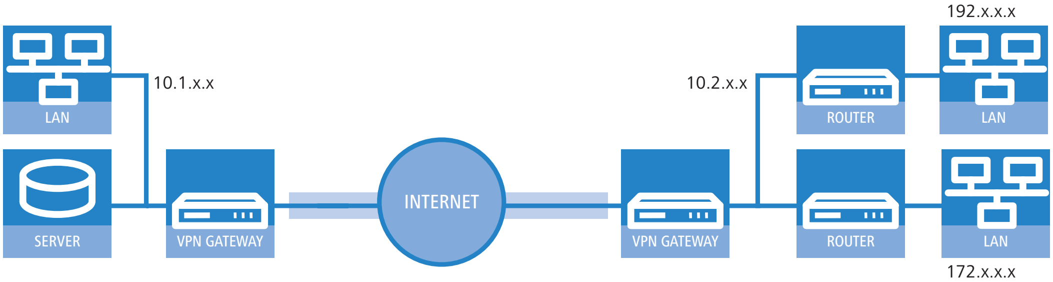
10.5.11 Establishing Security Associations collectively

Security Associations (SAs) are the basis for establishing a VPN tunnel between two networks. Parameters defined by a SA include:

- Source and destination network IP addresses
- Encyption, integrity check and authentication methods
- The key for the connection
- The key's lifetime

Security Associations are defined by automatically or manually generated VPN rules (also see ‘Prepare VPN network relationships’ → page 10-16 in the reference manual).

The establishment of Security Associations is normally initiated by an IP packet which is to be sent from a source network to a destination network. With keep-alive connections, this is an ICMP packet which is sent to the remote site by an entry in the polling table.



In complex network scenarios it is possible for multiple network relationships to be defined between two VPN gateways. If a single IP packet is transferred, then the SAs are established for this single packet and its corresponding network relationship only. To establish the other SAs, IP packets fitting to the other network relationships are needed.

It takes time to establish SAs based on data packets, and this can lead to the loss of packets as long as the SAs are not yet installed. This is often an undesirable side effect, particularly with keep-alive connections. Instead, **all** SAs relevant to the network relationships defined in the remote site should be established **immediately**. However, since the negotiation of SAs can make heavy demands on CPU performance—particularly in complex scenarios—the behavior can be defined with the parameter "Establish SAs collectively".

- **Establish SAs collectively**
  - Yes: All SAs defined in the device will be established.
  - No [default]: Only the SA which corresponds explicitly to a packet waiting for transfer is to be established.
  - Only with KeepAlive: All of the defined SAs will be established for remote stations in the VPN connection list with a hold time set to '9999' (Keep Alive).

WEBconfig: LCOS menu tree ▶ Setup ▶ VPN

In most cases and particularly where automatically generated VPN rules are in use, the setting which establishes only explicitly corresponding SAs is perfectly sufficient.

The SAs currently in effect can be seen under /Status/VPN.

10.5.12 Diagnosis of VPN connections

If the VPN connections fail to work after the configuration of the parameters, the following diagnostic methods can be applied:

- The command **show vpn spd** on the Telnet console calls the “Security Policy Definitions”.
- Use the command **show vpn sadb** to access information about the negotiated “Security Associations” (SAs).
- The command **trace + vpn** [status, packet] calls up the status and error messages for the current VPN negotiations.
  - The error message “No proposal chosen” indicates a fault in the configuration at the remote site.
  - The error message “No rule matched”, on the other hand, indicates a fault in the configuration of the local gateway.

10.6 Working with digital certificates

The security of communications via VPN fulfils three core requirements:

- **Confidentiality**: The transmitted data cannot be read by unauthorized persons (via encryption).
- **Integrity**: The data cannot be changed during transmission (via authentication).
- **Authenticity**: The receiver can be certain that received data has genuinely been sent by the supposed sender (via authentication).

A number of encryption and authentication methods exist which provide satisfactory solutions for the first two aspects, confidentiality and integrity. The use of digital certificates aims to provide assurance about the authenticity of the communications partner.

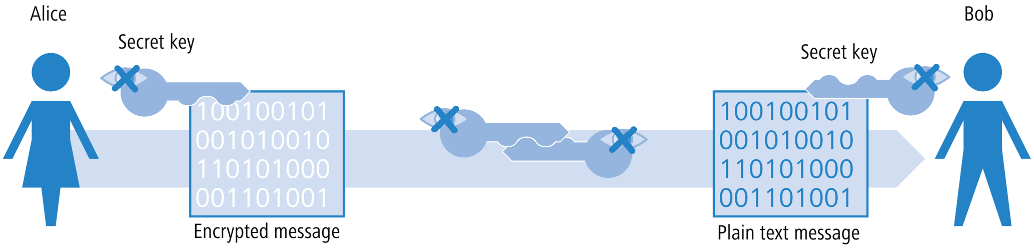
10.6.1 Basics

Encryption methods can be divided into two categories: Symmetrical and the asymmetrical encryption.

Symmetrical encryption

This is a method known for thousands of years and is based on the fact that the sender and the recipient both have access to a message by knowing a secret shared key. This key can take on a wide variety of forms: The Romans used a stick of a certain diameter for encryption and decryption.

Today's digital communications rely in the main upon a password as the key. Using this password and an encryption algorithm, the data from the sender are changed. The recipient uses the same key and the fitting encryption algorithm so that the data become legible again. Other persons who do not know the key cannot read the data. A common symmetrical method of encryption is 3DES, for example.



Example:

- Alice wants to send a confidential message to Bob. To do this, she encrypts the message with a secret key and a suitable method, e.g. 3DES. She sends the encrypted message to Bob informing him of the encryption method she used.
- Bob has the same key as Alice. Since he knows which encryption method was used, he can decrypt the message and transform it back into plain text.

Symmetrical encryption is simple and efficient but has two serious disadvantages:

- A different key is required for every secret communications relationship. If Alice and Bob are joined by Carol, three keys are necessary for secure data communications between all parties; with four participants, the number of keys required is six; with 12 participants, 66 keys are required and with 1000 participants, almost 500,000 keys are necessary! In a worldwide network with ever increasing demands for secure communications and higher numbers of participants, the serious nature of this problem is obvious.
- While this first disadvantage could be solved with technology, the second problem that is the core problem for symmetrical encryption: The secret key must be known at both ends of the communication and must not fall into the hands of unauthorized persons. Thus it is not possible for Alice simply to send the key to Bob per e-mail before the data connection has been secured sufficiently—which is the whole point of the encryption. She has to give the key to Bob in person, or at least make use of a communications method which is safe from eavesdroppers. This is a task which is almost impossible to handle in these times of worldwide dynamic communications.

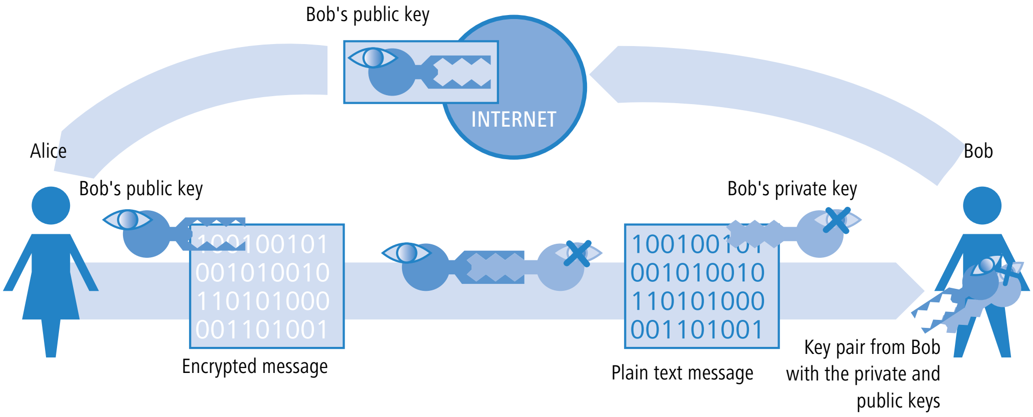
Asymmetric encryption

A totally new approach was developed in the 1970s; that of asymmetric encryption. This method no longer relies on a secret key that is known at both ends, but on a pair of keys instead:

- The first part of the key pair is used to **en**crypt the data that are to be sent to the key owner. This key, subsequently called the public key, can be made publicly available to anybody interested in communication.
- The second part of the key pair is the private key that is only used to **de**crypt the received message. This key is secret and may not fall into the hands of unauthorized persons.

The main difference to symmetrical methods: A publicly available key is used in this so-called "public key method". An example of an asymmetrical encryption method is RSA.

Let's take another look at the example with Alice and Bob:



- For secure communications, Bob first of all generates a key pair with a private key and a public key that belong together. The method used for generating this key ensures that the private key cannot be backwardly computed with knowledge of the public key. Bob can now publicize the public key without worry. He can send it to Alice per e-mail or simply publish it on a web server.

- Alice now encrypts the message for Bob with his public key. This now illegible message can only be decrypted by using Bob's private key. Even if the data are intercepted on the way from Alice to Bob, no-one but Bob can regenerate the plain text message.

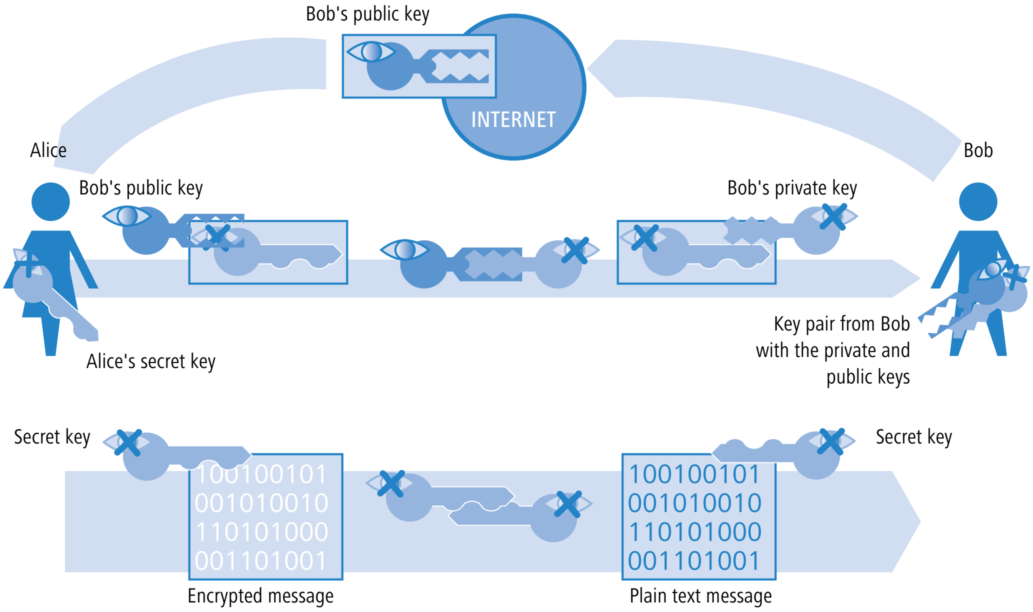
The asymmetrical encryption offers the following advantages over symmetrical variants:

- A key pair is not required for every communications relationship, but for each participant only. Even with 1000 participants, each user needs only his/her personal key pair, of which only the public key is publicly available. Instead of 500,000 secret keys, the public key method requires just 1000 key pairs.
- The risky transmission of a secret key to the communications partner is simply not necessary as knowledge is only required of the public key on the other side of the communications relationship. This is the solution to a significant problem in the dynamic encryption of data between multiple participants.

Combination of symmetrical and asymmetrical encryption

Asymmetrical encryption methods have quickly become established due to the security they offer. However, security has its price: Asymmetrical encryption methods are slow. The mathematics involved in the encryption and decryption of messages is far more complex that with symmetrical encryption methods and thus require more computing time—a critical factor when transmitting larger quantities of data.

The advantages of symmetrical and asymmetrical encryption can be used in suitable combinations of these methods. In this way, the higher security of the asymmetrical encryption is used to protect the transmission of the secret key. The actual data for transmission are then encrypted with the faster symmetrical method.



- First of all, Bob generates a key pair and publicizes the public key.
- Alice uses the public key to **en**crypt a secret symmetrical key and sends this to Bob. For each transmission, this secret key is newly defined according to a random procedure.
- Bob is the only one who can **de**crypt this secret key by using his private key.
- Alice and Bob then use this secret key to **en**crypt and **de**crypt the clearly much larger volume of the payload data.

Public key infrastructure

The combination of symmetrical and asymmetrical encryption methods enable initially unsecured connections to be used to establish secure data communications. Until now, the aspect of authenticity has been ignored. How should Alice know that the public key really does come from Bob? The use of public keys thus depends directly on the trust in the authenticity of the communications partner.

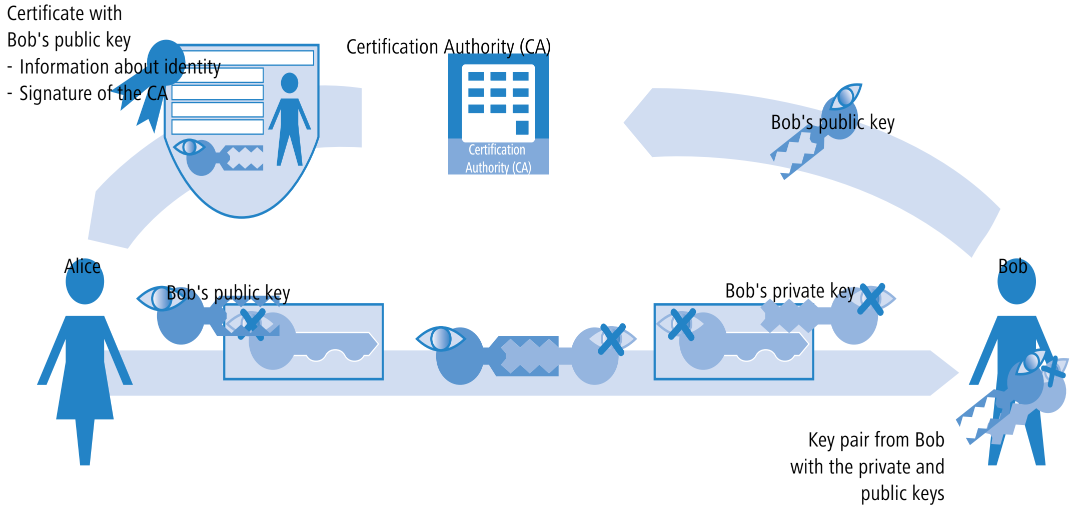
To secure this trust, a confirmation of the key pairs for use with asymmetrical encryption can be issued by publicly recognized and trustworthy authorities. In Germany, for example, the highest authority for the confirmation of digital keys is the Regulatory Authority for Telecommunications and Post (RegTP). The RegTP in turn issues accreditations to suitable service providers who are viewed as equally trustworthy.

ⓘ The RegTP web site (www.regtp.de) features up-to-date lists of accredited certification service providers and notification of revoked accreditations. Accredited service providers include numerous tax advisers and legal associations.

The task of this organization is to attribute a public key to just one person or organization. This attribution is recorded and officially publicized in a certificate. Consequently these providers are known as Certification Authorities, or CAs for short. The uppermost certification authority is known as the Root CA.

Bob can now approach a CA to have his public key certified as belonging to him. He submits his public key to the CA who then confirm that the key belongs to Bob.

The CA issues a certificate which lists the public key and further information about Bob, such as his identity, among other things.



The certificate carries the signature of the CA to show that the confirmation itself is genuine. The certificate takes up just a small amount of data and is suitable for exchange with an asymmetric method. With a signature, however, the asymmetric method is used in the opposite direction:

- The CA, too, has a key pair consisting of private and public keys. Since this is a trustworthy authority, their key pair can be considered as reliable.
- The CA calculates a hash value for the certificate, encrypts this and uses it in the signature in Bob's certificate. This acts to confirm the attribution of Bob's public key to his identity.

  This procedure behaves in the opposite manner to the normal asymmetrical encryption. In this case, the encryption does not fulfil the task of protecting the data from unauthorized persons, but confirms the signature of the CA instead.
- Any data communications participant anywhere in the world with the public key from the CA is now in a position to check the signed certificate.

  Only the CA is in a position to use their private key to generate signatures that can be decrypted again by using the CA's public key. This signature guarantees that the certificate is genuinely sourced from the issuing CA.

10.6.2 Advantages of certificates

In some cases the use of certificates for securing VPN connections can be an alternative to the otherwise widespread preshared key (PSK) method:

- Increase security of VPN client connections (with IKE Main Mode)

  Main Mode cannot be used when using PSK connections between peers that use dynamic IP addresses. In these cases, the aggressive mode must be used with its lower degree of security. Using certificates allows peers with dynamic IP addresses, such as dial-in computers with LANCOM Advanced VPN Client, to use the Main Mode and thus to increase the level of security.
- Higher security of the used keys and passwords

  Preshared keys are just as susceptible as other passwords, too. The way that users treat these passwords is a major factor in the securing of connections. With a certificate-based VPN establishment, the keys in the certificates are automatically generated with the desired key length. What's more, the random keys generated by computers offer more security from attack than the preshared keys of the same key length thought up by people.
- Possibility of authenicating remote sites

  When connecting with certificates oth remote stations must authenticate themselves. Further information can be contained in the certificates, which can be used for testing remote sites. The time limit of the certificates provide an additional protection, e.g. for users, who are only supposed to have access for a limited period of time.
- Providing tokens and smartcards

When saving certificates on external data media the integration of “Strong Security” environments, the readout of passwords from computers of networks is inhibited.

The advantages of certificates have to be considered in relation to the considerable increase in effort of introducing and maintaining a public key infrastructure (PKI).

10.6.3 Structure of certificates

Contents

A certificate contains a variety of information which is important for it to fulfil its purpose. Some information is obligatory, some is optional. A certificate can also be stored in a variety of different formats. An X.509-standard certificate contains the following information, for example:

- Version: This is the relevant version of the X.509 standard. The current (06.2005) version is 'v3'.
- Serial number: This is a unique number that identifies the certificate.
- Signature algorithm: This identifies the algorithm that the issuer used to sign the certificate. The digital signature of the issuer is also to be found here.
- Validity: Certificates are valid for a limited period of time. This entry indicates the duration of the certificate's validity.
- Issuer: This identifies the issuer, for example by name, e-mail address, nationality, etc.
- Subject: This identifies the certificate's owner, for example by name, institution, e-mail address, nationality, city, etc.
- Subject public key: Information indicating the method used to generate the public key used by the certificate's owner. The owner's public key is also to be found under this item.

Target application

When the certificates are generated, the possible uses of the certificate usually have to be selected. Some certificates are intentionally designed for transfer with web browsers or e-mails only, and others are more generally applicable to any use.

When you generate certificates, make sure that you enter its intended purpose.

Formats

The ITU standard X.509 is a wide spread format for certificates. When displayed as text, this type of certificate looks like the following:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature algorithm: md5WithRSAEncryption
        Issuer: C=XY, ST=Austria, L=Graz, O=TrustMe Ltd, OU=Certificate Authority, CN=CA/
Email=ca@trustme.dom
        Validity
            Not Before: Oct 29 17:39:10 2000 GMT
            Not After : Oct 29 17:39:10 2001 GMT
            Subject: C=DE, ST=Austria, L=Vienna, O=Home, OU=Web Lab, CN=anywhere.com/
Email=xyz@anywhere.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
                    d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
                    9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
                    90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
                    1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
                    7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
```

```
                50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
                8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
                f0:b4:95:f5:f9:34:9f:f8:43
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Alternative Name:
            email:xyz@anywhere.com
        Netscape Comment:
            mod_ssl generated test server certificate
        Netscape Cert Type:
            SSL Server
Signature Algorithm: md5WithRSAEncryption
    12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
    3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
    82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
    cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
    4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
    d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
    44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
    ff:8e
```

File types

There are various file types for digital certificates and private keys depending on the issuer. The following types are common:

- *.pfx and *.p12: PKCS#12 files
- *.pem, *.cer and *.crt: BASE-64-coded certificates
- *.cer, *.crt and *.der: DER coded certificates
- *.key: BASE64 or DER coded keys
- *.pvk: Microsoft-specific key format

Apart from the straightforward certificates, there is another file type that is of significance in the world of certificate-secured VPN connections: The PCK#12 files which can contain multiple components such as a certificate and a private key. To process the PKCS#12 file, a password has to be entered which was set when the certificate was exported.

BASE64-coded certificates have a header that typically features the following lines:

```
----- BEGIN CERTIFICATE -----
```

Validity

A further option is to refer to a certificate revocation list (CRL). CRLs list certificates that have lost their validity, for example if an employee has left the company and his certificate has been withdrawn. This information allows those who are checking certificates to refer to the appropriate CRL.

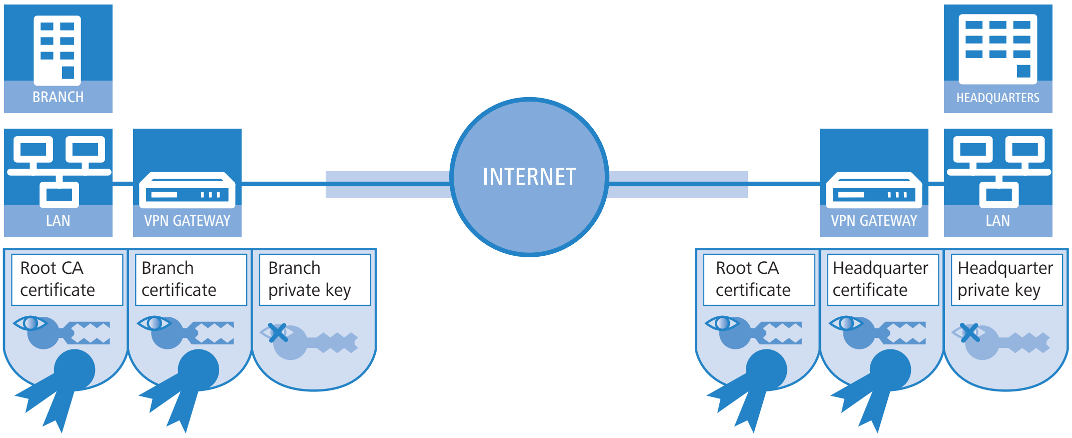
10.6.4 Security

Certain security aspects have to be observed even when dealing with certificates:

- Only ever transfer private keys via secure connections, e.g. with HTTPS.
- Passwords for keys or PKCS#12 files should be passphrases that are long enough and secure.

10.6.5 Certificates for establishing VPN connections

Along with basic information about certificates, this section now considers their concrete application in establishing VPN connections. For connection establishment with the support of certificates, certain information must be available at both ends of the connection (e.g. when connecting a branch office to the network at headquarters via LANCOM routers):



- The branch office has the following components:
  - The Root CA's certificate with the CA's public key
  - A certificate for its own device with its own public key and the confirmation of identity. The hash value of this certificate is signed with the CA's private key.
  - Its own private key
- The headquarters has the following components:
  - The Root CA's certificate with the CA's public key
  - A certificate for its own device with its own public key and the confirmation of identity. The hash value for this certificate is signed with the CA's private key.
  - Its own private key

Put simply, the following procedures are carried out during the VPN connection exchange in Main Mode (symmetrical in both directions):

① In an initial exchange of packets the peers negotiate, for example, the methods of encryption and authentication that are to be used. At this phase, both ends are not fully certain about who they are negotiating with, although this is not yet critical.

② At the next stage, common key material is negotiated for the continued communications, including among other things symmetrical keys and asymmetrical key pairs. At this phase, too, the two ends are not yet fully certain about who the keys are being negotiated with.

③ In the next stage, the certificate is used in a check to ensure that the peer involved in negotiating the key material really is the intended communication partner:

  - The branch office uses the current negotiation's key material to calculate a checksum (hash value) that can only be calculated by the two peers involved (branch office and headquarters) and only so long as the connection exists.
  - The branch office encrypts the hash with its own private key, generating a signature with it.
  - The branch office then transmits this signature together with its own certificate to the peer at headquarters.
  - The headquarters then checks the signature of the certificate received from the branch office. This can be done with the help of the public key at the Root CA, which is identical for both peers. If the signature in the branch office's certificate (generated with the CA's private key) can be decrypted with the CA's public key, then the signature is valid and the certificate is trustworthy.
  - In the next stage, the headquarters checks the signature of the encrypted hash. The branch office's public key in the corresponding certificate was found to be valid at the previous stage. The headquarters can thus check if the signed hash can be decrypted with the branch office's public key. The headquarters can calculate the same hash as the branch office using the key material for the current connection. If this check is successful then the peer "branch office" can be considered as authentic.

10.6.6 Certificates from certificate service providers

Certificates on offer from public certifiers are available in various security classes. The higher security classes require more effort on behalf of the applicants to demonstrate the authenticity of their identity to the CA. The Trustcenter AG in Hamburg, for example, uses the following classes:

- Class 0: These certificates are issued without an identity check and serve only for customer tests.

- Class 1: For this class, the existence of an e-mail address is the only check. These certificates are useful for private users wishing to sign their e-mails, for example.
- Class 2: This level, too, does not involve any personal proof of identity. The submission of an application along with, for example, a certificate of company registration is sufficient. This level is suitable for communications between companies that already know each other.
- Class 3: This level involves a personal check of the person or company. The information in the issued certificates is compared with a passport or a notarized copy of the certificate of company registration. This level is suitable for advanced applications such as e-business or online banking.

In your dealings with public certificate service providers, be sure to check in detail the security class or the proof of identity. This is the only way to be sure that the certificates really do meet with your security requirements.

10.6.7 Establishing a proprietary CA

Referring to public CAs for secure enterprise communications can only be recommended under certain conditions.

- There is considerable effort involved in the issue of new certificates and this can be slow.
- The keys in use are transferred via connections which are inadequately secured.
- Communication is based upon the trust in the CA.

An alternative for company communications is to establish a proprietary CA. Suitable packages are the Microsoft CA on a Microsoft Windows 2003 server or, as an open source version, OpenSSL. A proprietary CA empowers you to issue and manage all of the necessary certificates for secure data exchange with complete independence from any external parties.

Companies are recommended to use a proprietary CA rather than public certifiers. There are, however, several important issues to be considered when planning a CA. For example, even as early as during the installation of a Windows CA, the validity period for the Root CAs has to be defined and cannot be altered subsequently. Other aspects of planning include:

- The certificate policy or the level of security that is to be achieved with certificates
- The available name space
- Key lengths
- The duration of certificate validity
- Managing blocking lists

Precise planning is strongly recommended since corrections at a later date often imply considerable amounts of effort.

10.6.8 Requesting a certificate with Stand-alone Windows CA

For operations with a LANCOM, a combination of PKCS#12 file with root certificate, a proprietary device certificate and the device's public key offer the best services.

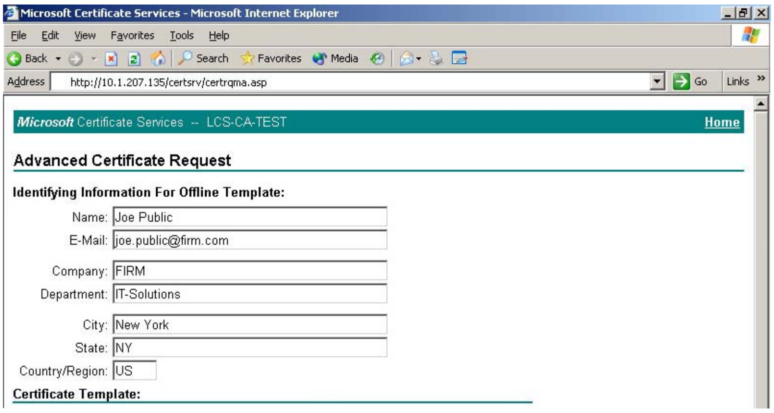
① Using your browser, access the start page of the Microsoft Certificate Services.

② For the certificate type, select 'Advance Certificate Request'.

③ The next step is to selection the option 'Generate and submit a certificate request '.

If, and only if, the root certificate is already available as a file, select the option 'BASE64'.

④ In the following step the information for identification is entered.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.1.207.135/certsrv/certrqma.asp
Go Links
Microsoft Certificate Services -- LCS-CA-TEST
Home

Advanced Certificate Request

Identifying Information For Offline Template:

Name: Joe Public
E-Mail: joe.public@firm.com
Company: FIRM
Department: IT-Solutions
City: New York
State: NY
Country/Region: US

Certificate Template:

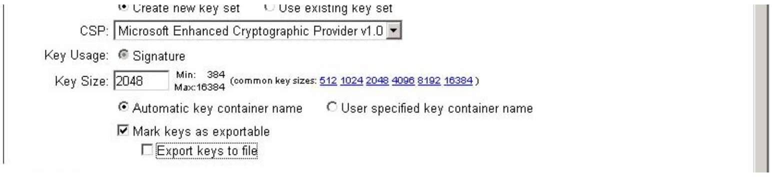
⑤ In the same dialog, select the certificate template as 'Other...' and then delete the value in 'Object ID'.

Other...

Object ID

Key Options:

⑥ Mark 'Create new key set'. The public and private keys for the current user will now automatically be generated by the CA.



● Create new key set ○ Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: ● Signature

Key Size: 2048 Min: 384 Max:16384 (common key sizes: 512 1024 2048 4096 8192 16384)

● Automatic key container name ○ User specified key container name

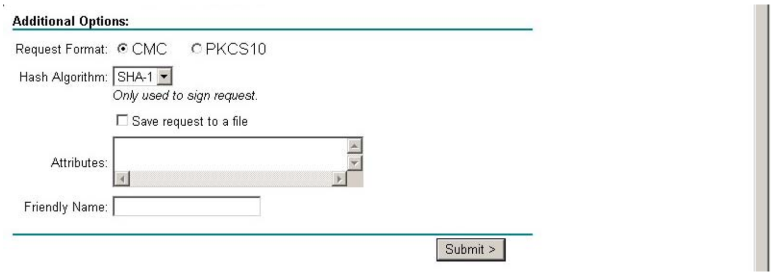
☑ Mark keys as exportable

□ Export keys to file

⑦ Select the key size according to certificate policy and activate the option to mark keys as exportable.

The key is not exported at this point and so a file name does not have to be specified. An export would create a Microsoft-specific *.pvk file, a format which is unsuitable for use with a LANCOM.

⑧ Finally, select the hash algorithm 'SHA-1' and send your certificate request with a click on **Submit**.



Additional Options:

Request Format: ● CMC ○ PKCS10

Hash Algorithm: SHA-1

Only used to sign request.

□ Save request to a file

Attributes:

Friendly Name:

You can check on the status of your certificate request at any time via the Windows CA start page. Certificate requests can only be viewed from the same computer used to submit the request.

⑨ The certificate can be installed on your computer once the CA administrator has checked the request and created the certificate.

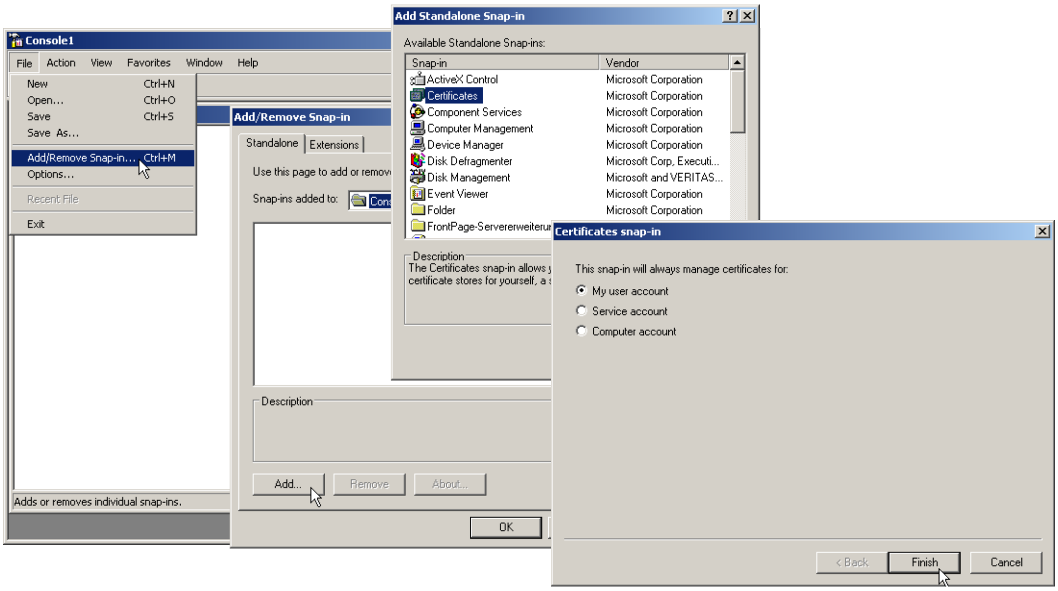
Certificates can only be installed on the same computer that was used for the request.

10.6.9 Export the certificate to a PKCS#12 file

The installation stores the certificate in your operating system but it is not yet available as a separate file. You will need this for installation to the LANCOM, though. For access to a certificate in file form, it has to be exported first.

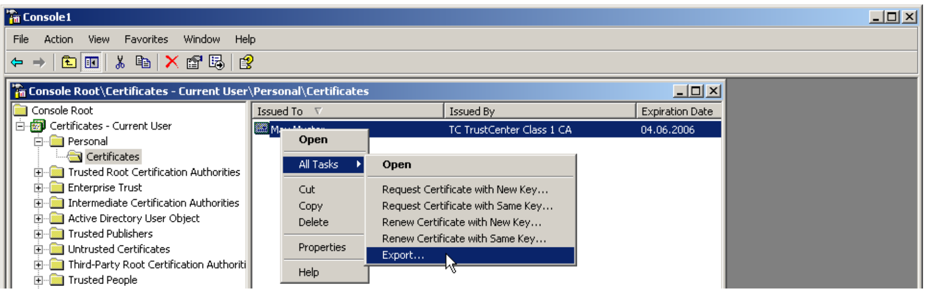
Export via the Windows console root

① Open the Management console with the command `mmc` at the command line and select the menu item **File** ▶ **Add/ Remove Snap-In**.

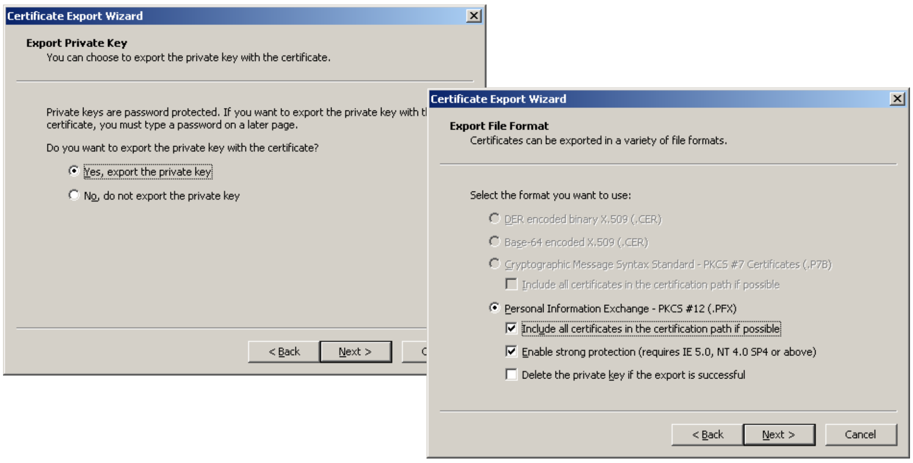

Console1
File Action View Favorites Window Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
Recent File
Exit
Adds or removes individual snap-ins.
Add/Remove Snap-in
Standalone Extensions
Use this page to add or remov
Snap-ins added to: Con
Description
Add... Remove About...
OK
Add Standalone Snap-in
Available Standalone Snap-ins:
Snap-in Vendor
ActiveX Control Microsoft Corporation
Certificates Microsoft Corporation
Component Services Microsoft Corporation
Computer Management Microsoft Corporation
Device Manager Microsoft Corporation
Disk Defragmenter Microsoft Corp, Executi...
Disk Management Microsoft and VERITAS...
Event Viewer Microsoft Corporation
Folder Microsoft Corporation
FrontPage-Serverweiterun
Description
The Certificates snap-in allows y
certificate stores for yourself, a s
Certificates snap-in
This snap-in will always manage certificates for:
● My user account
○ Service account
○ Computer account
< Back Finish Cancel

② Click on **Add...** and select 'Certificates'. Confirm with **Add**, then mark 'My user account' and click on **Finish**.

③ To export the desired certificate to a file, go to the Management console and click in the group **Certificates - current user ▶ My certificates▶ Certificates** with the right mouse key and, from the context menu, select **All tasks ▶Export**.


Console1
File Action View Favorites Window Help
Console Root\Certificates - Current User\Personal\Certificates
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoriti
Trusted People
Issued To Issued By Expiration Date
TC TrustCenter Class 1 CA 04.06.2006
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Request Certificate with Same Key...
Renew Certificate with New Key...
Renew Certificate with Same Key...
Export...

④ In the Certificate Export Wizard, activate the option to export the private key. You can optionally delete the private key from the system after exporting.


Certificate Export Wizard
Export Private Key
You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with t
certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
● Yes, export the private key
○ No, do not export the private key
< Back Next >
Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
○ DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
● Personal Information Exchange - PKCS #12 (.PFX)
☑ Include all certificates in the certification path if possible
☑ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
□ Delete the private key if the export is successful
< Back Next > Cancel

The option 'Include all certificates in the certification path' must be activated so that the root certificate is also exported to the PKCS#12 file.

⑤ You will be requested to enter a password to protect the private key. Ensure that you choose a secure password of sufficient length (passphrase). You will need this password later to install the certificated in the LANCOM.

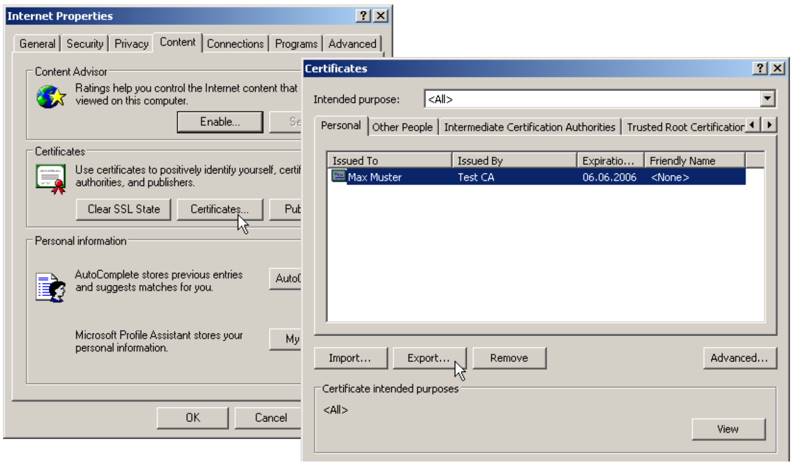
The term password is synonymous with other terms used in the different environments, e.g. "PIN".

Export via the Control Panel

As an alternative, you can open certificates on your system via the Control Panel.

① To do this, click on **Start ▶ Control Panel ▶ Internet Options**, the 'Contents' tab and the button **Certificates**.

② Choose the required certificate and click on **Export**.



Ratings help you control the Internet content that viewed on this computer.

Use certificates to positively identify yourself, certi authorities, and publishers.

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

Issued To	Issued By	Expiratio...	Friendly Name
Max Muster	Test CA	06.06.2006	<None>

The actions required in the Certificate Export Wizard that follows are identical to those described under 'Export via the Windows console root' → page 10-32.

10.6.10 Create certificates with OpenSSL

OpenSSL is a further possibility for creating proprietary certificates and to test certified connections. OpenSSL is an Open-Source project available for Linux and Windows at no cost; as a command-line tool, however, it does not offer the user-friendliness of other CA variants.

The configuration file openssl.cnf must be adapted to your specific needs. Further information is available in the OpenSSL documentation.

Installing OpenSSL

① Download the current version of OpenSSL from http://www.slproweb.com/products/Win32OpenSSL.html.

② Install the package and, in the directory `./bin/PEM/demoCA` create the following subdirectories:

- `/certs`
- `/newcerts`
- `/crl.`

③ In the file openssl.cnf, change the path in the `[CA_default]` group to: `dir= ./PEM/demoCA`

④ OpenSSL is started with a double-click on `openssl.exe` in the `./bin` directory.

Issue a certificate for Root CA

① Create a key for the CA with the command:

- `genrsa -des3 -out ca.key 2048`

Remember the password that you enter after the request for the CA key as you will need it again later!

This command creates the file 'ca.key' in the current directory.

② Create a certificate request for the CA with the command:

- `req -key ca.key -new -subj /CN="Test_CA" -out ca.req`

You will be requested to enter the password for the CA key here.

This command creates the file 'ca.req' in the current directory.

③ Create a certificate from the certificate request with the command:

□ `x509 -req -in ca.req -signkey ca.key -days 365 -out ca.crt`

Here, too, you will be requested to enter the password for the CA key.

This command signs the certificate request 'ca.req' with the key 'ca.key' and then issues the certificate 'ca.crt'.

Issue certificates for users or devices

① Create a key for the device or user with the command:

□ `genrsa -out device.key 2048`

This command creates the file 'device.key' in the current directory.

② Create a certificate request for the device or user with the command:

□ req -key device.key -new -subj /CN=DEVICE -out device.req

This command creates the file 'device.req' in the current directory.

Apart from this instruction further changes are necessary in the file "openssl.cnf" for the definition of a Extension.

③ Create a certificate from the certificate request with the command:

□ x509 -extfile openssl.cnf -req -in device.req -CAkey ca.key -CA ca.crt -CAcreateserial -days 90 -out device.crt

This command signs the certificate request 'device.req' with the key 'ca.key' and then issues the certificate 'device.cert'. The configuration file openssl.cnf is also involved in the procedure.

④ Export the certificate for the device or user with the command:

□ `pkcs12 -export -inkey device.key -in device.crt -certfile ca.crt -out device.p12`

This command combines and saves the key 'device.key', the certificate 'device.crt' and the root certificate 'ca.crt' in the file 'device.p12'. This PKCS#12 file can be uploaded directly to the required device ('Upload certificates to the LANCOM' → page 10-35).

10.6.11 Upload certificates to the LANCOM

The following components must be available in a LANCOM for the establishment of VPN connections that are secured by certificate.

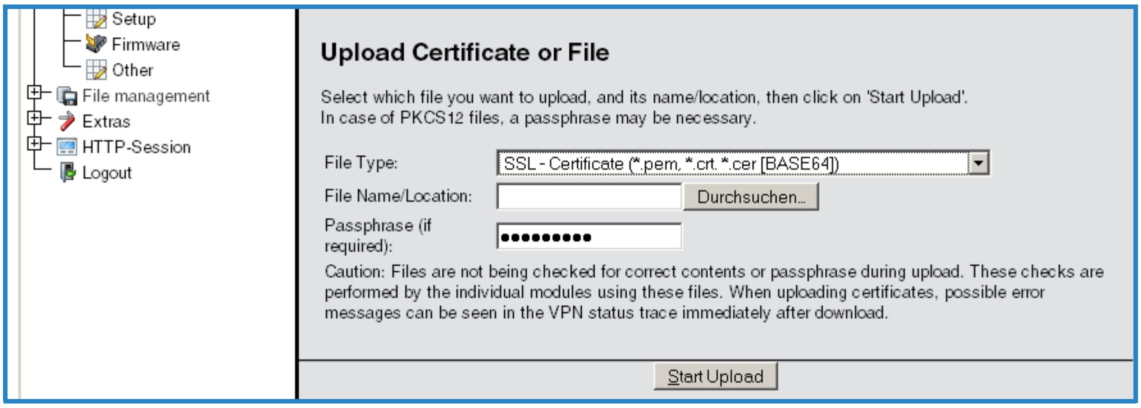
- The Root CA's certificate with the CA's public key
- A certificate for its own device with its own public key and the confirmation of identity. The hash value for this certificate is signed with the CA's private key.
- Its own private key

If you have followed the instructions for issuing certificates with a Windows CA and their export, then this information will now be available in the form of a combined PKCS#12 file. Alternatively you have used a different method and the individual components are available as separate files.

The certificate file can at this time only be uploaded to the devices with WEBconfig. Make sure that you use an HTTPS connection as the passphrase for the PKCS#12 file is transmitted unencrypted

① Use WEBconfig to log on to the required device; you will need administrator rights.

② Select the entry for **Upload Certificate or File**.



Upload Certificate or File

Select which file you want to upload, and its name/location, then click on 'Start Upload'.
In case of PKCS12 files, a passphrase may be necessary.

File Type: SSL - Certificate (*.pem, *.crt, *.cer [BASE64])

File Name/Location:

Passphrase (if required): ●●●●●●●●●●

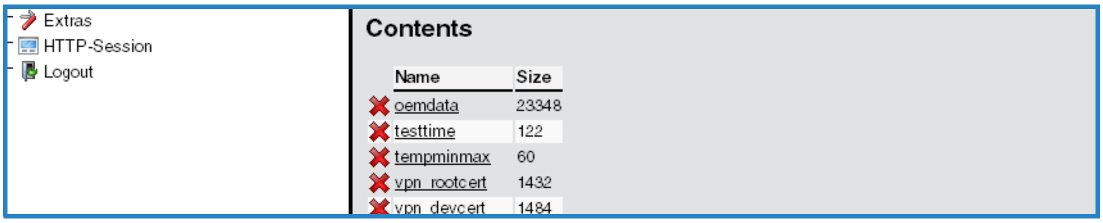
Caution: Files are not being checked for correct contents or passphrase during upload. These checks are performed by the individual modules using these files. When uploading certificates, possible error messages can be seen in the VPN status trace immediately after download.

③ Select the components that you wish to upload to the device:

- Root certificate
- Device certificate
- Private key for the device
- PKC#12 file with a combination of root certificate, device certificate and private key

The relevant password must be entered depending on the type of file to be uploaded.

The uploaded files can then be viewed in a list under **LCOS menu tree** ▶ **Status** ▶ **File system** ▶ **Content** .



Contents

Name	Size
oemdata	23348
testtime	122
tempminmax	60
vpn_rootcert	1432
vpn_devcert	1484

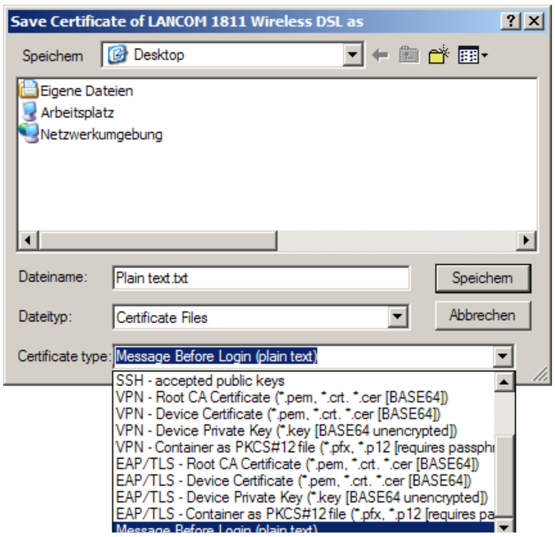
A combined PKCS#12 file is divided up into the necessary components upon upload.

10.6.12 Storing and uploading certificates

Various certificates can be used in a LANCOM for the encryption of certain services. These certificates can be uploaded to the devices by using LANconfig. Furthermore, the certificates in a device can also be read by LANconfig and stored to a file.

① Select the device which you want to upload a certificate into, or from which you want to save a copy.

② Click on the device with the right mouse key and from the context menu select **Configuration management** ▶ **Save certificate as file** or **Upload certificate from file**.



Save Certificate of LANCOM 1811 Wireless DSL as

Speichern: Desktop

Dateiname: Plain text.txt

Dateityp: Certificate Files

Certificate type: Message Before Login (plain text)

Eigene Dateien
Arbeitsplatz
Netzwerkumgebung
Speichern
Abbrechen
SSH - accepted public keys
VPN - Root CA Certificate (*.pem, *.crt, *.cer [BASE64])
VPN - Device Certificate (*.pem, *.crt, *.cer [BASE64])
VPN - Device Private Key (*.key [BASE64 unencrypted])
VPN - Container as PKCS#12 file (*.pfx, *.p12 [requires passphi
EAP/TLS - Root CA Certificate (*.pem, *.crt, *.cer [BASE64])
EAP/TLS - Device Certificate (*.pem, *.crt, *.cer [BASE64])
EAP/TLS - Device Private Key (*.key [BASE64 unencrypted])
EAP/TLS - Container as PKCS#12 file (*.pfx, *.p12 [requires pa
Message Before Login (plain text)

③ Select the storage location and the type of certificate to be saved or uploaded and confirm your selections with **Save**/ **Open**.

> ⓘ By selecting several devices, a certificate file can be uploaded to several devices at once. It is however not possible to simultaneously save the certificates from multiple devices. Depending on the type of certificate file, a passphrase may be necessary for uploading.

10.6.13 Set up VPN connections to support certificates

> ! VPN connections, which support certificates, can only be set up, if the LANCOM has the correct time. If the device does not has the actual correct time, the validity of the certificates can not be evaluated. The certificates will be rejected and no connection will be set up.

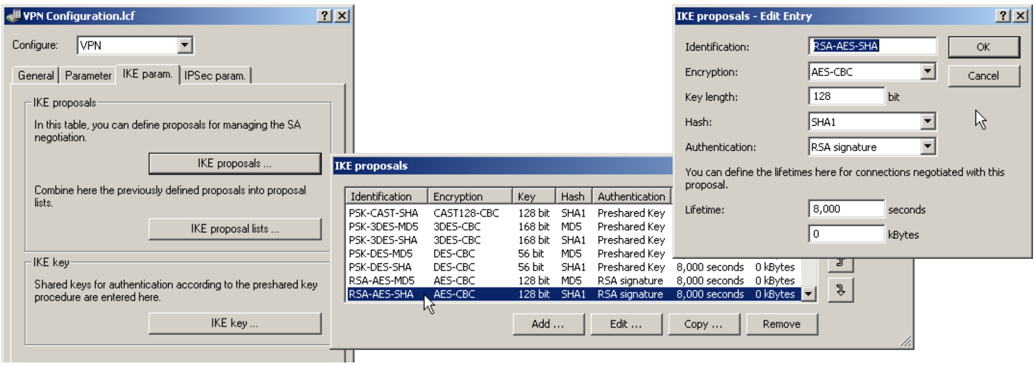
Several areas of the configuration have to be changed to set up VPN connections to support certificates.

- IKE proposals
- IKE proposal lists
- IKE key
- VPN parameters
- Connection parameters

> ⓘ Some of the values may already be available in your device depending on its firmware version. In this case you just have to check that the values are set correctly.

> ! If you are reconfiguring a remote device for certificate support with the method described below, and that device can only be reached via a VPN tunnel, then it is imperative that you reconfigure the remote device first before adjusting the connection in the local device. Changing the local configuration first would make the remote device unattainable!

① The proposals lists are to be supplemented with two new proposals with the exact description of 'RSA-AES-MD5' and 'RSA-AES-SHA', both of which use 'AES-CBC' for encryption and 'RSA signature' as the authentication mode, and which differ only in their hash method (MD5 and SHA1). I



In this table, you can define proposals for managing the SA negotiation.

Combine here the previously defined proposals into proposal lists.

Shared keys for authentication according to the preshared key procedure are entered here.

Identification	Encryption	Key	Hash	Authentication		
PSK-CAST-SHA	CAST128-CBC	128 bit	SHA1	Preshared Key		
PSK-3DES-MD5	3DES-CBC	168 bit	MD5	Preshared Key		
PSK-3DES-SHA	3DES-CBC	168 bit	SHA1	Preshared Key		
PSK-DES-MD5	DES-CBC	56 bit	MD5	Preshared Key		
PSK-DES-SHA	DES-CBC	56 bit	SHA1	Preshared Key	8,000 seconds	0 kBytes
RSA-AES-MD5	AES-CBC	128 bit	MD5	RSA signature	8,000 seconds	0 kBytes
RSA-AES-SHA	AES-CBC	128 bit	SHA1	RSA signature	8,000 seconds	0 kBytes

Identification: RSA-AES-SHA

Encryption: AES-CBC

Key length: 128 bit

Hash: SHA1

Authentication: RSA signature

You can define the lifetimes here for connections negotiated with this proposal.

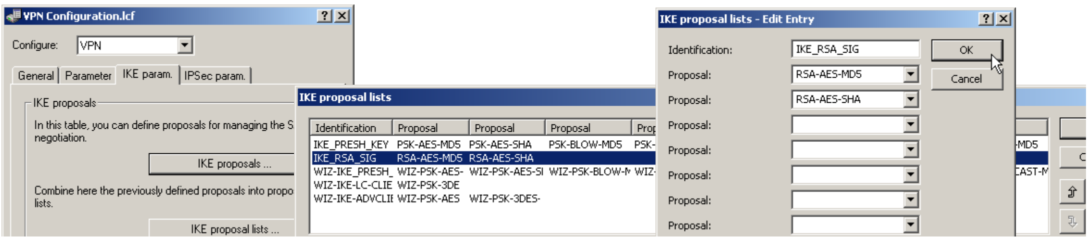
Lifetime: 8,000 seconds

0 kBytes

LANconfig: VPN ▶ IKE param. ▶ IKE proposals

WEBconfig: LCOS menu tree ▶ Setup ▶ VPN ▶ Proposals ▶ IKE

② A new list will be required in the proposals lists with the exact name 'IKE_RSA_SIG' which contains the two new proposals 'RSA-AES-MD5' and 'RSA-AES-SHA'.



In this table, you can define proposals for managing the S negotiation.

Combine here the previously defined proposals into propo lists.

Identification	Proposal	Proposal	Proposal	Prop
IKE_PRESH_KEY	PSK-AES-MD5	PSK-AES-SHA	PSK-BLOW-MD5	PSK-
IKE_RSA_SIG	RSA-AES-MD5	RSA-AES-SHA		
WIZ-IKE_PRESH_	WIZ-PSK-AES-	WIZ-PSK-AES-SI	WIZ-PSK-BLOW-M	WIZ-
WIZ-IKE-LC-CLIE	WIZ-PSK-3DE			
WIZ-IKE-ADVCLII	WIZ-PSK-AES	WIZ-PSK-3DES-		

Identification: IKE_RSA_SIG

Proposal: RSA-AES-MD5

Proposal: RSA-AES-SHA

Proposal:

Proposal:

Proposal:

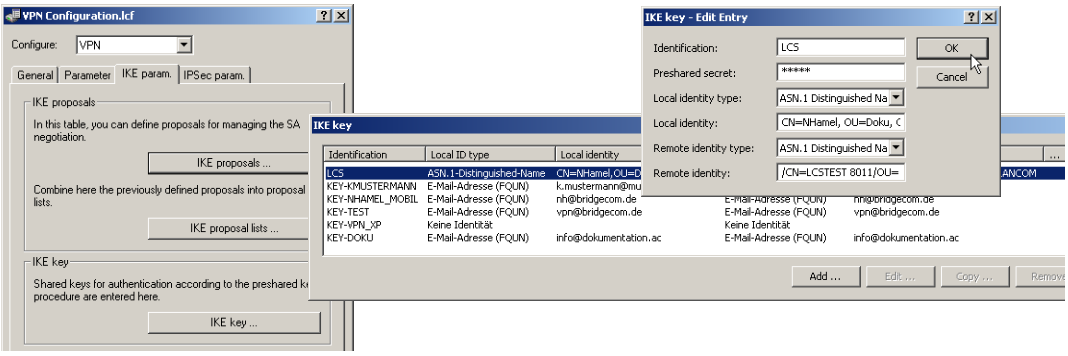
Proposal:

Proposal:

LANconfig: VPN ▶ IKE param. ▶ IKE proposal lists

WEBconfig: LCOS menu tree ▶ Setup ▶ VPN ▶ Proposals ▶ IKE proposal lists

③ In the list of IKE keys, all certificate connections must be set up with the corresponding identities.



In this table, you can define proposals for managing the SA negotiation.

Combine here the previously defined proposals into proposal lists.

Shared keys for authentication according to the preshared k procedure are entered here.

Identification	Local ID type	Local identity		
LCS	ASN.1-Distinguished-Name	CN=NHamel,OU=D		ANCOM
KEY-KMUSTERMANN	E-Mail-Adresse (FQUN)	k.mustermann@mu		
KEY-NHAMEL_MOBIL	E-Mail-Adresse (FQUN)	nh@bridgecom.de	E-Mail-Adresse (FQUN)	nh@bridgecom.de
KEY-TEST	E-Mail-Adresse (FQUN)	vpn@bridgecom.de	E-Mail-Adresse (FQUN)	vpn@bridgecom.de
KEY-VPN_XP	Keine Identität		Keine Identität	
KEY-DOKU	E-Mail-Adresse (FQUN)	info@dokumentation.ac	E-Mail-Adresse (FQUN)	info@dokumentation.ac

Identification: LCS

Preshared secret: *****

Local identity type: ASN.1 Distinguished Na

Local identity: CN=NHamel, OU=Doku, C

Remote identity type: ASN.1 Distinguished Na

Remote identity: /CN=LCSTEST 8011/OU=

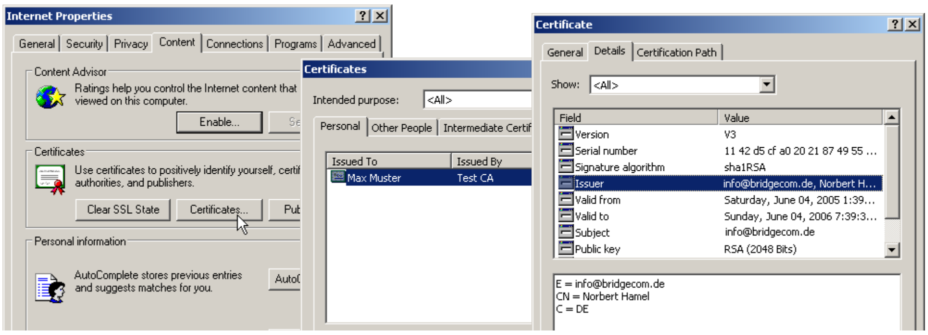
LANconfig: VPN ▶ IKE-Param. ▶ IKE key

WEBconfig: LCOS menu tree ▶ Setup ▶ VPN ▶ Proposals ▶ IKE-Keys

- Once it is no longer required, the preshared key can be deleted.
- The type of the identities is reset to ASN.1 Distinguished Names (local and remote).
- The identities are entered exactly as they stand in the certificates. The individual values such as 'CN', 'O' or 'OU' can be separated by commas or slashes.

  All of the values entered in the certificates must be listed in the same order. If necessary, check the certificate contents by using the Control Panel. To do this, click on **Start** ▶ **Control Panel** ▶ **Internet Options**, the 'Contents' tab and the button **Certificates**.

  Open the certificate and use the 'Details' tab to select the corresponding value. For the applicant you will find, for example, the necessary ASN.1 Distinguished Names and their abbreviations here. The values listed from top to bottom in the certificates must be entered into the IKE key from left to right. Observe the use of upper and lower case!



Internet Properties
General | Security | Privacy | Content | Connections | Programs | Advanced
Enable...
Clear SSL State
Certificates...
Certificates
Personal | Other People | Intermediate Certif
Certificate
General | Details | Certification Path

Content Advisor: Ratings help you control the Internet content that viewed on this computer.

Certificates: Use certificates to positively identify yourself, certif authorities, and publishers.

Personal information: AutoComplete stores previous entries and suggests matches for you.

Intended purpose: <All>

Issued To	Issued By
Max Muster	Test CA

Show: <All>

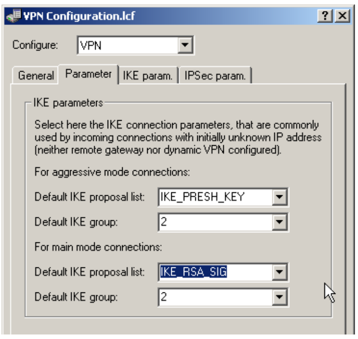
Field	Value
Version	V3
Serial number	11 42 d5 cf a0 20 21 87 49 55 ...
Signature algorithm	sha1RSA
Issuer	info@bridgecom.de, Norbert H...
Valid from	Saturday, June 04, 2005 1:39...
Valid to	Sunday, June 04, 2006 7:39:3...
Subject	info@bridgecom.de
Public key	RSA (2048 Bits)

E = info@bridgecom.de
CN = Norbert Hamel
C = DE

Special characters in the ASN.1 Distinguished Names can be entered by typing in the hexadecimal ASCII codes after a leading backslash. For example, "\61" corresponds to a small "a".

The display of certificates under Microsoft Windows shows for some values older short forms, for instance 'S' instead of 'ST' for 'stateOrPrivinceName' or 'G' instead of 'GN' for 'givenName'. Only use the new short forms 'ST' and 'GN'.

④ In the IKE connection parameters, the default IKE proposal lists for incoming aggressive-mode and main-mode connections must be set to the proposal list 'IKE_RSA_SIG'. Also observe the settings in the default IKE group which are adjusted in the following step as necessary.



Configure: VPN

IKE parameters

Select here the IKE connection parameters, that are commonly used by incoming connections with initially unknown IP address (neither remote gateway nor dynamic VPN configured).

For aggressive mode connections:

Default IKE proposal list: IKE_PRESH_KEY

Default IKE group: 2

For main mode connections:

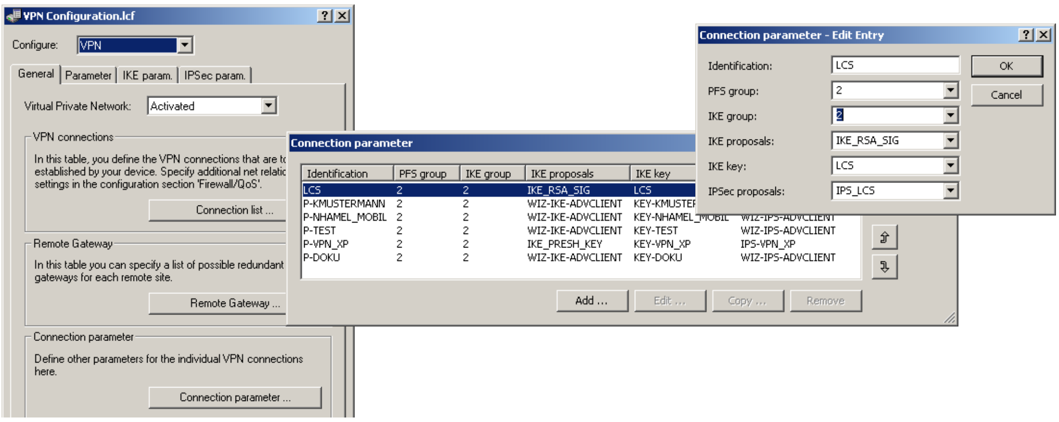
Default IKE proposal list: IKE_RSA_SIG

Default IKE group: 2

LANconfig: VPN ▶ Parameter

WEBconfig: LCOS menu tree ▶ Setup ▶ VPN

⑤ Finally, the VPN connection parameters must be set up to use the correct IKE proposals ('IKE_RSA_SIG'). The values for 'PFS group' and 'IKE group' must agree with the values set in the IKE connection parameters. Configuration with LANconfig



Configure: VPN

Virtual Private Network: Activated

VPN connections: In this table, you define the VPN connections that are to established by your device. Specify additional net relatio settings in the configuration section 'Firewall/QoS'.

Remote Gateway: In this table you can specify a list of possible redundant gateways for each remote site.

Connection parameter: Define other parameters for the individual VPN connections here.

Identification	PFS group	IKE group	IKE proposals	IKE key	
LCS	2	2	IKE_RSA_SIG	LCS	
P-KMUSTERMANN	2	2	WIZ-IKE-ADVCLIENT	KEY-KMUSTER	
P-NHAMEL_MOBIL	2	2	WIZ-IKE-ADVCLIENT	KEY-NHAMEL_MOBIL	WIZ-IPS-ADVCLIENT
P-TEST	2	2	WIZ-IKE-ADVCLIENT	KEY-TEST	WIZ-IPS-ADVCLIENT
P-VPN_XP	2	2	IKE_PRESH_KEY	KEY-VPN_XP	IPS-VPN_XP
P-DOKU	2	2	WIZ-IKE-ADVCLIENT	KEY-DOKU	WIZ-IPS-ADVCLIENT

Identification: LCS

PFS group: 2

IKE group: 2

IKE proposals: IKE_RSA_SIG

IKE key: LCS

IPSec proposals: IPS_LCS

LANconfig: VPN ▶ General ▶ Connection parameters

WEBconfig: LCOS menu tree ▶ Setup ▶ VPN ▶ VPN layers

10.6.14 Set up certificate-based VPN connections with the Setup Wizard

LANconfig is equipped with Setup Wizards with which you can set up certificate-based LAN coupling or RAS access via VPN.

VPN connections that support certificates can only be set up if the LANCOM is programmed with the correct time and if the corresponding certificates are loaded into the device. ('Upload certificates to the LANCOM' → page 10-35).

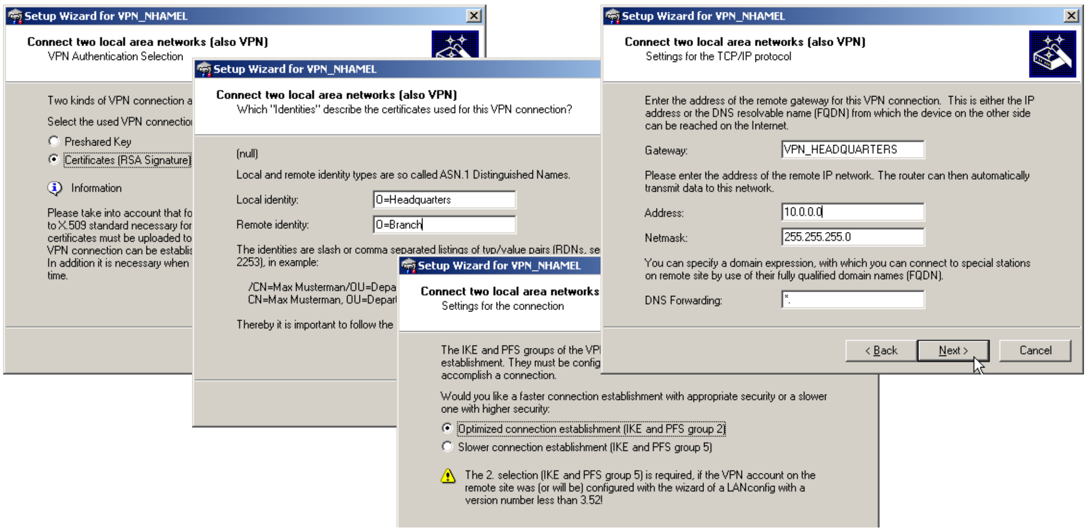
LAN coupling

① Choose the Wizard that connects two local area networks over VPN. In the appropriate dialog, select VPN connection authentication with certificates (RSA signature).

② Enter the identities contained in the certificates for the local and remote devices. Be sure to use the information from each certificate in full and in the right order: The ASN.1-Distinguished Names listed in Windows from top to bottom in the certificates must be entered into LANconfig from left to right.

Microsoft Windows displays some values in the certificates with outdated abbreviations, such as 'S' instead of 'ST' for 'stateOrProvinceName', or 'G' instead of 'GN' for 'givenName'. In these cases make sure that you use the current abbreviations 'ST' and 'GN'.

The Telnet command `show vpn cert` displays the content of the device certificate in a LANCOM, including the entered Distinguished Names (DN) under "Subject". The Distinguished Names are displayed in reverse order here until LCOS 6.00 and in the usual order as of LCOS 6.10!



Setup Wizard for VPN_NHAMEL

Connect two local area networks (also VPN)
VPN Authentication Selection

Two kinds of VPN connection a

Select the used VPN connectio

○ Preshared Key
● Certificates (RSA Signature)

Information

Please take into account that fo
to X.509 standard necessary for
certificates must be uploaded to
VPN connection can be establis
In addition it is necessary when
time.

Setup Wizard for VPN_NHAMEL

Connect two local area networks (also VPN)
Which "Identities" describe the certificates used for this VPN connection?

(null)

Local and remote identity types are so called ASN.1 Distinguished Names.

Local identity: O=Headquarters

Remote identity: O=Branch

The identities are slash or comma separated listings of typ/value pairs (RDNs, se
2253), in example:

/CN=Max Musterman/OU=Depa
CN=Max Musterman, OU=Depar

Thereby it is important to follow the

Setup Wizard for VPN_NHAMEL

Connect two local area networks
Settings for the connection

The IKE and PFS groups of the VP
establishment. They must be config
accomplish a connection.

Would you like a faster connection establishment with appropriate security or a slower one with higher security:

● Optimized connection establishment (IKE and PFS group 2)
○ Slower connection establishment (IKE and PFS group 5)

⚠ The 2. selection (IKE and PFS group 5) is required, if the VPN account on the remote site was (or will be) configured with the wizard of a LANconfig with a version number less than 3.52!

Setup Wizard for VPN_NHAMEL

Connect two local area networks (also VPN)
Settings for the TCP/IP protocol

Enter the address of the remote gateway for this VPN connection. This is either the IP address or the DNS resolvable name (FQDN) from which the device on the other side can be reached on the Internet.

Gateway: VPN_HEADQUARTERS

Please enter the address of the remote IP network. The router can then automatically transmit data to this network.

Address: 10.0.0.0

Netmask: 255.255.255.0

You can specify a domain expression, with which you can connect to special stations on remote site by use of their fully qualified domain names (FQDN).

DNS Forwarding: *.

③ If available choose the optimized connection establishment with IKE and PFS group 2. Only choose group 5 for IKE and PFS if this is required by the remote device. This will be the case if, for example, the VPN remote device is configured with LANconfig 3.52 or earlier.

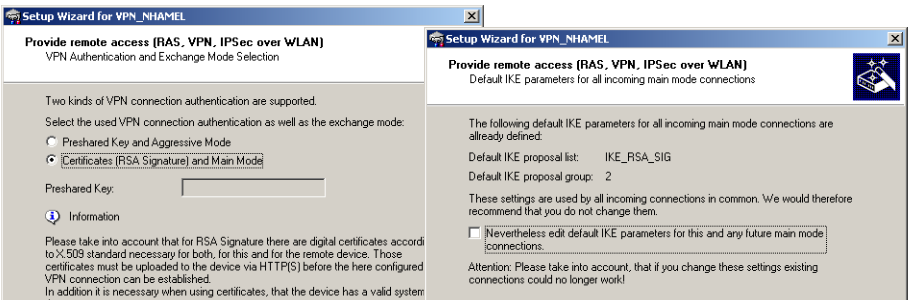
④ Enter the names of the VPN remote site, the IP address, the netmask for the remote network and, if applicable, the domain for the DNS forwarding. If required, activate the "Extranet" function and the "NetBIOS routing".

RAS connections

RAS connections that support certificates can be set up for the LANCOM Advanced VPN Client or for any other VPN client with user-defined parameters. The LANCOM Standard VPN Client does not support certificates.

Various parameters are requested depending on the choice of client or the options. This description shows all of the possible Wizard dialogs, some of which may not necessarily be relevant for your application.

① Choose the Wizard that provides remote access over VPN. In the appropriate dialog, select VPN connection authentication with certificates (RSA signature). The default "Exchange Mode" is the Main Mode.



Setup Wizard for VPN_NHAMEL

Provide remote access (RAS, VPN, IPSec over WLAN)
VPN Authentication and Exchange Mode Selection

Two kinds of VPN connection authentication are supported.

Select the used VPN connection authentication as well as the exchange mode:

○ Preshared Key and Aggressive Mode
● Certificates (RSA Signature) and Main Mode

Preshared Key:

Information

Please take into account that for RSA Signature there are digital certificates accordi
to X.509 standard necessary for both, for this and for the remote device. Those
certificates must be uploaded to the device via HTTP(S) before the here configured
VPN connection can be established.
In addition it is necessary when using certificates, that the device has a valid system

Setup Wizard for VPN_NHAMEL

Provide remote access (RAS, VPN, IPSec over WLAN)
Default IKE parameters for all incoming main mode connections

The following default IKE parameters for all incoming main mode connections are allready defined:

Default IKE proposal list: IKE_RSA_SIG

Default IKE proposal group: 2

These settings are used by all incoming connections in common. We would therefore recommend that you do not change them.

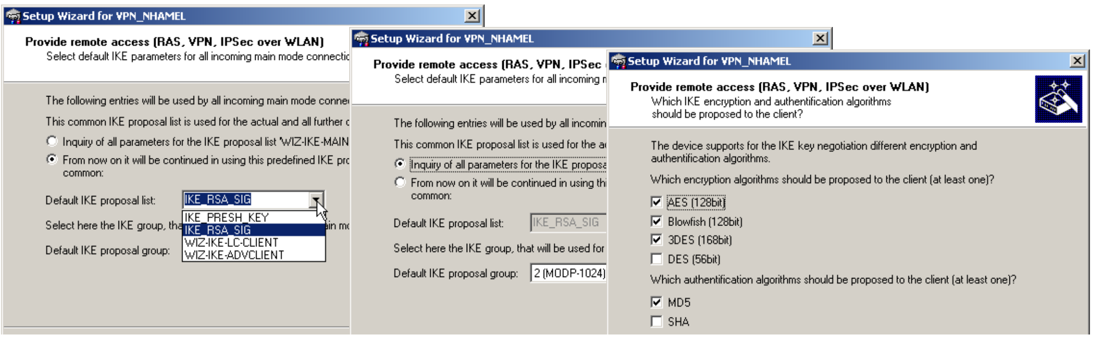
□ Nevertheless edit default IKE parameters for this and any future main mode connections.

Attention: Please take into account, that if you change these settings existing connections could no longer work!

Only in the case of a user-defined VPN client

② The configuration normally presents standard IKE parameters for incoming main mode connections in the standard IKE proposal list 'IKE_RSA_SIG'. If possible use the list of prepared IKE parameters.

③ If you wish to use different parameters for incoming main mode connections, you can adapt the standard IKE parameters to fit your requirements. You can either create a new list 'WIZ-IKE-MAIN-MODE' or you can select one of the existing IKE proposal lists as the new "Standard IKE proposal list". The list defined here will be used for all incoming main mode connections in the future. For a new IKE proposal list, you can select the encryption and authentication methods that are to be used by the client during the IKE negotiation.



Setup Wizard for VPN_NHAMEL

Provide remote access (RAS, VPN, IPSec over WLAN)
Select default IKE parameters for all incoming main mode connectio

The following entries will be used by all incoming main mode conne

This common IKE proposal list is used for the actual and all further c

○ Inquiry of all parameters for the IKE proposal list 'WIZ-IKE-MAIN
● From now on it will be continued in using this predefined IKE pro
common:

Default IKE proposal list: IKE_RSA_SIG

Select here the IKE group, tha

Default IKE proposal group:

Setup Wizard for VPN_NHAMEL

Provide remote access (RAS, VPN, IPSec
Select default IKE parameters for all incoming r

The following entries will be used by all incomin

This common IKE proposal list is used for the ac

● Inquiry of all parameters for the IKE proposa
○ From now on it will be continued in using thi
common:

Default IKE proposal list: IKE_RSA_SIG

Select here the IKE group, that will be used for

Default IKE proposal group: 2 (MODP-1024)

Setup Wizard for VPN_NHAMEL

Provide remote access (RAS, VPN, IPSec over WLAN)
Which IKE encryption and authentification algorithms
should be proposed to the client?

The device supports for the IKE key negotiation different encryption and authentification algorithms.

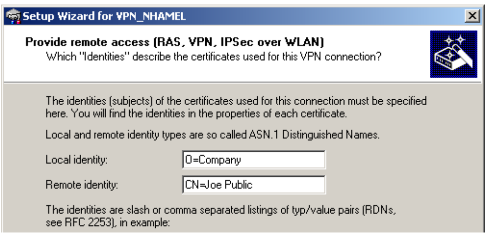
Which encryption algorithms should be proposed to the client (at least one)?

☑ AES (128bit)
☑ Blowfish (128bit)
☑ 3DES (168bit)
□ DES (56bit)

Which authentification algorithms should be proposed to the client (at least one)?

☑ MD5
□ SHA

④ Enter the identities contained in the certificates for the local and remote devices. Be sure to use the information from each certificate in full and in the right order: The ASN.1-Distinguished Names listed in Windows from top to bottom in the certificates must be entered into LANconfig from left to right.



Setup Wizard for VPN_NHAMEL

Provide remote access (RAS, VPN, IPSec over WLAN)
Which "Identities" describe the certificates used for this VPN connection?

The identities (subjects) of the certificates used for this connection must be specified here. You will find the identities in the properties of each certificate.

Local and remote identity types are so called ASN.1 Distinguished Names.

Local identity: O=Company

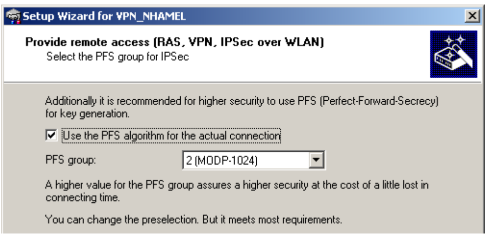
Remote identity: CN=Joe Public

The identities are slash or comma separated listings of typ/value pairs (RDNs, see RFC 2253), in example:

Microsoft Windows displays some values in the certificates with outdated abbreviations, such as 'S' instead of 'ST' for 'stateOrProvinceName', or 'G' instead of 'GN' for 'givenName'. In these cases make sure that you use the current abbreviations 'ST' and 'GN'.

The Telnet command `show vpn cert` displays the content of the device certificate in a LANCOM, including the entered Distinguished Names (DN) under "Subject". The Distinguished Names are displayed in reverse order here until LCOS 6.00 and in the usual order as of LCOS 6.10!

⑤ If available choose the optimized connection establishment with IKE and PFS group 2. Only choose group 5 as the PFS group if this is required by the client.



Setup Wizard for VPN_NHAMEL

Provide remote access (RAS, VPN, IPSec over WLAN)
Select the PFS group for IPSec

Additionally it is recommended for higher security to use PFS (Perfect-Forward-Secrecy) for key generation.

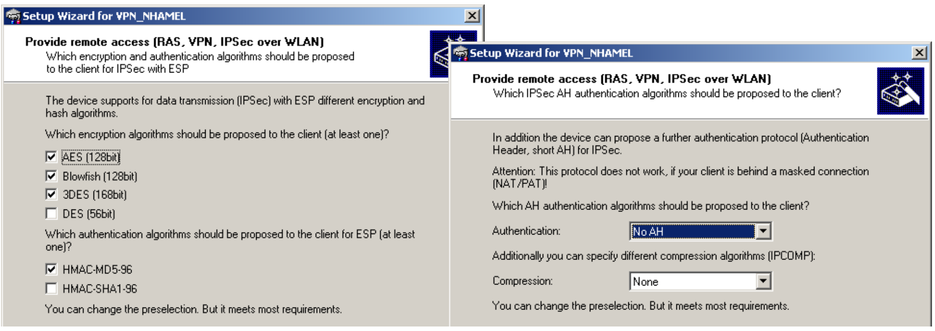
☑ Use the PFS algorithm for the actual connection

PFS group: 2 (MODP-1024)

A higher value for the PFS group assures a higher security at the cost of a little lost in connecting time.

You can change the preselection. But it meets most requirements.

⑥ The following dialogs define the encryption and authentication methods, the authentication header and the data compression that the client will use for the transfer of the payload data with IPSec. Use the preset values as much as possible as long as the client does not demand different settings.



Setup Wizard for VPN_NHAMEL

Provide remote access (RAS, VPN, IPSec over WLAN)
Which encryption and authentication algorithms should be proposed to the client for IPSec with ESP

The device supports for data transmission (IPSec) with ESP different encryption and hash algorithms.

Which encryption algorithms should be proposed to the client (at least one)?

☑ AES (128bit)
☑ Blowfish (128bit)
☑ 3DES (168bit)
☐ DES (56bit)

Which authentication algorithms should be proposed to the client for ESP (at least one)?

☑ HMAC-MD5-96
☐ HMAC-SHA1-96

You can change the preselection. But it meets most requirements.

Setup Wizard for VPN_NHAMEL

Provide remote access (RAS, VPN, IPSec over WLAN)
Which IPSec AH authentication algorithms should be proposed to the client?

In addition the device can propose a further authentication protocol (Authentication Header, short AH) for IPSec.

Attention: This protocol does not work, if your client is behind a masked connection (NAT/PAT)!

Which AH authentication algorithms should be proposed to the client?

Authentication: No AH

Additionally you can specify different compression algorithms (IPCOMP):

Compression: None

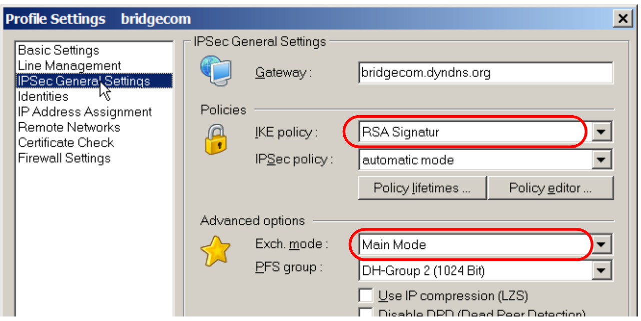
You can change the preselection. But it meets most requirements.

⑦ Enter the IP address of the client and for the address range that is to be accessible in the local network. If required, activate "NetBIOS routing".

10.6.15 Set up LANCOM Advanced VPN Client for certificate connections

To use the LANCOM Advanced VPN Client to dial-in to a LANCOM router, the appropriate profile settings must be adjusted to allow for the use of certificates.

① In the IPSec General Settings for the profile, set the IKE policy to 'RSA signature'.



Profile Settings bridgecom

IPSec General Settings

Gateway: bridgecom.dyndns.org

Policies

IKE policy: RSA Signatur

IPSec policy: automatic mode

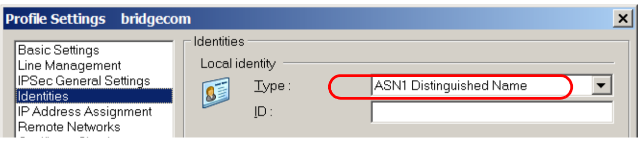
Advanced options

Exch. mode: Main Mode

PFS group: DH-Group 2 (1024 Bit)

☐ Use IP compression (LZS)
☐ Disable DPD (Dead Peer Detection)

② Switch the identity to 'ASN1 Distinguished Names'. The 'identity' can remain blank since this information is taken from the certificate.



Profile Settings bridgecom

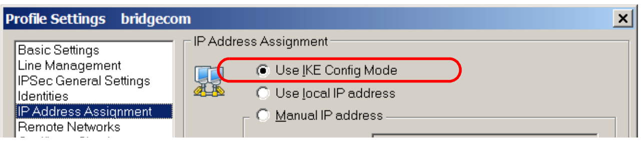
Identities

Local identity

Type: ASN1 Distinguished Name

ID:

③ For the IP address assignment use the 'IKE Config Mode'.

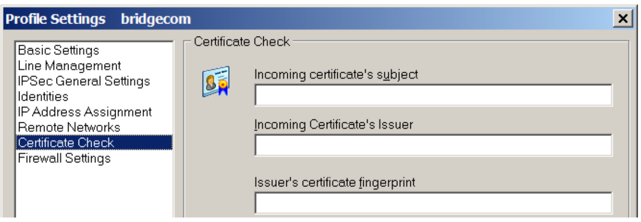


Profile Settings bridgecom

IP Address Assignment

● Use IKE Config Mode
○ Use local IP address
○ Manual IP address

④ For the Certificate Check you can optionally place a limitation on the certificates accepted by the LANCOM Advanced VPN Client. To do this, you define the user and/or the issuer of the incoming certificate and, if applicable, the associated "fingerprint".



Profile Settings bridgecom

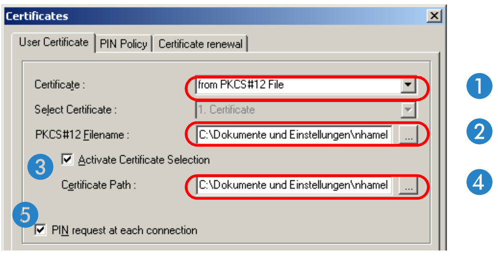
Certificate Check

Incoming certificate's subject

Incoming Certificate's Issuer

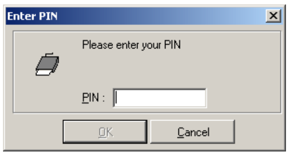
Issuer's certificate fingerprint

⑤ After storing the adapted connection profile, click on the menu item **Configuration** ▶ **Certificates** to open the settings for the User Certificate.



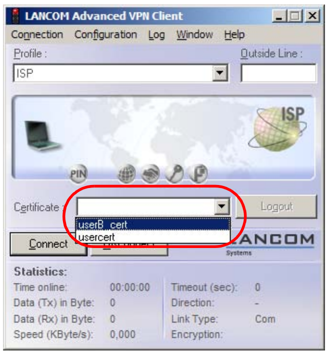
Certificate : from PKCS#12 File
Select Certificate : 1. Certificate
PKCS#12 Filename : C:\Dokumente und Einstellungen\nhamel
☑ Activate Certificate Selection
Certificate Path : C:\Dokumente und Einstellungen\nhamel
☑ PIN request at each connection

- □ Select the certificate type 'from PKCS#12 file' ❶ and set the required certificate file ❷.
- □ To work with various certificates, activate the option 'Certificate Selection' ❸ and enter the path for the folder where the certificate files are stored ❹.
- □ Define whether or not the PIN (password) has to be entered before connection establishment ❺. Alternatively, you can save the PIN in the LANCOM Advanced VPN Client under the menu item **Connection ▶ Enter PIN** .



Please enter your PIN
PIN :

- □ If Certificate Selection is activated, the certificate corresponding to the connection can be chosen from a list displayed in the main window of the LANCOM Advanced VPN Client, as befits the selected profile.



Profile : ISP
Outside Line :
Certificate : userB_cert / usercert

Statistics:
Time online: 00:00:00
Data (Tx) in Byte: 0
Data (Rx) in Byte: 0
Speed (KByte/s): 0,000
Timeout (sec): 0
Direction: -
Link Type: Com
Encryption:

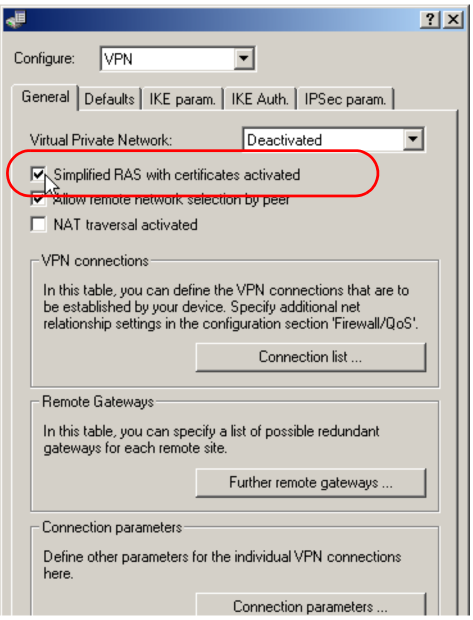
10.6.16 Simplified RAS with certificates

When dialling in, the identity of computers that use varying IP addresses is unknown at the initial stages of the IKE negotiation (Phase 1), so communication is facilitated by using default values for IKE proposal lists and IKE proposal groups. During negotiation, the identity is communicated and this is used to determine the parameters for phase 2 (IPSec proposal list and PFS group). For this to occur, every single user must be entered individually into the VPN router configuration.

With certificate-based RAS, the identity is communicated via the certificate. To avoid having to make individual user entries in the router configuration, common parameters for phase 2 can be defined for all users who are identified by certificate. All the user requires for simplified RAS is a valid certificate with a signature from the publisher of the root certificate in the device. Furthermore, the parameters used by the client during dial-in must agree with the default values in the VPN router.

Information about configuring the VPN client is available in the relevant documentation from the software manufacturer.

This function has to be activated to configure the simplified dial-in. The default parameters can be altered according to requirements.



Configure: VPN

Virtual Private Network: Deactivated

☑ Simplified RAS with certificates activated

☑ Allow remote network selection by peer

☐ NAT traversal activated

VPN connections

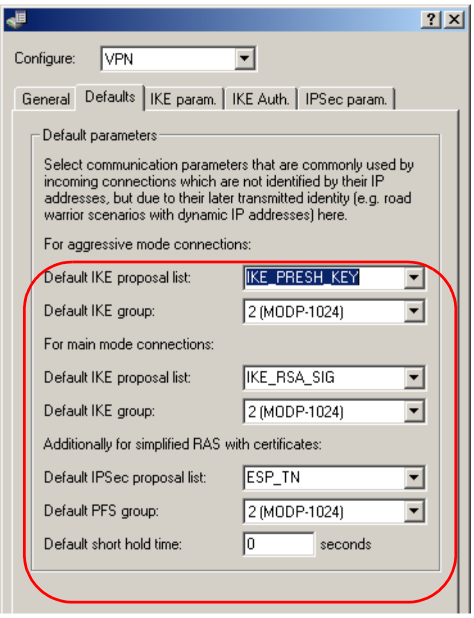
In this table, you can define the VPN connections that are to be established by your device. Specify additional net relationship settings in the configuration section 'Firewall/QoS'.

Remote Gateways

In this table, you can specify a list of possible redundant gateways for each remote site.

Connection parameters

Define other parameters for the individual VPN connections here.



Configure: VPN

Default parameters

Select communication parameters that are commonly used by incoming connections which are not identified by their IP addresses, but due to their later transmitted identity (e.g. road warrior scenarios with dynamic IP addresses) here.

For aggressive mode connections:

Default IKE proposal list: IKE_PRESH_KEY

Default IKE group: 2 (MODP-1024)

For main mode connections:

Default IKE proposal list: IKE_RSA_SIG

Default IKE group: 2 (MODP-1024)

Additionally for simplified RAS with certificates:

Default IPSec proposal list: ESP_TN

Default PFS group: 2 (MODP-1024)

Default short hold time: 0 seconds

LANconfig: VPN ▶ General and VPN ▶ General ▶ Defaults

WEBconfig: LCOS menu tree ▶ Setup ▶ VPN

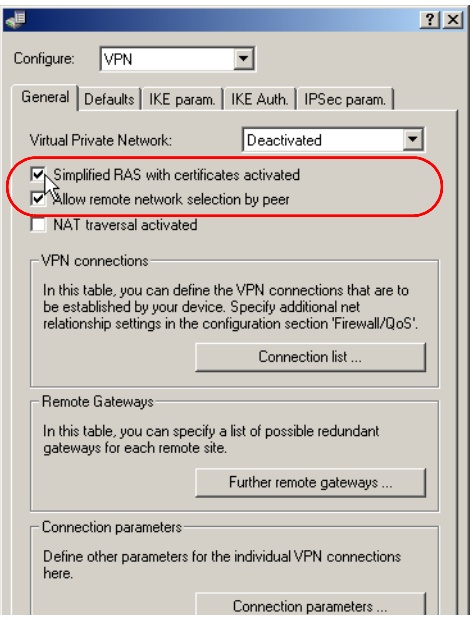
By activating the simplified RAS with certificates, **all** clients that have a valid certificate signed by the publisher of the device's root certificate can dial in to the corresponding network. No further configuration of the router is necessary! Unwanted dial-ins are then prevented exclusively by using a CRL and blocking the certificates there.

10.6.17 Simplified network connection with certificates – proadaptive VPN

In cases where large network infrastructures are coupled via VPN, it is advantageous for the costs and effort in configuring a new subnetwork to be limited to the local VPN router and that the central dial-in router configuration remains unchanged. In order to achieve this simplified network connection, the dial-in devices transmit their identity with the help of a digital certificate.

If simplified dial-in with certificates is activated for the LANCOM Router at the headquarters, then the remote routers can suggest a network to be used for the connection during the IKE negotiation in phase 2 This network is entered, for example, when setting up the VPN connection on the remote router. The LANCOM Router at the headquarters accepts the suggested network when the option 'Allow remote station to select the remote network' is activated. Moreover, the parameters used by the client during dial in must agree with the default values in the VPN router.

When configuring the dial-in remote stations, be sure to note that each remote station requests a specific network so that no network address conflicts arise.



Configure: VPN

Virtual Private Network: Deactivated

☑ Simplified RAS with certificates activated

☑ Allow remote network selection by peer

☐ NAT traversal activated

VPN connections

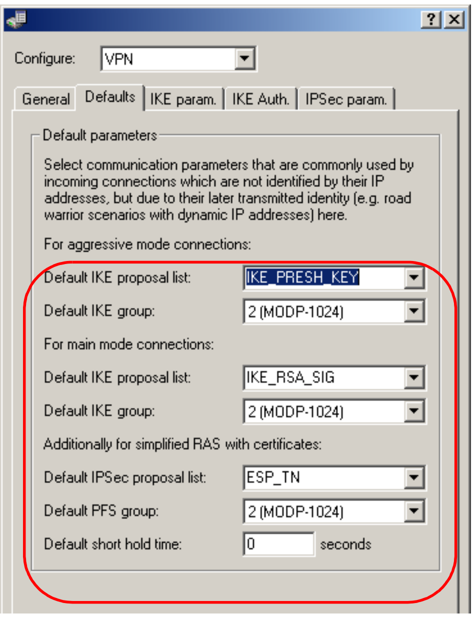
In this table, you can define the VPN connections that are to be established by your device. Specify additional net relationship settings in the configuration section 'Firewall/QoS'.

Remote Gateways

In this table, you can specify a list of possible redundant gateways for each remote site.

Connection parameters

Define other parameters for the individual VPN connections here.



Configure: VPN

Default parameters

Select communication parameters that are commonly used by incoming connections which are not identified by their IP addresses, but due to their later transmitted identity (e.g. road warrior scenarios with dynamic IP addresses) here.

For aggressive mode connections:

Default IKE proposal list: IKE_PRESH_KEY

Default IKE group: 2 (MODP-1024)

For main mode connections:

Default IKE proposal list: IKE_RSA_SIG

Default IKE group: 2 (MODP-1024)

Additionally for simplified RAS with certificates:

Default IPSec proposal list: ESP_TN

Default PFS group: 2 (MODP-1024)

Default short hold time: 0 seconds

LANconfig: VPN ▶ General and VPN ▶ General ▶ Defaults

WEBconfig: LCOS menu tree ▶ Setup ▶ VPN

By activating the simplified RAS dial in, **all** remote routers that have a valid certificate signed by the publisher of the device's root certificate can dial in to the corresponding network. No further configuration of the router is necessary! Unwanted dial-in connections are then prevented exclusively by blocking the certificates and using a CRL.
The simplified connection of networks with certificates is therefore limited to LANCOM Router models that support certificate revocation lists (CRL).

10.6.18 Request certificates using CERTREQ

During IPSec negotiations authenticated with the use of RSA signatures, some VPN gateways expect the remote station to request the certificates to be exchanged via a "certificate request" (CERTREQ). Among other things, this allows the gateway to select the certificate to be used providing that the gateway trusts more than one CA.

In order to establish a connection to these VPN gateways, the LANCOM VPN Router sends a corresponding CERTREQ when the connection is initiated. This is received by the publisher of the root certificate stored in the LANCOM.

10.6.19 Certificate revocation list - CRL

Certificates for VPN connections have a validity period by a start date and an end date. During this period, the certificate can be used to establish a VPN connection. Should an employee leave the company, then it should be possible for certificates, for example that were used for mobile VPN access, to be declared as invalid. This prevents continued access to the company network and does not require any changes to the VPN router configuration.

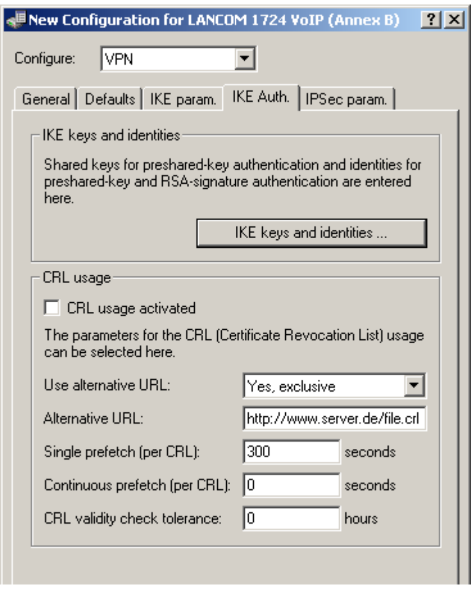
The certificate is physically located with the ex-employee and cannot be changed, which is why a certificate revocation list is of use. Certificates which are no longer valid are entered into the CRL, which are supported by Microsoft CA and OpenSSL, for example. The CRL is available from a suitable server. The URL to be used by a router to download the CRL into its own memory is entered into the root certificate of the VPN router and/or into the configuration of the device itself.

The CRL is renewed by the CA on a regular basis, enabling changes in the CRL, such as withdrawn certificates, to be recognized by the VPN routers in good time. During the setup at the CA, a schedule is defined for the regular updating of the CRL. After an update to the CRL and its storage to the server (manual or automatic), the VPN router then has to update its infomation, too. To do this, the router reads out the validity period of the CRL and, briefly before expiry, attempts to load a current version. Alternatively, a regular update which depends on the validity period of the CRL can be set in the LANCOM.

When a connection is being established, the VPN router checks if the remote station's certificate is in the current CRL. Connections to remote stations without a valid certificate are rejected.

Configuring the CRL function

Configuration of the CRL function involves the definition of the path to the CRL and additional parameters such as the update interval.



New Configuration for LANCOM 1724 VoIP (Annex B)

Configure: VPN

IKE keys and identities

Shared keys for preshared-key authentication and identities for preshared-key and RSA-signature authentication are entered here.

CRL usage

□ CRL usage activated

The parameters for the CRL (Certificate Revocation List) usage can be selected here.

Use alternative URL: Yes, exclusive

Alternative URL: http://www.server.de/file.crl

Single prefetch (per CRL): 300 seconds

Continuous prefetch (per CRL): 0 seconds

CRL validity check tolerance: 0 hours

LANconfig: VPN ▶ IKE Auth.

WEBconfig: LCOS menu tree ▶ Setup ▶ VPN ▶ Certificates-and-Keys ▶ CRLs

- **CRL function [Default: Off]**
  - □ Enabled: During the certificate check, the CRL (if available) will be considered as well.

If this option is activated but no valid CRL is available (e.g. if the server can't be reached), then all connections will be rejected and existing connections will be interrupted.

- **Use alternative URL [Default: No**
  - □ No: Only the URL defined in the root certificate is to be used.
  - □ Yes, always: The alternative URL will always be used even if a URL is entered into the root certificate.
  - □ Yes, alternative: The alternative URL will only be used if there is no URL entered into the root certificate.
- **Alternative URL**
  - □ This is an alternative URL which can be used to retrieve a CRL.
- **Single prefetch [Default: 300 seconds]**
  - □ The point in time prior to expiry of the CRL when the new CRL can be loaded. This value is increased by a random value to prevent server overload from multiple simultaneous queries. Once within this time frame, any coinciding regular planned updates will be stopped.

If the first attempt to load the CRL fails, new attempts are made at regular short intervals.

- **Continous prefetch [Default: 0 seconds]**
  - □ The time period after which periodic attempts are made to retreive a new CRL. Useful for the early retreival of CRLs published at irregular intervals. The entry '0' disables regular retreival.

If with regular updates the CRL cannot be retreived, no further attempts will be started until the next regular attempt.

- **Validity tolerance**
  - □ Even after expiry of the CRL, certificate-based connections will continue to be accepted for the period defined here. This tolerance period can prevent the unintentional rejection or interruption of connections if the CRL server should be temporarily unavailable.

Within the time period defined here, even certificates in the CRL which have expired can still be used to maintain or establish a connection.

CRL status display in LANmonitor

Information about the validity period and the publisher of the current CRL in the LANCOM can be inspected in LANmonitor.

10.6.20 Diagnosis of VPN certificate connections

If the VPN connection establishment does not work as desired, then entering the following commands at the LANCOM console can provide useful information.

- `trace + vpn-status`

  Displays a trace of the current VPN connections.
- `show vpn long`

  Displays the contents of the VPN configuration, including the entered Distinguished Names (DN).
- `show vpn ca`

  Displays the content of the root certificate.
- `show vpn cert`

  Displays the content of the device certificate.

The Distinguished Names are displayed in reverse order here until LCOS 6.00 and in the usual order as of LCOS 6.10!

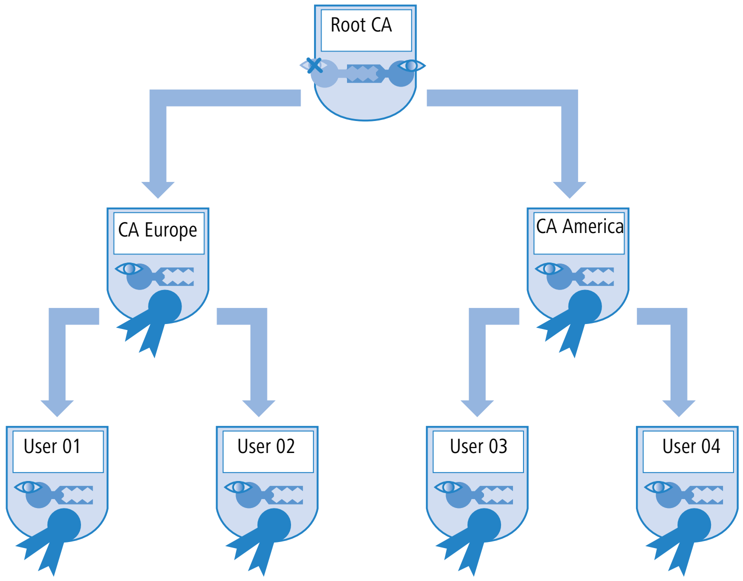
10.7 Multi-level certificates for SSL/TLS

New with LCOS 7.6:

- Multi-level certificates for SSL/TLS

10.7.1 Introduction

Larger or geographically dispersed organizations often make use of multi-level certificate hierarchies that rely on one or more intermediate CAs to issue certificates. The interim CAs themselves are certified by the Root CA.



To authenticate final certificates, it must be possible to check the entire certificate hierarchy.

10.7.2 SSL/TLS with multi-level certificates

For applications based on SSL/TLS (e. g. EAP/802.1x, HTTPS or RADSEC), the SSL (server) certificate together with the private key and intermediate level CA certificate(s) are loaded into the device as a PKCS#12 container.

The remote devices establishing a connection only have to send their own device certificates to the LANCOM. The certificate chain is checked for validity in the LANCOM.

10.7.3 VPN with multi-level certificates

For the certificate-based establishment of VPN connections, the following are stored to the file system in the LANCOM: A private key, a device certificate, and the CA certificate. With single-layer certificate solutions this can be handled with the individual files or with a PKCS#12 file. After uploading and entering the password, a container is separated into the three components indicated above.

In the case of a multi-level certificate hierarchy, however, a PKCS#12 container has to be used that includes the CA certificates from all levels in the certificate chain. After uploading and entering the password, the private key, the device certificate and the certificate from the next CA "above" the LANCOM are unpacked—the other certificates remain in the PKCS#12 container. The unpacked certificates and the certificates from the container are imported when the VPN configuration is updated. A remote station establishing a VPN connection transfers its own device certificate only and not the entire chain. The LANCOM then checks this certificate against the hierarchy available to it.

The certificate structures in the two stations must match to one another, i.e. the hierarchy in the VPN device making the request should not demand certificates that are not included in the other VPN device's hierarchy.

10.8 Certificate enrollment via SCEP

An increasing number of certificate-based VPN connections are being used to provide secure communications via public networks. The high levels of security provided by certificates comes at the price of significantly higher levels of effort in the administration and distribution of certificates. Most of this effort arises at branch offices or home offices within a geographically dispersed network structure.

A LANCOM VPN Router router requires the following components to establish a certificate-based VPN connection from a remote site to network at headquarters:

- The Root CA's certificate with the CA's public key. The headquarters also requires a certificate issued by the same CA.
- The device's own certificate with its own public key. This certificate is signed with the CA's private key and serves identity confirmation.
- Own private key.

The current version of LCOS supports only a public key infrastructure (PKI) with a root CA.

In the case of a conventionally structured VPN with certificates, the keys and certificates have to be loaded into each device manually and exchanged before they expire. The Simple Certificate Enrollment Protocol (SCEP) enables a secure and automatic distribution of certificates via a suitable server, so reducing the effort of roll-out and maintaining certificate-based network structures. There is no need for the key pair for the device to be generated by an external application and subsequently transferred to the device. Instead, the key pair is generated directly by the LANCOM VPN Router itself; the private portion of the key never has to leave the device, which results in a significant gain in security. A LANCOM VPN Router can automatically retrieve the CA root certificate and its own certificate from a central location.

10.8.1 SCEP server and SCEP client

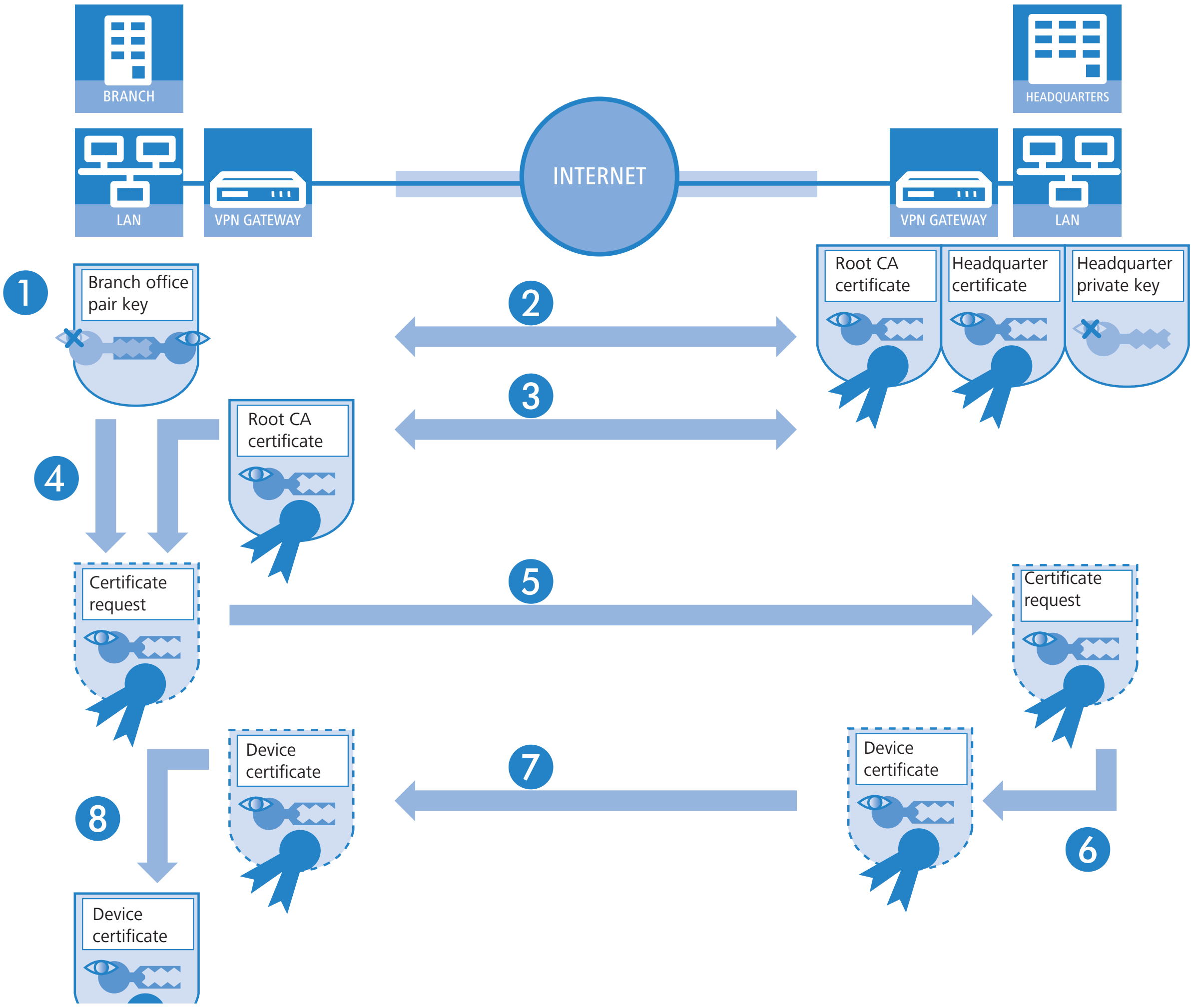
Provisioning and administration of the certificates is handled by an SCEP server that fulfills the usual function of a Certificate Authority (CA) as well as the SCEP functions. This server can, for example, be implemented as a Windows 2003 Server CA by using a special plug-in (mscep.dll). There are also a number of other CA solutions which work with SCEP, such as the OpenSource solution OpenCA (www.openca.org).

The SCEP extension such as with mscep.dll creates an additional instance on the server and processes requests from SCEP clients for forwarding to the actual CA. This instance is referred to as the Registration Authority (RA).

The VPN devices (i.e. the LANCOM VPN Router) are SCEP clients that attempt to automatically retrieve the necessary certificates from the central server. Also generally required by the SCEP procedure are the RA (Registration Authority) certificates as signed by the CA. For VPN operations the LANCOM VPN Routers mainly require valid system certificates (device certificates). Any other certificates which may be in use only apply to the SCEP procedure.

10.8.2 Distributing certificates

In brief, the procedure for distributing certificates via SCEP is as follows:



① Generate key pair in the LANCOM VPN Router.

A key pair is generated in the LANCOM VPN Router. The public part of this key pair is later sent together with the request to the SCEP server. The private key remains in the SCEP client (LANCOM VPN Router). The fact that the private key never has to leave the device is a major security gain over manual certificate distribution, for example with PKCS#12 containers.

② Retrieve CA and RA certificates.

For communication with the RA/CA, the appropriate RA and CA certificates must be available in the LANCOM VPN Router. To ensure that CA certificates retrieved via SCEP do genuinely originate from the CA, an automated check can be carried out with the use of a fingerprint which is defined in advance. SCEP itself has no mechanism for clients to conduct automated authentication of CA certificates. If the administrator of the LANCOM VPN Router does not have direct access to the CA then the fingerprint can be checked manually, for example with a telephone call to the CA admin.

③ Generate and encrypt the request for a device certificate.

To place a request for a system or device certificate, the SCEP client collects all of the configured information such as the identity of the requester device and, if applicable, the "challenge phrase" or password for automatic request processing by the SCEP server. This request is signed with the private key.

④ Send the request to the SCEP.

The SCEP client then sends the request along with its public key to the SCEP server.

⑤ Check the certificate request on the SCEP server and issue the device certificate.

The SCEP server can decrypt the request and subsequently issues a system or device certificate to the requester. SCEP has two different methods for request processing:

- Automatic processing requires the requester's authenticity to be assured by means of the challenge phrase. The challenge phrase can, for example, be generated automatically by a Windows CA server using mscep.dll. The phrase is valid for one hour. If the challenge phrase submitted with the certificate request agrees with the valid value, the system certificate is issued automatically.
- For manual processing, the SCEP server puts the certificate request "on hold" until the acceptance or rejection has been received from the CA administrator. While waiting, the SCEP client regularly checks with the SCEP server to see if the certificate has been issued yet.

⑥ Retrieve device certificate from the SCEP server

Once the certificate has been issued, the client's regular polling informs it that the certificate is ready for retrieval.

⑦ Check the device certificate and present it for VPN operation

10.8.3 Configuring SCEP

To configure SCEP, global parameters are defined for SCEP operations and for the CAs where the device certificates are to be retrieved.

In addition to the configuration of the SCEP parameters, it may be necessary to adapt the VPN configurations.

WEBconfig: LCOS menu tree ▶ Setup ▶ VPN ▶ Certificates-and-Keys ▶ SCEP

Global SCEP parameters

- **Active**

  Switches SCEP on or off.

  - Values: Yes, No
  - Default: No

- **Retry-After-Error-Interval**

  Interval in seconds between retries after errors of any type.

  - Default: 22

- **Check-Pending-Requests-Interval**

  Interval in seconds for checks on outstanding certificate requests.

  - Default: 101

- **Device-Certificate-Update-Before**

  Preparation time in days for the timely request for new system certificates (device certificates).

- Default: 2

- **CA-Certificate-Update-Before**

  Preparation time in days for the timely retrieval of new RA/CA certificates.

  - Default: 1

Actions

- **Reinit**

  Starts the manual reinitialization of the SCEP parameters. As with the standard SCEP initialization, the necessary RA and CA certificates are retrieved from the CA and stored within the LANCOM Router's file system so that they are **not yet** ready for use in VPN operations.

  - If the available system certificate fits to the retrieved CA certificate, then the system certificate, CA certificate and the device's private key can be used for VPN operations.
  - If the existing system certificates **do not** fit to the retrieved CA certificate, then the next step is for the SCEP server to submit a new certificate request. Only once a new system certificate that fits to the retrieved CA certificate has been issued and retrieved can the system certificate, CA certificate and the device's private key can be used for VPN operations.

- **Update**

  Manually triggers a request for a new system certificate, irrespective of the remaining period of validity. A new key pair is generated at the same time.

- **Clear-SCEP-Filesystem**

  Starts a clean-up of the SCEP file system.

  - Deleted are: RA certificates, pending certificate requests, new and inactive CA certificates, new and inactive private keys.
  - Retained are: System certificates currently in use for VPN operations, associated private keys, and the CA certificates currently in use for VPN operations.

Configuring the CAs

- **Name**

  Configuration name of the CA.

- **URL**

  The CA's URL.

- **DN**

  Distinguished name of the device. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration.

- **Enc-Alg**

  This algorithm encrypts the payload of the certificate request.

  - Values: DES, 3-DES, Blowfish.
  - Default: DES.

- **Identifier**

  CA identifier (as required by some web server to identify the CA).

- **RA-Autoapprove**

  Some CAs provide the option of using an earlier certificate issued by this CA as proof of authenticity for future requests. This option defines whether an existing system certificate should be used to sign new requests.

  - Values: Yes, No.
  - Default: No.

- **CA-Signature-Algorithm**

  The certificate request is signed with this algorithm.

  - Values: MD5, SHA1.
  - Default: MD5.

- **CA-Fingerprint-Algorithm**

  Algorithm for signing the fingerprint. This determines whether the CA certificate is to be checked by means of fingerprint, and which algorithm is used for this. The CA fingerprint has to agree with the checksum which results when this algorithm is applied.

  - Values: Off, MD5, SHA1.
  - Default: Off.
- **CA-Fingerprint**

  The authenticity of a received CA certificate can be checked by means of the the checksum (fingerprint) entered here (corresponding to the set CA fingerprint algorithm).

Configuring the system certificates

- **Name**

  The certificate's configuration name.
- **CADN**

  Distinguished name of the CA. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration.
- **Subject**

  Distinguished name of the subject of the requester.
- **ChallengePwd**

  Password (for the automatic issue of device certificates on the SCEP server).
- **SubjectAltName**

  Further information about the requester, e.g. domain or IP address.
- **KeyUsage**

  Any comma-separated combination of:

  - digitalSignature
  - nonRepudiation
  - keyEncipherment
  - dataEncipherment
  - keyAgreement
  - keyCertSign
  - cRLSign
  - encipherOnly
  - decipherOnly
  - critical (possible but not recommended)
- **Extended Key Usage**

  Any comma-separated combination of:

  - critical
  - serverAuth
  - clientAuth
  - codeSigning
  - emailProtection
  - timeStamping
  - msCodeInd
  - msCodeCom
  - msCTLSign
  - msSGC
  - msEFS
  - nsSGC
  - 1.3.6.1.5.5.7.3.18 für WLAN-Controller
  - 1.3.6.1.5.5.7.3.19 für Access Points im Managed-Modus

- **Device-Certificate-Keylength**
  The length of the key to be generated for the device itself.
- **Application**
  Shows the application of the registered certificates. It will be asked for the registered certificates only for the corresponding application.

10.9 NAT Traversal (NAT-T)

The insufficient number of publicly valid IP addresses has lead to the development of procedures such as IP masquerading or NAT (Network Address Translation), where a whole local network is masked by a single, publicly valid IP address. In this way, all clients in a LAN use the same IP address to exchange data with public networks such as the Internet. The assignment of the incoming and outgoing data packets to the different participants in the network is ensured by connecting the internal IP addresses to corresponding port numbers.

This process has proven its worth in the last few years and has since become the standard in almost all Internet routers. However, new difficulties arise when the hidden data packets are processed using VPN. As data connections over VPN are highly secured, mechanisms such as authentication and encryption are of great importance here.

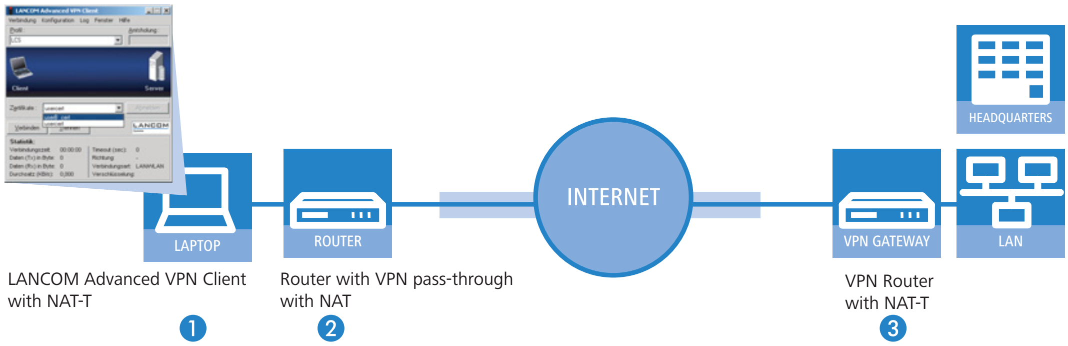
Converting internal IP addresses to the gateway's central, publicly valid IP address and converting source and target ports can lead to problems in many applications, for example where the UDP port 500 that is usually used during the IKE negotiation has been changed and the IKE can no longer be successfully completed as a result. The address change using NAT is therefore assessed by a VPN gateway as a security-critical data packet change, the VPN negotiation fails and no connection is made. In fact these problems occur, for example, when you dial in using some UMTS mobile telephone networks where the network operator's servers do not support the address conversion in combination with IPSec-based VPNs.

So you can successfully create a VPN connection even in such cases, NAT-T (NAT Traversal) provides a process that can overcome the problems described when handling data packets with changed addresses.

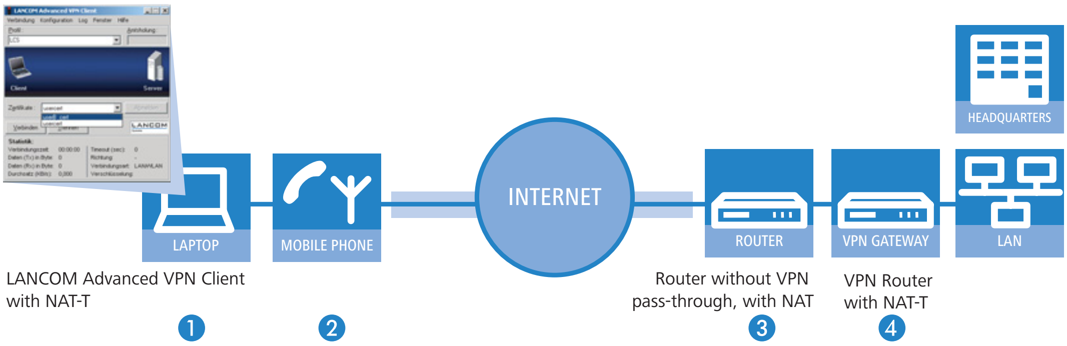
> NAT-T can only be used with VPN connections that use ESP (Encapsulating Security Payload) for authentication. Unlike AH (Authentication Header), ESP does not consider the IP header of the data packets when determining the hash value for authentication. The hash value calculated by the receiver is therefore also equivalent to the hash value entered in the packets.
>
> If the VPN uses AH for authentication, then in principle no connection can be established over sections with Network Access Translation, as the AH hash values similarly change when the IP addresses change, and the recipient would classify the data packets as untrustworthy.

The NAT Traversal process eliminates the problems that occur when establishing a VPN connection at the end points of the VPN tunnel. The following scenarios can be distinguished from one another:

- A member of the field staff uses a LANCOM Advanced VPN Client to dial into the company VPN router **without** "VPN pass-through" support (i.e. IPSec masking) but **with** Network Address Translation.

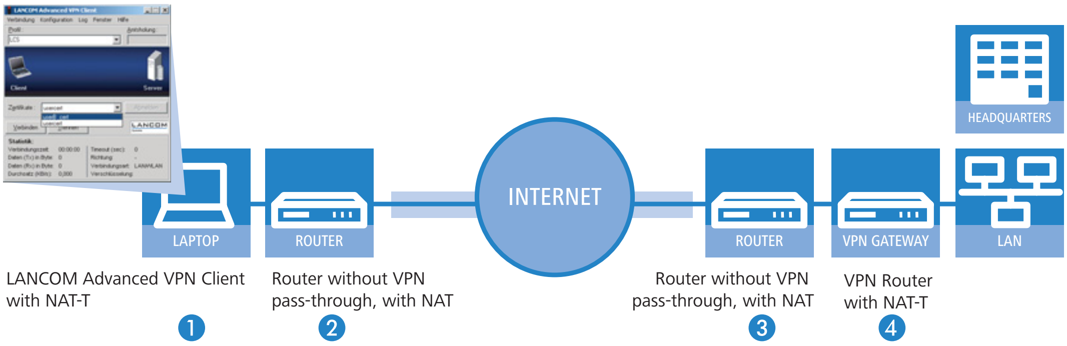

LAPTOP
ROUTER
INTERNET
VPN GATEWAY
HEADQUARTERS
LAN
LANCOM Advanced VPN Client with NAT-T
①
Router with VPN pass-through with NAT
②
VPN Router with NAT-T
③

  - □ Both tunnel end points LANCOM Advanced VPN Client ① and VPN router ③ support NAT-T and can therefore also establish a VPN connection through the intermediary router.
  - □ Router ② as a NAT device between the VPN end points performs straight forward NAT address conversion.
    This router does not require NAT but firewall ports 500 and 4500 must be open in order to enable NAT communication between both tunnel end points.
- In the second example application, the travelling field worker dials in to the network at the headquarters with his notebook ① and a mobile telephone or modem ②.



- □ At the headquarters, the VPN router ❹ is located behind a terminating router ❸, which only provides Internet access with the address conversion.
- □ Both tunnel end points LANCOM Advanced VPN Client ❶ and VPN router ❹ support NAT-T and can therefore establish a VPN connection, as in the first example.
- □ In the terminating router ❷, the firewall ports 500 and 4500 have to be activated, as does port forwarding.

■ In both of these cases, the two ends of the connection are the straight-forward NAT routers ❷ and ❸. Teh VPN connection is established between the LANCOM Advanced VPN Client ❶ and VPN router ❹.


LAPTOP
ROUTER
INTERNET
ROUTER
VPN GATEWAY
LAN
HEADQUARTERS
LANCOM Advanced VPN Client with NAT-T
Router without VPN pass-through, with NAT
Router without VPN pass-through, with NAT
VPN Router with NAT-T
❶
❷
❸
❹

The two routers ❷ and ❸ have to permit the NAT-T connection between the two tunnel endpoints in that the firewall ports 500 and 4500 are activated, and port forwarding has to be activated in the terminating router at the headquarters, as well.

To enable this process, both ends of the VPN connection have to work with NAT-T. The process of establishing the VPN connection (reduced to the NAT-T-relevant operations) appears as follows:

① At an early stage of the IKE negotiation, there is a check to see if both ends of the VPN connection are NAT-T-compatible.

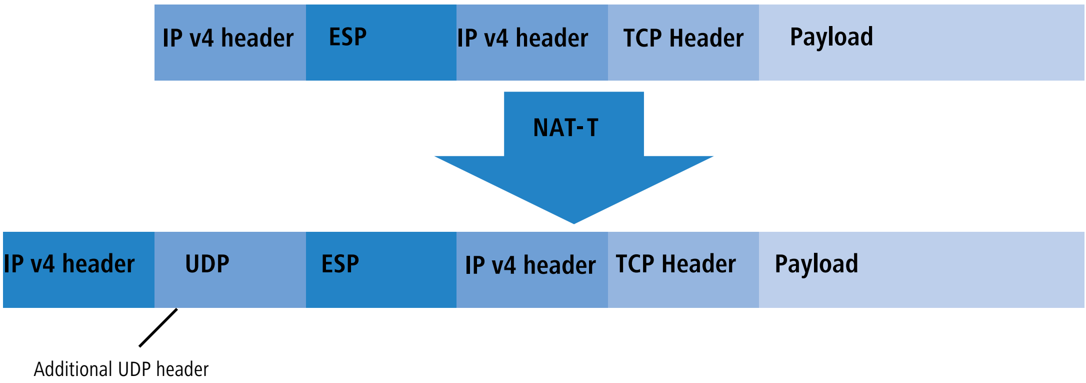
② In the second step, there is a check to see if the address is converted to NAT on the section between the two tunnel end points, and at what point in the connection the NAT devices are located.

③ To deal with problems with ports that may have changed, all negotiation and data packets are subsequently sent only via UDP port 4500 when a NAT device has been detected.

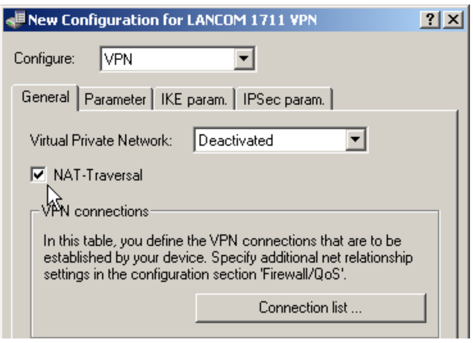
ⓘ If the LANCOM functions as a NAT router between the VPN end points, ensure that UDP ports 500 and 4500 are activated in the firewall when you use NAT-T! This port is activated automatically if you use the firewall assistant in LANconfig.

If the VPN connections are first created on devices with LCOS version 5.20 or above using the VPN assistant and later with the firewall assistant from LANconfig, then no additional firewall settings are required for the NAT router.

④ In the diagram below, the data packets are packed again into UDP packets (UDP encapsulation) and are also sent using port 4500. As a result of this additional encapsulation, changing the IP addresses for the VPN negotiation is no longer relevant and the VPN tunnel can be established without any problems. At the other end of the connection, the IP data is released again by the additional UDP header and can be processed by the router without further action.



In order to use this process, both ends of the VPN connection (such as the WLANmonitor and a LANCOM router) have to use NAT-T.


New Configuration for LANCOM 1711 VPN

Configure: VPN

General | Parameter | IKE param. | IPSec param.

Virtual Private Network: Deactivated

☑ NAT-Traversal

VPN connections

In this table, you define the VPN connections that are to be established by your device. Specify additional net relationship settings in the configuration section 'Firewall/QoS'.

LANconfig: VPN ▶ General

WEBconfig: LCOS menu tree ▶ Setup ▶ VPN ▶ NAT-T Operating

10.10 Extended Authentication Protocol (XAUTH)

10.10.1 Introduction

RADIUS servers are often used to authenticate users for remote sites dialing-in over WAN connections (such as via PPP). Over time, conventional WAN connections increasingly gave way to secure (encrypted) and more cost-effective VPN connections. However, the structure of VPN connections over IPSec with IKE does not permit unidirectional authentication of users by RADIUS or similar technologies.

The Extended Authentication Protocol (XAUTH) provides the ability to extend authentication in the negotiation of IPSec connections by an additional level in which user data can be authenticated. An additional authentication with XAUTH user name and XAUTH password is performed between the first and second IKE negotiation phases. This authentication is protected by the encryption negotiated in advance. A RADIUS server can be used for this authentication, enabling existing RADIUS databases to continue to be used in the migration of dial-in clients to use VPN connections. Alternatively, authentication can use an internal user table of the device.

In order make XAUTH particularly secure, dial-in via RSA-SIG (certificates) was to be used instead of the preshared key method (PSK) whenever possible. Here it is important to ensure that the VPN gateway accepts only the certificate of the correct remote site (and not all certificates issued by the same CA).

10.10.2 XAUTH in LCOS

In the LANCOM, the XAUTH protocol uses entries in the PPP table for remote site authentication. Use of the entries in the PPP table is dependent on which direction the connection is established, i.e. on the XAUTH operating mode:

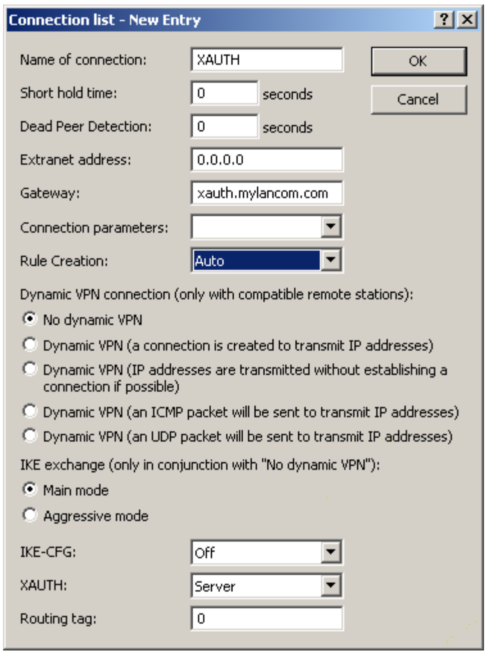
XAUTH operating mode	Server	Client
XAUTH user name	Remote site from the PPP table. The PPP-table entry is selected for which the PPP remote site corresponds to the transferred XAUTH user name. The PPP remote site must also match the VPN remote site used.	User name from the PPP table. The entry selected from the PPP table is that for which the PPP remote site corresponds to the VPN remote site used.
XAUTH password	Password from the PPP table.	Password from the PPP table.

In LCOS version 7.60 in XAUTH operating mode, the XAUTH user name has to agree with the name of the VPN remote site. For this reason only one user can be authenticated by XAUTH for each VPN remote site. Authentication by RADIUS server is not available with LCOS 7.60.

10.10.3 Configuring XAUTH

The application of the XAUTH protocol is set up separately for each VPN remote site. Only the XAUTH operating mode is specified.

LANconfig: VPN ▶ General ▶ Connection list



Connection list - New Entry

Name of connection: XAUTH

Short hold time: 0 seconds

Dead Peer Detection: 0 seconds

Extranet address: 0.0.0.0

Gateway: xauth.mylancom.com

Connection parameters:

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

IKE-CFG: Off

XAUTH: Server

Routing tag: 0

WEBconfig: Setup ▶ VPN ▶ VPN peers

- **XAUTH**

  Enables the use of XAUTH for the VPN remote site selected.

  Possible values:

  - Client: In the XAUTH client operating mode, the device starts the initial phase of IKE negotiation (Main mode or Aggressive mode) and then waits for the authentication request from the XAUTH server. The XAUTH client responds to this request with the user name and password from the PPP table entry in which the PPP remote site corresponds to the VPN remote site defined here. There must therefore be a PPP remote site of the same name for the VPN remote site. The user name defined in the PPP table normally differs from the remote site name.
  - Server: In the XAUTH server operating mode, the device (after successful negotiation of the initial IKE negotiation) starts authentication with a request to the XAUTH client, which then responds with its user name and password. The XAUTH server searches for the user name in the PPP table and, if a match is found, it checks the password. The user name for this entry in the PPP table is not used.
  - Off: No XAUTH authentication is performed for the connection to this remote site.

  Default:

  - Off

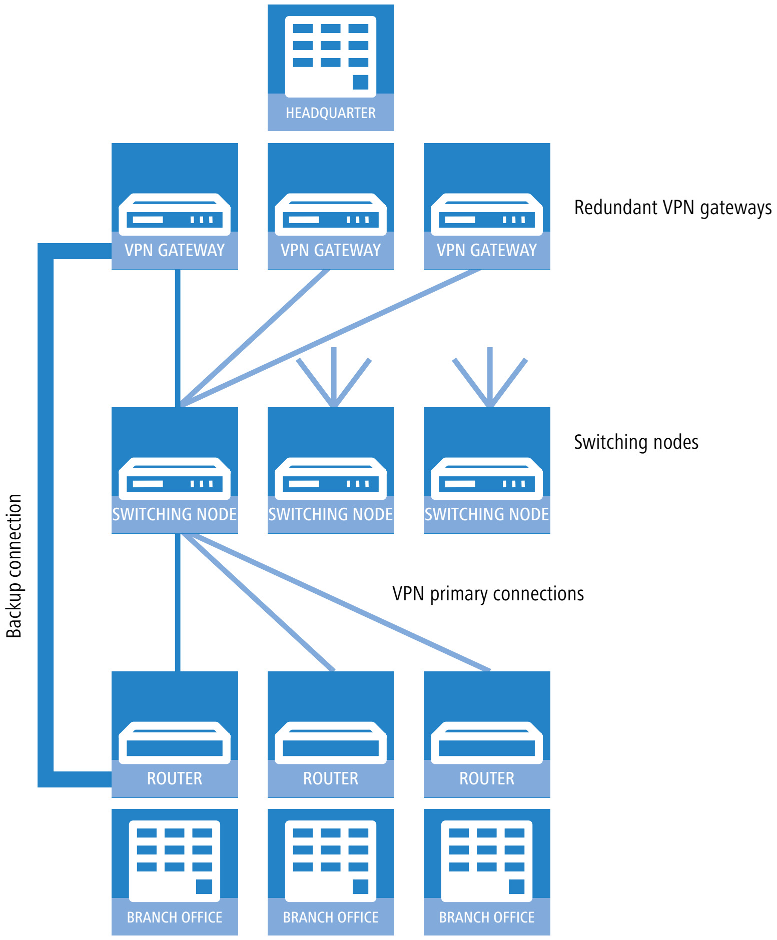
If XAUTH authentication is enabled for a VPN remote site, the IKE-CFG option must be set to the same value.

10.11 Backup via alternative VPN connection

10.11.1 Introduction

The subject of backup connections is vital to the availability of business-critical applications, especially at distributed sites with several branch offices connected via VPN to the main office. The subject of backups is easy to resolve where routers at the branch offices relate directly to redundant routers at the main office: If a router at the main office can be not reached over the Internet, the branch office simply dials-in to another router at the main office. RIP ensures that the devices can communicate over the available routes.

However, in very large networks branch offices are rarely connected directly to the main office. Instead, several sites initially merge at switching nodes, and these in turn are connected to the main office. If the branch office temporarily loses contact to the switching node, the branch office could establish a direct backup connection to main office.



However, this only works via an ISDN connection, often an undesirable solution due to the costs and limited bandwidth. A parallel backup connection directly over VPN does not achieve the objective for the following reasons:

- Only the switching nodes are defined as VPN remote sites in the main office – all routes to the branch offices pass through these switching nodes. If a branch office attempts to establish a direct connection to the main office, the attempt is rejected. And even if this connection were successful, the routes to the branch offices via the switching nodes remain in place at the main office because the switching node is, from the viewpoint of the main office, still accessible.
- The switching node knows nothing about any potential direct connection from branch office to main office. It therefore cannot access the destinations in the network at the branch office by detouring via the main office.
- Both the network of the switching node and the network of the branch office are accessible from the main office via the standard VPN connection. However, a direct VPN connection of the branch office to the main office only provides access to the branch-office network. It is because of these different characteristics that the router at the main office cannot accept the direct connection as a backup for the standard connection.
- The branch office can no longer establish the standard connection to the switching node because the principle of unambiguousness in IPsec rules does not permit a second connection with the same set of rules. Along with the specifications on encryption, IPSec rules also contain "network relationships", i.e. the IP addresses of the networks at both ends of the connection. These network relationships may only appear once in the VPN rule set. For a backup, however, two rules would have to exist for the same network relationship – once for the backup connection and once for the newly established primary connection.

10.11.2 Backup-capable network infrastructure

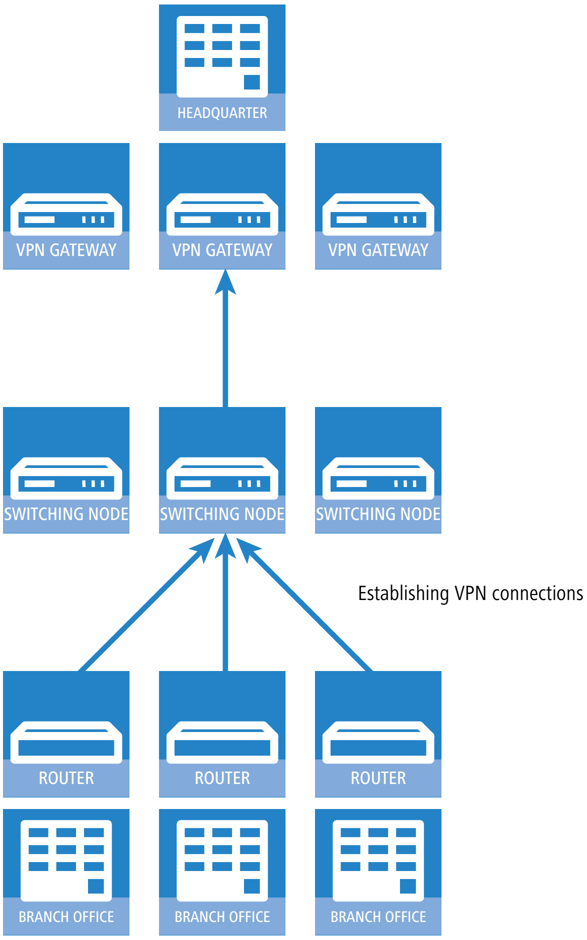
In order to also build up an operational backup solution for these applications, the points described in the following sections must be satisfied.

Basic prerequisites

The basic prerequisite for the backup function described here are; the configuration of a "Dynamic VPN" connection between branch offices and switching nodes; and the functions “Simplified RAS with certificates“ and “Allow remote site to select the remote network“ must be enabled in the VPN gateways at the main office.

Hierarchy for establishing VPN connections

In order for branch offices to connect to the network at the main office for backup purposes, a defined hierarchy must be observed when establishing the connection. Connections are only established from the "lower" to the "upper" networks, i.e. from the branch office to the switching node, from the switching node to the main office.



Thus connections only have to be accepted passively at the main office. The switching nodes also accept the branch office connections passively, but establish the connections to the main office actively. This hierarchy is a prerequisite for the later definition of VPN rules.

Network definitions

The branch offices establish network relationships with the switching nodes and with the main office - this must be allowed by the appropriate rules. In addition, either all conceivable network relationships must be stored individually or the networks have to be defined such that all required network relationships can be allowed with a single rule. This is possible if, for example, the IP addresses in the networks have the following structure:

- Central network 10.1.1.0/255.255.255.0
- Switching nodes 10.x.1.0/255.255.255.0
- Branch offices 10.x.y.0/255.255.255.0

Using the following VPN rule in the VPN gateways at the main office permits all required network relationships, i. e. all remote sites from the 10.x... range of addresses can establish connections to all gateways:

- Source 10.0.0.0/255.0.0.0
- Destination 10.0.0.0/255.0.0.0

Because branch offices communicate with the main office via the intermediate level of the switching nodes, corresponding VPN rules must also be created in the switching nodes. If communication with other sub-nodes and branch offices is also to be made possible, all of the required network relationships are permitted with the following VPN rule in the switching nodes:

- Source 10.x.0.0/255.255.0.0
- Destination 10.0.0.0/255.0.0.0

Routing information

During normal operation, the routes from main office to individual branch offices run via the switching nodes. These routes must be adapted for backup situations. For this adaptation to be performed automatically, "Simplified RAS with certificates" is enabled in the VPN gateways at the main office. This allows a shared configuration to apply for all incoming connections (using default settings) if the certificates of the remote sites have been signed with the root certificate of the VPN gateways in the main office. This also allows remote sites to select the remote network. The routers at the branch offices can then suggest a network (during IKE negotiations in phase 2) to be used for the connection.

Enabling the two functions “Simplified RAS with certificates“ and “Allow remote site to select the remote network“ is a necessary condition for the backup function described here.

The routing information at the switching nodes must also be adapted in backup situations. The switching nodes are normally accessed directly from the branch offices. In backup situations, the switching nodes must be able to receive the data from the branch offices via the main office detour. This is made possible with a route that transmits the entire combined network (10.x.0.0/255.255.0.0 in the example or, if communication with other nodes is to be possible: 10.0.0.0/255.0.0.0) to the main office.

In order for the routes to be switched automatically, “Allow remote site to select the remote network“ must also be activated at the switching nodes.

This results in the following sequence of events when establishing VPN connections:

- The switching node establishes the connection to the main office and requests all network relationships to the branch offices (i. e. it requests the 10.x.0.0/255.255.0.0 network).
- The branch office establishes the connection to the switching node and requests its network (10.x.y.0/255.255.255.0).

  Data can now be transferred from the branch office to the main office via the switching node.

The following happens if the VPN connection between branch office and main office now fails:

- The switching node detects the loss by polling (DPD) and removes the route to the branch office.
- At some point the branch office establishes the backup connection to the main office and requests its network (10.x.y.0/255.255.255.0).

  Data can now be transferred from the branch office to the main office.

  If the networks have been combined and the switching nodes always route the combined network (as in the example, network 10.x.0.0/255.255.0.0 or 10.0.0.0/255.0.0.0) to the main office, data can be transmitted from the branch office to the switching node via the main office.

Once the backup event is over, the branch office reestablishes the primary connection to the switching node:

- The branch office tears down the backup connection and the main office deletes the route to the branch office.
- The branch office again requests its network (10.x.y.0/255.255.255.0) from the switching node.

  Smooth communication between branch office and switching node now exists again.

  Because the branch office network is a sub-network of the network in the switching node, immediate communication between branch office and main office via the switching node is also possible again. The main office no longer has its own route to the branch office and therefore resumes transfers data for the branch office via the switching node again.

If network addresses cannot be structured as described above, the route to the branch office must be configured statically at the main office and point to the switching node. If the branch office then establishes the backup connection, the statically registered route is overwritten by the dynamically registered route. If the backup connection is torn down again, the dynamic route is deleted and the static route re-enabled. If, in this case, communication between branch offices and switching node is to be guaranteed for backup as well, the routes to the branch offices must also be configured statically in the switching nodes.

Establishing a backup connection

In order to conform to the basic principle of unambiguous IPSec rules, backup situations require VPN rules for the primary connection to be deleted first, and then new rules for the backup connection are created.

If the establishment of a backup connection fails, the backup module selects the next backup connection (if several are configured). If the next backup connection uses an ISDN connection, it is established completely normally, i.e. no IPSec rules need be reformulated.

If the backup at the main office is based on ISDN, it is important to avoid coupling the backup connection with the normal VPN connections to the other branch offices. In the event of a backup, these primary VPN connections carry not only the data traffic to the branch offices, but all traffic to the switching nodes and all other branch offices as well. This coupling can be prevented in two ways:

- A very high distance for the branch-office network is entered into the ISDN backup connection. This way the route can be overwritten by the routes automatically communicated via the VPN.
- Alternatively, the routes can be controlled using WAN RIP. For this, an ISDN connection with WAN RIP support is set up for every B-channel.

Re-establishing the primary connection

The device attempts to restore the primary connection while the backup connection is being established. During this attempt to connect, the VPN rule set must not be recreated again – otherwise the backup connection would fail or an existing VPN connection would simply be torn down.

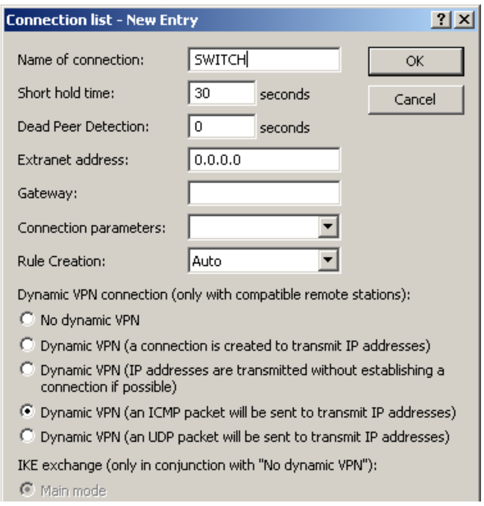
To prevent this, initial "Dynamic VPN" negotiations with the primary connection's remote site are performed. If these negotiations are successful, the primary connection can be reestablished. To this end, the backup connection is disconnected and the backup status is reset. This prevents the backup connection from being reestablished immediately. Only after this is the primary connection reestablished with the original VPN rules.

! The use of the "Dynamic VPN" connection between branch office and switching node is a necessary condition for the backup function described here.

10.11.3 Configuring the VPN backup

For configuring the VPN backup, the devices at the branch offices, main office and switching nodes must be considered separately.

- Branch office
  - "Dynamic VPN" over ICMP/UDP must be configured for the primary connection.



Connection list - New Entry

Name of connection: SWITCH

Short hold time: 30 seconds

Dead Peer Detection: 0 seconds

Extranet address: 0.0.0.0

Gateway:

Connection parameters:

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)

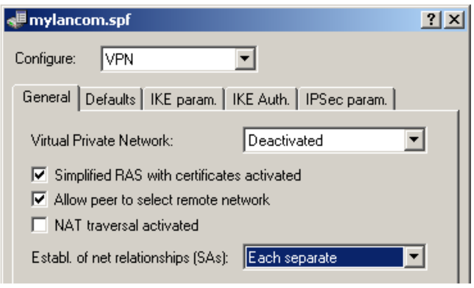
● Dynamic VPN (an ICMP packet will be sent to transmit IP addresses)

○ Dynamic VPN (an UDP packet will be sent to transmit IP addresses)

IKE exchange (only in conjunction with "No dynamic VPN"):

● Main mode

  - The backup connection has no requirement for "Dynamic VPN".
  - The backup is configured in the backup table, as with ISDN backup.
  - At the branch office, the main office must be configured as a backup remote site.
- Main office
  - Simplified RAS with certificates must be enabled.
  - Selection of the remote network by the remote site must be enabled.
  - A configuration in the backup table is not necessary here.



mylancom.spf

Configure: VPN

General | Defaults | IKE param. | IKE Auth. | IPSec param.

Virtual Private Network: Deactivated

☑ Simplified RAS with certificates activated

☑ Allow peer to select remote network

☐ NAT traversal activated

Establ. of net relationships (SAs): Each separate

- Switching nodes
  - The VPN connection to the main office must be completely configured.
  - Simplified RAS with certificates must be enabled.
  - Selection of the remote network by the remote site must be enabled.

If the system does not have "combined networks" (i.e. the branch office network is a sub-network of the switching node and the switching node network is a sub-network of the central network), then the switching node's route to the branch office must point to the main office in order for the branch office to be able to reach the switching node in backup situations. In normal operation, this route is overwritten by the route passed by the branch office in the VPN (because remote sites may provide network relationships) and is therefore only used when the direct connection is torn down and the branch office establishes the backup connection.

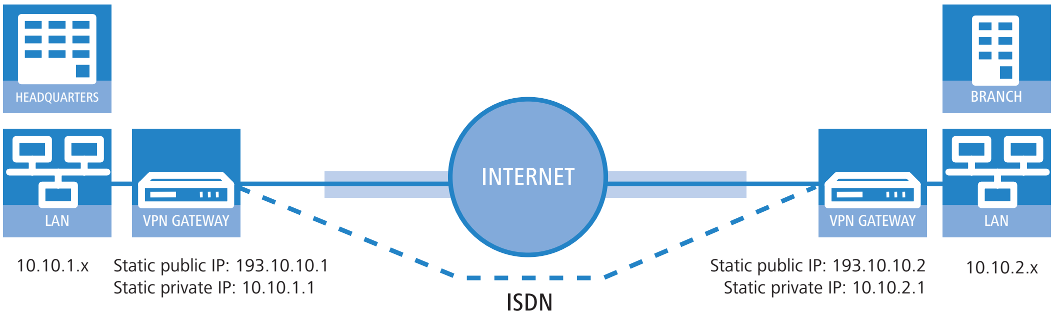
10.12 Specific examples of connections

This section covers the 4 possible types of VPN connections with concrete examples. These 4 different connection types are categorized by the type of IP address of the two VPN gateways:

- static/dynamic
- dynamic/static (the dynamic peer initiates the connection)
- static/dynamic (the static peer initiates the connection)
- dynamic/dynamic

There is a section for each of these types, together with a description of all required configuration information in the familiar table form.

10.12.1 Static/static

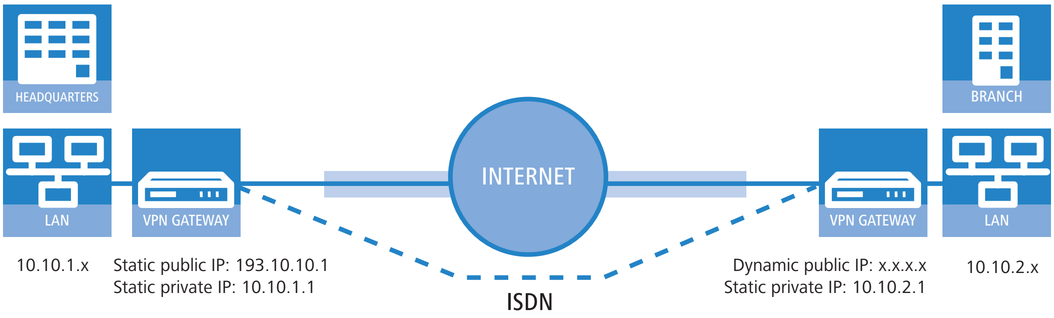

HEADQUARTERS
BRANCH
LAN
VPN GATEWAY
INTERNET
VPN GATEWAY
LAN
10.10.1.x
Static public IP: 193.10.10.1
Static private IP: 10.10.1.1
ISDN
Static public IP: 193.10.10.2
Static private IP: 10.10.2.1
10.10.2.x

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

Entry	Headquarters		Branch_office
IP address of the remote device	193.10.10.2		193.10.10.1
IP-network address of the remote network	10.10.2.0		10.10.1.0
Netmask of the remote network	255.255.255.0		255.255.255.0

10.12.2 Dynamic/static


HEADQUARTERS
BRANCH
LAN
VPN GATEWAY
INTERNET
VPN GATEWAY
LAN
10.10.1.x
Static public IP: 193.10.10.1
Static private IP: 10.10.1.1
ISDN
Dynamic public IP: x.x.x.x
Static private IP: 10.10.2.1
10.10.2.x

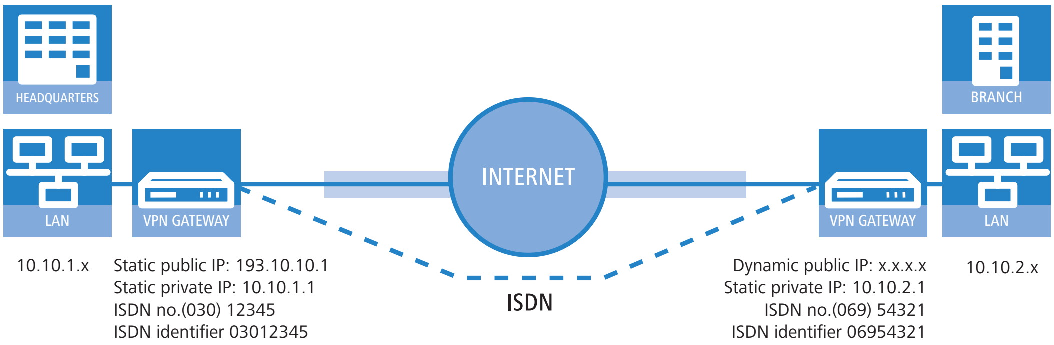
The VPN gateway **Branch office** initiates a VPN connection to the gateway **Headquarters**. **Branch office** has a dynamic IP address that was chosen and assigned by the Internet service provider upon dialling in, whereas **Headquarters** has a fixed, static address. When the connection is set up, **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

An ISDN line is not necessary for establishing this type of connection. The dynamic end communicates its IP address encrypted via the Internet protocol ICMP (or alternatively via UDP).

10.12.3 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.

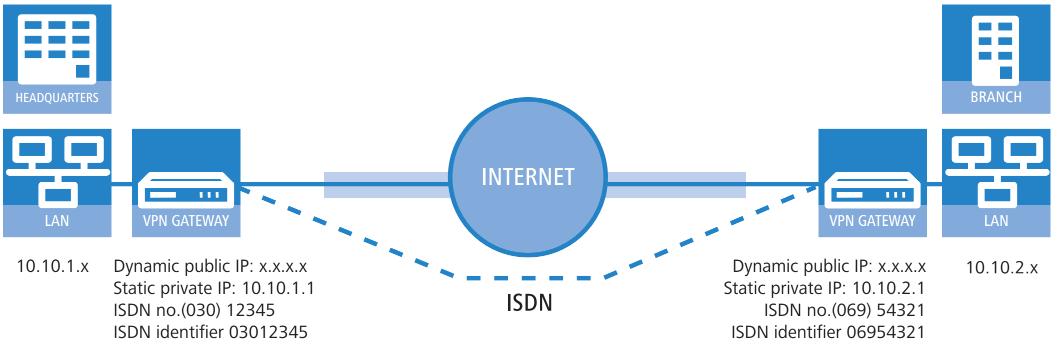
The entries for the ISDN connection are needed for the transmission of the actual dynamic IP address solely. The Internet access wizard configures the connection to the Internet.

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 10-9.

Entry	Headquarters		Branch_office
Type of local IP address	static	⤨	dynamic
Type of remote IP address	dynamic		static
Name of the local device	Headquarters	⤨	Branch_office
Name of the remote device	Branch_office		Headquarters
ISDN-calling number of the remote device	06954321		03012345
ISDN-caller ID of the remote device	06954321		03012345
Password for the secure transmission of the IP address	confidential	↔	confidential
Shared Secret for encryption	secret	↔	secret
IP address of the remote device			193.10.10.1
IP-network address of the remote network	10.10.2.0		10.10.1.0
Netmask of the remote network	255.255.255.0		255.255.255.0

The described connection set up requires an ISDN connection for both VPN gateways.

10.12.4 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 10-9.

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

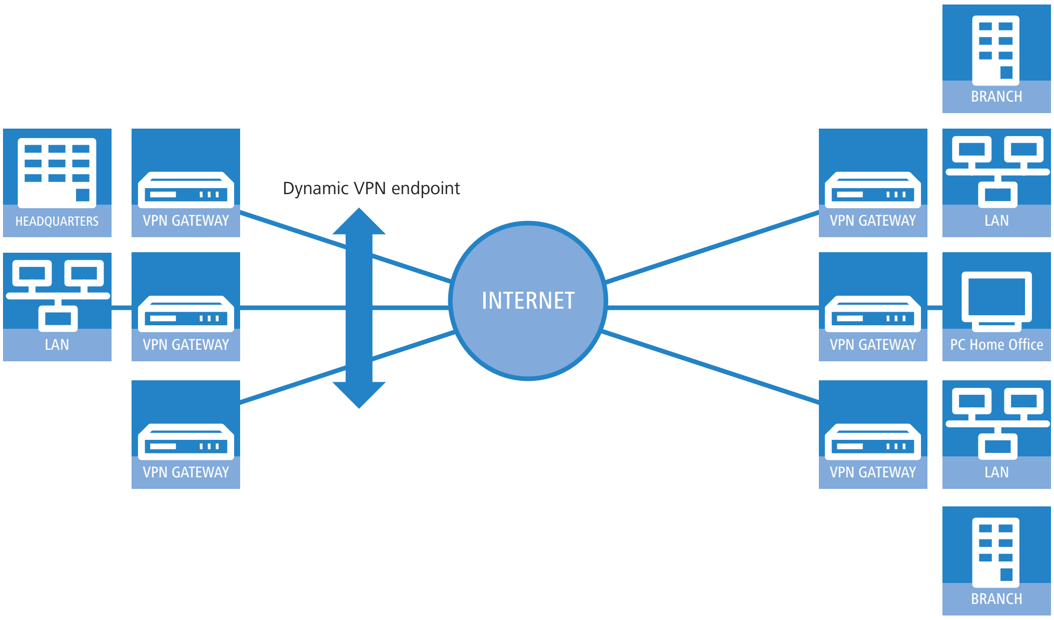
Entry	Headquarters		Branch_office
Password for the secure transmission of the IP address	confidential	↔	confidential
Shared Secret for encryption	secret	↔	secret
IP-network address of the remote network	10.10.2.0		10.10.1.0
Netmask of the remote network	255.255.255.0		255.255.255.0

Dynamic VPN works only between LANCOM that each feature at least one ISDN port that can be used for the ISDN connection

10.12.5 VPN connections: High availability with VPN load balancing

Multiple VPN gateway addresses

In decentralized company structures that rely on VPN for networking the various locations, the availability of the central VPN gateway is of particular significance. The company-wide communications only remain reliable as long as these central dial-in nodes are working properly.



With the option of configuring several "remote gateway" addresses as "dynamic VPN endpoints" for a VPN connection, LANCOM VPN gateways offer a high level of availability by using redundant devices. This involves multiple gateways at the headquarters being set up with identical VPN configurations. On location at the satellite sites, all of these available gateways are entered as possible remote stations for the VPN connection. If one of the gateways is unavailable, the remote router automatically redirects the request to one of the other routers.

To ensure that the computers in the LAN at the headquarters know which VPN gateway it to be used to reach a particular satellite station, the outband router currently connected to the remote site is propagated via RIPv2 to the network at the headquarters.

A powerful mechanism for high availability with constant load balancing between the VPN gateways at the headquarters is attained with the configuration of the satellite stations to select the remote site for VPN connection on a random basis.

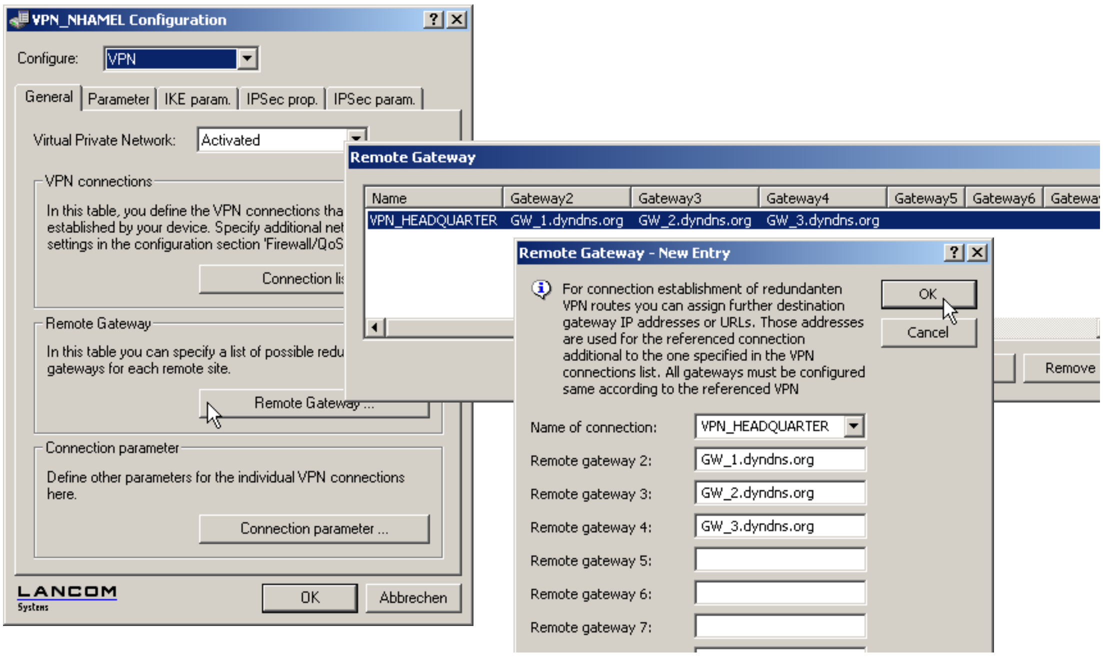
Configuration

During configuration, additional destinations for a VPN connection should be entered in the list of "Remote gateways". The list consists of the following entries:

- Name: Name of the remote site from the VPN connection list, the "target" of the VPN connection.
- Gateway 2 to Gateway 9: Address of the alternative gateways, as an IP address or DNS-translatable address.
- Begin with: In which order should the entries are to be tried. You can select from:
  - Last used: Selects the entry for the VPN connection which was successfully used most recently.
  - First: Selects the first of the configured remote stations.

- Random: Selects one of the configured remote stations at random. This setting provides an effective measure for load balancing between the gateways at the headquarters.

The entry for the gateway in the VPN connection list can be left blank if all of the possible gateways are entered into the list of "Remote gateways".



Configure: VPN

Virtual Private Network: Activated

VPN connections

In this table, you define the VPN connections tha established by your device. Specify additional net settings in the configuration section 'Firewall/QoS

Remote Gateway

In this table you can specify a list of possible redu gateways for each remote site.

Connection parameter

Define other parameters for the individual VPN connections here.

Remote Gateway

Name	Gateway2	Gateway3	Gateway4	Gateway5	Gateway6	Gatewa
VPN_HEADQUARTER	GW_1.dyndns.org	GW_2.dyndns.org	GW_3.dyndns.org			

Remote Gateway - New Entry

For connection establishment of redundanten VPN routes you can assign further destination gateway IP addresses or URLs. Those addresses are used for the referenced connection additional to the one specified in the VPN connections list. All gateways must be configured same according to the referenced VPN

Name of connection: VPN_HEADQUARTER

Remote gateway 2: GW_1.dyndns.org

Remote gateway 3: GW_2.dyndns.org

Remote gateway 4: GW_3.dyndns.org

Remote gateway 5:

Remote gateway 6:

Remote gateway 7:

LANconfig: VPN ▶ General ▶ Remote gateway

WEBconfig: LCOS menu tree ▶ Setup ▶ Config ▶ Remote-gateway-list

The following options are available for defining the strategy for the utilization of the configured remote-gateway addresses:

- `last used`
- `first`
- `random`

Example:

The following command sets three gateways as target at the headquarters, one of which is to be selected at random:

```
set VPN_HEADQUARTERS 213.217.69.75 213.217.69.76 213.217.69.77 * * * * * random
```

10.13 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.

10.13.1 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 Sec**urity Protocol" and was originally the name used by a working group of the IETF, the **I**nternet **E**ngineering **T**ask **F**orce. Over the years, this group has developed a framework for a secure IP protocol that is generally referred to as IPSec today.

It is important to note that IPSec itself is not a protocol, but merely the standard for a protocol framework. IPSec actually consists of a variety of protocols and algorithms for encryption, authentication and key management. These standards will be introduced in the following sections.

Security in an IP environment

IPSec has been implemented almost completely within level 3 of the OSI model, i.e. in the network layer. The transfer of data packets using the IP protocol is realized on level 3 of IP networks.

IPSec thus replaces the IP protocol. Under IPSec, the packets have a different internal structure than IP packets. Their external structure remains fully compatible to IP, however. IPSec packets can therefore be transported without problems by existing IP networks. The devices in the network responsible for the transport of the packets cannot distinguish IPSec packets from IP packets on the basis of their exterior structure.

The exceptions in this case are certain firewalls and proxy servers that access the contents of the packets. Problems can arise from the (often function dependent) incompatibilities of these devices to the existing IP standard. These devices must therefore be adapted to IPSec.

IPSec will be firmly implemented in the next generation of the IP standard (IPv6). For this reason, we can assume that IPSec will remain the most important standard for virtual private networks in the future.

10.13.2 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 **P**oint-to-**P**oint **T**unneling **P**rotocol (PPTP) early on. Cisco presented a similar protocol with **L**ayer **2** **F**orwarding (L2F). Both manufacturers agreed on a joint effort and the IETF produced the **L**ayer **2** **T**unnel **P**rotocol (L2TP).

Their main advantage over IPSec is that any network protocol can be used with such a network connection, especially NetBEUI and IPX.

A major disadvantage of the described protocols is the lack of security at the packet level. What's more, these protocols were designed specifically for dial-up connections.

Security at higher levels – SSL, S/MIME, PGP

Communications can also be secured with encryption at higher levels of the OSI model. Well known examples of this type of protocol are SSL (**S**ecure **S**ocket **L**ayer) mainly used for web browser connections, S/MIME (**S**ecure **M**ultipurpose **I**nternet **M**ail **E**xtensions) for e-mails and PGP (**P**retty **G**ood **P**rivacy) for e-mails and files.

In all of the above protocols, an application handles the encryption of the data, for example the Web browser on one end and the HTTP server on the other.

A disadvantage of these protocols in the limitation to specific applications. In addition, a variety of keys is generally required for the different applications. The configuration must be managed on the individual computers and can not be administered conveniently on the gateways only, as is the case with IPSec. Security protocols at the application level tend to be more intelligent as they know the significance of the data being transferred. They are usually much more complex, however.

All of these layer-2 protocols only support end-to-end connections; they are therefore not suitable for coupling entire networks.

On the other hand, these mechanisms do not require the slightest changes to the network devices or access software. And unlike protocols in lower network levels, they are still effective when the data content is already in the computer.

Combinations are possible

All of the alternatives listed above are compatible to IPSec and can therefore be used parallel to it. This permits a further increase of the security level. It would be possible, for example, to dial into the Internet using an L2TP 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.

10.14 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.

10.14.1 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

10.14.2 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.

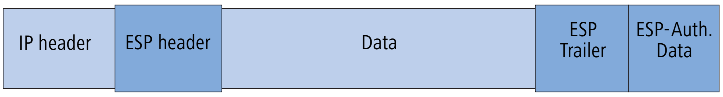
The SAs are managed in an internal database of the IPSec device that also contains the advanced connection parameters. These parameters include the algorithms and keys used, for example.

10.14.3 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 **N**ational **I**nstitute of **S**tandards and **T**echnology (NIST) selected the Rijndael algorithm (pronounced: "Rinedoll") and declared it as the AES in 2001.

  AES is a symmetric key algorithm with variable block and encryption lengths. It has been developed by the Belgian scientists Joan Daemen and Vincent Rijmen, and features outstanding security, flexibility and efficiency.

- **DES – Data Encryption Standard**
  DES was developed by IBM for the NSA (National Security Agency) in the early 1970s and was the worldwide security standard for years. The key length of this symmetrical process is 56 bits. Today, it is considered to be insecure due to its short key length and in the year 2000 the NIST replaced it with the AES (Rijndael algorithm). It is no longer suitable for use.

- **Triple DES** (a.k.a. 3-DES)
  A further development of DES. The conventional DES algorithm is applied three times consecutively. Two or three different keys, each with a length of 56 bits are used. The key for the first run is reused for the third DES run. The result is a nominal key length of 168 bit, with an effective key length of 112 bits.

  Triple-DES combines the sophisticated DES technology with a sufficiently long key and is therefore considered to be highly secure. Triple-DES is slower than other processes, however.

- **Blowfish**
  This development by the renowned cryptographer Bruce Schneier is a symmetrical encryption process. Blowfish achieves outstanding data throughput on multifunction processors. The process is reputed to be extremely efficient and secure.

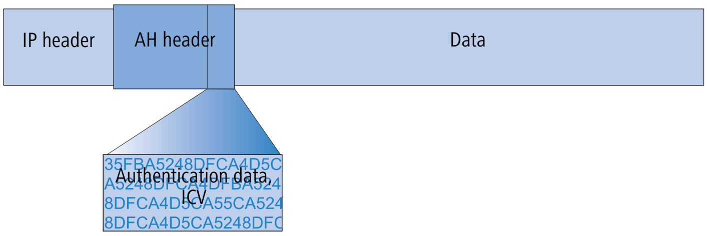
- **CAST** (from the authors **C**arlisle **A**dams and **S**tafford **T**avares)
  is a symmetrical process with a key length of 128 bits. CAST permits the modification of parts of the algorithm at runtime.

ⓘ The encryption settings can be modified in the LCOS menu tree within LANconfig. Modifications of this sort are generally only required when setting up VPN connections between devices from different manufacturers. LANCOM gateways offer the encryption as standard either after AES (128 bit), Blowfish (128 bit) or Triple-DES (168 bit).

10.14.4 Authentication – the AH protocol

The AH protocol (**A**uthentification **H**eader) guarantees the integrity and authenticity of the data. Integrity is frequently regarded as a component of authenticity. In the following, we will consider integrity to be a separate problem that is resolved by AH. In addition to integrity and authenticity, AH also provides effective protection against the replay of received packets (Replay Protection).

AH adds its own header to IP packets immediately after the original IP header. The most important part of this AH header is a field containing authentication data, often referred to as the **I**ntegrity **C**heck **V**alue (ICV).



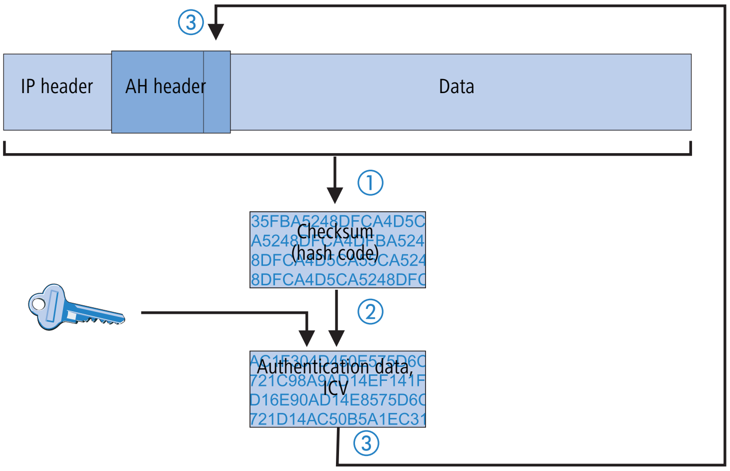
The AH process in the sender

In the sender, the authentication data is generated in 3 steps.

① A checksum is calculated for the complete package using a hash algorithm.

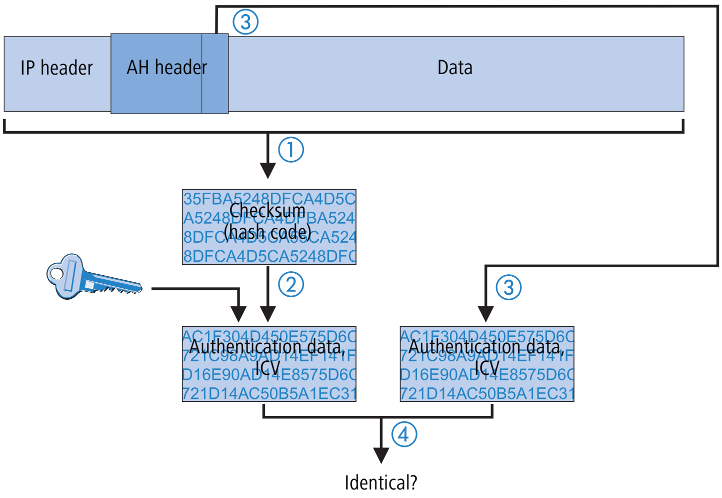
② This checksum is once again sent through a hash algorithm together with a key known to both the sender and the recipient.

③ This results in the required authentication data which is inserted in the AH header.



Checking of integrity and authenticity by the recipient

The AH protocol works in a very similar manner at the recipient's end. The recipient also uses his key to calculate the authentication data for the received packet. The comparison with the sent ICV of the packet determines the integrity and authenticity of the packet.



Determining the checksum for the integrity check

AH adds a checksum to each packet before it is sent to guarantee the integrity of the transferred packets. At the recipients end, AH checks whether the checksum and the contents of the package match. If this is not the case, the packet was either incorrectly transferred or deliberately manipulated. Such packets are discarded immediately and are not forwarded to higher protocol levels.

A variety of so-called hash algorithms are available to determine the checksum. Hash algorithms are distinguished by the fact that their results (the hash code) are a unique fingerprint of the original data. Conversely, the original data cannot be determined on the basis of the hash code. In addition, minimum changes of the input value entail a completely different hash code with a high-grade hash algorithm. Systematic analyses of several hash codes thus are made more difficult.

LANCOM VPN supports the two most common hash algorithms: MD5 and SHA-1. Both methods work without keys, i.e. on the basis of fixed algorithms. Keys do not play a role until a later step of AH: the final generation of the authentication data. The integrity checksum is only a necessary intermediate result on the way there.

Generation of the authentication data

In the second step, AH generates a new hash code using the checksum and a key, the final authentication data. A variety of standards are available under IPSec for this process as well. LANCOM VPN supports HMAC (**H**ash-based **M**essage **A**uthentication **C**ode). The hash functions MD5 and SHA-1 are available as hash algorithms. The HMAC versions are accordingly known as HMAC-MD5-96 and HMAC-SHA-1-96.

This clarifies why AH leaves the packet itself unencrypted. Only the checksum of the packet and the local key are added to the packet together with the ICV, the authentication data, in encrypted form as a verification criterion.

Replay protection – protection against replayed packets

In addition to the ICV, AH assigns a unique sequence number to each packet. The recipient can thus recognize which packets were intercepted by a third party and resent. Attacks of this type are known as “packet replay“.

ⓘ AH does not cater for the masking of IPSec tunnels unless additional measures, such as NAT-Traversal or an outer Layer-2-Tunneling (e.g. PPPT/L2TP), are used that offer “changeable” IP headers.

10.14.5 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.

LANCOM reference manual part 4

- Wireless LAN - WLAN
- Virtual LANs (VLANs)

Version: LCOS 7.6 with addendum 7.7 (see appendix)
(last update August 2009)

LANCOM
Systems

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

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

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen
Deutschland

www.lancom.de

Würselen, August 2009

110650/0809

Contents

11 Wireless LAN – WLAN

11.1 Introduction

The following sections are a general description of the LCOS operating system functions relating to wireless networks. The functions provided by your specific device are outlined in the manual supplied with it.

This chapter gives you a brief introduction to wireless networking technology. It also provides an overview of the many different applications, fraction and capabilities of LANCOM WLAN devices.

A wireless LAN connects individual end-user devices (PCs and mobile computers) to form a local network (also called – **L**ocal **A**rea **N**etwork). In contrast to a traditional LAN, communication takes place over a wireless connection and not over network cables. For this reason it is referred to as a **W**ireless **L**ocal **A**rea **N**etwork (WLAN).

A wireless LAN provides the same functionality as a cable-based network: Access to files, servers, printers etc. as well as the integration of individual work stations into a corporate mail system or access to the Internet.

There are obvious advantages to wireless LANs: Notebooks and PCs can be installed where they are needed—problems with missing connections or structural changes are a thing of the past with wireless networks. Apart from that, wireless LANs can also be used for connections over longer distances. Expensive leased lines and the associated construction measures can be saved.

LANCOM Systems differentiates between two different types of WLAN device, each with its own field of application and consequently offering specialized functions and configuration options.

- LANCOM Access Points are generally used to connect one or more WLANs to a cabled LAN. As such, they merely function as a "bridge" to transfer data to and from the from the clients. Routing into the Internet or to other remote stations is handled by other network components. LANCOM Access Points generally have just one or more Ethernet interfaces.
- In addition to one or more Ethernet interfaces, LANCOM Wireless Routers are equipped with WAN interfaces for ADSL, DSL and/or ISDN. In a single device, they combine WLAN functions with the task of routing data into the Internet or to other remote stations.

The following sections mostly refer to "access points" as a synonym for both types of device, unless we explicitly differentiate between a LANCOM Wireless Router and a LANCOM Access Point.

LANCOM Wireless Routers and LANCOM Access Points can be operated either as self-sufficient Access Points with their own configuration (WLAN modules in "Access Point mode“) or as components in a WLAN infrastructure, which is controlled from a central WLAN-Controller ("managed mode").

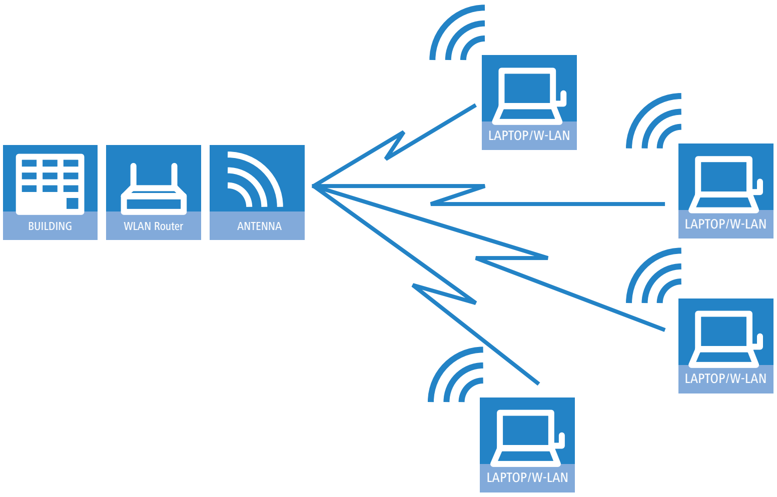
11.2 Application scenarios

Wireless LAN systems can act as an extension to or even as a replacement for cabled networks. In some cases wireless LANs even provide completely new application possibilities, which can mean a major advance in the way work is organized, or significant cost savings.

- Extensive wireless LANs, possibly connected to a LAN, with one or more access points (infrastructure mode)
- Hotspot or guest access
- Connecting two LANs over a wireless link (point-to-point mode)
- Relay function for connecting networks via multiple access points.
- Connecting devices with an Ethernet interface via an access point (client mode)
- Central management by a LANCOM WLAN Controller (managed mode)
- WDS (Wireless Distribution System)
- Data transfer to mobile objects in industrial environments.
- Transmission of VPN-encrypted connections with VPN pass through
- Simple, direct connection between terminal devices with an access point (ad-hoc mode)

11.2.1 Infrastructure mode

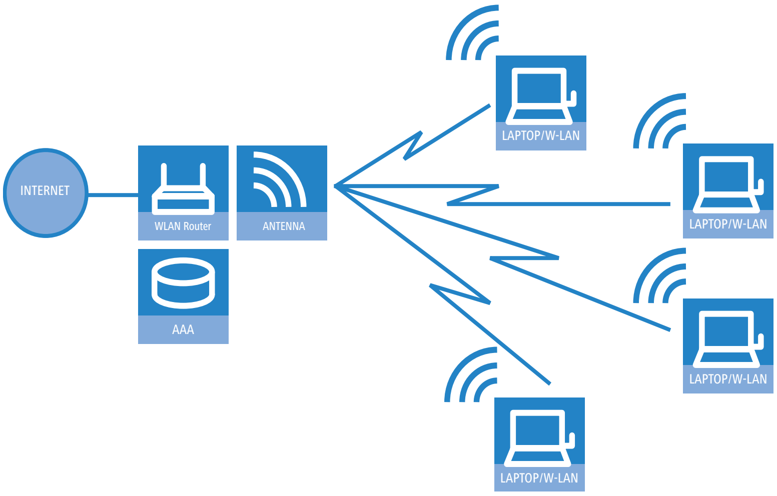
In infrastructure mode, WLAN clients connect to a central access point. The access point provides one or more wireless LAN networks. It regulates the client's rights to access the radio cell, communications between the clients, and access to further networks. In larger scale WLAN scenarios (e.g. in companies with offices extending between several buildings or floors) multiple access points can provide WLAN clients with access to a common, shared network. The clients can roam between the different access points, if necessary. A common term used here is "campus coverage" because this solution is used by a large number of colleges and universities to provide students and staff with network access.



11.2.2 Hotspot or guest access

A hotspot is a special variant of the infrastructure mode described above. Whereas the normal infrastructure mode provides the members of a closed user group with access to a network that includes all the necessary services, a hotspot provides network access (generally restricted to Internet only) to wireless LAN clients at a fee. In addition to the differences in Access Point configuration, setting up a hotspot requires authentication, authorization and accounting (AAA) functions such as those provided by e.g. Public Spot options Hotspots are generally set up at public locations where people have a short-term need to access the Internet, such as at airports, cafés or hotels.

A hotspot provides network access to a WLAN client for a limited time period and without having to configure the access point. This method is often used by companies, for example to provide guests with temporary Internet access.

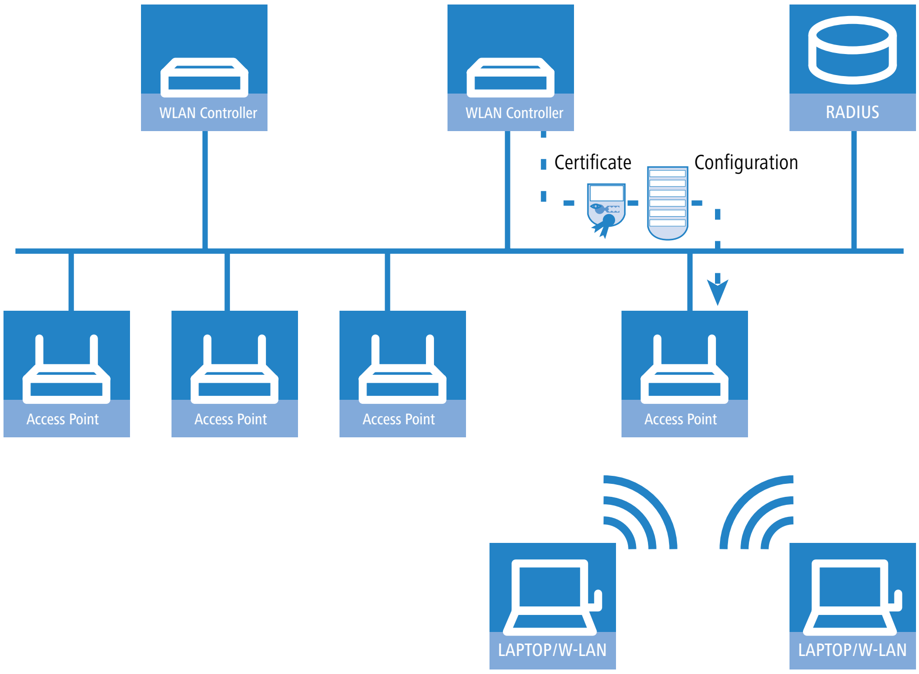


11.2.3 Managed mode

The widespread use of wireless Access Points and wireless routers provides great convenience and flexibility in network access for businesses, universities and other organizations. With centralized WLAN management, the Access Points in managed mode are not configured themselves but at a central location, the WLAN-Controller.

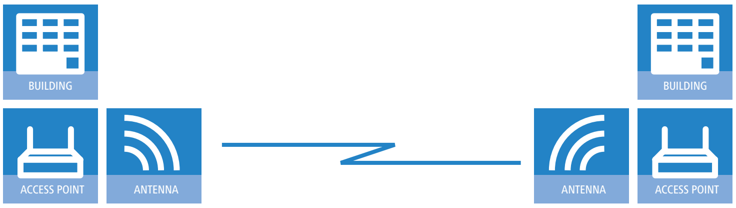
The WLAN-Controller authenticates the Access Points and transmits a certificate and the correct configuration to the approved devices. This allows for convenient configuration of the WLAN from a central point and the changes to the configuration affect all of the Access Points simultaneously.

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

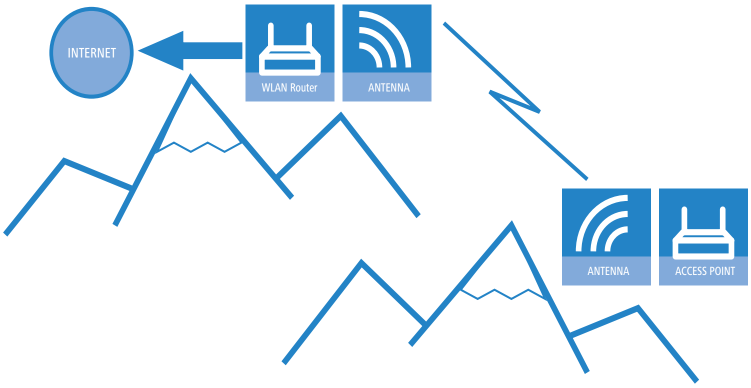


11.2.4 WLAN bridge (point-to-point)

Whereas the scenarios discussed so far have involved connecting multiple WLAN clients to one Access Point (point-to-multipoint), outdoor wireless LAN systems are particularly advantageous for providing a link between two Access Points (point to point). By setting up a wireless link between two Access Points, a distant production building on extensive company premises can be very easily integrated into the company network, for example.



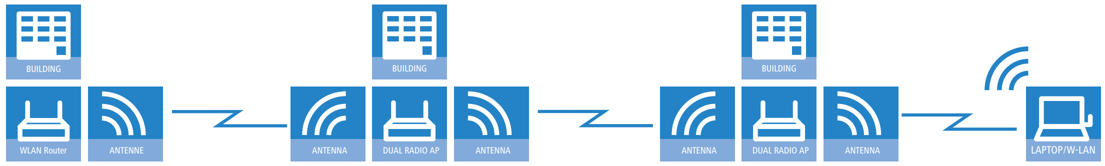
A point-to-point connection can also be used in difficult terrain (such as mountainous areas or islands) to provide Internet access in areas where cabling would be too expensive. With a direct line of sight between the two Access Points and a sufficient fresnel zone, distances of several kilometers can be bridged by this type of wireless link.



11.2.5 WLAN bridge in relay mode

In some cases, the distance between the two locations to be connected exceeds the range of a single wireless link. This may be the case when the distance between the Access Points exceeds the radio range, or when obstacles exist in the line of site between the two Access Points

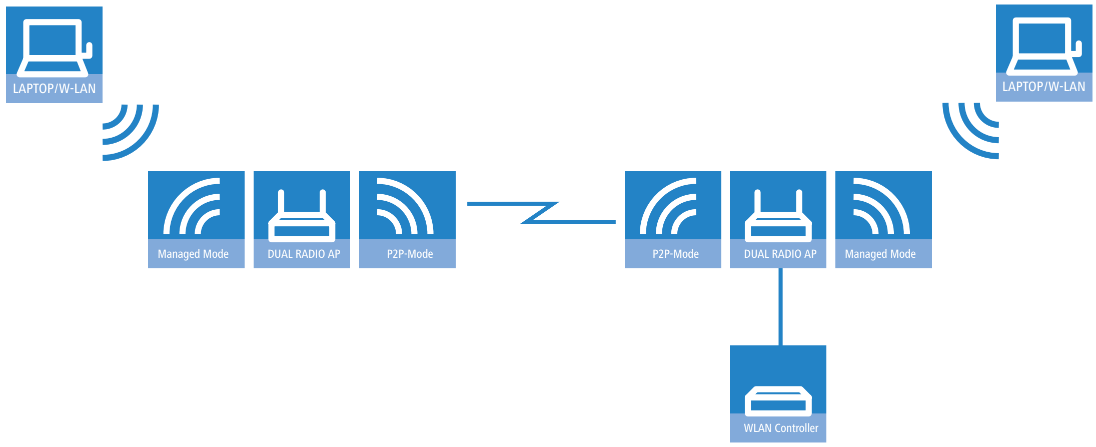
In these cases, the two end points can be connected by stringing together multiple Access Points, each of which has two WLAN modules. Because the intermediate Access Points often operate solely as relay stations, the operating mode of these Access Points is referred to as "relay mode".



Although LANCOM Access Points can run several P2P links simultaneously on each wireless module in addition to supporting wireless LAN clients, for performance reasons we recommended the use of LANCOM Access Points with two wireless modules for the relay stations.

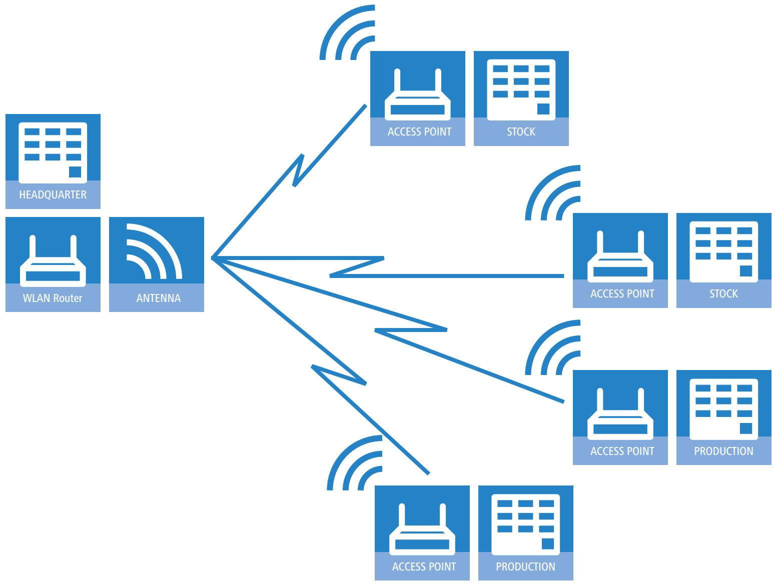
11.2.6 WLAN bridge to an access point – managed and unmanaged mixed

WLAN-Controllers managed from a central Access Point are generally connected to the network via cabled Ethernet. Where this is not possible, managed Access Points can be integrated into the LAN via a WLAN bridge, assuming that these are equipped with two WLAN modules. In this scenario, one WLAN module operates as a managed Access Point which obtains its configuration from the central WLAN-Controller. The other WLAN module is permanently configured as a WLAN bridge.



11.2.7 Wireless Distribution System (point-to-multipoint)

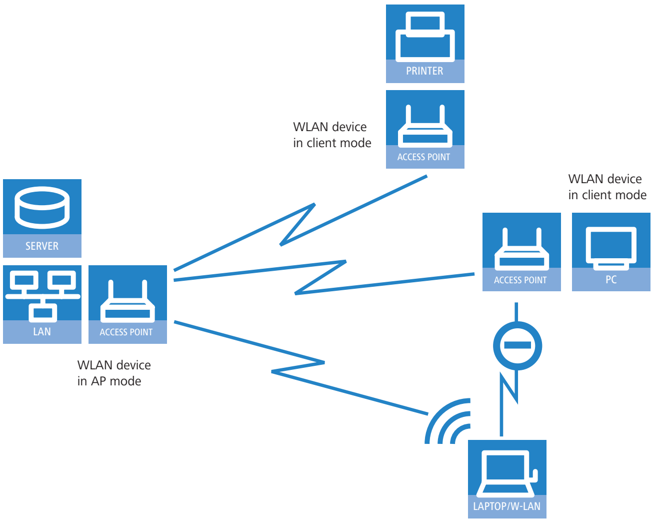
A special type of wireless link is the connection of several distributed Access Points to a central point – the point-to-multipoint wireless LAN (P2MP) is also referred to as a Wireless Distribution System (WDS). This mode of operation allows for example several buildings on a company's premises to be connected to the central administrative building. The central Access Point or Wireless Router is configured as "master" and the remote WDS stations as "slaves".



11.2.8 Client mode

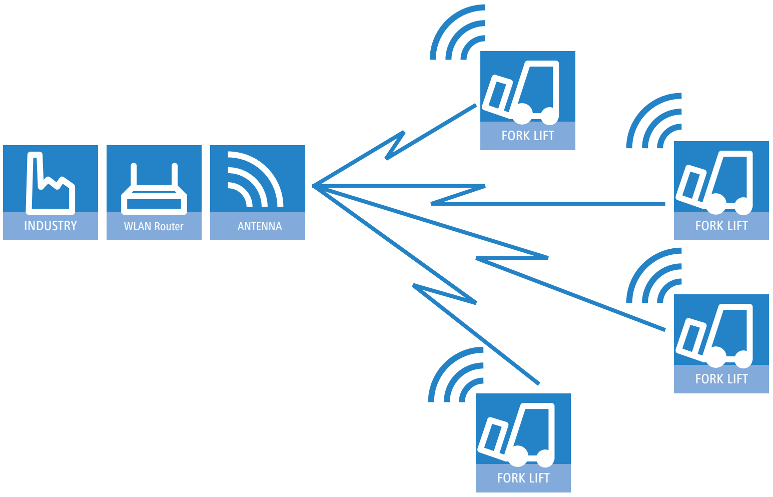
In order for individual devices equipped with an Ethernet interface to be connected to a wireless LAN, LANCOM Access Points can be switched to client mode, in which they act as conventional wireless LAN adapters and not as access points

(AP). Special client devices are offered alternatively, which can be operated in this mode only. The use of client mode therefore allows devices fitted with only an Ethernet interface, such as PCs and printers, to be integrated into a wireless LAN.



11.2.9 Client mode with mobile objects in industry

Completely new applications allow wireless LAN systems in industrial environments to transmit data to mobile objects. In logistics, for example, this means that fork-lift trucks can stay continuously connected to the company network via the wireless LAN. In combination with mobile barcode scanners, inventory movements within a warehouse can be monitored in real time and passed on to an ERP system, which then provides all employees with up-to-the-minute information on current inventories at all times.



11.3 WLAN standards

IEEE 802.11

LANCOM WLAN devices operate with the IEEE 802.11 standard. This is a collection of standards that build on the earlier IEEE standards for LANs. The best known of these is IEEE 802.3 for Ethernet. Among the various IEEE 802.11 standards, some specify wireless transmissions in various frequency bands and at different speeds. LANCOM Access Points and AirLancer client adapters are available which support a number of these standards:

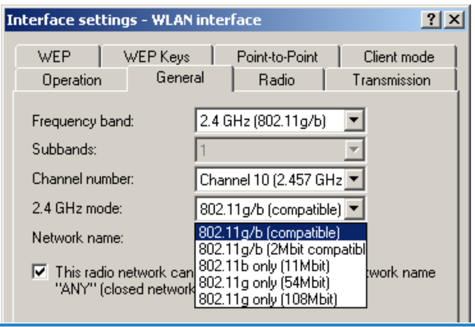
- IEEE 802.11n with up to 300 Mbps data rate in the 5 GHz or 2.4 GHz frequency bands, featuring new mechanisms such as MIMO, 40-MHz channels, packet aggregation, and block acknowledgement.
- IEEE 802.11a with up to 54 Mbps data rate in the 5 GHz frequency band, up to 108 Mbps with Turbo Mode (extension to the standard).
- IEEE 802.11g with up to 54 Mbps data rate in the 2.4 GHz frequency band, up to 108 Mbps with Turbo Mode (extension to the standard).
- Even though modern WLAN adapters generally operate with 802.11a/g/n, LANCOM Access Points remain compatible to older WLAN adapters supporting 802.11b with up to 11 Mbps in the 2.4-GHz frequency band.

By observing these IEEE standards, LANCOM WLAN products operate with devices from other manufacturers reliably and without problems. Depending on the model, your LANCOM Access Point supports the standards IEEE 802.11g (backwardly compatible to IEEE 802.11b) and/or IEEE 802.11a and IEEE 802.11n draft 2.0.

The WLAN module in the Access Points only operates in one frequency band at a time, i.e. either at 2.4 GHz or 5 GHz. It is impossible to operate at different frequencies with a single WLAN module. However, Access Points with two WLAN modules (dual radio) can operate each module at a different frequency. As the standards in the 2.4 GHz band IEEE 802.11b/g/n are backwardly compatible, various standards can be operated simultaneously on a single WLAN module, although lower data rates are incurred

Data rates in compatibility mode

Please note that data rates available with IEEE 802.11b/g/n devices depend upon the 2.4-GHz mode being used. If slower units become active in a wireless network in compatibility mode, the overall datarate will drop.



Frequency band: 2.4 GHz (802.11g/b)

Subbands: 1

Channel number: Channel 10 (2.457 GHz

2.4 GHz mode: 802.11g/b (compatible)

Network name:

- 802.11g/b (compatible)
- 802.11g/b (2Mbit compatibl
- 802.11b only (11Mbit)
- 802.11g only (54Mbit)
- 802.11g only (108Mbit)

☑ This radio network can ... work name "ANY" (closed network

Please note that not all of the available frequencies are approved for use in all countries! A table of frequencies and licensing regulations is to be found in the appendix of the manual for each device.

11.3.1 IEEE 802.11n

The new wireless LAN standard 802.11n features a number of technical developments that provide up to five-times the wireless-LAN performance in the 5 GHz or 2.4 GHz frequency bands. The changes have not yet been officially approved by the IEEE, but the foreseeable technological leap is so enticing that the industry is already bringing updated WLAN devices to market before the standards have been adopted. Current discussions are embodied by what is known as "draft 2.0", which is the basis for devices currently available on the market.

Any reference to "802.11n" in this document always implies the current draft 2.0, which is not a standard adopted by the IEEE.

Some of the improvements refer to the physical layer (PHY), which describes the transmission of individual bits over the physical medium—in this case the air represents the physical medium. Other additions are concerned with the MAC (medium access control) that among other things governs access to the transmission medium. The two areas are treated separately below.

Advantages of 802.11n

The new technology includes the following advantages:

- **Higher effective data throughput**

  802.11n draft 2.0 includes a number of new mechanisms to significantly increase available bandwidth. Current wireless LAN standards based on 802.11a/g enable physical data rates (gross data rates) of up to 54 Mbps, which turn out to be approx. 22 Mbps net. Networks based on 802.11n **currently** achieve a gross data throughput of up to 300 Mbps (in reality approx. 120 to 130 Mbps net) – theoretically the standard defines up to 600 Mbps with four data streams. For the first time, maximum speeds exceed the 100 Mbps of cable-based Fast Ethernet networks, which are currently standard in most workplaces.

- **Improved and more reliable wireless coverage**

  The new 802.11n technologies do not just increase date throughput but bring about improvements in the range and reduce the wireless dead spots in existing a/b/g installations.

  This results in better signal coverage and improved stability for significantly better utilization of wireless networks, in particular for users in professional environments.

- **Greater range**

  Data throughput generally decreases when the distance between receiver and transmitter increases. The overall improved data throughput allows wireless LANs based on 802.11n to achieve greater ranges, as a significantly stronger wireless signal is received by the Access Point over a given distance than in 802.11a/b/g networks.

Compatibility with other standards

The 802.11n standard is backwardly compatible to previous standards (IEEE 802.11a/b/g). However, some of the advantages of the new technology are only available when, in addition to the access points, the wireless LAN clients are also compatible with 802.11n.

In order to allow the co-existence of wireless LAN clients based on 802.11a/b/g (called "legacy clients") 802.11n access points offer special mechanisms for mixed operation, where performance increases over 802.11a/b/g are not as high. Only in all-802.11n environments is the "greenfield mode" used, which can exploit all the advantages of the new technology. In greenfield mode both access points and wireless LAN clients support the 802.11n Draft, and access points reject connections with legacy clients.

The physical layer

The physical layers describes how data must be transformed in order for them to be transmitted as individual bits over the physical medium. In this process the following steps are performed in a wireless LAN device:

- Modulation of digital data into analog carrier signals
- Modulation of the carrier signal into a radio signal in the selected frequency band, which for a wireless LAN is either 2.4 or 5 GHz.

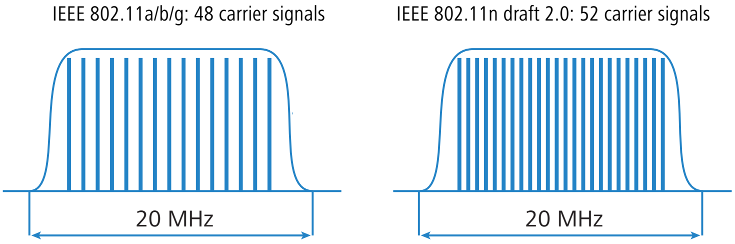
The second modulation step in IEEE 802.11n occurs in the same way as in conventional wireless LAN standards and is therefore not covered here. However, there are a number of changes in the way digital data are modulated into analog signals in 802.11n.

Technical aspects of 802.11n

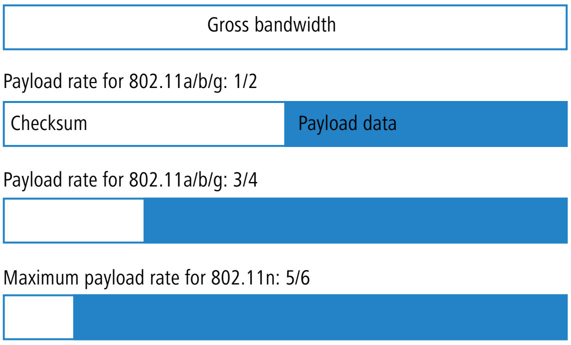
- **Improved OFDM modulation (MIMO-OFDM)**

Like 802.11a/g, 802.11n uses the OFDM scheme (Orthogonal Frequency Division Multiplex) as its method of modulation. This modulates the data signal not on just one carrier signal but in parallel over several. The data throughput that can be achieved with OFDM modulation depends on the following parameters, among other things:

- Number of carrier signals: Whereas 802.11a/g uses 48 carrier signals, 802.11n can use a maximum of 52.


IEEE 802.11a/b/g: 48 carrier signals
20 MHz
IEEE 802.11n draft 2.0: 52 carrier signals
20 MHz

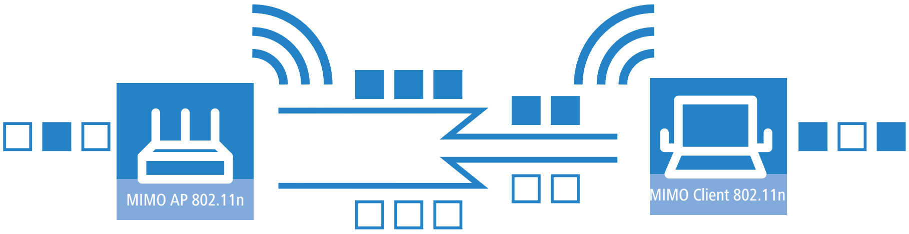
- Payload data rate: Airborne data transmission is fundamentally unreliable. Even small glitches in the WLAN system can result in errors in data transmission. Check sums are used to compensate for these errors, but these take up a part of the available bandwidth. The payload data rate indicates the ratio between theoretically available bandwidth and actual payload. 802.11a/g can operate at payload rates of 1/2 or 3/4 while 802.11n can use up to 5/6 of the theoretically available bandwidth for payload data.


Gross bandwidth
Payload rate for 802.11a/b/g: 1/2
Checksum
Payload data
Payload rate for 802.11a/b/g: 3/4
Maximum payload rate for 802.11n: 5/6

These two features increase the maximum useable bandwidth of 54 Mbps for 802.11a/g to 65 Mbps for 802.11n. This increase is not exactly spectacular, but it can be further improved by using the following features:

■ MIMO technology

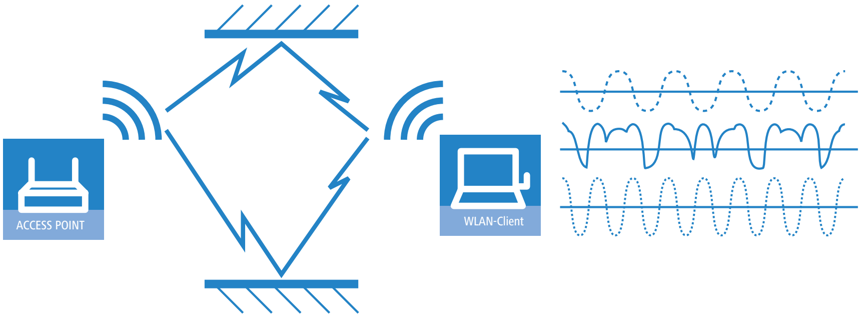
MIMO (multiple input multiple output) is the most important new technology contained in 802.11n. MIMO uses several transmitters and several receivers to transmit up to four parallel data streams on the same transmission channel (currently only two parallel data streams have been implemented). The result is an increase in data throughput and improved wireless coverage.



For example, the Access Point splits the data into two groups which are then sent simultaneously via separate antennas to the WLAN client. Data throughput can therefore be doubled using two transmitting and receiving antennas.

But how can several signals be transmitted on a single channel simultaneously? This was considered impossible with previous WLAN applications.

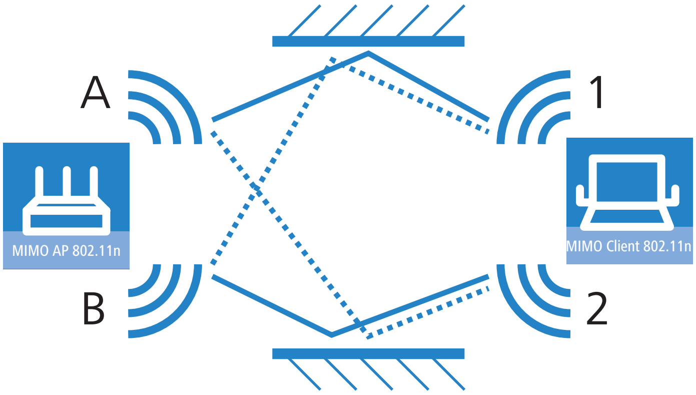
Let us consider how data is transmitted in "normal" wireless LAN networks: Depending on antenna type, an Access Point's antenna broadcasts data in several directions simultaneously. These electromagnetic waves are reflected by the surrounding surfaces causing a broadcast signal to reach the WLAN client's antenna over many different paths; this is also referred to as "multipath propagation". Each of these paths has a different length meaning that individual signals reach the client with a different time delay.



These time-delayed signals interfere with each other at the WLAN client and significantly weaken the original signal. For this reason, conventional WLAN networks should always have a direct line of sight (LOS) between transmitter and receiver in order to reduce the influence of reflections.

MIMO technology transforms this weakness in WLAN transmission into a strength that allows an enormous increase in data throughput. As mentioned above, it is virtually impossible to transmit different signals on the same channel simultaneously as the receiver cannot distinguish between them. MIMO uses the reflection of electromagnetic waves and the associated spatial aspect to obtain a third criterion for identifying the signals.

A signal sent by transmitter A and received by receiver 1 follows a different path than a signal from transmitter B to receiver 2. Due to the different reflections and changes in polarization that both signals experience along their paths, each of these paths takes on its own characteristics. When data transmission starts, a training phases records the characteristics of the path by transmitting standardized data. Subsequently, the data received here is used to calculate which data stream the signals belong to. The receiver decides for itself which of the incoming signals is to be processed, thus avoiding loss from interference.



MIMO thus allows the simultaneous transmission of several signals over one shared medium, such as the air. Individual transmitters and receivers must be positioned a minimum distance apart from one another, although this is just a few centimeters. This separation results in differing reflections and signal paths that can be used to separate the signals.

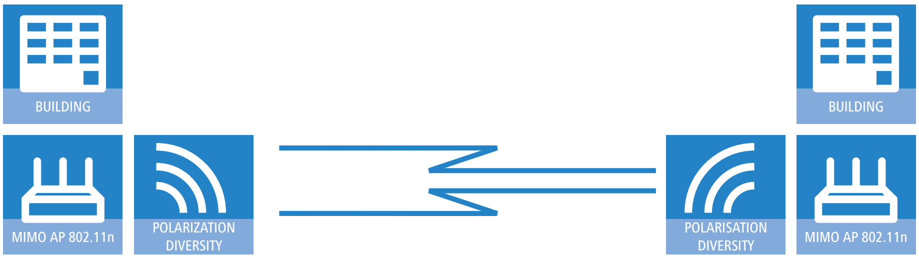
Generally speaking, MIMO can provide up to four parallel data streams, which are also called "spatial streams". However, the current generation of chips can only implement two parallel data streams as the separation of data streams based on characteristic path information demands high levels of computing power, which consumes both time and electricity. The latter tends to be undesirable particularly for WLAN systems, where attempts are often made to achieve independence from power sockets at the WLAN client or when using PoE as the electricity supply for the Access Point.

Even if the aim of four spatial streams has not yet been achieved, the use of two separate data connections results in a doubling of data throughput, which represents a true technological leap in the area of WLAN systems. Combined with the improvements in OFDM modulation, the data throughput that can be attained increases to 130 Mbps.

The short description "transmitter x receiver" expresses the actual number of transmitting and receiving antennas. 3x3 MIMO describes three transmitting and three receiving antennas. However, the number of antennas does not equate with the number of data streams: the antennas available only limit the maximum number of spatial streams. The reason for using more antennas than strictly necessary for data stream transmission relates to the method of allocating the signals according to their characteristic path: A third signal is used to transmit additional spatial information. If the data from the first two signals cannot be uniquely identified, their computation can still be performed with the aid of the third signal. The use of additional antennas does not contribute to an increase in data throughput, but it does result in a more even, stronger coverage for clients.

MIMO in outdoor use

Outdoor 802.11n applications cannot use natural reflections since signal transmission usually takes place over the direct path between directional antennas. In order to transmit two data streams in parallel, special antennas are employed that use polarization channels turned through 90° to each other. These so-called "dual-slant" antennas are really two antennas in one housing. Since a third signal does not offer additional reliability, outdoor applications generally use as many antennas (or polarization channels) as there are data streams for transmission.

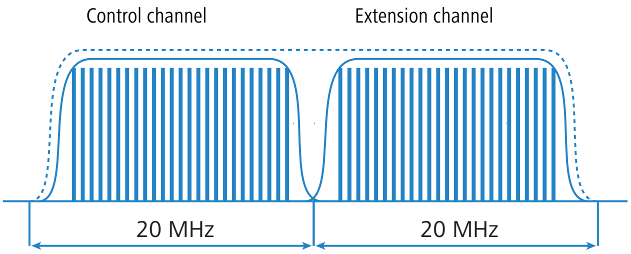


40 MHz channels

As the above explanation of OFDM modulation states, data throughput rises with an increasing number of carrier signals because this allows several signals to be transmitted simultaneously. If a channel with a bandwidth of 20 MHz supports no more than 48 (802.11a/g) or 52 (802.11n) carrier signals, the obvious choice would be to use a second channel with additional carrier signals.

This method was used in the past by a number of manufacturers (including LANCOM Systems) and was referred to as "turbo mode", allowing data rates of up to 108 Mbps. Turbo mode does not form part of the official IEEE standard but is frequently employed on point-to-point connections, for example, because compatibility to other manufacturers tends to play a secondary role.

However, the success of the underlying technology has lead to its incorporation into 802.11n. IEEE 802.11n draft 2.0 uses the second transmission channel in a way that maintains compatibility to IEEE 802.11a/g devices. 802.11n transmits data over two contiguous channels. One of these assumes the task of a control channel that, among other things, handles the administration of data transmission. Concentrating these basic tasks into the control channel means that devices supporting a transmission at 20 MHz only can also be connected. The second channel is an extension that only comes into effect if the remote client also supports data transmission at 40 MHz. The use of the second channel remains optional throughout, with transmitter and receiver deciding dynamically whether one or two channels should be employed.

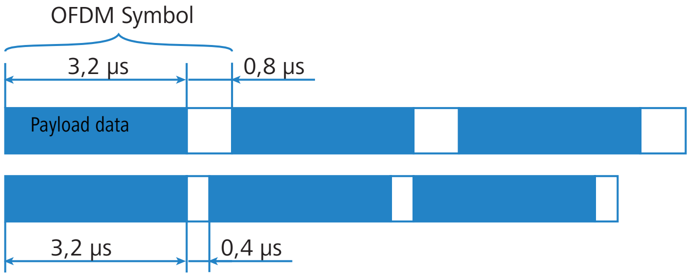


As the implementation of 40 MHz with separate control and extension channels is more efficient in the 802.11n draft than in the conventional turbo mode, more than double the amount of carrier signals can be obtained (108 in total). The maximum data throughput when using improved OFDM modulation and two parallel data streams thus rises to 270 Mbps.

- **Short guard interval**

The final improvement of the 802.11n draft is the improvement in the chronological sequence of data transmission. A signal that is to be transmitted in a WLAN system is not broadcast at a distinct point in time but is "held up" for a certain, constant transmission period. In order to prevent interference at the receiving end, a short break is made following the transmission period before the transmission of the next signal commences. The entire duration of transmission period and break are referred to in WLAN terminology as "symbol length" and the break itself is known as the "guard interval".

IEEE 802.11a/g uses a symbol length of 4 µs: the information transmitted on the carrier signal changes following transmission of 3.2 µs and a break of 0.8 µs. 802.11n reduces the break between transmissions to the so-called "short guard interval" of only 0.4 µs.



Transmitting data in shorter intervals thus increases the maximum data throughput when using improved OFDM modulation, two parallel data streams and transmission at 40 MHz to 300 Mbps.

Optimizing net data throughput

The methods described so far are intended to improve the maximum physically possible data throughput. The methods described below are used in 802.11n networks to optimize net data throughput, i.e. the throughput of actual payload data.

- **Frame aggregation**

In addition to the actual payload data, each data packet includes management information, which is important for the smooth exchange of data. Frame aggregation is used to combine several data packets (frames) into one large packet. As a consequence, management information only needs to be specified once for the complete data packet, and the proportion of payload data to the total data volume increases.

- **Block acknowledgement**

Each data packet is acknowledged on receipt. In this way, the transmitter is informed that the packet was received correctly and does not need to be repeated. This principle also applies to aggregated frames in 802.11n.

However, some packets in an aggregated frame may be delivered successfully while others are not. In order to avoid having to retransmit an entire aggregated frame from which perhaps just one data packet was **not** delivered, a separate acknowledgement is generated for every single WLAN packet in the aggregated frame. These acknowledgements are again combined to form a block and relayed back to the sender as a group (block acknowledgement). The sender receives information about the receipt status of every single WLAN packet and can, if necessary, resend only those specific packets that were not successful.

The MAC layer

- **Frame aggregation**

The improvements in the physical layer brought about by the new 802.11n initially describe only the theoretical data throughput of the physical medium. However, the share of this theoretical bandwidth that is actually available for payload data is limited by two factors:

- in addition to the actual payload data, each data packet in a wireless LAN system contains additional information such as a preamble and MAC address information.
- Time is lost to the management events that occur when the transmission medium is actually accessed. Thus the transmitter must negotiate access authorization with the other receivers before transmitting each data packet (frame); further delays are caused by data packet collisions and other events.

This loss, referred to as "overhead", can be reduced by combining several data packets together to form one large frame and transmitting them together. In this process, information such as the preamble are only transmitted once for all the combined data packets and delays due to negotiating access to the transmission medium only occur at longer intervals.

The use of this method, known as frame aggregation, is subject to certain restrictions:

- As information such as MAC address only needs to be transmitted once for the aggregated frame, only those data packets intended for the same address can be combined.
- All data packets that are to be combined into a single large frame must be available at the sender at the time of aggregation—as a consequence some data packets may have to wait until enough data packets for the same destination are available with which they can be combined. This aspect may represent a significant limitation for time-critical transmissions such as voice over IP.

- **Block acknowledgement**

Each data packet directed to a specific address (i.e. not broadcast or multicast packets) is acknowledged immediately after receipt. In this way, the transmitter is informed that the packet was received correctly and does not need to be repeated. This principle also applies to aggregated frames in 802.11n.

Two different methods are used for frame aggregation. These are not explained in detail here, but they differ in the way aggregated frames are acknowledged.

- Mac Service Data Units Aggregation (MSDUA) combines several Ethernet packets together to form one common wireless LAN packet. This packet is acknowledged only once and the acknowledgment is valid for all aggregated packets. If there is no acknowledgement the whole block is resent.
- Mac Protocol Data Units Aggregation (MPDUA) combines individual wireless LAN packets together to form one large common wireless LAN packet. In this case, each wireless LAN packet is acknowledged and the acknowledgements are combined and transmitted as a block. In contrast to MSDUA, the sender receives information about the receipt status of every single WLAN packet and can, if necessary, resend only those specific packets that were not successful.

Resulting data throughput

The overall data throughput in a 802.11n network is determined by applying the methods described above. A specific combination of modulation method, payload data rate and number of spatial streams is referred to as modulation coding scheme (MCS). Data throughput also depends on whether the short guard interval and channel bundling to 40 MHz are used.

802.11n uses the term "data throughput" instead of the term "data rate" used in older WLAN standards, because data rate is no longer an adequate description. The following table shows the maximum data throughput when using the short guard interval with 40 MHz channels.

The net data throughput, i.e. the actual number of IP packets transferred, can be up to 90 Mbps for one 802.11n data stream and, accordingly, for two spatial streams up to 180 Mbps. The net data throughput currently (early 2008) observed in practice is usually between 80 and 130 Mbps, depending on how mature the hardware and software are and also on how well the different manufacturers' chip sets work together.

Data streams	Modulation	Payload data rate	Data throughput (GI=0.4 µs, 40 MHz)
1	BPSK	1/2	15
1	QPSK	1/2	30
1	QPSK	3/4	45
1	16QAM	1/2	60
1	16QAM	3/4	90
1	64QAM	1/2	120

Data streams	Modulation	Payload data rate	Data throughput (GI=0.4 µs, 40 MHz)
1	64QAM	3/4	135
1	64QAM	5/6	150
2	BPSK	1/2	30
2	QPSK	1/2	60
2	QPSK	3/4	90
2	16QAM	1/2	120
2	16QAM	3/4	180
2	64QAM	1/2	240
2	64QAM	3/4	270
2	64QAM	5/6	300

11.3.2 IEEE 802.11a: 54 Mbps

IEEE 802.11a specifies the operation of wireless LANs in the 5-GHz frequency band (5.15 GHz to 5.75 GHz) with datarates of up to 54 Mbps. Actual throughput depends on the distance and the quality of the connection. With longer distances and lower connection quality datarates sink to 48 Mbps, thereafter to 36 Mbps and so on until a minimum of 6 Mbps is reached. The range of transmission in the open can reach up to 125m. Inside of buildings this would typically be 25m. The IEEE 802.11a standard operates with OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing).

OFDM

OFDM is a modulation technique that uses multiple carrier frequencies to form the data signal. The technique modulates these carrier frequencies with a reduced datarate. OFDM is highly resistant to the effects of echos and other impairments, and it enables higher datarates.

Turbo mode

In 'Turbo Mode' LANCOM Router base stations can use two radio channels simultaneously to increase datarates to a maximum of 108 Mbps. Turbo mode works with the IEEE 802.11a standard between LANCOM base stations and AirLancer wireless network cards. This increase in datarate must be activated in the base station. This can cause a reduction in transmitting power and range.

11.3.3 IEEE 802.11h – ETSI 301 893

In November 2002, the 5 GHz band was released for private use in Germany, and opened up the path for significantly faster WLAN connections according to the IEEE 802.11a standard, which had already been available for a while. The wider use of 5 GHz WLANs was, however, restricted by its exclusive use in closed spaces and the relatively low transmission power.

With the 802.11h enhancement of September 2003, the private use of the 5 GHz band was finally possible even outside closed spaces. To protect military applications in the 5 GHz band, the DFS (Dynamic Frequency Selection) and TPC (Transmission Power Control) procedures were prescribed. However, when using DFS and TPC with a maximum of 1000 mW (or 4000 mW for commercial network operators in compliance with "Broadband Fixed Wireless Access" regulations), much higher transmission powers can be operated than allowed by previous standards.

ETSI standards

ETSI adopted the first standard for controlling remote data transfers as early as 1996 under the name of Hiperlan (High Performance Radio Local Area Networks). The first version (Hiperlan Type 1) was intended for use in the frequency range of 5.15 to 5.30 GHz with a transmission rate of 20 Mbps. As no manufacturers took up this standard, Hiperlan initially had no practical significance.

With the new version in 2000, Hiperlan Type 2, ETSI introduced a WLAN solution that operates in the 5 GHz band similar to IEEE 802.11a, and also provides a gross data rate of 54 Mbps. However, as the frequencies and the OFMD modulation method that was also used for 802.11a overlapped, it was necessary to adapt the standards between IEEE and ETSI to avoid disruptions to the systems.

European harmonization

To standardize the use of the 5 GHz band in Europe, the European Commission issued the ETSI 301 893 standard on July 11, 2005. The member states of the EU were obliged to implement this by October 31, 2005.

Instead of the three sub-bands described in the 802.11a/h standards (5150 - 5350 MHz, 5470 - 5725 MHz and 5725 - 5875 MHz for the UK), the ETSI 301 893 standard regulates the three following areas with different specifications:

- 5150 - 5250 MHz
- 5250 - 5350 MHz

- 5470 - 5725 MHz

The guidelines focus on preventive measures for avoiding disruptions to other systems that use the same frequency band. This includes radar equipment that counts as "primary applications". The "secondary applications" such as WLAN have to change the frequency as soon as a conflict is detected.

Special regulations for the 5 GHz band

- Dynamic Frequency Selection – DFS

Certain requirements must be observed for the outdoor operation of 5-GHz WLANs if you wish to utilize the maximum permitted performance of 1 or 4 watts. It is vital to avoid interference with radar systems that are active in this spectrum (e.g. meteorological, military). For this reason the European regulatory authority ETSI requires WLAN devices operating at 5 GHz to employ the dynamic frequency selection (DFS) mechanism.

This ensures that radar and WLAN systems can co-exist without interfering with one another and that capacity utilization is spread evenly across available frequencies. When starting a WLAN wireless cell, the access point must check all channels for the presence of radar systems. The check requires an inactive period of one minute, during which the wireless cell cannot be used. As a result, the access point generates a list of radar-free channels which is valid for 24 hours. The best possible channel for operation is selected from this list. During operation, the current channel is continuously checked for radar activity.

If a radar system subsequently starts operation, the channel must be released immediately. In this case, the access point selects the next best available channel, informs the participants in the wireless cell of the impending change, and switches the channel.

The currently selected channel can be used for any length of time, unless radar signals are detected or if the radio cell is restarted (e.g. due to device reconfiguration, firmware upload or reboot).

If the system is able to respond to a channel switch instantaneously, the check must be repeated within 24 hours following a one-minute period of inactivity. The parameter "DFS Rescan Hours" (LCOS menu tree under "Setup/ Interfaces/WLAN/Radio settings") allows a time to be set for conducting the channel check (assuming that the time is available, for example via NTP).

DFS is stipulated for the frequency ranges from 5250 - 5350 MHz, 5470 - 5725 MHz and from 5775 – 5875 (BFWA). It is optional for the frequency range of 5150 - 5250 MHz.

- Transmission Power Control – TPC

  Automatic adjustment of the transmission power reduces radio interference.

  Without DFS and TPC, a maximum of only 200 mW EIRP is permitted. When operating DFS and TPC, a maximum of 200 mW (5150 to 5350 MHz) and 1000 mW EIRP (5470 to 5725 MHz) is permitted as transmitting power (compare 100 mW for 802.11b/g, 2.4 GHz, where DFS and TPC are unnecessary). The higher maximum transmission power not only compensates for the higher attenuation of 5 GHz radio waves in air, it also makes significantly longer ranges possible than in the 2.4 GHz range.

- BFWA (broadband fixed wireless access)

  In Germany in July, 2007, the Federal Network Agency released additional frequencies for broadband fixed wireless bridges in the 5 GHz band. These additional frequencies located in the range between 5755 MHz - 5875 MHz are also referred to as BFWA (Broadband Fixed Wireless Access). The additional frequencies are intended for long-distance point-to-point (P2P) or point-to-multipoint (P2M) links used for providing high-speed Internet access to other users from a central node. This method is intended to provide rural areas with high-speed Internet access.

  The operation of BFWA is restricted to commercial providers only. There are no charges for using these frequencies, but registration is required by the Federal Network Agency. This band covers 120 MHz and offers 6 channels with a bandwidth of 20 MHz each. Maximum transmission power is 36 dBm or 4000 mW. TPC and DFS have to be used when operating BFWA links.

Differences from USA and Asia

The USA and Asia use different frequency bands and maximum signal strengths that are different than the European standard.

In the USA, three subbands, each 100 MHz wide, are used for wireless networks in the 5 GHz band. The "lower band" ranges from 5150 - 5250 MHz, the "middle band" ranges from 5250 - 5350 MHz and the "upper band" ranges from 5725 - 5825 MHz. In the lower band, a maximum average EIRP of 50 mW is permitted; in the middle band this is 250 mW and 1 W in the upper band.

In Japan, the use of the 5 GHz band is possible to a limited extent: only the lower band of 5150 - 5250 MHz is approved for private use.

Available channels in the 5 GHz band

In the available frequency range of 5.13 to 5.875 GHz, the following channels are available in Europe, divided into frequency ranges to which different conditions of use can apply:

- 5150 -5350 MHz (channels 36, 40, 44 and 48)
- 5250 -5350 MHz (channels 52, 56, 60 and 64)
- 5470 - 5725 MHz (channels 100, 104, 108, 112, 116, 132, 136 and 140)
- 5755 - 5875 MHz
  - □ Channels 151, 155, 159 , 163, 167: In Germany is for commercial use only and only in combination with DFS (BFWA).
  - □ Channels 149, 153, 157, 161, 165: For FCC use in the USA, without DFS.

Channels 120, 124 and 128 have been available in the past and are now blocked.

The following overview shows which channels may be used in the different regions:

* Note: Please note that the frequency ranges and radio channels in band 3 are subject to certain restrictions depending on country (e.g. in Germany only permitted for public "Broadband Fixed Wireless Access" communications providers).

Frequency ranges for indoor/outdoor use in the 5 GHz band

The use of the methods described in ETSI 301 893 for reducing mutual interference in the 5 GHz band (TPC and DFS) is not stipulated for all fields of application. The following table provides information about the permitted use and corresponding transmission powers within the EU:

Frequency (GHz)	Transmission-power (mW/dBm)	Use	DFS	TPC
5,15-5,25	200/23	Indoor		
5,25-5,35	200/23	Indoor	✔	✔
5,470-5,725	1000/30	Indoor/Outdoor	✔	✔
5,755-5,875	4000/36	Outdoor (BFWA)	✔	✔

Other regulations may apply for use in other countries. Please refer to the current wireless network regulations for the country in which you wish to operate a wireless LAN device, and ensure that you set the country of operation in the wireless LAN settings.

11.3.4 IEEE 802.11g: 54 Mbps

The IEEE 802.11g standard also works with datarates of up to 54 Mbps in the 2.4 GHz ISM frequency band. Unlike IEEE 802.11b, the IEEE 802.11g standard works with OFDM modulation, as used by the earlier standard IEEE 802.11a. IEEE 802.11g features a specialized compatibility mode for backwards compatibility with the widely available IEEE 802.11b standard. However, operating this compatibility mode incurs performance losses. IEEE 802.11g is not compatible to IEEE 802.11a as they operate at different frequencies. IEEE 802.11g products offer similar ranges to IEEE 802.11b products.

Turbo mode

The 802.11g standard can also be operated with Turbo Mode, which uses two radio channels in parallel to increase datarates to a maximum of 108 Mbps. Because the 2.4-GHz band has fewer channels to offer than the 5-GHz band, operating Turbo Mode places clear limits on the choice of available channels.

11.3.5 IEEE 802.11b: 11 Mbps

IEEE 802.11b specifies the operation of local wireless networks in the ISM frequency band (**I**ndustrial, **S**cientific, **M**edical: 2.4 to 2.483 GHz). Maximum datarates are up to 11 Mbps. Actual throughput depends on the distance and the quality of the connection. With longer distances and lower connection quality datarates sink to 5.5 Mbps, thereafter to 2 Mbps and then to 1 Mbps. The range of transmission in the open can reach up to 150 m. Inside of buildings this would typically be 30 m. IEEE 802.11b is not compatible to IEEE 802.11a as they operate at different frequencies.

DSSS

To protect against interference from other transmitters operating on the same frequency, the 2.4-GHz frequency band for IEEE 802.11b offers the DSSS procedure (**D**irect **S**equence **S**pread **S**pectrum). Generally, a transmitter occupies only a very narrow band of the available frequencies. If this band is also being used by another transmitter, interference may occur. The DSSS method uses a broader band of the available frequency range, making it less sensitive to narrow-band interference.

11.4 WLAN security

11.4.1 Basics

Even though one constantly hears the blanket term 'Security' when talking about computer networks, it is still important for the coming exposition to differentiate a little more closely between the requirements it actually entails.

Authentication

The first point in security is access security:

- Here, a protective mechanism is involved which allows access to the network only to authorized users.
- On the other hand, however, it must also be ensured that the client is connected to the precise desired access point, and not with some other access point with the same name which has been smuggled in by some nefarious third party. Such an authentication can be provided, for example, using certificates or passwords.

Authenticity

Authenticity: Proof of the authorship of the data and the originality of the data content; the process of establishing this proof is known as authentication.

Integrity

Once access is provided, one would like to ensure that data packets reach the receiver without any falsification, that is, that no-one can change the packets or insert other data into the communication path. The manipulation of data packets themselves cannot be prevented, but changed packets can indeed be identified using suitable checksum processes, and then dropped.

Confidentiality

Quite separate from access security is confidentiality, that is, unauthorized third parties must not be able to read the data traffic. To this end, the data are encrypted. This sort of encryption process is exemplified by DES, AES, RC4, or Blowfish. Along with encryption, of course, there must also be a corresponding decryption on the receiving end, generally with the same key (a so-called symmetric encryption process). The problem naturally then arises, how the sender can give the key to the receiver for the first time—a simple transmission could very easily be read by a third party, who could then easily decrypt the data traffic.

In the simplest case, this problem is left to the user, that is, one simply assumes that the user can make the key known at both ends of the connection. In this case, one speaks of pre-shared keys, or 'PSK'.

More sophisticated processes come into play when the use of pre-shared keys is impractical, for instance in an HTTP connection built over SSL—in this case, the user can't retrieve a key from a remote web server quite so easily. In this case, so-called assymetric encryption methods such as RSA can be used, that is, to **de**crypt the data, a different key is used than the one used to **en**crypt it, meaning that key pairs are used. Such methods are, however, much slower than symmetric encryption methods, which leads to a two-phase solution:

- The sender possesses an asymmetric key pair. It transmits the public part of the key pair, i.e. the key for **en**cryption, to the receiver as a certificate, for example. Since this part of the key pair cannot be used for **de**cryption, there are no misgivings with regard to security.
- The receiver selects any symmetrical key. This symmetrical key that is used both for **en**cryption and for **de**cryption, must now be securely transmitted to the sender. It is encrypted with the sender's public key and returned to the sender. The only way that the symmetrical key can be decrypted again is with the sender's private key. Potential eavesdroppers observing the key exchange cannot decrypt this information, and consequently the transmission of the symmetrical key is secure.

11.4.2 IEEE 802.11i /WPA2

In mid-2004 the IEEE adopted the standard 802.11i, also known as WiFi Protected Access 2 (WPA2). WPA2 is currently the highest standard of security available for WLANs. It enables the authentication and authorization of users by IEEE 802.1X. It also supports AES encryption, which is a far more secure technique than WEP or WPA. The following sections outline some relevant technical aspects.

EAP and IEEE 802.1x

A clear increase in WLAN security can be achieved by using keys that are dynamically negotiated instead of keys with fixed values. 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 key for the next session is more or less a byproduct. Figure 2 shows the basic process of a session secured by EAP.

In principle, EAP / 802.1X can be used in combination with WEP. However, this method is generally employed with WLANs using WPA2.

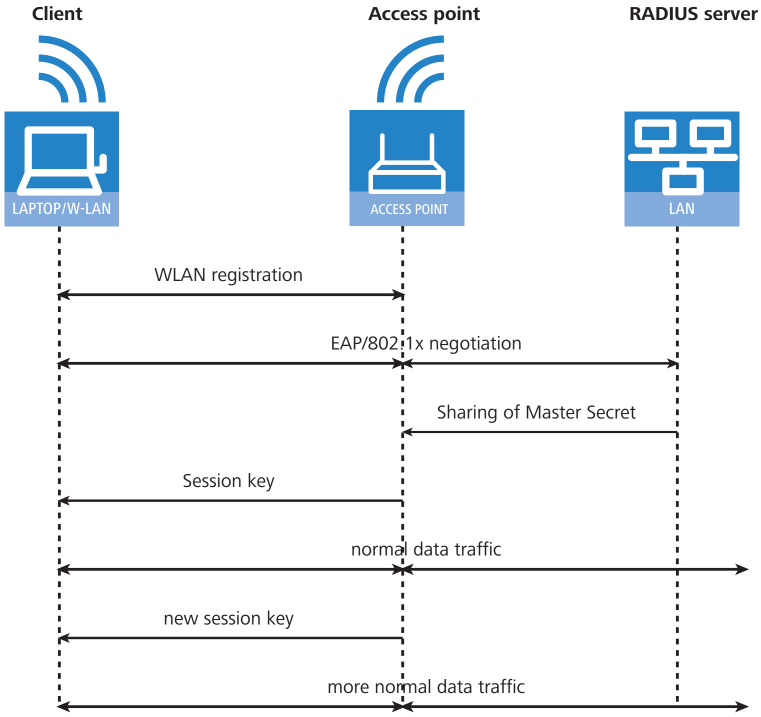


Figure 2: Schematic process of a WLAN session with EAP/802.1x

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 the formerly used WEP—but not with EAP, because in this state the client still doesn't have a key to secure its data traffic from eavesdropping. Instead, the client is in an 'intermediate state' from the point of view of the access point, in which only particular packets from the client are forwarded, and these are only directed to an authentication server. These packets are the EAP/802.1x mentioned previously. The access point packs these packets in RADIUS queries and sends them on to the authentication server. The access point converts the replies coming from the RADIUS server back into EAP packets, and sends them back to the client.

The access point is thus a sort of middle man between client and server. it doesn't have to check the contents of these packets, it just has to check that no other data traffic to or from the client can occur. Over this "tunnel" through the access point, the client and server authenticate one another, that is, the server checks the client's access privilege to the network, and the client checks that it is talking to the right network. "Wild" access points set up by hackers can be recognized in this way.

A whole series of authentication processes exist which can be used in this tunnel. A current process (and one supported by Windows XP) is for instance TLS, in which server and client exchange certificates; another is TTLS, in which only the server supplies a certificate—the client is authenticated using only a username and password.

After the authentication phase, a secure tunnel even without encryption has been set up, in which the access point is connected in the next step. For this, the RADIUS server sends the so-called 'Master Secret', a session key calculated during the negotiation, to the access point. The LAN behind the access point is considered secure in this scenario, so that this transmission can be performed in clear text.

With this session key, the access point now takes over the tunnel and can use it to provide the actual key to the client. Depending on the capabilities of the access point hardware, this can be a true session key, i.e. a key which will only be used for data packets between the access point and precisely this client. Older WEP uses a hardware group key, which the access point will use for communication with multiple clients.

The particular advantage of this procedure is that the access point can regularly change the key over the EAP tunnel, that is, it can perform a so-called rekeying. In this way, 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 keys might be 5 minutes.

WPA with passphrase

The handshake described in the EAP/802.1X section runs strictly under WPA, i.e. the user will never have to define any keys. In environments in which no RADIUS server is available to provide master secrets (for instance in smaller companies), WPA therefore provides the PSK method besides authentication using a RADIUS server; here, the user must enter a passphrase of 8 to 63 characters on the access point and on all stations, from which the master secret is calculated along with the SSID used using a hash procedure. The master secret is therefore constant in such a PSK network, although different session keys still result.

In a PSK network both access security and confidentiality depend on the passphrase not being divulged to unauthorized people. As long as this is the case, WPA-PSK provides significantly improved security against break-ins and eavesdropping over any WEP variant. For larger installations in which such a passphrase would have to be made known to too large a user community for it to be kept secret, EAP/802.11i is used in combination with the key handshake described here.

TKIP

TKIP stands for **T**emporal **K**ey **I**ntegrity **P**rotocol. As the name suggests, it involves an intermediate solution for temporary use until a truly strong encryption procedure is introduced, but which dealt with the problems of the then popular WEP, never the less. Employing TKIP is only recommended for operating older WLAN clients which do not support AES.

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. Not all older WLAN chips support TKIP, so 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. Using AES is optional.

The suffix CCM denotes the way in which AES is used in WLAN packets. The process is actually quite complicated, for which reason CCM is only sensibly implemented in hardware—software-based implementations are possible, but would result in significant speed penalties due to the processors commonly used in access points.

In contrast to TKIP, AES only requires a 128-bit key, with which both the encryption and protection against undetected changes to packets is achieved. Furthermore, CCM is fully symmetric, i.e. the same key is used in both communications directions—a standards compliant TKIP implementation, on the other hand, requires the use of different Michael keys in the send and receive directions, so that CCM is significantly simpler in use than TKIP.

Similar to TKIP, CCM uses a 48-bit Initial Vector in each packet—an IV repetition is impossible in practice. As in TKIP, the receiver notes the last IV used and drops packets with an IV which is equal to or less than the comparison value.

Pre-authentication and PMK caching

802.11i is intended to help with the use of WLAN for speech connections (VoIP) in enterprise networks. Especially in connection with WLAN-based wireless telephony, quick roaming (switching from one access point to another without lengthy interruptions) is of special significance. In telephone conversations, interruptions of 100 milliseconds are irritating, but the full authentication process over 802.1x, including the subsequent key negotiation with the access point, can take significantly longer.

For this reason, the so-called PMK caching was introduced as a first measure. The PMK serves as the basis for key negotiation in an 802.1x authentication between client and access point. In VoIP environments it is possible that a user moves back and forth among a relatively small number of access points. Thus it may happen that a client switches back to an access point in which it was already registered earlier. In this case it wouldn't be sensible to repeat the entire 802.1x authentication again. For this reason, the access point can provide the PMK with a code, the so-called PMKID, which it transmits to the client. Upon a new registration, the client uses the PMKID to ask whether this PMK is still stored. If yes, the 802.1x phase can be skipped and the connection is quickly restored. This optimization is unnecessary if the PMK in a WLAN is calculated from a passphrase as this applies everywhere and is known.

A second measure allows for some acceleration even in the case of first-time registration, but it requires a little care on the part of the client. The client must already detect a degrading connection to the access point during operation and select a new access point while it is still in communication with the old access point. In this case it has the opportunity to perform the 802,1x negotiation with the new access point over the old one, which again reduces the "dead time" by the time required for the 802.1x negotiation.

11.4.3 TKIP and WPA

As clarified in the last section, the WEP algorithm is flawed and insecure in principle; the measures taken so far were largely either 'quick fixes' with limited improvement, or so complicated that they were basically impractical for home use or smaller installations.

After the problems with WEP became public knowledge, the IEEE began with the development of the standard IEEE 802.11i. As an interim solution, the WiFi Alliance defined the Wifi Protected Access (WPA) 'standard'. WPA uses the following changes:

- TKIP and Michael as replacement for WEP
- A standardized handshake procedure between client and access point for determination/transmission of the session key.
- A simplified procedure for deriving the Master Secret mentioned in the last section, which can be performed without a RADIUS server.
- Negotiation of encryption procedure between access point and client.

Encryption makes use of components familiar from WEP but benefits from decisive improvements with the "Michael hash" from improved encryption and the TKIP method for calculation of the RC4 key. Furthermore, the internally incremented IV transmitted in clear text in the packet is 48 bits long instead of 24--thus the problem with the repeating IV value is practically excluded.

As a further detail, TKIP also mixes the MAC address of the sender into the calculation of the key. This ensures that the use of identical IVs by different senders cannot lead to identical RC4 keys and thus again to attack possibilities.

The Michael hash does not, however, represent a particularly tough cryptographic hurdle: if the attacker can break the TKIP key or get encrypted packets past the CRC check via modifications similar to those for WEP, then not many barriers remain. For this reason, WPA defines countermeasures if a WLAN module 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.

Negotiating the encryption method

Since the original WEP definition specified a fixed key length of 40 bits, the registration of a client at an access point only had to communicate whether encryption should be used or not. Key lengths exceeding 40 bits require that the key length is announced. WPA provides a mechanism with which client and access point can agree on the encryption and authentication procedures to be used. The following information is made available:

- A list of encryption methods which the access point provides for the pairwise key—here, WEP is explicitly disallowed.
- A list of authentication methods a client may use to show itself to the WLAN as authorized for access—possible methods are currently EAP/802.1x or PSK.

As mentioned, the original WPA standard specifies only TKIP/Michael as an improved encryption method. With the further development of the 802.11i standard, the AES/CCM method described below was added. In a WPA network it is now possible for some clients to communicate with the access point using TKIP, while other clients use AES.

11.4.4 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.

> ! WEP offers far lower security that IEEE 802.1x/WPA2. For reasons of compatibility to older WLAN clients, LANCOM Access Points continue to support this method of encryption. However, LANCOM Systems expressly recommends the use of a better form of WLAN security (e. g. IEEE 802.1X/WPA2).

11.4.5 LEPS – LANCOM Enhanced Passphrase Security

LEPS remedies the security issues presented by global passphrases.

The modern encryption methods WPA and IEEE 802.11i provide data traffic in the WLAN with far improved security from eavesdroppers than the older WEP can. It is very easy to handle a passphrase as a central key; a RADIUS server such as that for 802.1x installations is not required.

However, the use of WPA and IEEE 802.11i still has some weak spots:

- A passphrase applies **globally** for **all** WLAN clients
- The passphrase may fall into unauthorized hands if treated carelessly
- The "leaked" passphrase then offers any attacker free access to the wireless network

This means in practice that: Should the passphrase "go missing" or an employee with knowledge of the passphrase leaves the company, then the passphrase in the access point needs to be changed in the interests of security—in every WLAN client, too. As this is not always possible, an improvement would be to have an individual passphrase for each user in the WLAN instead of a global passphrase for all WLAN clients. In the case mentioned above, the situation of an employee leaving the company requires merely his "personal" passphrase to be deleted; all others remain valid and confidential.

With LEPS (**L**ANCOM **E**nhanced **P**assphrase **S**ecurity), LANCOM Systems has developed an efficient method that makes use of the simple configuration of IEEE 802.11i with passphrase, but that avoids the potential security loopholes that come with global passphrases.

LEPS uses an additional column in the ACL (access-control list) to assign an **individual** passphrase consisting of any 8 to 63 ASCII characters to each MAC address. The connection to the access point and the subsequent encryption with IEEE 802.11i or WPA is only possible with the right combination of passphrase and MAC address.

This combination makes the spoofing of the MAC addresses futile—and LEPS thus shuts out a potential attack on the ACL. If WPA or IEEE 802.11i is used for encryption, the MAC address can indeed be intercepted—but this method never transmits the passphrase over wireless. This greatly increases the difficulty of attacking the WLAN as the combination of MAC address and passphrase requires both to be known before an encryption can be negotiated.

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

ⓘ An additional security aspect: LEPS can also be used to secure single point-to-point (P2P) connections with an individual passphrase. Even if an access point in a P2P installation is stolen and the passphrase and MAC address become known, all other WLAN connections secured by LEPS remain secure, particularly when the ACL is stored on a RADIUS server.

Configuration

The configuration of LEPS merely involves the assignment of an individual passphrase to the MAC address of each client that is approved for the WLAN. To this end, the MAC filter is set to positive, i.e. the data from clients entered here will be transmitted.

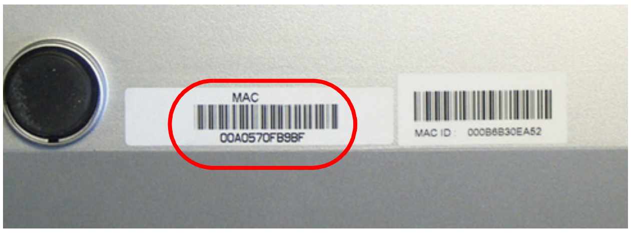
ⓘ The passphrases should consist of a random string at least 32 characters long.

11.4.6 Standard WEP encryption

Ex-factory, WEP128 encryption is activated for every unconfigured LANCOM Wireless Router as standard. This encryption is only to be used until the WLAN is configured for the first time.

Ex-factory, LANCOM Access Points are set to "managed mode" as standard, and the WLAN modules are switched off. For this reason the first-time configuration of LANCOM Access Points via WLAN is not possible. This WEP encryption in WLAN devices being managed by a LANCOM WLAN Controller is overwritten by the central encryption settings in the profiles of the WLAN Controller.

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



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

To use a WLAN adapter to establish a connection to a new LANCOM access point, the WEP128 encryption must be activated for the WLAN adapter and the standard 13-character WEP key entered.

ⓘ After registering for the first time, switch the WLAN encryption to WPA2/802.11i to ensure that you have a secure connection.

! Note that a reset causes the WLAN key settings to be lost from the device and the standard WEP key comes into effect again. WLAN access can only work after a reset if the standard WEP key is programmed into the WLAN client as well.

11.4.7 Background WLAN scanning

To detect other access points within range, LANCOM Wireless Routers actively scan all of the available channels (just as a WLAN client would do to find an available access point). If another access point is active, the relevant information is stored to the scan table. Since this recording occurs in the background in addition to the access points' "normal" radio activity, it is called a "background scan".

Background scanning is mainly used for the following tasks:

- Rogue AP detection
- Fast roaming for WLAN clients

Rogue AP detection

WLAN devices that make unauthorized attempts at accessing a WLAN by posing as an access point or client are called rogues. An example of rogue APs are access points that a company's employees connect to the network without the knowledge or permission of the system administrators, thereby consciously or unconsciously making the network vulnerable to potential attackers via unsecured WLAN access. Not quite as dangerous, but disruptive all the same are access points that belong to third-party networks yet are within the range of the local WLAN. If such devices also use the same SSID and channel as the local AP (default settings), then local clients could attempt to log on to external networks.

Unidentified access points within the range of the local network frequently pose a possible threat and security gap. At the very least, they are a disturbance. Therefore, background scanning identifies rogue APs and helps to decide whether further measures in securing the local network need to be introduced.

Fast roaming in client mode

However, the background scanning method can be used for objectives other than rogue AP detection. A LANCOM Access Point in client mode that logs itself on to another access point can also use the roaming procedure in a mobile installation. This is the case, for example, when a LANCOM Access Point used in an industrial application scenario is mounted to a forklift that navigates its way through multiple warehouses with separate access points. Under normal circumstances, the WLAN client would only log on to another access point when the connection to the access point it had been using until that moment was lost. With the background scanning function, the LANCOM Access Point using the client mode can collect information about other available access points in advance. In this case the client is not switched to another access point once the existing connection has been lost completely, but rather when another access point within its range has a stronger signal.

Evaluating the background scan

The information on the access points found can be viewed in the LANCOM Access Point statistics. The WLANmonitor presents the scan results quite conveniently and also offers additional functions such as access point grouping or automatic notification via e-mail whenever a new WLAN device appears.

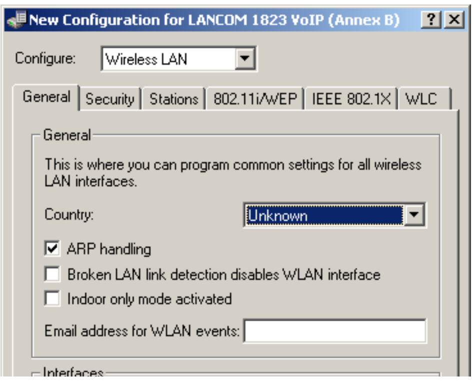
Please refer to ’Rogue AP and rogue client detection with the WLANmonitor’ → page 3-25 for further information.

11.5 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 interfaces. Some LANCOM models have just one WLAN interface (single radio access point), and others have a second WLAN module integrated (dual radio access point). The settings for the physical WLAN interface apply to all of the logical wireless networks supported by this module. These parameters include, for example, the transmitting power of the antenna and the operating mode of the WLAN module (access point or client).
- Other parameters are related solely to the logical wireless network that is supported by a physical interface. These include, among others, the SSID or activation of the encryption, such as 802.11i with AES.
- 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.

11.5.1 General WLAN settings



Configure: Wireless LAN

General

This is where you can program common settings for all wireless LAN interfaces.

Country: Unknown

☑ ARP handling

☐ Broken LAN link detection disables WLAN interface

☐ Indoor only mode activated

Email address for WLAN events:

LANconfig: Wireless LAN ▶ General

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN

- **Country setting**

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

- **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 module if the access point loses contact to the LAN.

- **Indoor function for WLAN channels**

  When selecting the frequency band (2.4 or 5 GHz), among other things, you must determine the channels which may possibly be used for transmission. From these possible channels, under automatic channel selection, a LANCOM Wireless Router selects a free channel, for example, in order to avoid interference with other radio signals.

  In some countries, there are special regulations on the frequency bands and channels which may be used for WLAN for indoor and outdoor operation. For example, in France, not all available channels in the 2.4 GHz band may be used in outdoor operation. In some countries the DFS procedure is required for outdoor operation in the 5 GHz band in order to avoid interference from radar systems.

  With the option 'indoor-only' a LANCOM Wireless Router can be restricted exclusively to operation in closed buildings. This restriction on the other hand allows the channels to be managed more flexibly under automatic channel selection.

Activating the indoor-only function can only be relied upon if the country in which the access point is being operated has been set.

Activating the indoor-only function is only permitted when the access point and all connected clients are located in a closed space.

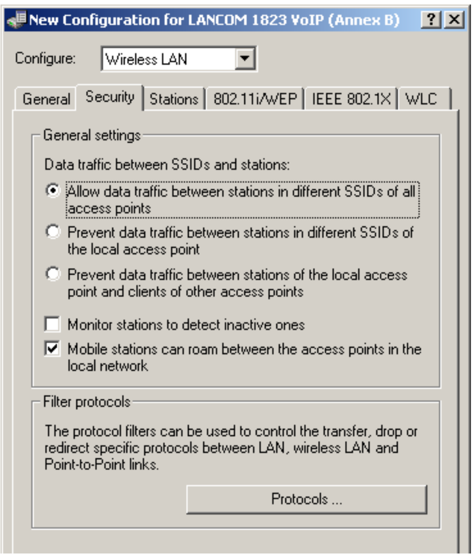
- **Mail address**

  Information about events in the WLAN is sent to this e-mail address.

11.5.2 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



General settings

Data traffic between SSIDs and stations:

● Allow data traffic between stations in different SSIDs of all access points

○ Prevent data traffic between stations in different SSIDs of the local access point

○ Prevent data traffic between stations of the local access point and clients of other access points

□ Monitor stations to detect inactive ones

☑ Mobile stations can roam between the access points in the local network

Filter protocols

The protocol filters can be used to control the transfer, drop or redirect specific protocols between LAN, wireless LAN and Point-to-Point links.

LANconfig: Wireless LAN ▶ Security

- **Data traffic between SSIDs and stations**

  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. Communications between clients in different SSIDs can be allowed or stopped with this option. For models with multiple WLAN modules, this setting applies globally to all WLANs and all modules.

Communications between clients in a logical WLAN is controlled separately by the logical WLAN settings (Inter-Station-Traffic). If the Inter-SSID-Traffic is activated and the Inter-Station-Traffic deactivated, a client in one logical WLAN can communicate with clients in another logical WLAN. This option can be prevented with the VLAN settings or protocol filter.

- **Monitor stations to detect stations that are inactive**

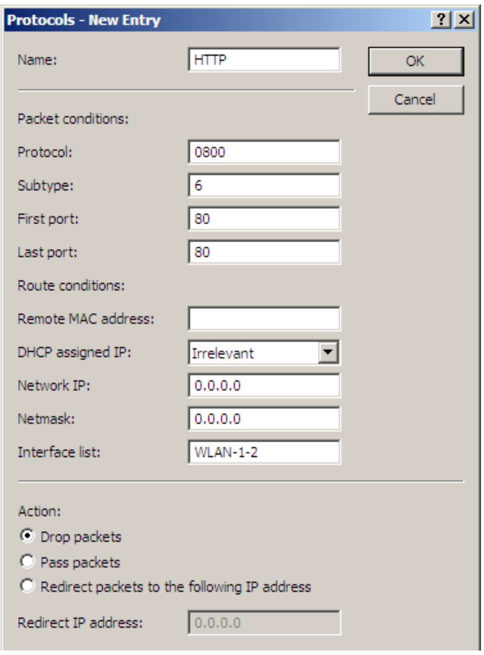
  In particular for public WLAN access points (public spots), the charging of usage fees requires the recognition of stations that are no longer active. Monitoring involves the access point regularly sending packets to logged-in stations. If the stations do not answer these packets, then the charging systems recognizes the station as no longer active.

- **Mobile stations can switch between base stations in the local network (roaming)**

  In addition to controlling the communication between clients, you can also define whether neighboring access points can exchange information via the IAPP. The Inter Access Point Protocol (IAPP) controls communications between access points. The "outgoing" access point receives information that a WLAN client associated with it is switching to another access point, and that the client can be removed from its list.

Protocol filters

With the protocol filter you can influence the handling of certain protocols during transfer from the WLAN to the LAN. The use of appropriate rules allows the definition of which data packets should be inspected, interfaces for which the filter applies and which action should be performed on the data packets.



Protocols - New Entry

Name:	HTTP
Packet conditions:	
Protocol:	0800
Subtype:	6
First port:	80
Last port:	80
Route conditions:	
Remote MAC address:	
DHCP assigned IP:	Irrelevant
Network IP:	0.0.0.0
Netmask:	0.0.0.0
Interface list:	WLAN-1-2

Action:

● Drop packets

○ Pass packets

○ Redirect packets to the following IP address

Redirect IP address: 0.0.0.0

LANconfig: Wireless LAN ▶ Security ▶ Protocols

WEBconfig: LCOS menu tree ▶ Setup ▶ LAN bridge ▶ Protocol table

Similar to a firewall rule, a protocol filter consists of two parts:

- The packet conditions defines the conditions that must be satisfied in order for the filter to be applied to a packet.
- The action defines what happens to the packet if the condition is met.

A packet filter is described by the following parameters:

- **Name**: A name of your choice for the filter entry
- **Protocol**: The protocol that this filter is valid for. If '0' is entered as the protocol, the filter applies to **all** packets.
- **Subtype**: The sub-protocol for which this filter is valid. If '0' is entered as the sub-protocol, the filter applies to **all** packets of the protocol entered.
- **Start port** and **end port**: The port range that this filter is to be valid for. If '0' is entered as the start port, this filter will be applied to all ports of the corresponding protocol/sub-protocol. If '0' is entered as the end port, the start port becomes an end port.

Lists of the official protocol and port numbers are available in the Internet under www.iana.org.

- **Destination MAC address**: The MAC address of the client to which the packet is to be sent. If no destination MAC address is entered, the filter is applied to **all** packets.
- **DHCP source MAC**: Enabling of DHCP address tracking.
  - **Yes**: The rule applies if the source MAC address of the packet is listed in the table under `Status > LAN Bridge Statistics > DHCP Table` as an address which obtained an IP address using DHCP.
  - **No**: The rule applies if this is not the case.
  - **Irrelevant**: The source MAC address is not considered.

If DHCP address tracking is enabled, any IP addresses usually entered are disregarded. Please refer to ’DHCP address tracking’ → page 11-25 for further information.

- **IP network** and **IP netmask**: The IP address of the network mask to which this filter applies. Only those IP packets whose source and destination IP addresses lie within this network are captured by the rule.

  If no network is entered, the filter applies to **all** packets.
- **Interface list**: List of the interfaces to which the filter applies.

  All of the LAN interfaces, DMZ interfaces, logical WLAN networks and point-to-point connections in the WLAN may be entered as interfaces.

  The following examples illustrate how interfaces are specified: 'LAN-1' for the first LAN interface, 'WLAN-2-3' for the third logical WLAN network on the second physical WLAN interface, 'P2P-1-2' for the second point-to-point connection on the first physical WLAN interface.

Groups of interfaces may be specified in the form 'WLAN-1~WLAN-1-6' (logical WLANs 1 to 6 on the first physical WLAN interface) or with a wildcard as 'P2P-1-*' (all P2P connections on the first physical interface).

Only filter rules with valid entries in the interface list are active. A rule with no specification of the interfaces does not apply to all of them - it is ignored instead.

- **Action**: Action performed for the data packets captured using this rule:
- **Redirect IP address**: Destination IP address for the "Redirect" action

  On redirection, the destination IP address of the packets is replaced by the Redirect IP address entered here. Furthermore, the destination MAC address is replaced by the MAC address determined using ARP for the Redirect IP address.

If ARP was unable to determine the destination MAC address, the packet is dropped rather than redirected.

Example:

Name	DHCP source MAC:	Destination MAC address.	Prot.	IP address	IP network:	Subtype	Start port	End port	Interface list	Action	Redirect IP address
ARP	irrelevant	000000000000	0806	0.0.0.0	0.0.0.0	0	0	0	WLAN-1-2	Pass	0.0.0.0
DHCP	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	17	67	68	WLAN 1-2	Pass	0.0.0.0
TELNET	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	6	23	23	WLAN 1-2	Redirect	192.168.11.5
ICMP	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	1	0	0	WLAN 1-2	Pass	0.0.0.0
HTTP	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	6	80	80	WLAN 1-2	Redirect	192.168.11.5

ARP, DHCP, ICMP are allowed to pass, Telnet and HTTP are redirected to 192.168.11.5 and all other packets are rejected.

- **Procedure for filter test**

If no filter rules are defined for an interface, all packets from and destined to it are transmitted without alteration. As soon as a filter rule has been defined for an interface, all packets to be transferred via this interface are checked prior to being processed.

① As a first step, the information required for checking is read out of the packets:

- □ DHCP source MAC:
- □ Destination MAC address of the packet:
- □ Protocol, e.g. IPv4, IPX, ARP
- □ Sub-protocol, e.g. TCP, UDP or ICMP for IPv4 packets, ARP Request or ARP Response for ARP packets
- □ IP address and network mask (source and destination) for IPv4 packets
- □ Source and destination port for IPv4 TCP or IPv4 UDP packets

② As a second step, this information is checked against the information from the filter rules. All those rules in which the source **or** destination interface is included in the interface list are considered. Checking of the rules for the individual values is as follows:

- □ For DHCP source MAC, protocol and sub-protocol, the values read out of the packets are checked for consistency with the values defined in the rule.
- □ With IP addresses, the source **and** destination address of the packet are checked to see whether they lie within the range formed by the IP address and the network mask of the rule.
- □ Source and destination ports are checked to see whether they lie in the range between start port and end port.

If none of the rule values specified (not filled by wildcards) agree with the values read out of the packet, the rule is not considered applicable and is disregarded. If several rules apply, the most accurate rule action is carried out. Parameters are more accurate the further down the list of parameters they are or the further right they appear in the protocol table.

If rules are defined for an interface, but there is no match with one of the rules for a packet from/for this interface, the default rule for this interface is used for the packet. The default rule is pre-configured for each interface with the 'drop' action but this is not visible in the protocol table. To modify a default rule for an interface, a rule with the name 'default-drop' is defined. Besides the interface naming, this rule can only contain wildcats and the required action.

Checking of MAC addresses in packets sent over the respective interface takes on a different form to that with incoming packets.

- □ With out-going packets, the source MAC address read out of the packet is checked against the destination MAC address entered in the rule.
- □ The destination MAC addresses read out of the packet are then checked to see whether they are listed as currently active DHCP clients.
- □ Rules with the 'Redirect' action are ignored if they apply for an interface over which the packet is to be sent.

③ In the third step, the action associated with the applicable rule is carried out.

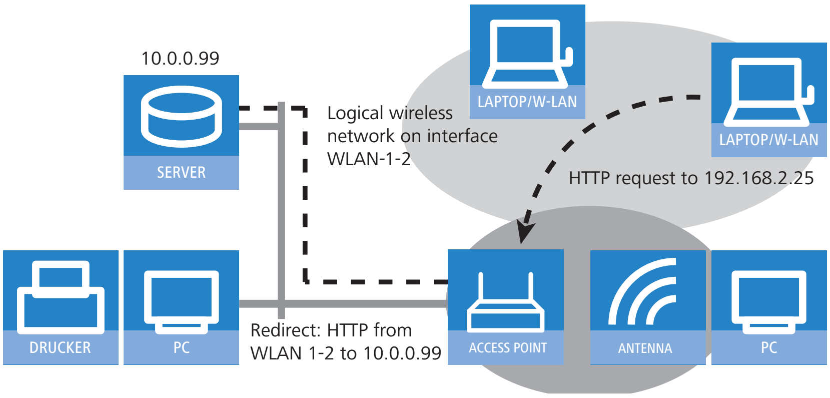
■ Redirect function

With the Redirect action, IPv4 packets can not only be transferred and dropped, they can also be communicated specifically to a particular destination. As a general rule, the destination IP address of the packet is replaced by the Redirect IP address entered. The destination MAC address of the packet is replaced by the MAC address determined by ARP and associated with the Redirect IP address.

In order for the redirected packets to find the correct sender on their "return trip", a dynamic table is compiled with automatic filter rules that apply to packets leaving via this interface. This table can be viewed under `Status > LAN bridge > Connection table`. Rules in this table have a higher priority than other matching rules with the 'Transfer' or 'Drop' actions.

Clients within wireless networks often have one aspect in common: a high degree of mobility. Consequently, clients are not necessarily always connected to the same access point, but frequently change between access points and the related LANs.

The redirect function assists WLAN client applications to automatically find the correct target computer in the LAN. If a WLAN client's HTTP request from a particular logical wireless network is to be always directed to a particular server in the LAN, a filter setting with the "Redirect" action is set up for the appropriate protocol for the desired logical WLAN interface.


10.0.0.99
SERVER
Logical wireless network on interface WLAN-1-2
LAPTOP/W-LAN
LAPTOP/W-LAN
HTTP request to 192.168.2.25
DRUCKER
PC
Redirect: HTTP from WLAN 1-2 to 10.0.0.99
ACCESS POINT
ANTENNA
PC

All requests with this protocol from this logical wireless network are automatically redirected to the target server in the LAN. The returning data packets are sent to the senders' addresses and ports according to the entries in the connection statistics, ensuring trouble-free operation in both directions.

■ DHCP address tracking

DHCP address tracking keeps a record of which clients have received their IP addresses using DHCP. The relevant information for an interface is automatically maintained in a table under `Status > LAN Bridge Statistics > DHCP Table`. DHCP tracking is enabled on an interface if, for this interface, a minimum of one rule is defined where 'DHCP Source MAC' is set to 'Yes'.

ⓘ The number of clients which may be connected to an interface via DHCP can be configured in the Port table under `Setup > LAN Bridge > Port Data`. Setting the entry to '0' means that any number of clients can register at this interface via DHCP. If the maximum number of DHCP clients is exceeded by a further attempt to register, the oldest entry in the list is deleted.

When checking data packets, IP addresses and the IP network mask defined in the rule are not used. Consequently no check is made as to whether the destination IP address of the packet lies within the range specified. Instead, a check is made as to whether the source IP address of the packet matches the IP address assigned to the client via DHCP. The connection of the two IP addresses is made based on the source MAC address.

This check can be used to block clients which have received an IP address via DHCP, but which actually use a different IP address (either intentionally or inadvertently). A rule in which the DHCP Source MAC parameter is set to 'Yes' would not apply since the two addresses do not match. The packet would instead be processed either by other rules or the default rule.

In order for DHCP tracking to work, at least two more rules must be set up for this interface, rules which are not dependent on DHCP tracking. This is necessary since the required DHCP information is not exchanged until the end of DHCP handshake. This is why packets due to be sent beforehand must be allowed by rules which do not use DHCP tracking. These usually included TCP/UDP packets on port 67 and 68 and ARP packets.

If DHCP tracking is enabled on an interface, packets received on this interface from DHCP servers are automatically dropped.

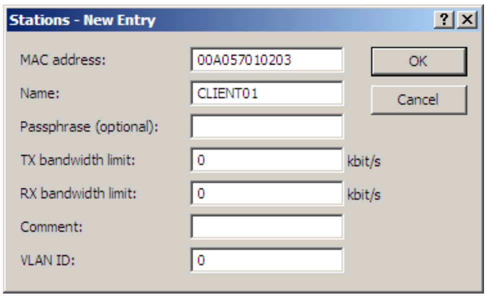
11.5.3 Selecting approved stations for the WLAN

Access-control list

With the **A**ccess **C**ontrol **L**ist (ACL) you can permit or prevent the access to your wireless LAN by individual clients. The decision is based on the MAC address that is permanently programmed into wireless LAN adapters.

When working with central management of LANCOM Wireless Routers and LANCOM Access Points by LANCOM WLAN Controller, the table of stations is to be found in the area 'WLAN Controller' on the 'Stations' tab and then with the **Stations** button.

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'.



MAC address: 00A057010203
Name: CLIENT01
Passphrase (optional):
TX bandwidth limit: 0 kbit/s
RX bandwidth limit: 0 kbit/s
Comment:
VLAN ID: 0

LANconfig: Wireless LAN ▶ Stations ▶ Stations

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN ▶ Access list

- **MAC address**

  MAC address of the WLAN client for this entry.

- **Name**

  WLAN client name for easy identification, e.g. employees.

- **Passphrase**

  Passphrase for the WLAN client in networks with 802.11i/WPA/AES-PSK.

- **TX bandwidth limit**

  Permitted bandwidth tor this WLAN client. Also see 'Bandwidth limits in the WLAN' → page 11-78

- **RX bandwidth limit**

  Permitted bandwidth tor this WLAN client. Also see 'Bandwidth limits in the WLAN' → page 11-78

- **VLAN ID**

  This VLAN ID is assigned to packets that are received from the client with the MAC address entered here. In case of VLAN-ID 0, the station is not assigned a specific VLAN ID. Instead, the VLAN ID for the radio cell (SSID) applies.

11.5.4 Encryption settings

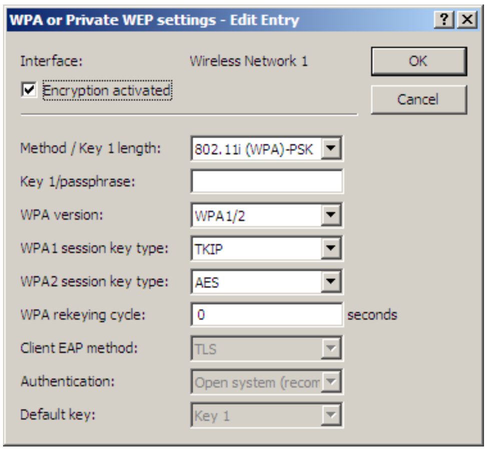
Access points of the LANCOM range support the most up-to-date methods of encryption and security for data that is transferred via WLAN.

- The IEEE standard 802.11i/WPA stands for the highest degree of security that is currently available for WLAN connections. This standards uses a new encryption procedure (AES-CCM) which, in combination with other methods, achieves levels of security equaled 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 'WLAN security' → page 11-15.

WPA and private WEP settings



WPA or Private WEP settings - Edit Entry

Interface: Wireless Network 1

☑ Encryption activated

Method / Key 1 length: 802.11i (WPA)-PSK

Key 1/passphrase:

WPA version: WPA1/2

WPA1 session key type: TKIP

WPA2 session key type: AES

WPA rekeying cycle: 0 seconds

Client EAP method: TLS

Authentication: Open system (recom

Default key: Key 1

LANconfigWireless LAN ▶ 802.11i/WEP ▶ WPA or Private WEP settings

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ 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. Select this setting if no RADIUS server is available and authentication is based on a pre-shared key.
  - 802.11i (WPA)-802.1x – If authentication is handled by a RADIUS server, select the option '802.11i (WPA)-802.1x'. When using this setting, additionally ensure that the RADIUS server is configured in the 802.1x settings.
  - 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.

- **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 11-29.

- **WPA version**

  WPA version for encryption offered by the access point to the WLAN clients.

  - WPA1: WPA1 only
  - WPA2: WPA2 only
  - WPA1/2: WPA1 and WPA2 in one SSID (radio cell)

- **WPA1 session key type**

  If '802.11i (WPA)-PSK' has been entered as the encryption method, the procedure for generating a session or group key for WPA 1 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.

- **WPA 2 session key type**

  Procedure for generating a session or group key for WPA 2.

- **WPA rekeying cycle**

  A 48-bit long initialization vector (IV) impedes attackers in their attempts to calculate the WPA key. The true key consisting of the IV and WPA key only repeats every 16 million packets. In high-traffic WLANs, the key is repeated only after several hours. To avoid repetition of the key, WPA automatically renegotiates the key at regular intervals. This takes place before repetition of the key.

  Enter a value in seconds after which the key is renegotiated.

  The standard value is '0' and the key is not negotiated in advance.

- **Client EAP method**

  In WLAN client operating mode, LANCOM Access Points can authenticate themselves to another access point using EAP/802.1X. To activate the EAP/802.1X authentication in client mode, the client EAP method is selected as the encryption method for the first logical WLAN network.

  Note that the selected client EAP method must match the settings of the access point that the LANCOM Access Point is attempting to log onto.

ⓘ In addition to setting the client EAP method, also be sure to observe the corresponding setting for the WLAN client operation mode!
The client EAP method setting has no function on logical WLAN networks other than WLAN 1.

- **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.

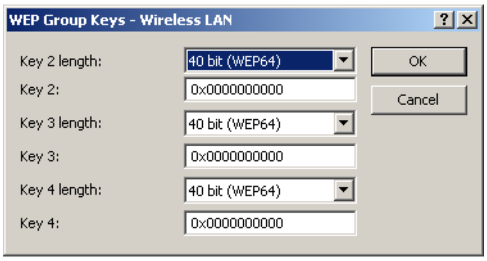
  Rules of the entry of the keys can be found in the description of the WEP group key ’Rules for entering WEP keys’ → page 11-29.

WEP group keys

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 11-29.


WEP Group Keys - Wireless LAN

Key 2 length: 40 bit (WEP64)
Key 2: 0x0000000000
Key 3 length: 40 bit (WEP64)
Key 3: 0x0000000000
Key 4 length: 40 bit (WEP64)
Key 4: 0x0000000000

LANconfigWireless LAN ▶ 802.11i/WEP ▶ WEP group keys

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ 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

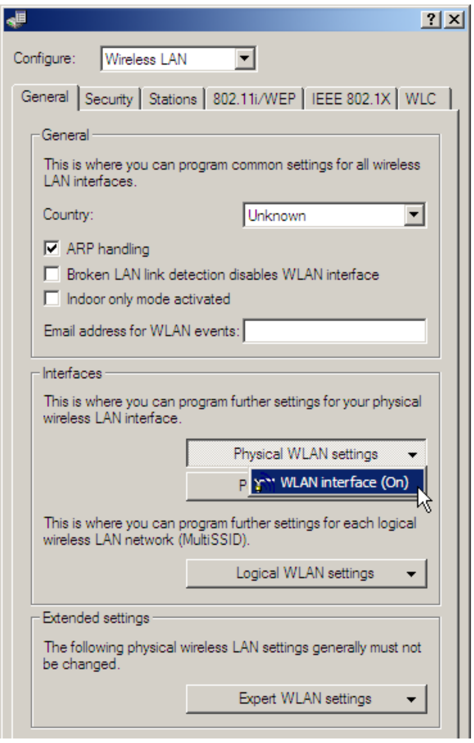
The ASCII character set includes the characters '0' to'9', 'a' to 'z', 'A' to 'Z' and the following special characters:
! ” # $ % & ´ () * + , - ./ : ; < = > ? @ [\ ] ^ _ ‘ { | } ~

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.

11.5.5 The physical WLAN interfaces

In addition to the general WLAN parameters, a variety of settings apply specifically to each WLAN module in the access point.


Configure: Wireless LAN

General

This is where you can program common settings for all wireless LAN interfaces.

Country: Unknown

☑ ARP handling
☐ Broken LAN link detection disables WLAN interface
☐ Indoor only mode activated

Email address for WLAN events:

Interfaces

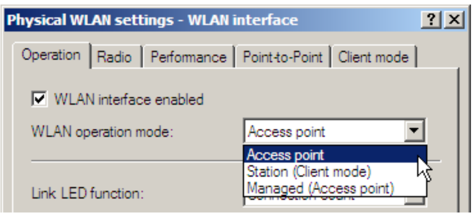
This is where you can program further settings for your physical wireless LAN interface.

This is where you can program further settings for each logical wireless LAN network (MultiSSID).

Extended settings

The following physical wireless LAN settings generally must not be changed.

Operating settings



Physical WLAN settings - WLAN interface

☑ WLAN interface enabled

WLAN operation mode: Access point

Access point
Station (Client mode)
Managed (Access point)

Link LED function:

LANconfig: Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Operation

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ Operational

- **WLAN operating modes**

  LANCOM Access Points can be operated in various operating modes:

  - As an access point, it forms the link between WLAN clients and the cabled LAN.
  - In client mode, the device itself locates the connection to another access point and attempts to register with a wireless network. In this case the device serves to link a cabled network device to an access point over a wireless connection.
  - As a managed Access Point, the device searches for a central WLAN-Controller from which it can obtain a configuration.

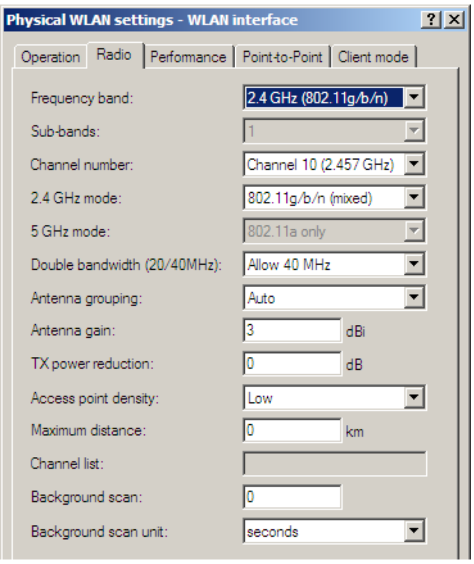
  If the WLAN interface is not required, it can be completely deactivated.

- **Link LED function**

  When setting up point-to-point connections or operating the device as a WLAN client, the best possible positioning of the antennas is facilitated if the signal strength can be recognized at different positions. The WLAN link LED can be used for displaying the signal quality during the set-up phase. In the corresponding operation mode, the WLAN link LED blinks faster the better the reception quality in the respective antenna position is.

  - Number of connections: In this operation mode, the LED uses "inverse flashing" in order to display the number of WLAN clients that are logged on to this access point as clients. There is a short pause after the number of flashes for each client. Select this operation mode when you are operating the LANCOM Wireless Router in access point mode.
  - Client signal strength: In this operation mode, this LED displays the signal strength of the access point with which the LANCOM Access Point has registered itself as a client. The faster the LED blinks, the better the signal. Select this operation mode only if you are operating the LANCOM Access Point in client mode.
  - P2P1 to P2P6 signal strength: In this operation mode, the LED displays the signal strength of respective P2P partner with which the LANCOM Access Point forms a P2P path. The faster the LED blinks, the better the signal.

Radio settings



Physical WLAN settings - WLAN interface

Frequency band: 2.4 GHz (802.11g/b/n)

Sub-bands: 1

Channel number: Channel 10 (2.457 GHz)

2.4 GHz mode: 802.11g/b/n (mixed)

5 GHz mode: 802.11a only

Double bandwidth (20/40MHz): Allow 40 MHz

Antenna grouping: Auto

Antenna gain: 3 dBi

TX power reduction: 0 dB

Access point density: Low

Maximum distance: 0 km

Channel list:

Background scan: 0

Background scan unit: seconds

LANconfig: Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Radio

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ Radio settings

- **Frequency band, Subband**

  When selecting the frequency band on the 'Radio' tab under the physical interface settings, you decide whether the WLAN module operates in the 2.4 GHz or in the 5 GHz band (also see 'WLAN standards' → page 11-5), 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.

With the DFS method (Dynamic Frequency Selection) an unused frequency is automatically selected, for example, to avoid interference from radar systems or to distribute WLAN devices as evenly as possible over the entire frequency band. After switching on or booting, the device randomly selects one of the available channels (e.g. based on the country settings). It checks whether radar signals exist on this channel, and whether it is already in use by another WLAN. This scan procedure repeats until a channel is found that is free of radar signals and which has the lowest possible number of other networks. The selected channel is then monitored for radar signals for a further 60 seconds. For this reason, data traffic may be interrupted for a period of 60 seconds while the frequencies are scanned for a free channel.

To avoid these pauses in data transmission every time the channel is changed, LANCOM devices carry out the scan **before** a channel is chosen. Information about scanned channels is stored to an internal database.

- □ Was a radar signal detected on the channel?
- □ How many other networks were found on the channel?

This database helps the WLAN device to select a channel from the list that is free of radar signals and that has the lowest number of other networks (the operating channel). After the channel has been selected, data transmission can continue immediately without any waiting.

- □ The "blacklist" in the database stores the channels to be blocked due to the detection of radar signals. This entries are removed from the list every 30 minutes in order to keep the information up to date.
- □ The "whitelist" in the database stores the channels where no radar was detected. These entries remain valid for 24 hours, although if radar signals be detected in the meantime, an entry is made to the blacklist.

The access point generally uses the operating channel selected after the first scan permanently. Connections can now be operated for any length of time on the channel selected by the DFS algorithm until either a radar signal is detected or the radio cell is restarted (e.g. by changing the device configuration, firmware upload, or restart).

When is it necessary to carry out a new 60-second scan?

- □ The device is switched on or cold-started. Under these circumstances the database is empty. The device cannot select a channel from the whitelist, and so a scan has to be carried out.
- □ Within the first 24 hours of scanning, it becomes necessary to switch channels because a radar signal is detected within range of the access point. In this case, the access point can refer to alternatives in the whitelist. It then informs associated WLAN clients and/or P2P partners of the new operating channel and switches to this channel. This process takes place within about a second, so the switch can be considered to be uninterrupted.
- □ The device is in operation for 24 hours already, and then a channel switch becomes necessary. Entries in the whitelist are out of date and thus discarded. The access point has no alternative channel to which it can switch directly. In this case the database requires new information from a scan and WLAN operation is interrupted for one minute.

> i To avoid having the 60 second pause at an inconvenient time, you can set the time of the scan and thus the database update. Do this with WEBconfig or telnet in the menu `Setup/Interfaces/WLAN/Radio settings`. To define the time you can use the options provided by cron commands, e.g. '1,6,13' to force a DFS scan at 01:00h, 06:00h or 13:00h, or '0-23/4' for a DFS scan between 0:00h and 23:00h every 4 hours. Forced DFS scans require that the device is set with the correct system time.

The ETSI standard 301 893 version 1.4.1 is the latest set of regulations concerning the operation of 5-GHz wireless LANs. In the context of the wireless LAN modules used in the LANCOM Wireless Routers and LANCOM Access Points, this standard is also referred to as DFS 2.

This standard makes tougher demands on the radar detection patterns used when operating 5-GHz WLANs. The standard applies to all devices brought into circulation after April 01, 2008. Devices brought into circulation before this date do not have to meet this standard. In particular devices with older WLAN chips (two- or three-chip modules) do not have to meet this standard and, as such, do not have to be upgraded.

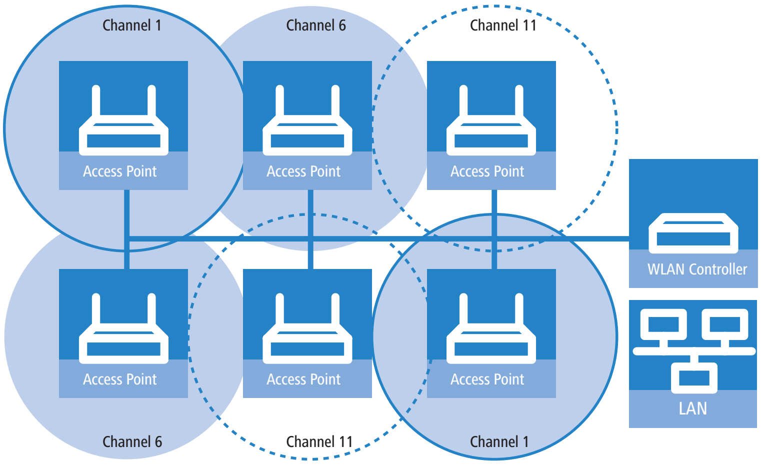
LANCOM Systems supplies LCOS firmware of the versions 7.30 (for the current Wireless Routers and Access Points) and 7.52 (for LANCOM Wireless L-310agn and LANCOM Wireless L-305agn) with DFS 2 support. These firmware versions have different threshold values for radar-pattern recognition than with the former DFS.

In principle the operator of the WLAN is responsible for maintaining the new ETSI standards. For this reason LANCOM Systems recommends that you perform an update to a firmware version with DFS 2 support.

- **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.



- **2.4-GHz mode**

  Three different wireless standards are based on the 2.4-GHz band: IEEE 802.11b, IEEE 802.11g and IEEE 802.11n. If 2.4 GHz is selected as the operating frequency, the compatibility mode can be selected in addition.

Please observe that clients supporting only the slower standards may not be able to register with the WLAN if compatibility mode is set to a high value.

The 802.11gbn 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 module 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 principle 802.11n is backwardly compatible to the previous IEEE 802.11b/g wireless LAN standards, although not all 802.11n functions are supported in this mode.

In the 2.4 GHz band you can allow operation in accordance with 802.1b/g/n either exclusively or in various mixed modes. When 802.11b is supported you can also select whether only 11 Mbps mode or the older 2 Mbps should be supported.

Compatibility is always achieved at the expense of performance. It is therefore recommended to allow only those modes of operation that are absolutely necessary for the wireless LAN clients in use.

- **5-GHz mode**

  Using two neighboring, vacant channels for wireless transmissions can increase the transfer speeds up to 108 Mbps. With the base station in the 108Mbit/s Turbo mode, only those WLAN clients that also support the 108Mbit/s Turbo mode can connect to this base station.

  In the 5 GHz band you can choose to allow either greenfield mode (802.11n only) or mixed operation with 802.11a. Greenfield mode should be chosen if there are only 802.11n devices in operation in a network, as these guarantee the highest possible throughput rates.

802.11n only

- **Double bandwidth (20/40 MHz)**

  A wireless LAN module normally uses a frequency range of 20 MHz in which data to be transmitted is modulated to the carrier signals. 802.11a/b/g use 48 carrier signals in a 20 MHz channel. The use of double the frequency range of 40 MHz means that 96 carrier signals can be used, resulting in a doubling of the data throughput.

  802.11n can use 52 carrier signals in one 20 MHz channel for modulation and up to 108 in a 40 MHz channel. The use of the 40 MHz option for 802.11n therefore means a performance gain of more than double.

802.11n only

- **Antenna grouping**

  LANCOM Access Points with 802.11 support can use up to three antennas for transmitting and receiving data. Using several antennas with 802.11n can have different purposes:

  - □ Improved data throughput: Using "spatial multiplexing" allows parallel data streams to be implemented to transmit double the amount of data.
  - □ Improving wireless coverage: Cyclic shift diversity (CSD) can be used to transmit a radio signal in different phases. This reduces the risk of the signal being erased at certain points in the radio cell.

  Depending on the application the use of the antennas can be set:

  - □ When using the device in access point mode to connect wireless LAN clients it is generally recommended to use all three antennas in parallel in order to achieve good network coverage.
  - □ To work with 2 parallel data streams; for example for point-to-point links with an appropriate dual slant antenna, the antenna ports 1 + 2 **or** 1 + 3 are used. The unused antenna port is deactivated.
  - □ For applications with only one antenna (for example an outdoor application with just one antenna) the antenna is connected to port 1 and ports 2 and 3 are deactivated
  - □ The ''Auto' setting means that all available antennas are used

> Please note the following when connecting antennas:
>
> Antenna connector 1 must always be used. Depending on the mounting and cabling, the second antenna may be connected either to connector 2 or connector 3.
>
> The configuration of the device software must agree with the actual antenna connections.

802.11abg only

- **Diversity settings**

  The diversity settings specify which antennas should be used for transmission and for reception:

  - □ 'Transmit via the primary antenna only' (RX diversity): In this default setting, the antenna connected to the access point's main connector is used for data transmission. For reception (RX), the antenna with the best signal is selected (at Main or AUX).
  - □ 'Automatically select the best antenna for transmission' (TX and RX diversity): If the diversity function is used for transmission (TX) as well, the antenna with the strongest signal is taken.
  - □ 'Send via the primary antenna and receive via the secondary antenna' (no diversity): The main antenna only is used for transmission, and for reception the antenna at the AUX connector is preferred. Using this alternative, high-performance antennas that are legally prohibited from transmitting can be used for reception.

- **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 'Geometric dimensioning of outdoor wireless network links' → page 11-48.

> 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. Information on 'access point density' is sent with the beacons for processing by older Agere clients.

- **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.

- **Background scan interval**

  If a value is entered here, the LANCOM Wireless Router searches the frequencies in the active band that are currently not in use in cycles within this interval in order to find available access points.

  - The background scan function is usually deployed for rogue AP detection for the LANCOM Wireless Router in access point mode. This scan interval should correspond to the time span within which unauthorized access points should be recognized, e.g. 1 hour.
  - Conversely, for the LANCOM Wireless Router in client mode, the background scan function is generally used for improved mobile WLAN client roaming. In order to achieve fast roaming, the scan time is limited here, for example, to 260 seconds.
  - When the background scan time is '0' the background scanning function is deactivated.

- **Time unit for background scanning**

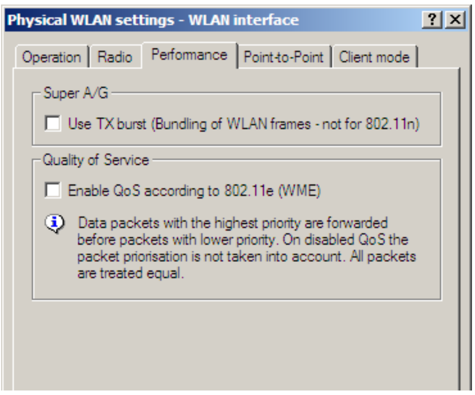
  The background scan interval sets the time period between searches by a Wireless Router or Access Point for third-party WLAN networks within range.

  The time interval allows the entered value to be defined in milliseconds, seconds, minutes, hours or days.

To avoid adverse effects on data transfer rates, the interval between channel scans in access-point mode should be at least 20 seconds. Lesser values will be corrected to this minimum value automatically. For example, with 13 channels to scan in the 2.4GHz band, one scan of the full spectrum takes at least 13 x 20s = 260 seconds.

Background scanning can be limited to a lower number of channels when indoor mode is activated. This allows roaming for the mobile LANCOM Wireless Router in client mode to be improved even further.

Performance



□ Use TX burst (Bundling of WLAN frames - not for 802.11n)

□ Enable QoS according to 802.11e (WME)

Data packets with the highest priority are forwarded before packets with lower priority. On disabled QoS the packet priorisation is not taken into account. All packets are treated equal.

LANconfig: Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Performance

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ Performance

- **TX burst**

  Enables/prevents packet bursting for increasing throughput. Bursting leads to less fairness on the medium.

- **Hardware compression**

  Allows or prohibits the hardware packet compression.

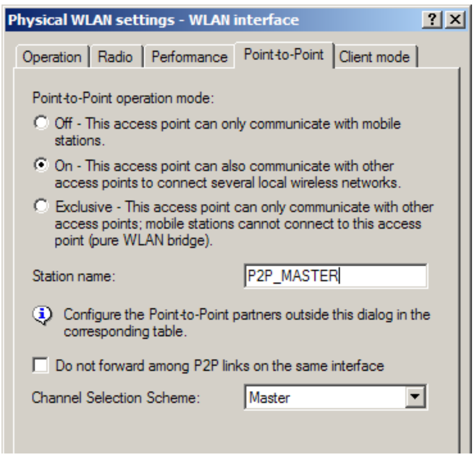
- **QoS according to 802.11e**

  With the extension to the 802.11 standard, 802.11e, Quality of Service can be provided for transfers via WLAN. Among others, 802.11e supports the prioritization of certain data-packet types. This extension is an important basis for the use of voice applications in WLANs (Voice over WLAN, VoWLAN). The WiFi alliance certifies products that support Quality of Service according to 802.11e, and refer to WMM (WiFi Multimedia, formerly known as WME or Wireless Multimedia Extension). WMM defines four categories (voice, video, best effort and background) which make up separate queues to be used for prioritization. The 802.11e standard sets priorities by referring to the VLAN tags or, in the absence of these, by the DiffServ fields of IP packets. Delay times (jitter) are kept below 2 milliseconds, a magnitude which is inaudible to the human ear. 802.11e controls access to the transfer medium with EDCF, the Enhanced Distributed Coordination Function.

Priorities can only be set if the WLAN client and the access point both support 802.11e or WMM, and also if the applications are able to mark the data packets with the corresponding priorities.

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.



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.

○ Exclusive - This access point can only communicate with other access points; mobile stations cannot connect to this access point (pure WLAN bridge).

Station name: P2P_MASTER

Configure the Point-to-Point partners outside this dialog in the corresponding table.

□ Do not forward among P2P links on the same interface

Channel Selection Scheme: Master

LANconfig: Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Point-to-point

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ Interpoint settings

- **Point-to-point operation mode**
  - 'Off': The access point only communicates with mobile clients
  - 'On': The access point can communicate with other access points and with mobile clients
  - 'Exclusive': The access point only communicates with other access points
- **Station name**

  For this physical WLAN interface, enter a name which is unique in the WLAN: This name can be used by other WLAN devices to connect this base station over point-to-point.

  You can leave this field empty if the device has only one WLAN interface and already has a device name which is unique in the WLAN, or if the other base stations identify this interface by means of the WLAN adapter's MAC address.
- **Do not forward packets between P2P links on the same interface**

  Allows or prohibits the transmission of packets between P2P links on the same WLAN interface
- **Channel selection scheme**

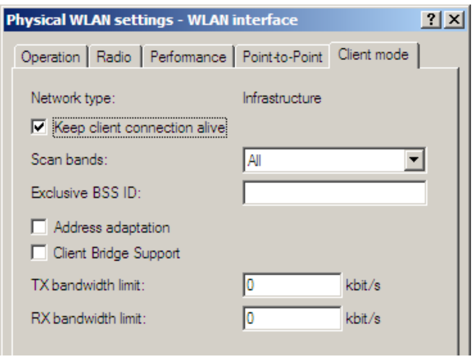
  In the 5-GHz band, the automatic search for vacant WLAN channels can lead to several simultaneous test transmissions from multiple access points, with the result that they do not find each other. This stalemate situation can be avoided with the appropriate "Channel selection scheme".

  Thus it is recommended for the 5GHz band that one central access point should be configured as 'Master' and all other point-to-point partners should be configured as 'Slave'. In the 2.4GHz band, too, this setting simplifies the establishment of point-to-point connections if the automatic channel search is activated.
  - Master: This access point takes over the leadership when selecting a free WLAN channel.
  - Slave: All other access points will search for a channel until they have found a transmitting Master.

The purpose of this area is to define general P2P parameters only—the actual connections to remote WLAN stations themselves are defined under the following paths:
LANconfigWireless LAN ▶ General ▶ Point to point partners
WEBconfig: Setup ▶ Interfaces ▶ WLAN Interpoint peers

Client mode

If the LANCOM Router device is operating as a client, the tab 'Client mode' can be used for further settings that affect the behavior as a client.



Physical WLAN settings - WLAN interface

Operation | Radio | Performance | Point-to-Point | Client mode

Network type: Infrastructure

☑ Keep client connection alive

Scan bands: All

Exclusive BSS ID:

□ Address adaptation

□ Client Bridge Support

TX bandwidth limit: 0 kbit/s

RX bandwidth limit: 0 kbit/s

LANconfig: Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Client mode

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ Client modes

- **Keep client connection alive**

  This option ensures that the client station keeps the connection to the access point alive even if the connected devices are not exchanging any data packets. If this option is disabled, the client station is automatically logged off the wireless network if no packets are transferred over the WLAN connection within a specified time.

- **Scan bands**

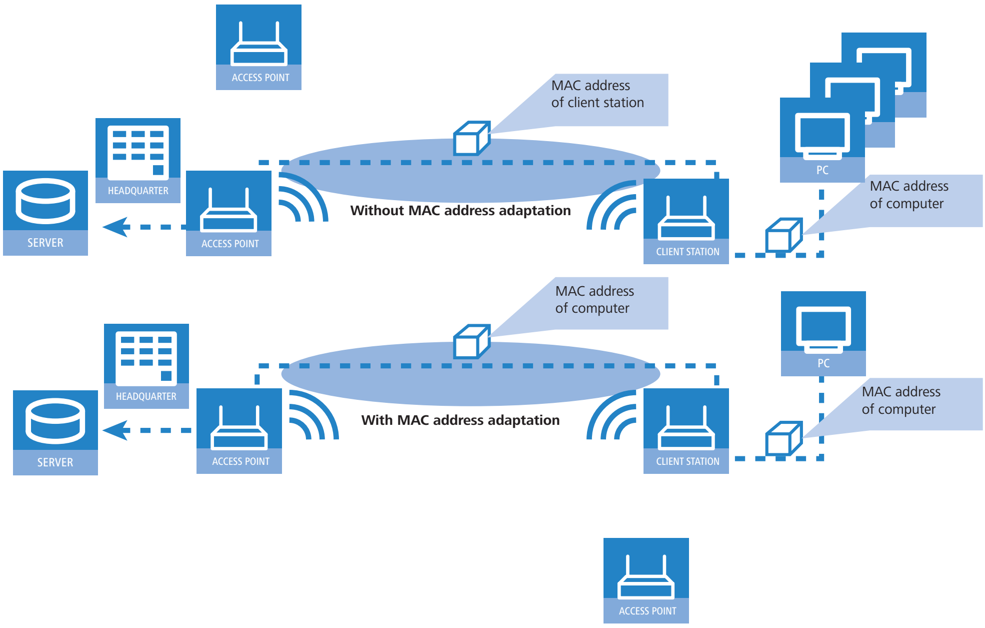
  This defines whether the client station scans just the 2.4 GHz, just the 5 GHz, or all of the available bands for access points.

- **Preferred BSS ID**

  If the client station is to log onto one particular access point only, the MAC address of the WLAN module in this access point can be entered here.

- **Address adaptation**

  In client mode, the client station normally replaces the MAC addresses in data packets from the devices connected to it with its own MAC address. The access point at the other end of the connection only ever “sees” the MAC address of the client station, not the MAC address of the computer(s) connected to it.

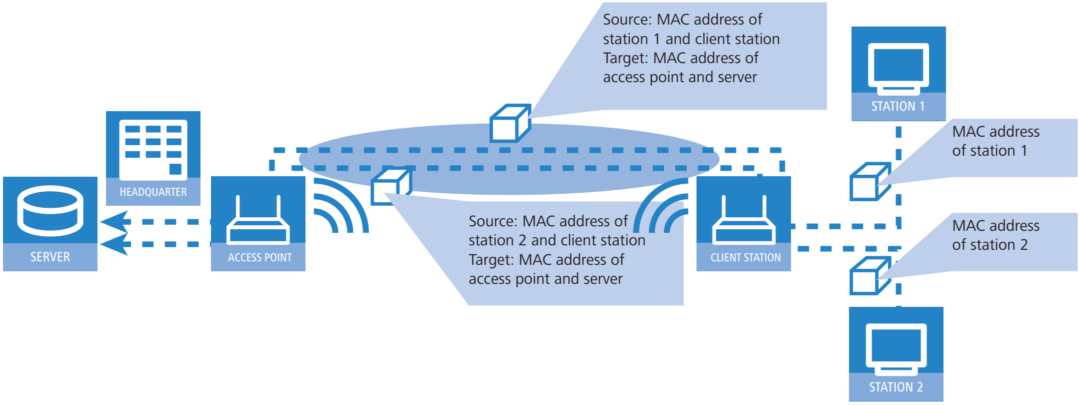


In some installations it may be desirable for the MAC address of a computer to be transmitted to the access point and not the MAC address of the client station. The option ‘Address adaptation’ prevents the MAC address from being replaced by the client station. Data packets are transferred with their original MAC addresses—in the WLAN, the Access Point takes the client's MAC address.

Address adaptation only works when just **one** computer is connected to the client station.

- **Client-bridge support**

  Whereas address adaptation allows only the MAC address of a **single** attached device to be visible to the access point, client-bridge support provides transparency in that all MAC addresses of the LAN stations behind the client stations are transferred to the access point.


Source: MAC address of station 1 and client station
Target: MAC address of access point and server
HEADQUARTER
SERVER
ACCESS POINT
Source: MAC address of station 2 and client station
Target: MAC address of access point and server
CLIENT STATION
STATION 1
MAC address of station 1
MAC address of station 2
STATION 2

Furthermore, the three MAC addresses usual in client mode are not used for this operating mode (in this example for server, access point and client station), but rather four addresses as with point-to-point connections (the fourth is the MAC address of the station in the LAN of the client station). The fully transparent connection of a LAN to the client station allows targeted transmission of data packets in the WLAN and hence functions such as TFTP downloads, initiated by a broadcast.

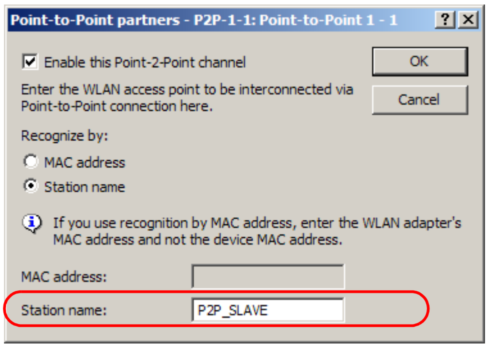
The client-bridge mode offers the following advantages:

- Unlike the "normal" client mode, address translation (masking) in the client station is omitted.
- In relation to point-to-point connections, the occasionally undesirable entry of MAC addresses or station names is omitted. Furthermore, the client-bridge mode allows more than six connections (limitation with P2P) to be set up.
- The client station can roam, which is not possible with point-to-point (this applies both to the client-bridge mode and to the standard client mode).

Client-bridge mode can only be used between two LANCOM devices. Likewise, the use of the client-bridge mode must be enabled in the settings for the logical network of the access point.

11.5.6 Point-to-point peers

Up to six point-to-point connections can be activated for each WLAN module.


Point-to-Point partners - P2P-1-1: Point-to-Point 1 - 1

☑ Enable this Point-2-Point channel

Enter the WLAN access point to be interconnected via Point-to-Point connection here.

Recognize by:

○ MAC address
● Station name

If you use recognition by MAC address, enter the WLAN adapter's MAC address and not the device MAC address.

MAC address:

Station name: P2P_SLAVE

LANconfigWireless LAN ▶ General ▶ Point to point partners

WEBconfig: Setup ▶ Interfaces ▶ WLAN Interpoint peers

- **Recognize by**

  Here you select the characteristics to be used to identify the P2P peer.

- **MAC address**

  MAC address of the P2P remote station.

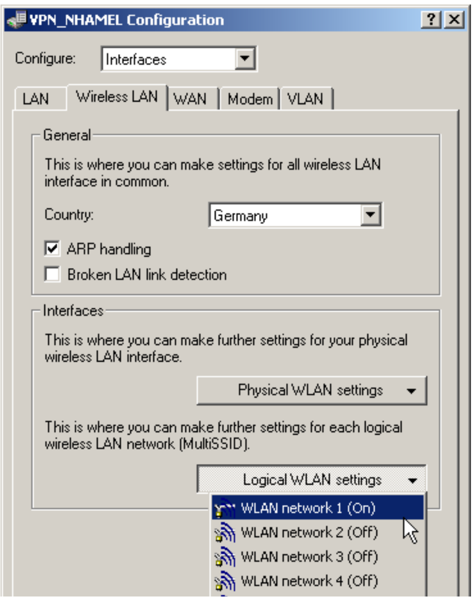
- **Station name**

  Station name of the P2P remote station.

If you work with detection by MAC address, enter the MAC address of the WLAN adapter here and not that of the device itself.

11.5.7 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.



VPN_NHAMEL Configuration

Configure: Interfaces

General

This is where you can make settings for all wireless LAN interface in common.

Country: Germany

☑ ARP handling

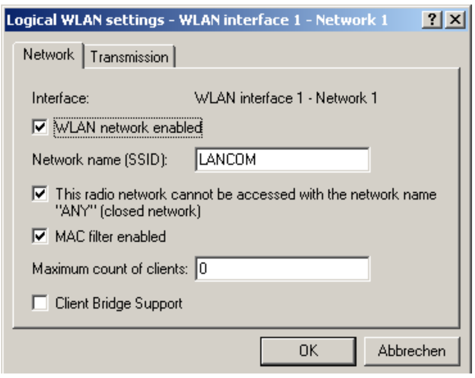
□ Broken LAN link detection

Interfaces

This is where you can make further settings for your physical wireless LAN interface.

This is where you can make further settings for each logical wireless LAN network (MultiSSID).

Network settings



Logical WLAN settings - WLAN interface 1 - Network 1

Interface: WLAN interface 1 - Network 1

☑ WLAN network enabled

Network name (SSID): LANCOM

☑ This radio network cannot be accessed with the network name "ANY" (closed network)

☑ MAC filter enabled

Maximum count of clients: 0

□ Client Bridge Support

LANconfig: Wireless LAN ▶ General ▶ Logical WLAN settings ▶ Network

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ Network

- **Wireless LAN enabled/operating**

  This switch allows the logical WLAN to be activated/deactivated separately.

- **Network name (SSID)**

  Define a unique SSID (the network name) for each of the logical wireless LANs required. Only network cards that have the same SSID can register with this wireless network.

- **Suppress SSID broadcast**

  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 without the SSID being named. By suppressing SSIDs in the broadcasts, you place your wireless LAN into a privacy mode. 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 suppression of SSID broadcasting if you wish to prevent WLAN clients from registering with your network without naming the SSID.

- **MAC filter enabled**

  The MAC addresses of the clients that are allowed to associate with an access point are stored in the MAC filter list (**Wireless LAN ▶ Stations ▶ Stations**). The 'MAC filter activated' switch can be used to switch off the use of the MAC filter list for individual logical networks.

Use of the MAC filter list is required for logical networks in which the clients register via LEPS with an individual passphrase. The passphrase used by LEPS is also entered into the MAC filter list. The MAC filter list is always consulted for registrations with an individual passphrase, even if this option is deactivated.

- **Maximum number of clients**

  Here you set the maximum number of clients that may associate with this access point. Additional clients wanting to associate will be rejected.

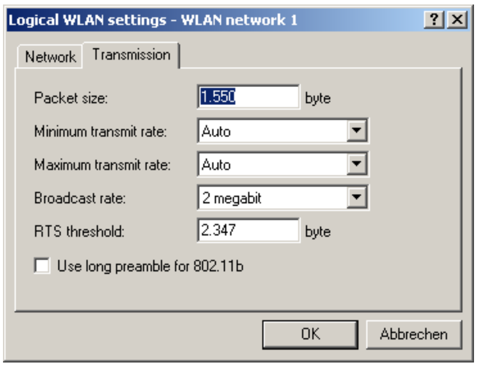
- **Client-bridge support**

  Enable this option for an access point if you have enabled the client-bridge support for a client station in WLAN client mode ('Client-bridge support' → page 11-37).

Client-bridge mode can only be used between two LANCOM devices.

Transmission settings

Details for the data transfer over the logical interface are set on the 'Transmission' tab.



Logical WLAN settings - WLAN network 1

Network | Transmission

Packet size: 1.550 byte

Minimum transmit rate: Auto

Maximum transmit rate: Auto

Broadcast rate: 2 megabit

RTS threshold: 2.347 byte

☐ Use long preamble for 802.11b

LANconfig: Wireless LAN ▶ General ▶ Logical WLAN settings ▶ Transmission

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ Transmission

- **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. 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.

802.11n only

- **Modulation Coding Scheme (MCS)**

  A specific MCS number denotes a unique combination from the modulation of the individual carriers (BPSK, QPSK, 16QAM, 64QAM), coding rate (i. e. proportion of error correction bits in the raw data and number of spatial streams. 802.11n uses this term instead of the term "data rate" used in older wireless LAN standards because data rate is no longer an unequivocal description.

MCS index	Data streams	Modulation	Coding rate	Data throughput (GI=0.4 µs, 40 MHz)
0	1	BPSK	1/2	15
1	1	QPSK	1/2	30
2	1	QPSK	3/4	45
3	1	16QAM	1/2	60
4	1	16QAM	3/4	90
5	1	64QAM	1/2	120
6	1	64QAM	3/4	135
7	1	64QAM	5/6	150

MCS index	Data streams	Modulation	Coding rate	Data throughput (GI=0.4 µs, 40 MHz)
8	2	BPSK	1/2	30
9	2	QPSK	1/2	60
10	2	QPSK	3/4	90
11	2	16QAM	1/2	120
12	2	16QAM	3/4	180
13	2	64QAM	1/2	240
14	2	64QAM	3/4	270
15	2	64QAM	5/6	300

The MCS selection therefore indicates the type and minimum or maximum number of modulation parameters that should be used for one or two spatial data streams. Within these limits, the appropriate MCS is selected when the connection is established depending on the current conditions and may be adapted during the connection if required. This also defines the maximum attainable data throughput, indicated in the last column of the table (here for the short guard interval GI = 0.4 µs using the 40 MHz channel).

- **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".

802.11n only

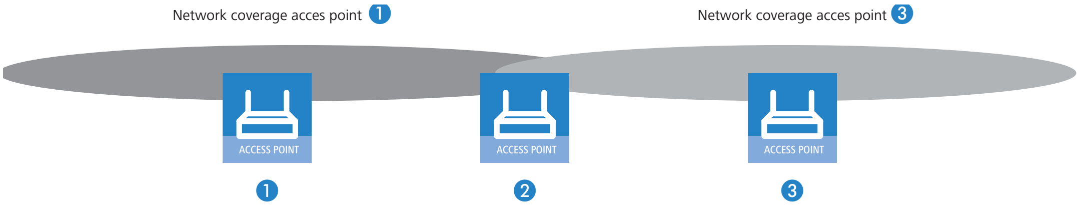
- **Number of spatial streams**

  The spatial multiplexing function allows several separate data streams to be transmitted over separate antennas in order to increase data throughput. The use of this function is only recommended when the remote device can process the data streams with corresponding antennas.

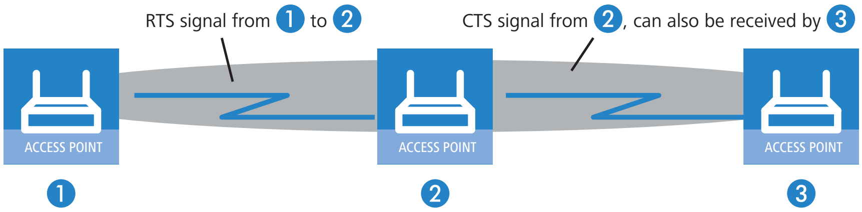
With the 'Auto' setting all spatial streams that are supported by the wireless LAN module in question are used.

- **RTS threshold**

  The RTS threshold prevents the occurrence of the "hidden station" phenomenon.


Network coverage acces point ❶
Network coverage acces point ❸
ACCESS POINT
ACCESS POINT
ACCESS POINT
❶
❷
❸

Here, the three access points ❶, ❷, and ❸ are positioned such that no direct wireless connection between the two outer devices is possible. If ❶ sends a packet to ❷, ❸ is not aware of this as it is outside of ❶'s coverage area. ❸ may also try, during the transmission from ❶, to send a packet to ❷ as well, because ❸ has no knowledge of the medium (in this case the wireless connection) being blocked. A collision results and neither of the transmissions from ❶ nor ❸ to ❷ will be successful. The RTS/CTS protocol is used to prevent collisions.



To this end, ❶ precedes the actual transmission by sending an RTS packet to ❷, that ❷ answers with a CTS. The CTS sent by ❷ is now within "listening distance" of ❸, so that ❸ can wait with its packet for ❷. 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.

The RTS/CTS threshold value also has to be set in the WLAN client, as far as the driver and/or operating system allow this.

- **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.

802.11n only

- **Short guard interval**

  This option is used to reduce the transmission pause between two signals from 0.8 µs (default) to 0.4 µs (short guard interval). This increases the effective time available for data transmission and thus the data throughput. However, the wireless LAN system becomes more liable to disruption that can be caused by interference between two consecutive signals.

  The short guard interval is activated in automatic mode, provided that the remote station supports this. Alternatively the short guard mode can be switched off.

802.11n only

- **Frame aggregation**

  Frame aggregation is used to combine several data packets (frames) into one large packet and transmit them together. This method serves to reduce the packet overhead, and the data throughput increases.

  Frame aggregation is not suitable when working with mobile receivers or time-critical data transmissions such as voice over IP.

With WEBconfig only

- **Hard retries**

  This value defines the number of times that the hardware should attempt to send packets before a Tx error message is issued. Smaller values mean that a packet which cannot be sent blocks the sender for less time.

With WEBconfig only

- **Soft retries**

  If the hardware was unable to send a packet, the number of soft retries defines how often the system repeats the attempt to transmit.

  The total number of attempts is thus (soft retries + 1) * hard retries.

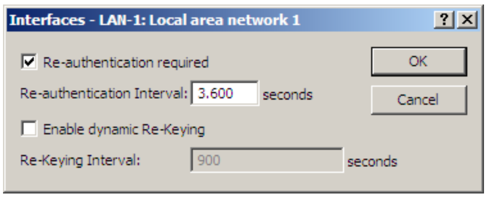
  The advantage of using soft retries at the expense of hard retries is that the rate-adaption algorithm immediately begins the next series of hard retries with a lower datarate.

11.5.8 IEEE 802.1x/EAP

The international industry standard IEEE 802.1x and the **E**xtensible **A**uthentication **P**rotocol (EAP) enable access points to carry out reliable and secure access checks. The access information 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 WPA2.

The IEEE-802.1x technology has already been fully integrated since Windows XP. Client software exists for other operating systems.



Interfaces - LAN-1: Local area network 1

☑ Re-authentication required

Re-authentication Interval: 3.600 seconds

☐ Enable dynamic Re-Keying

Re-Keying Interval: 900 seconds

LANconfig: Wireless LAN ▶ General ▶ 802.1X

WEBconfig: LCOS menu tree ▶ Setup ▶ IEEE802.1x

- **Regularly update authentication**

  Here you activate regular re-authentication. If a new authentication starts, the user remains registered during the negotiation. A typical value as a re-authentication interval is 3,600 seconds.

- **Re-authentication interval**

  The interval for regular re-authentication.

- **Activate dynamic re-keying and key transmission**

  Here you activate the regular generation and transmission of a dynamic WEP key.

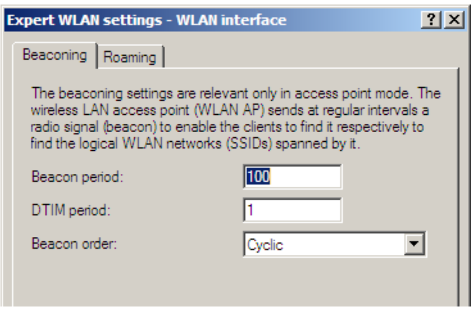
- **Re-keying interval**

  Interval for the regular generation of the key.

11.5.9 Expert WLAN settings

The beaconing table

Settings in the beaconing table influence the transmission of beacons by the access point in AP mode. In part this can influence the roaming behavior of clients, and in part this serves to optimize the MultiSSID mode for older WLAN clients.



The beaconing settings are relevant only in access point mode. The wireless LAN access point (WLAN AP) sends at regular intervals a radio signal (beacon) to enable the clients to find it respectively to find the logical WLAN networks (SSIDs) spanned by it.

Beacon period: 100

DTIM period: 1

Beacon order: Cyclic

LANconfig: Wireless LAN ▶ Expert WLAN settings ▶ Beaconing

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ Beaconing

- **Beacon period**

  This value defines the time interval in Kµs between beacon transmission (1 Kµs corresponds to 1024 microseconds and is a measurement unit of the 802.11 standard. 1 Kµs is also known as a Timer Unit (TU)). Smaller values result in a shorter beacon timeout period for the client and enable quicker roaming in case of failure of an access point, but they also increase the WLAN overhead.

- **DTIM period**

  This value defines the number of beacons which are collected before multicasts are broadcast. Higher values enable longer client sleep intervals, but worsen the latency times.

- **Beacon order**

  Beacon order refers to the order in which beacons are sent to the various WLAN networks. For example, if three logical WLAN networks are active and the beacon period is 100 Kµs, then the beacons will be sent to the three WLANs every 100 Kµs. Depending on the beacon order, the beacons are transmitted at times as follows:

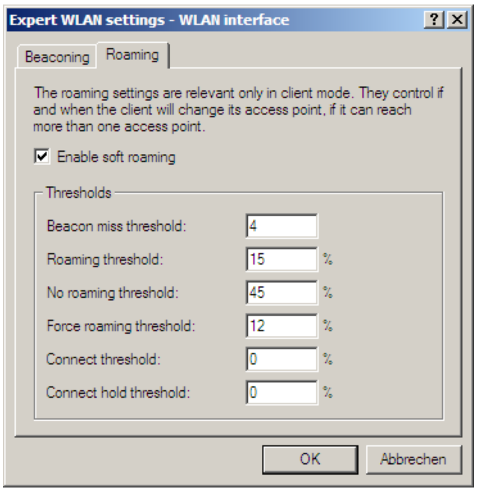
  - Cyclic: In this mode the access point transmits the first beacon transmission at 0 Kµs to WLAN-1, followed by WLAN-2 and WLAN-3. For the second beacon transmission (100 Kµs) WLAN-2 is the first recipient, followed by WLAN-3 and then WLAN-1. For the third beacon transmission (200 Kµs) the order is WLAN-3, WLAN-1, WLAN-2. Thereafter the order starts at the beginning again.
  - Staggered: In this mode, the beacons are not sent together at a particular time, rather they are divided across the available beacon periods. Beginning at 0 Kµs, WLAN-1 only is sent; after 33.3 Kµs WLAN-2, after 66.6 Kµs WLAN-3. At the start of a new beacon period, transmission starts again with WLAN-1.
  - Simple burst: In this mode the access point always transmits the beacons for the WLAN networks in the same order. The first beacon transmission (0 Kµs) is WLAN-1, WLAN-2 and WLAN-3; the second transmission is in the same order, and so on.
  - Default: Cyclic

  Some older WLANs are unable to process the quick succession of beacons which occur with simple burst. Consequently these clients often recognize the first beacons only and can only associate with this network.

  Staggered transmission of beacons produces better results but increases load on the access point's processor. Cyclic transmission proves to be a good compromise as all networks are transmitted first in turn.

The roaming table

The roaming table contains various threshold values which influence the precise control over the LANCOM Wireless Router's behavior when roaming in the 'Client' operating mode.



The roaming settings are relevant only in client mode. They control if and when the client will change its access point, if it can reach more than one access point.

☑ Enable soft roaming

Thresholds

Beacon miss threshold: 4
Roaming threshold: 15 %
No roaming threshold: 45 %
Force roaming threshold: 12 %
Connect threshold: 0 %
Connect hold threshold: 0 %

LANconfig: Wireless LAN ▶ Expert WLAN settings ▶ Roaming

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ Roaming

- **Soft roaming**

  This option enables a client to use scan information to roam to the strongest access point (soft roaming). Roaming due to connection loss (hard roaming) is unaffected by this. The roaming threshold values only take effect when soft roaming is activated.

- **Beacon miss threshold**

  This defines how many access-point beacons can be missed before an associated client starts searching again.

  Higher values will delay the recognition of an interrupted connection, so a longer time period will pass before the connection is re-established.

  The smaller the value set here, the sooner a potential interruption to the connection will be recognized; the client can start searching for an alternative access point sooner.

Values which are too small may cause the client to detect lost connections more often than necessary.

- **Roaming threshold**

  This value is the percentage difference in signal strength between access points above which the client will switch to the stronger access point.

Other contexts require the value of signal strengths in dB. The following conversion applies:
64dB - 100%
32dB - 50%
0dB - 0%

- **No roaming threshold**

  This threshold refers to the field strength in percent. Field strengths exceeding the value set here are considered to be so good that no switching to another access point will take place.

- **Forced roaming threshold**

  This threshold refers to the field strength in percent. Field strengths below the value set here are considered to be so poor that a switch to another access point is required.

- **Connect threshold**

  This value defines field strength in percent defining the minimum that an access point has to show for a client to attempt to associate with it.

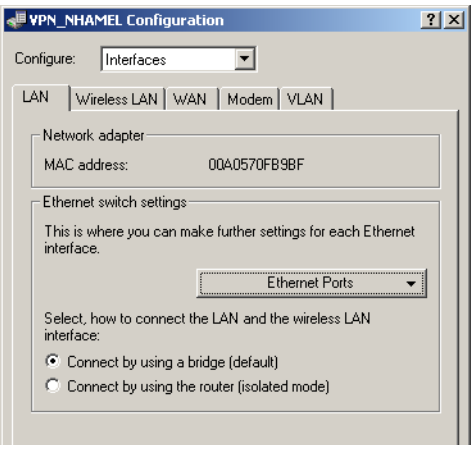
- **Connect hold threshold**

  This threshold defines field strength in percent. A connection to an access point with field strength below this value is considered as lost.

11.5.10 WLAN routing (isolated mode)

The standard setting allows data traffic to be "bridged" between LAN and WLAN, i.e. layer-2 transparent transmission. Data traffic between the cabled network and the wireless LAN is **not** directed via the IP router. Consequently, the firewall and Quality of Service functions integrated into the firewall are not available for traffic between LAN and WLAN. In order to be able to use these functions, the WLAN interfaces are set to "isolated mode"and the data traffic is intentionally routed via the IP router.

To ensure that the IP router can correctly transmit the data between the LAN and WLAN, the two areas must have different IP address ranges. Further information is available in the Advanced Routing and Forwarding (ARF) area.



VPN_NHAMEL Configuration

Configure: Interfaces

Network adapter

MAC address: 00A0570FB9BF

Ethernet switch settings

This is where you can make further settings for each Ethernet interface.

Select, how to connect the LAN and the wireless LAN interface:

● Connect by using a bridge (default)

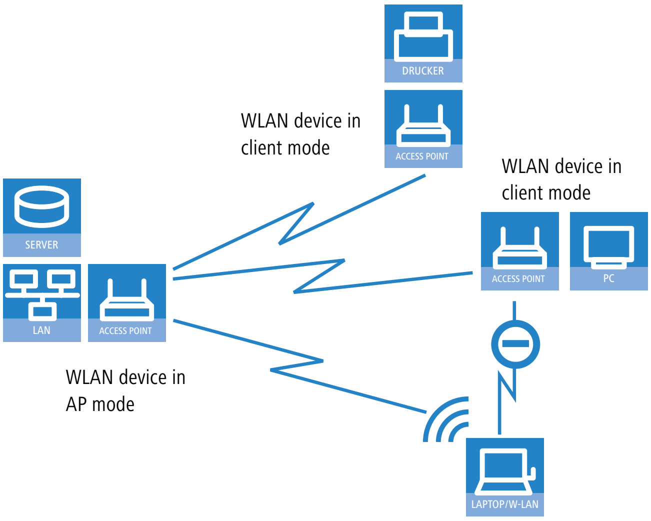
○ Connect by using the router (isolated mode)

LANconfig: Interfaces ▶ LAN

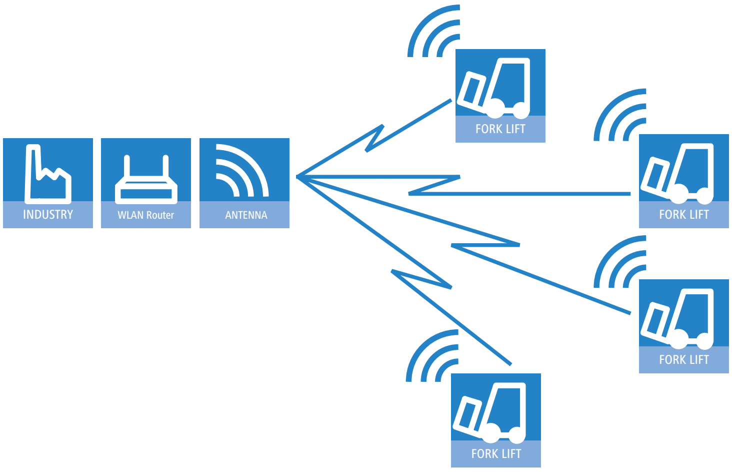
WEBconfig: LCOS menu tree ▶ Setup ▶ LAN bridge ▶ Isolated mode

11.6 Configuring the client mode

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



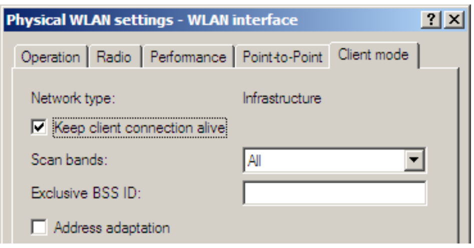
Multiple WLAN clients can register with a WLAN device in AP mode, which is not the case for a WLAN device in client mode.



11.6.1 Client settings

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

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


Physical WLAN settings - WLAN interface

Network type: Infrastructure
☑ Keep client connection alive
Scan bands: All
Exclusive BSS ID:
☐ Address adaptation

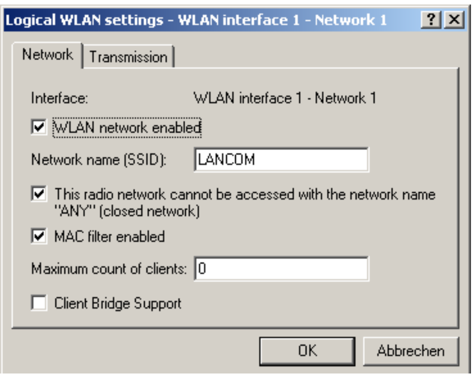
① To edit the settings for client mode in LANconfig, go to the 'Client mode' tab under the physical WLAN settings for the desired WLAN interface.

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

11.6.2 Set the SSID of the available networks

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

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


Logical WLAN settings - WLAN interface 1 - Network 1

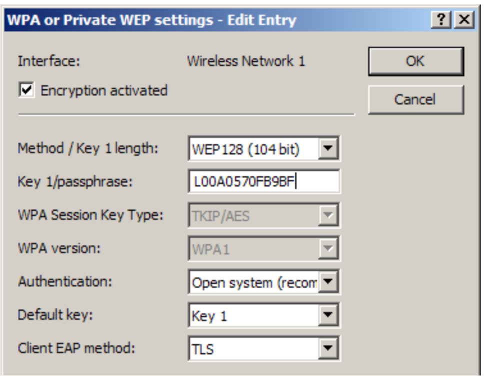
Interface: WLAN interface 1 - Network 1
☑ WLAN network enabled
Network name (SSID): LANCOM
☑ This radio network cannot be accessed with the network name "ANY" (closed network)
☑ MAC filter enabled
Maximum count of clients: 0
☐ Client Bridge Support

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

11.6.3 Encryption settings

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

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



WPA or Private WEP settings - Edit Entry

Interface: Wireless Network 1

☑ Encryption activated

Method / Key 1 length: WEP128 (104 bit)

Key 1/passphrase: L00A0570FB9BF

WPA Session Key Type: TKIP/AES

WPA version: WPA1

Authentication: Open system (recom

Default key: Key 1

Client EAP method: TLS

② Enable encryption and match the encryption method to the settings for the access point.

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

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

□ For TTLS and PEAP – the EAP/TLS root certificate only; the key is entered as a combination username:password.

□ For TLS in addition; the EAP/TLS device certificate including the private key.

When working with WPA or 802.1X, settings may need to be made in the RADIUS server.

11.6.4 Roaming

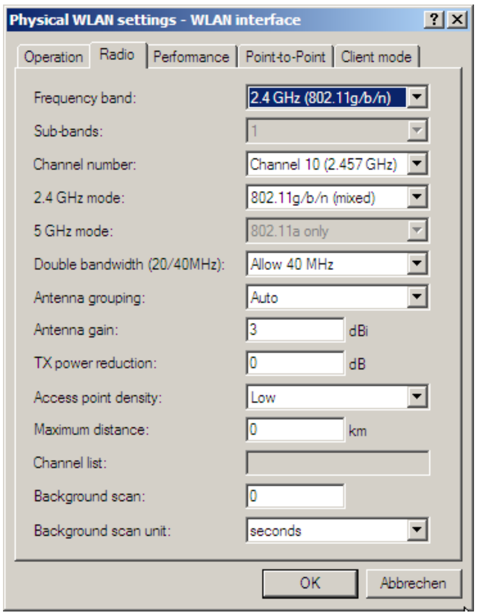
Roaming is defined as the transfer of a WLAN client to another access point once the connection to the access point used so far can no longer be kept alive. To allow roaming, at least one additional access point must be within range of the client, it must provide a network with an identical SSID and matching radio and encryption settings.

Under normal circumstances the WLAN client would only log onto another access point if the connection to the access point used up to that point was lost completely (hard roaming). Soft roaming on the other hand enables the client to use scan information to roam to the strongest access point. With the background scanning function, the LANCOM Wireless Router in client mode can gather information on other available access points prior to the connection being lost. In this case the client is not switched to another access point once the existing connection has been lost completely, but rather when another access point within its range has a stronger signal.

① To enable soft roaming in WEBconfig or telnet, change to Setup > Interfaces > WLAN > Roaming and select the physical WLAN interface.

② Enable soft roaming and, if required, set the other parameters (such as threshold levels and signal level).

③ To configure background scanning in LANconfig, go to the 'Radio' tab under the physical WLAN settings for the desired WLAN interface.



Physical WLAN settings - WLAN interface

Frequency band: 2.4 GHz (802.11g/b/n)

Sub-bands: 1

Channel number: Channel 10 (2.457 GHz)

2.4 GHz mode: 802.11g/b/n (mixed)

5 GHz mode: 802.11a only

Double bandwidth (20/40MHz): Allow 40 MHz

Antenna grouping: Auto

Antenna gain: 3 dBi

TX power reduction: 0 dB

Access point density: Low

Maximum distance: 0 km

Channel list:

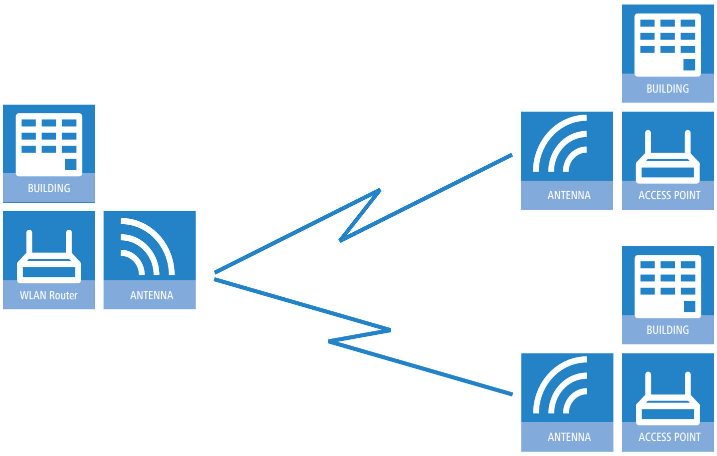
Background scan: 0

Background scan unit: seconds

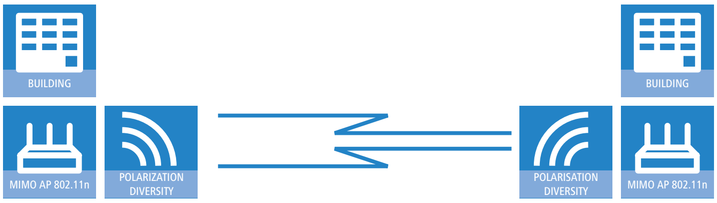
④ Enter the background scan interval as the time in which the LANCOM Wireless Router cyclically searches the currently unused frequencies of the active band for available access points. To achieve fast roaming the scan time is set, for example, to 260 seconds (2.4 GHz) or 720 seconds (5 GHz).

11.7 Configuring point- to- point connections

LANCOM Access Points can serve not only as central stations in a wireless network, they can also operate in point-to-point mode to bridge longer distances. For example, they can provide a secure connection between two networks that are several kilometers apart — without direct cabling or expensive leased lines.



When using Access Points and appropriately polarized antennas in accordance with IEEE 802.11n two wireless links can be established simultaneously between the end points of a point-to-point connection. This allows higher data throughput to be achieved or greater distances to be covered than when using other standards.



Depending on the WLAN standard and WLAN antenna being used, the following data-throughput rates can be achieved:

Access Point	antenna	Data throughput	Range
802.11n indoor AP	Directional antenna with 9° beam spread, lightning protection, 10m cable	240Mbps gross	1km
802.11n indoor AP	Directional antenna with 9° beam spread, lightning protection, 10m cable	15Mbps gross	8,9km
802.11n outdoor AP	Directional antenna with 9° beam spread, lightning protection, 2m cable	240Mbps gross	2,1km
802.11n outdoor AP	Directional antenna with 9° beam spread, lightning protection, 2m cable	15Mbps gross	18km
802.11a indoor AP	Directional antenna with 9° beam spread, lightning protection, 10m cable	54Mbps gross	0,4km
802.11a indoor AP	Directional antenna with 9° beam spread, lightning protection, 10m cable	6Mbps gross	6km
802.11a outdoor AP	Directional antenna with 9° beam spread, lightning protection, 2m cable	54Mbps gross	1,3km
802.11a outdoor AP	Directional antenna with 9° beam spread, lightning protection, 2m cable	6Mbps gross	13km
802.11g indoor AP	Directional antenna with 30° beam spread, lightning protection, 10m cable	54Mbps gross	0,08km
802.11g indoor AP	Directional antenna with 30° beam spread, lightning protection, 10m cable	6Mbps gross	1km
802.11g outdoor AP	Directional antenna with 30° beam spread, lightning protection, 2m cable	54Mbps gross	0,28km
802.11g outdoor AP	Directional antenna with 30° beam spread, lightning protection, 2m cable	6Mbps gross	2,5km

Highly optimized wireless bridges based on IEEE 802.11n are capable of high data transfer rates even over long distances.

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

11.7.1 Geometric dimensioning of outdoor wireless network links

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

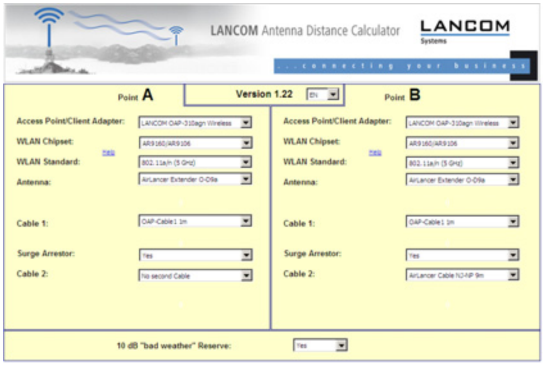
- Which antennas are necessary for the desired application?
- How do the antennas have to be positioned to ensure problem-free connections?
- What performance characteristics do the antennas need to ensure sufficient data throughput within the legal limits?

Selection of antennas using the LANCOM Antenna Calculator

You can use the LANCOM Antenna Calculator to calculate the output power of the access points as well as the achievable distances and data rates. The program can be downloaded from our Web site at www.lancom.de.

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

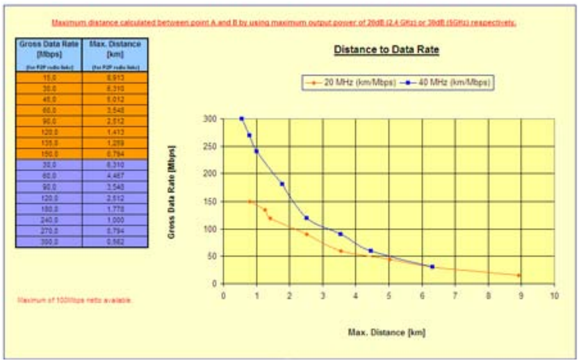
Please note that when using 5 GHz antennas additional technologies such as dynamic frequency selection (DFS) may be stipulated depending on the country of use. The operator of the wireless LAN system is responsible for ensuring that local regulations are met.


LANCOM Antenna Distance Calculator
LANCOM Systems
...connecting your business

Point A | Version 1.22 EN | Point B

	Point A		Point B
Access Point/Client Adapter:	LANCOM OAP-310agn Wireless	Access Point/Client Adapter:	LANCOM OAP-310agn Wireless
WLAN Chipset:	AR9160/AR9106	WLAN Chipset:	AR9160/AR9106
WLAN Standard:	802.11a/n (5 GHz)	WLAN Standard:	802.11a/n (5 GHz)
Antenna:	AirLancer Extender O-D9a	Antenna:	AirLancer Extender O-D9a
Cable 1:	OAP-Cable1 1m	Cable 1:	OAP-Cable1 1m
Surge Arrestor:	Yes	Surge Arrestor:	Yes
Cable 2:	No second Cable	Cable 2:	AirLancer Cable NJ-NP 9m

10 dB "bad weather" Reserve: Yes



Maximum distance calculated between point A and B by using maximum output power of 20dB (2.4 GHz) or 30dB (5GHz) respectively.

Gross Data Rate [Mbps] (for P2P radio links)	Max. Distance [km] (for P2P radio links)
15.0	8.913
30.0	6.310
45.0	5.012
60.0	3.548
90.0	2.512
120.0	1.413
135.0	1.259
150.0	0.794
30.0	6.310
60.0	4.467
90.0	3.548
120.0	2.512
180.0	1.778
240.0	1.000
270.0	0.794
300.0	0.562

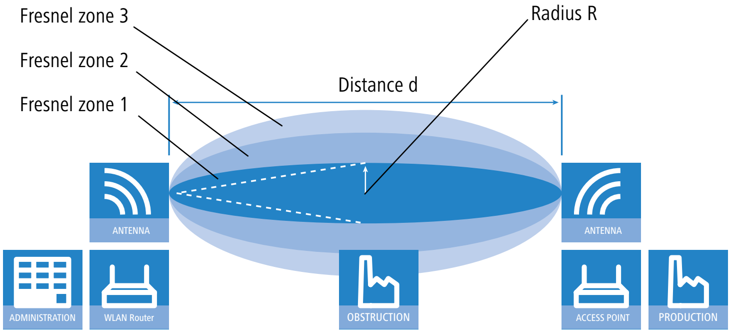
Maximum of 100Mbps netto available.

Positioning the antennas

Antennas do not broadcast their signals linearly, but within an angle that depends on the model in question. The spherical expansion of the signal waves produces amplification or interference of the effective power output at certain distances along the connection between the transmitter and receiver. The areas where the waves amplify or cancel themselves out are known as Fresnel zones.

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

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



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

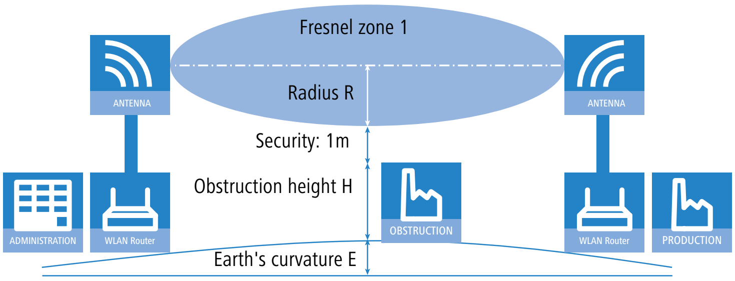
The radius (R) of Fresnel zone 1 is calculated with the following formula assuming that the signal wavelength (λ) and the distance between transmitter and receiver (d) are known.

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

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

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

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



M = R + 1m + H + E (earth's curvature)

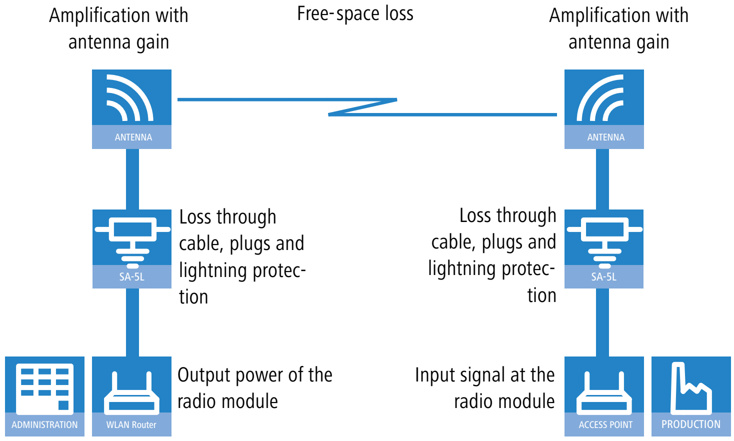
The allowance for the curvature of the earth (E) can be calculated at a distance (d) as E = d² * 0.0147 – i.e. at a distance of 8 km this is almost 1m

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

Antenna power

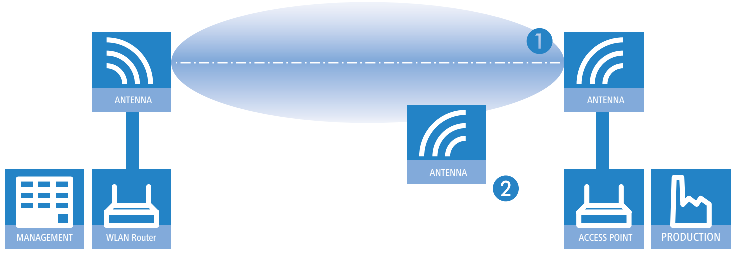
The power of the antennas must be high enough to ensure acceptable data transfer rates. On the other hand, the country-specific legal regulations regarding maximum transmission power should not be exceeded.

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


Amplification with antenna gain
Free-space loss
Amplification with antenna gain
ANTENNA
ANTENNA
Loss through cable, plugs and lightning protection
SA-5L
Loss through cable, plugs and lightning protection
SA-5L
ADMINISTRATION
WLAN Router
Output power of the radio module
Input signal at the radio module
ACCESS POINT
PRODUCTION

11.7.2 Antenna alignment for P2P operations

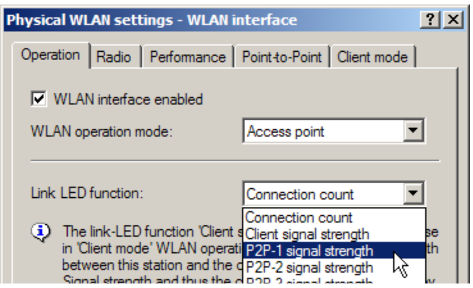
The precise alignment of the antennas is of considerable importance in establishing P2P connections. The more central the receiving antenna is located in the "ideal line" of the transmitting antenna, the better are the actual performance and the effective bandwidth ①. If the receiving antenna is outside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



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

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

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



Physical WLAN settings - WLAN interface

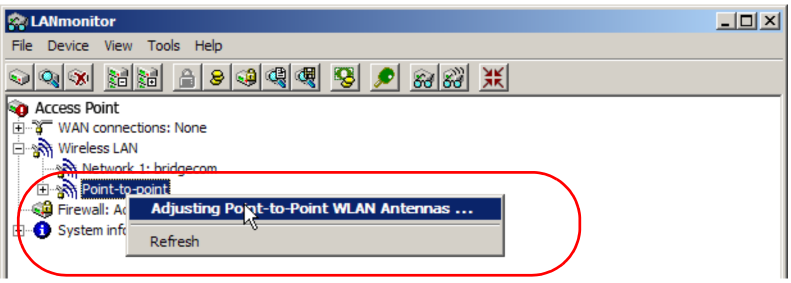
☑ WLAN interface enabled

WLAN operation mode: Access point

Link LED function: Connection count

The link-LED function 'Client s... in 'Client mode' WLAN operati... between this station and the ... Signal strength and thus the d...

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

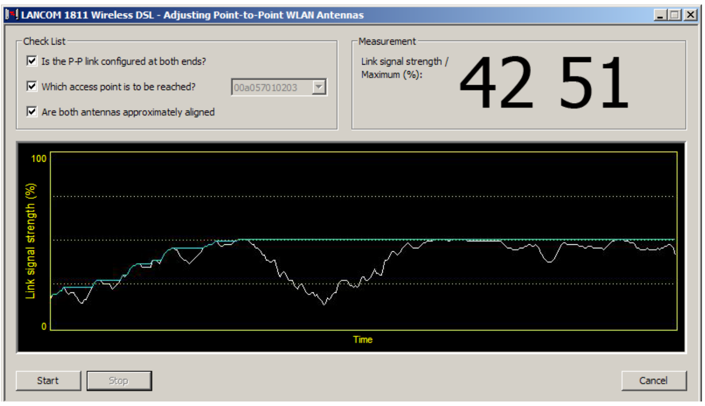


The 'Point-to-point' entry is only visible in the LANmonitor if the monitored device has at least one base station defined as a remote site for a P2P connection (LANconfig: **Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Point-to-Point**).

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

- Is the P2P connection configured at both ends (remote base station defined with MAC address or station name)?
- Is the point-to-point mode of operation activated?
- Which access point is to be monitored? All of the base stations defined as P2P remote sites in the device concerned can be selected here.
- Are both antennas approximately aligned? The basic P2P connection has to be working before fine-tuning can be performed with the aid of LANmonitor.

Once signal monitoring has commenced, the P2P dialog displays the absolute values for the current signal strength and the maximum value since starting the measurement. The development of the signal strength over time and the maximum value are displayed in a diagram, too.



LANCOM 1811 Wireless DSL - Adjusting Point-to-Point WLAN Antennas

Check List

☑ Is the P-P link configured at both ends?

☑ Which access point is to be reached? 00a057010203

☑ Are both antennas approximately aligned

Measurement

Link signal strength / Maximum (%): 42 51

Initially only one of the two antennas should be adjusted until a maximum value is achieved. This first antenna is then fixed and the second antenna is then adjusted to attain the best signal quality.

11.7.3 Measuring wireless bridges

After planning and installation, the wireless bridge can be analyzed to determine the actual data throughput. Further information about the available tools and taking measurements can be found in the LANCOM Techpaper "The performance of outdoor P2P connections", available as a download from www.lancom.de.

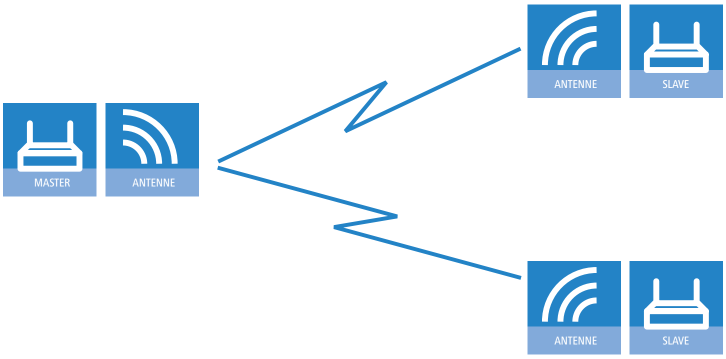
11.7.4 Activating point-to-point operation mode

The behavior of an access point when exchanging data with other access points is defined in the "Point-to-point operation mode".

- **Off:** The access point only communicates with mobile clients
- **On:** The access point can communicate with other access points and with mobile clients
- **Exclusive:** The access point only communicates with other base stations

In the 5 -GHz band, the automatic search for vacant WLAN channels can lead to several simultaneous test transmissions from multiple access points, with the result that they do not find each other. This stalemate situation can be avoided with the appropriate "Channel selection scheme":

- **Master:** This access point takes over the leadership when selecting a free WLAN channel.
- **Slave:** All other access points will search for a channel until they have found a transmitting Master.



Thus it is recommended for the 5 GHz band that one central access point should be configured as 'Master' and all other point-to-point partners should be configured as 'Slave'. In the 2.4 GHz band, too, this setting simplifies the establishment of point-to-point connections if the automatic channel search is activated.

It is imperative that the channel selection scheme is configured correctly if the point-to-point connections are to be encrypted with 802.11i/WPA (a master as authentication server and a slave as client).

11.7.5 Configuration of P2P connections

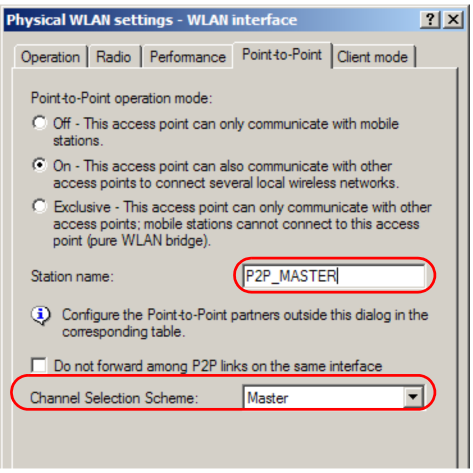
In the configuration of point-to-point connections, entries have to be made for the point-to-point operation mode and the channel selection scheme, along with the MAC addresses or station names of the remote sites.

The configuration of the P2P connections can also be carried out with the WLAN Wizards in LANconfig.

① Click on the button **Physical WLAN settings** to open the corresponding WLAN interface and select the tab for 'Point-to-Point'.

② Activate the suitable point-to-point operation mode here and set the channel selection scheme to either 'Master' or 'Slave'. If the peers of the P2P connections are to be identified via their station names, then enter a unique name for this WLAN station.

For models with multiple WLAN modules, the station name can be entered separately for each physical WLAN interface.



Physical WLAN settings - WLAN interface

Operation | Radio | Performance | 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.

○ Exclusive - This access point can only communicate with other access points; mobile stations cannot connect to this access point (pure WLAN bridge).

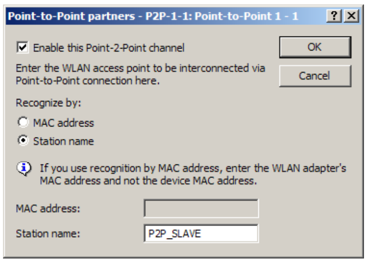
Station name: P2P_MASTER

Configure the Point-to-Point partners outside this dialog in the corresponding table.

□ Do not forward among P2P links on the same interface

Channel Selection Scheme: Master

③ Close the physical WLAN settings and open the list of **Point-to-point partners**. For each of the maximum of six P2P connections, enter either the MAC address of the WLAN card at the remote station or enter the WLAN station's name (depending on the chosen method of identification).



Point-to-Point partners - P2P-1-1: Point-to-Point 1 - 1

☑ Enable this Point-2-Point channel

Enter the WLAN access point to be interconnected via Point-to-Point connection here.

Recognize by:

○ MAC address

● Station name

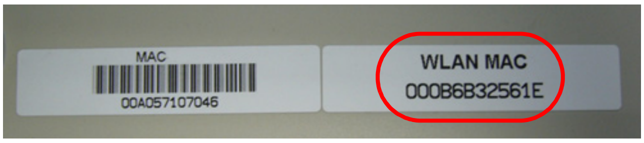
If you use recognition by MAC address, enter the WLAN adapter's MAC address and not the device MAC address.

MAC address:

Station name: P2P_SLAVE

Please observe that only the MAC addresses of the WLAN cards at the other end of the connections are to be entered here! Not the access point's own MAC address, and not the MAC addresses from any other interfaces that may be present in the access points.

You will find the WLAN MAC address on a sticker located under each of the antenna connectors. Only use the string that is marked as the "WLAN MAC" or "MAC-ID". The other addresses that may be found are not the WLAN MAC address but the LAN MAC address.



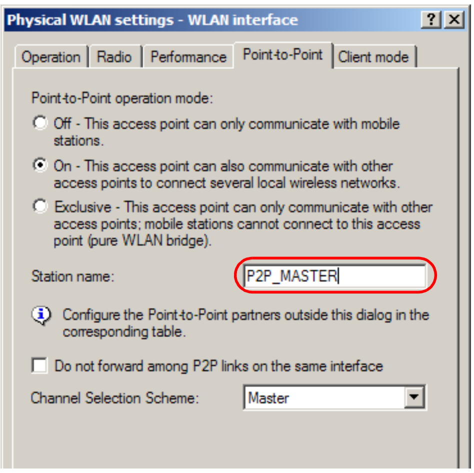
Connecting point-to-point remote stations by station name

When configuring point-to-point connections, an alternative to the MAC addresses is to use the station names of the remote stations.

First of all the station name is entered into the point-to-point settings in the Wireless Routers or Access Points.

- LANconfig: **Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Point to point**
- WEBconfig: **Setup ▶ Interfaces ▶ WLAN interpoint settings**

For models with multiple WLAN modules, the station name can be entered separately for each physical WLAN interface.



Physical WLAN settings - WLAN interface

Operation | Radio | Performance | 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.

○ Exclusive - This access point can only communicate with other access points; mobile stations cannot connect to this access point (pure WLAN bridge).

Station name: P2P_MASTER

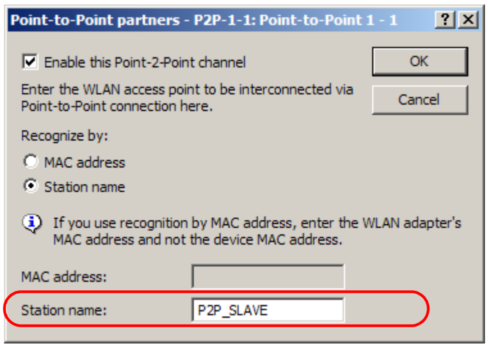
Configure the Point-to-Point partners outside this dialog in the corresponding table.

□ Do not forward among P2P links on the same interface

Channel Selection Scheme: Master

In the point-to-point configuration, select the identification by station name and enter the name of the corresponding station.

- LANconfig: **Wireless LAN ▶ General ▶ Point to point partners**
- WEBconfig: **Setup ▶ Interfaces ▶ WLAN interpoint peers**



Point-to-Point partners - P2P-1-1: Point-to-Point 1 - 1

☑ Enable this Point-2-Point channel

Enter the WLAN access point to be interconnected via Point-to-Point connection here.

Recognize by:

○ MAC address

● Station name

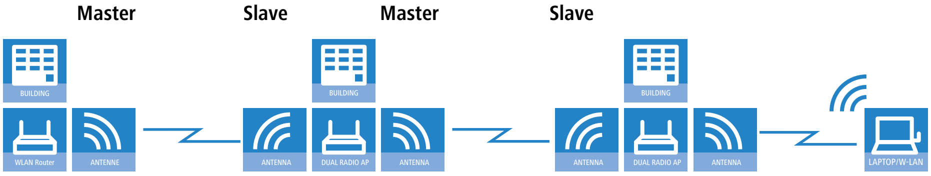
If you use recognition by MAC address, enter the WLAN adapter's MAC address and not the device MAC address.

MAC address:

Station name: P2P_SLAVE

11.7.6 Access points in relay mode

Access points equipped with two wireless modules can be used to establish wireless bridges across multiple stations. Each wireless module is configured as a 'Master' and then 'Slave' in turn.



Employing relay stations with two WLAN modules each also cuts down on the problems from "hidden stations".

11.7.7 Security for point-to-point connections

IEEE 802.11i can be used to attain a significant increase in the security of WLAN point-to-point connections. All of the advantages of 802.11i such as the simple configuration and the powerful encryption with AES are thus available for P2P mode, as are the improved security of the passphrase from the LANCOM Enhance Passphrase Security (LEPS).

Encryption with 802.11i/WPA

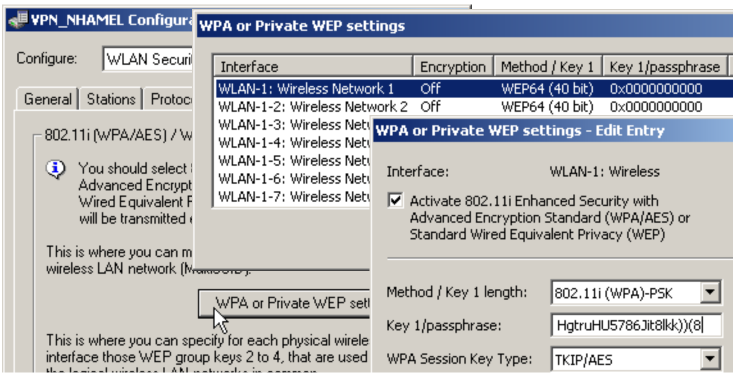
To activate the 802.11i encryption for a correctly configured P2P connection, adjust the settings for the first logical WLAN network in the appropriate WLAN interface (i.e. WLAN-1 if you are using the first WLAN module for the P2P connection, WLAN-2 if you are using the second module, e.g. as with an access point with two WLAN modules).

- Activate the 802.11i encryption.
- Select the method '802.11i (WPA)-PSK'.
- Enter the passphrase to be used.

The passphrases should consist of a random string at least 32 characters long.

When set as P2P Master, the passphrase entered here will be used to check the Slave's authorization to access. When set as P2P Slave, the access point transfers this information to register with the remote site.

For configuration with LANconfig you will find the encryption settings under the configuration area 'Wireless LAN' on the '802.11i/WEP' tab.



Interface	Encryption	Method / Key 1	Key 1/passphrase
WLAN-1: Wireless Network 1	Off	WEP64 (40 bit)	0x0000000000
WLAN-1-2: Wireless Network 2	Off	WEP64 (40 bit)	0x0000000000
WLAN-1-3: Wireless Netw			
WLAN-1-4: Wireless Netw			
WLAN-1-5: Wireless Netw			
WLAN-1-6: Wireless Netw			
WLAN-1-7: Wireless Netw			

Interface: WLAN-1: Wireless

☑ Activate 802.11i Enhanced Security with Advanced Encryption Standard (WPA/AES) or Standard Wired Equivalent Privacy (WEP)

Method / Key 1 length: 802.11i (WPA)-PSK

Key 1/passphrase: HgtruHU5786Jit8lkk))(8

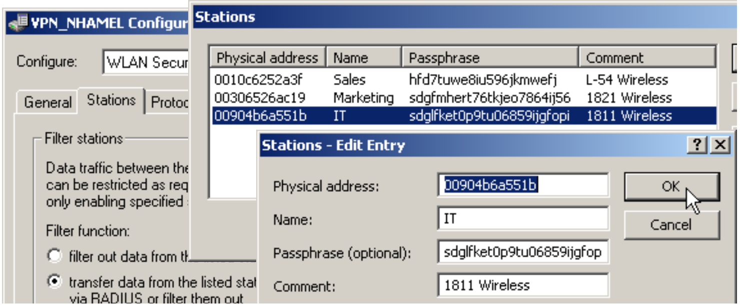
WPA Session Key Type: TKIP/AES

LEPS for P2P connections

A further gain in security can be attained by additionally using LANCOM Enhanced Passphrase Security (LEPS) which involves the matching of MAC address and passphrase.

LEPS can be used to secure single point-to-point (P2P) connections with an individual passphrase. Even if an access point in a P2P installation is stolen and the passphrase and MAC address become known, all other WLAN connections secured by LEPS remain secure.

When using LANconfig for the configuration, you enter the passphrases of the stations approved for the WLAN in the configuration area 'Wireless LAN' on the 'Stations' tab under the button **Stations**.



Physical address	Name	Passphrase	Comment
0010c6252a3f	Sales	hfd7tuwe8iu596jkmwefj	L-54 Wireless
00306526ac19	Marketing	sdgfmhert76tkjeo7864ij56	1821 Wireless
00904b6a551b	IT	sdglfket0p9tu06859ijgfopi	1811 Wireless

Physical address: 00904b6a551b

Name: IT

Passphrase (optional): sdglfket0p9tu06859ijgfop

Comment: 1811 Wireless

11.8 Centralized WLAN management

The widespread use of wireless Access Points and wireless routers provides great convenience and flexibility in network access for businesses, universities and other organizations.

Yet in spite of the numerous advantages WLAN infrastructures offer, there are still a number of unsettled issues:

- All wireless Access Points must be configured and require appropriate monitoring in order to recognize unwelcome WLAN clients, etc. The administration of the Access Points, especially for larger WLAN infrastructures with the appropriate security mechanisms, requires advanced qualifications and experience on the part of those responsible, and it ties up considerable resources in the IT departments.
- The manual customization of the configurations in the Access Points when changes are made to the WLAN infrastructure can be time-consuming, with the result that different configurations can be present in the WLAN at the same time.
- Combined utilization of the shared communications medium (air) requires effective coordination of the Access Points to avoid frequency interference and optimize network performance.
- Access Points in public places are a potential security risk because the devices themselves, including the security-related data in them such as passwords, etc., are susceptible to theft. In addition, rogue Access Points may be able to connect to the LAN unnoticed, bypassing the security policies that are in place.

Centralized WLAN management is the solution to these problems. The configuration of the Access Point is then no longer carried out in the devices themselves but by a central authority instead, the WLAN-Controller. The WLAN-Controller authenticates the Access Points and transmits the correct configuration to the approved devices. This allows for convenient configuration of the WLAN from a central point and the changes to the configuration affect all of the Access Points simultaneously. Optionally the configuration provided by the WLAN-Controller is **not** stored in the Access Point's flash memory but in RAM, so security-related data cannot fall into the hands of unauthorized persons in the event that devices are stolen. Only in "self-sufficient" operation ('Self-sufficient operation' → page 11-61) is the configuration optionally saved for a defined period to flash memory (in an area that cannot be read out with LANconfig or other tools).

11.8.1 The CAPWAP standard

The CAPWAP protocol (Control And Provisioning of Wireless Access Points) introduced by the IETF (Internet Engineering Task Force) is a draft standard for the centralized management of large WLAN infrastructures.

CAPWAP uses two channels for data transfer:

- Control channel, encrypted with DTLS. This channel is used to exchange administration information between the WLAN-Controller and the Access Point.

Datagram Transport Layer Security (DTLS) is an encryption protocol based on TLS but, in contrast to TLS itself, it can be used for transfers over connectionless, unsecured transport protocols such as UDP. DTLS therefore combines the advantages of the high security provided by TLS with the fast transfer via UDP. This also makes DTLS suitable for the transfer of VoIP packets (unlike TLS) because, even after the loss of a packet, the subsequent packets can be authenticated again.

- Data channel, optionally also encrypted with DTLS. The payload data from the WLAN is transferred through this channel from the Access Point via the WLAN-Controller into the LAN—encapsulated in the CAPWAP protocol.

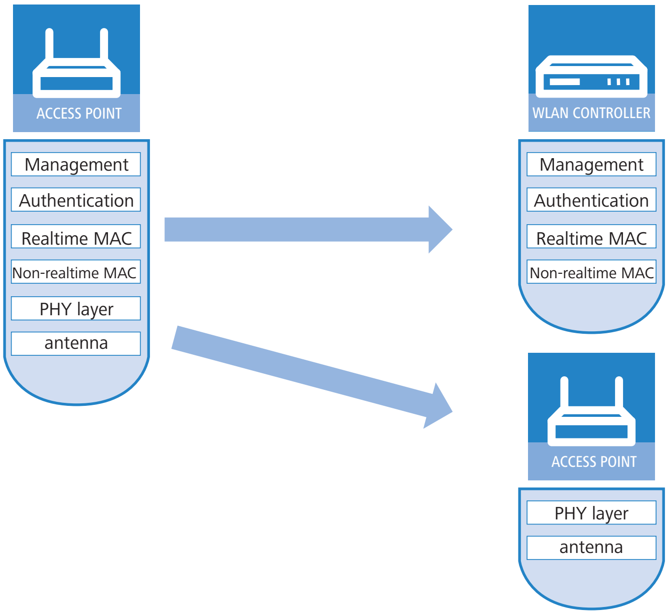
11.8.2 Smart controller technology

In a decentralized WLAN structure with stand-alone Access Points (operating as so-called "rich access points") all functions for data transfer take place in the PHY layer, the control functions in the MAC layer, and the management functions are integrated in the Access Points. Centralized WLAN management divides these tasks among two different devices:

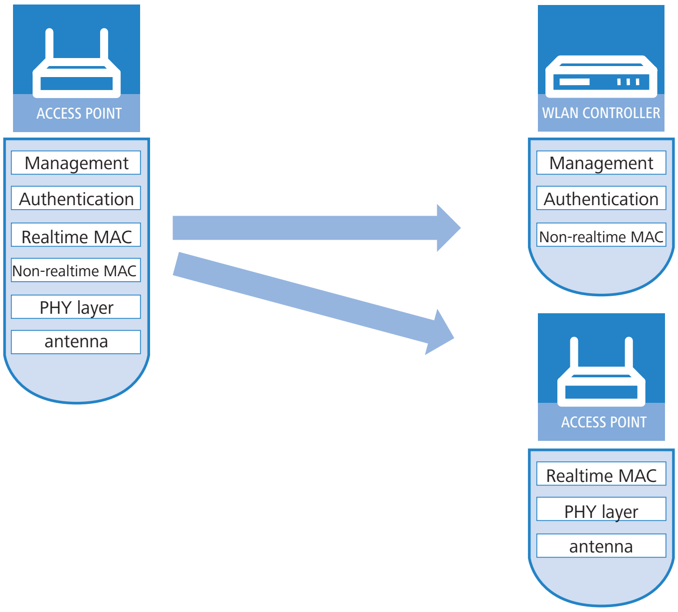
- The central WLAN-Controller assumes the administration tasks.
- The decentralized Access Points handle the data transfer at the PHY layer and the MAC functions.
- A RADIUS or EAP server can be added as a third component for authentication of WLAN clients (which can also be the case in stand-alone WLANs).

CAPWAP describes three different scenarios for the relocation of WLAN functions to the central WLAN-Controller.

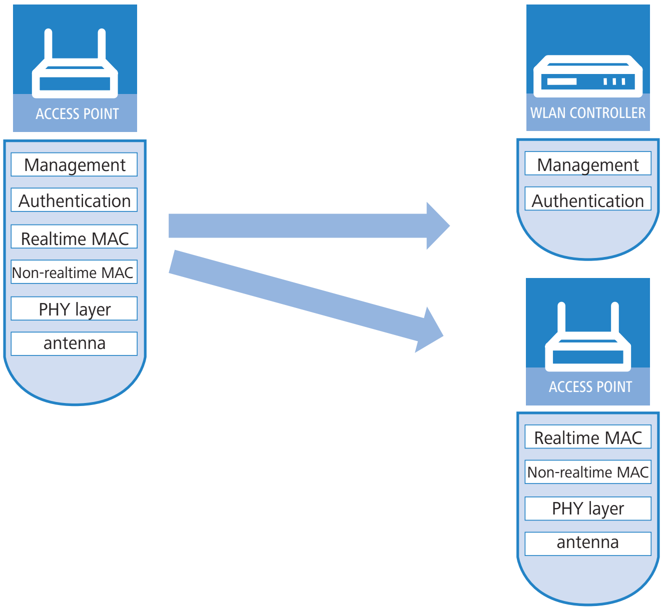
- Remote MAC: In this case, all of the WLAN functions are transferred from the Access Point to the WLAN-Controller. Here, the Access Points only serve as "extended antennas" without independent intelligence.



- Split MAC: With this variant, only a portion of the WLAN functions are transferred to the WLAN-Controller. Normally, realtime applications will continue to be processed in the Access Point; the non-realtime applications are processed via the central WLAN-Controller.



- Local MAC: The third possibility provides for complete management and monitoring of the WLAN data traffic directly in the Access Points. The only information exchanged between the Access Point and the WLAN-Controller is for network management and ensures that the Access Points have a uniform configuration.



Smart Controller Technology from LANCOM Systems uses the local MAC procedure. Thanks to the reduction of centralized tasks, these WLAN infrastructures offer optimum scalability. At the same time, infrastructure of this type prevents the WLAN-Controller from becoming a central bottleneck that has to process large portions of the overall data traffic. In remote MAC and split MAC architectures, **all** payload data is forced to run centrally via the WLAN-Controller. However, in local MAC architectures data can alternatively be directly released from the Access Points into the LAN, so providing high-performance data transfer. This makes WLAN-Controllers from LANCOM suitable for WLANs adhering to the IEEE 802.11n standard, so offering significantly higher bandwidths than conventional WLANs. With break-out into the

LAN, data can also be directly routed into special VLANs. This makes it very easy to set up closed networks, such as for guest access accounts.

CAPWAP tunneling and layer-3 roaming

From one of the later LCOS versions, LANCOM WLAN Controllers also support transfer of the payload data through a CAPWAP tunnel.

- This allows selected applications such as VoIP to be routed via the central WLAN-Controller, for example. If WLAN clients change to a different radio cell, the underlying IP connection will not be interrupted because it continues to be managed by the central WLAN-Controller (layer-3 roaming). In this way, mobile SIP telephones can easily roam even during a call—between Ethernet subnets.
- Managing data streams centrally can also make configuring VLANs at the switch ports unnecessary in environments with numerous VLANs because all CAPWAP tunnels are centrally managed on the WLAN-Controller.

11.8.3 Communication between the Access Point and the WLAN-Controller

As of firmware version LCOS 7.20 there is a difference between LANCOM Access Points (e. g. the LANCOM L-54ag) and LANCOM Wireless Routers (e. g. the LANCOM 1811 Wireless) with regard to the ex-factory standard settings in the WLAN modules. In the following specifications, the general term Access Point will be used for the most part.

Communication between an Access Point and the WLAN-Controller is always initiated by the Access Point. In the following cases, the devices search for a WLAN-Controller that can assign a configuration to them:

- A LANCOM Access Point has the factory settings and is not yet configured. In these settings the WLAN modules are deactivated; the Access Point searches for a WLAN-Controller in the LAN.
- A LANCOM Access Point is already configured; at least one WLAN module is manually set to operate as 'managed' ('Configuring the Access Points' → page 11-73). The Access Point searches for a WLAN-Controller in the LAN on behalf of the one or more corresponding WLAN modules.
- A LANCOM Wireless Router is already configured; at least one WLAN module is manually set to operate as 'managed'. The wireless router searches for a WLAN-Controller in the LAN on behalf of the one or more corresponding WLAN modules.

At the beginning of communications, the Access Point sends a "Discovery Request Message" to find any available WLAN-Controllers. This request is sent as a broadcast. However, because in some structures a potential WLAN-Controller cannot be reached by a broadcast, special addresses from additional WLAN-Controllers can also be entered into the configuration of the Access Points.

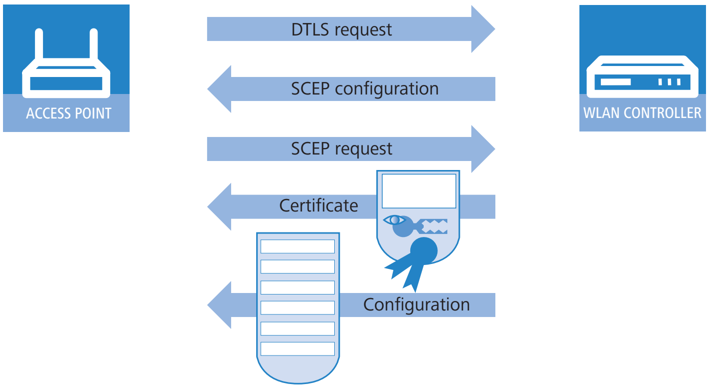
DNS names of WLAN-Controllers can also be resolved. All Access Points with LCOS 7.22 or higher have the default name 'WLC-Address' pre-configured so that a DNS server can resolve this name to a LANCOM WLAN Controller. The same applies to the DHCP suffixes learned via DHCP. This also makes it possible to reach WLAN-Controllers that are not located in the same network, without having to configure the Access Points.

From the available WLAN-Controllers, the Access Point selects the best one and queries it for the structure of the DTLS connection. The "best" WLAN-Controller for the Access Point is the one with the least load, i.e., the lowest ratio of managedAccess Points compared to the maximum possible Access Points. In case of two or more equally "good" WLAN-Controllers, the Access Point selects the nearest one in the network, i.e., the one with the fastest response time.

The WLAN-Controller then uses an internal random number to determine a unique and secure session key which it uses to protect the connection to the Access Point. The CA in the WLAN-Controller issues the Access Point certificate via SCEP. The certificate is protected by a one-time-only "challenge" (password). The Access Point uses this certificate for authentication at the WLAN-Controller to collect the certificate.

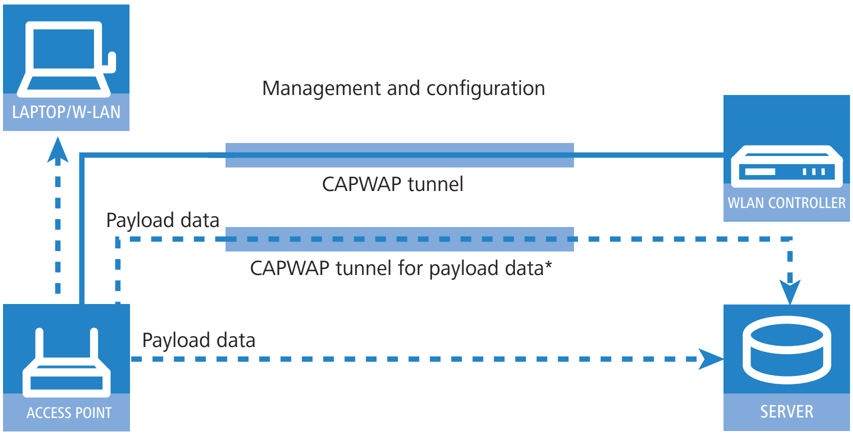
The Access Point is provided with the configuration for the integrated SCEP client via the secure DTLS connection – the Access Point is then able to retrieve its certificate from the SCEP CA via SCEP. Once this is done, the assigned configuration is transferred to the Access Point.

SCEP stands for Simple Certificate Encryption Protocol; CA for Certification Authority.



Authentication and configuration can both be carried out either automatically or only with a corresponding entry of the Access Point's MAC address in the AP table of the WLAN-Controller. If the Access Point's WLAN modules were deactivated at the beginning of the DTLS communication, these will be activated after successful transfer of the certificate and configuration (provided they are not explicitly deactivated in the configuration).

The management and configuration data will then be transferred via the CAPWAP tunnel. The payload data from the WLAN client is then released in the Access Point directly into the LAN and transferred, for example, to the server.



* Not yet available with early shipments

11.8.4 Zero-touch management

With their ability to automatically assign a certificate and configurations to the requesting Access Points, LANCOM WLAN Controllers implement true "zero-touch management". Simply connect new Access Points to the LAN—no further configuration is necessary. This simplification to only having to install devices reduces the workload for IT departments, especially in decentralized structures, because no special IT or WLAN expertise is required for the setup at the remote locations.

11.8.5 Split management

LANCOM Access Points can locate their WLAN-Controller in remote networks—a simple IP connection, e.g. via a VPN path, is all that you need. As the WLAN-Controllers only influence the WLAN part of the configuration in the Access Point, all other functions can be managed separately. This division of the configuration tasks makes LANCOM WLAN Controllers perfect for establishing a company-wide WLAN infrastructure that is based at the headquarters and includes all of the branch and home offices connected to it.

11.8.6 General settings

Most of the parameters for configuring the LANCOM WLAN Controller correspond with those of the Access Points. For this reason, this section does not explicitly describe all of the WLAN parameters, but only those aspects necessary for operating the WLAN-Controller.

This area is for the basic settings of your WLAN-Controller.

- **Automatically accept new APs (Auto-accept)**

  Enables the WLAN-Controller to provide all new Access Points with a configuration, even those not in possession of a valid certificate.

  Enables the WLAN-Controller to provide a certificate to all new Access Points **without** a valid certificate. One of these two conditions must be fulfilled for this:

- □ A configuration for the Access Point is entered into the AP table under its MAC address.
- □ The option 'Automatically provide APs with the default configuration' is activated.

■ **Automatic provision of the default configuration**

This enables the WLAN-Controller to assign a default configuration to every new Access Point (even those **without** a valid certificate), even if no explicit configuration has been stored for it. In combination with auto-accept, the LANCOM WLAN Controller can accept all managed-mode Access Points which are found in the WLAN infrastructure managed by it (up to the maximum number of Access Points that can be managed by one WLAN-Controller). Access Point accepted by default are also entered into the MAC list.

This option can also lead to the acceptance of unintended Access Points into the WLAN infrastructure. For this reason this option should only be activated during the start-up phase when setting up a centrally managed WLAN infrastructure.

Combining the settings for auto-accept and default configuration can cater for a variety of different situations for the setup and operation of Access Points:

Auto-accept	Default configuration	Suitable for
On	On	Rollout phase: Use this combination only if you can be sure that **no unintended Access Point** are connected with the LAN and thus accepted into the WLAN infrastructure.
On	Off	Controlled rollout phase: Use this combination if you have entered all of the approved Access Points into the AP table along with their MAC addresses, assuming that these are to be automatically accepted into the WLAN infrastructure.
Off	Off	Normal operation: No new Access Points will be accepted into the WLAN infrastructure without the administrator's approval.

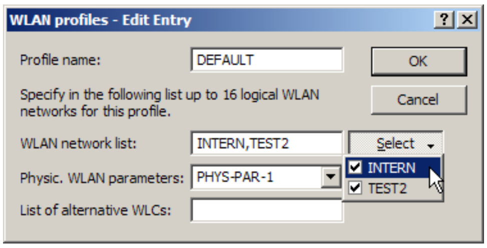
11.8.7 Profiles

The profiles area is used to define the logical WLAN networks, physical WLAN parameters, and the WLAN profiles which combine these two elements.

WLAN profiles

WLAN profiles are collections of the various settings that are to be assigned to the Access Points. The allocation of WLAN profiles to the Access Points is set in the AP table.

The following parameters can be defined for every WLAN profile:



Profile name: DEFAULT

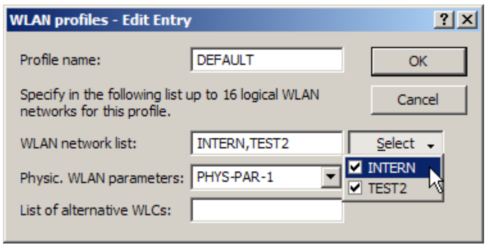
Specify in the following list up to 16 logical WLAN networks for this profile.

WLAN network list: INTERN,TEST2

☑ INTERN
☑ TEST2

Physic. WLAN parameters: PHYS-PAR-1

List of alternative WLCs:


WLAN profiles - Edit Entry

Profile name: DEFAULT

Specify in the following list up to 16 logical WLAN networks for this profile.

WLAN network list: INTERN,TEST2

☑ INTERN
☑ TEST2

Physic. WLAN parameters: PHYS-PAR-1

List of alternative WLCs:

LANconfig: WLAN-Controller ▶ Profiles ▶ WLAN profiles

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN management ▶ AP configuration ▶ Common profiles

■ **Profile name**

Name of the profile under which the settings are saved.

■ **WLAN network list**

List of the logical WLAN networks that are assigned via this profile.

From this list, Access Points use only the first eight entries that are compatible with their own hardware. This means that eight WLAN networks for purely 2.4 GHz operations and eight for purely 5 GHz operations can be defined in a profile. Consequently, each LANCOM Access Point—be it a model offering 2.4 GHz or 5 GHz support—can choose from a maximum of eight logical WLAN networks.

- **Physical WLAN parameters**

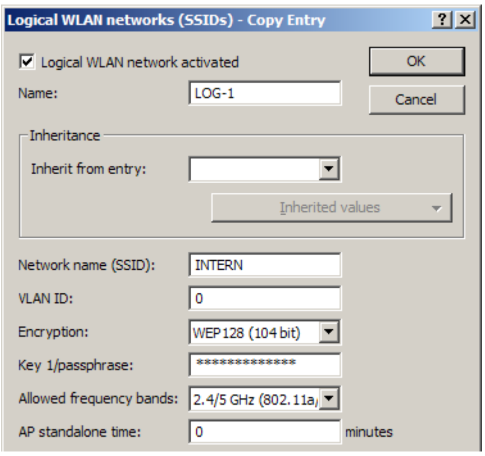
  A set of physical parameters that the Access Point WLAN modules are supposed to work with.

- **IP address of alternative WLAN-Controllers**

  A list of WLAN-Controllers that the Access Points should attempt to connect with. The Access Point starts searching for a WLAN-Controller with a broadcast. Defining alternative WLAN-Controllers is worthwhile when a broadcast cannot reach all WLAN-Controllers (e.g. if the WLAN-Controller is located in another network).

Logical WLAN networks

Here the logical WLAN networks are set for assignment to the Access Points. The following parameters can be defined for each logical WLAN network:



Logical WLAN networks (SSIDs) - Copy Entry

☑ Logical WLAN network activated

Name: LOG-1

Inheritance

Inherit from entry:

Network name (SSID): INTERN

VLAN ID: 0

Encryption: WEP128 (104 bit)

Key 1/passphrase: **************

Allowed frequency bands: 2.4/5 GHz (802.11a,

AP standalone time: 0 minutes

LANconfig: WLAN-Controller ▶ Profiles ▶ Logical WLAN networks

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN management ▶ AP configuration ▶ Network profiles

- **Network name**

  Name of the logical WLAN network under which the settings are saved. This name is only used for internal administration of logical networks.

- **Inheritance**

  Selection of a logical WLAN network defined earlier and from which the settings are to be inherited ('Inheritance of parameters' → page 11-67).

- **SSID**

  Service Set Identifier – this name under which the WLAN network is offered to the WLAN clients.

- **VLAN ID**

  VLAN ID for this logical WLAN network ('Dynamic VLAN assignment' → page 11-70).

Please note that to use VLAN IDs in a logical WLAN network requires a management VLAN ID to be set ('Management VLAN ID' → page 11-62). If you define a VLAN-ID for a WLAN profil the VLAN module is automatically activated on the managing access points

- **Self-sufficient operation**

  The time in minutes that a managed-mode Access Point continues to operate in its current configuration.

  The configuration is provided to the Access Point by the WLAN-Controller and is optionally stored in flash memory (in an area that is not accessible to LANconfig or other tools). Should the connection to the WLAN-Controller be interrupted, the Access Point will continue to operate with the configuration stored in flash for the time period entered here. The Access Point can also continue to work with this flash configuration after a local power outage.

  If there is still no connection to the WLAN-Controller after this time period has expired then the flash configuration is deleted and the Access Point goes out of operation. As soon as the WLAN-Controller can be reached again, the configuration is transmitted again from the WLAN-Controller to the Access Point.

This option enables an Access Point to continue operating even if the connection to the WLAN-Controller is temporarily interrupted. Furthermore this represents an effective measure against theft as all security-related configuration parameters are automatically deleted after this time has expired.

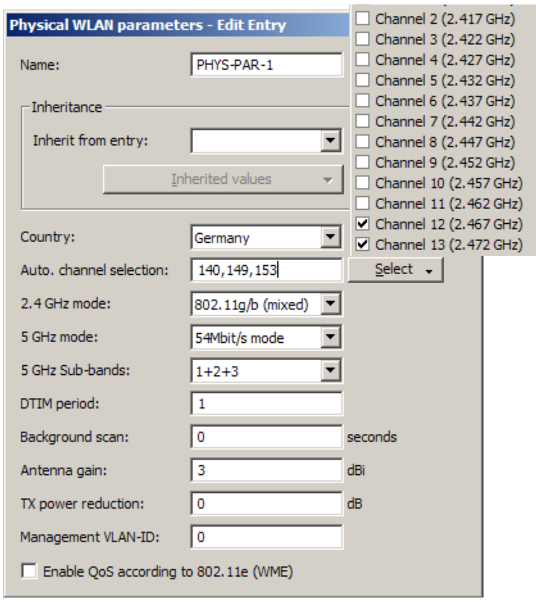
If the Access Point establishes a backup connection to a secondary WLAN-Controller then the countdown to the expiry of self-sufficient operation is halted. The Access Point and its WLAN networks remain active as long as it has a connection to a WLAN-Controller.

Please note that the delay before deletion of the flash configuration is the time of self-sufficient operation, not the time after power loss!

All other WLAN network parameters correspond to those for the standard configuration of Access Points.

Physical WLAN parameters

Here the physical WLAN parameters are set for assignment to the Access Points. The following parameters can be defined for each set of physical WLAN parameters:



Physical WLAN parameters - Edit Entry

Name: PHYS-PAR-1

Inheritance

Inherit from entry:

Inherited values

Country: Germany

Auto. channel selection: 140,149,153

Select

□ Channel 2 (2.417 GHz)
□ Channel 3 (2.422 GHz)
□ Channel 4 (2.427 GHz)
□ Channel 5 (2.432 GHz)
□ Channel 6 (2.437 GHz)
□ Channel 7 (2.442 GHz)
□ Channel 8 (2.447 GHz)
□ Channel 9 (2.452 GHz)
□ Channel 10 (2.457 GHz)
□ Channel 11 (2.462 GHz)
☑ Channel 12 (2.467 GHz)
☑ Channel 13 (2.472 GHz)

2.4 GHz mode: 802.11g/b (mixed)

5 GHz mode: 54Mbit/s mode

5 GHz Sub-bands: 1+2+3

DTIM period: 1

Background scan: 0 seconds

Antenna gain: 3 dBi

TX power reduction: 0 dB

Management VLAN-ID: 0

□ Enable QoS according to 802.11e (WME)

LANconfig: WLAN-Controller ▶ Profiles ▶ Physical WLAN parameters

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN management ▶ AP configuration ▶ Radio profiles

- **Name**

  Unique name for this combination of physical WLAN parameters.

- **Inheritance**

  Selection of a physical WLAN parameter set defined earlier and from which the settings are to be inherited ('Inheritance of parameters' → page 11-67).

- **Country**

  The country in which the Access Point is to be operated. This information is used to define country-specific settings such as the permitted channels, etc.

- **Automatic channel selection**

  As standard the Access Points can use all of the channels permitted in the country of operation. To limit the selection to certain channel, the desired channels can be entered here as a comma-separated list. Ranges can also be defined (e.g. '1,6,11').

- **Management VLAN ID**

  The VLAD ID for the management network that is to manage the Access Points.

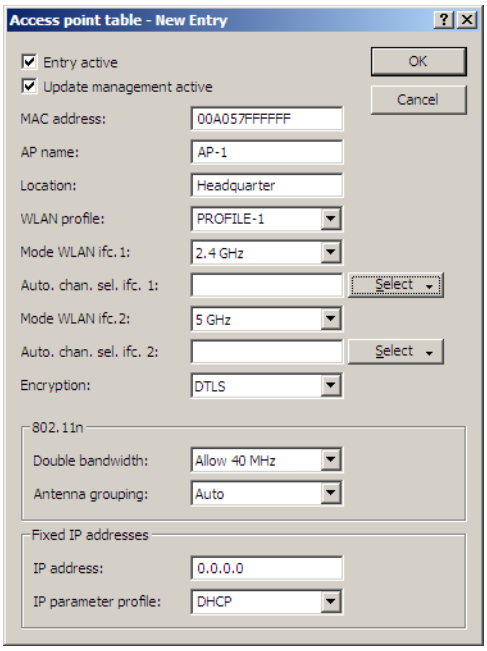
The Management VLAN ID **must** be set to a value not equal to zero so that VLANs can be used over the WLAN networks. This also applies when the management network itself is not to be tagged with VLAN IDs (Mgmt-VLANID=1).

VLAN activation only applies to WLAN networks which are connected by means of these physical WLAN parameters.

All other physical WLAN parameters correspond to those for the standard configuration of Access Points.

11.8.8 List of Access Points

The AP table is a central element of the configuration for WLAN-Controllers. Here, Access Points are assigned with WLAN profiles (i.e. the combinations of logical and physical WLAN parameters) via their MAC addresses. Furthermore, the existence of an entry in the AP table for an Access Point affects its ability to connect to a WLAN-Controller. The following parameters can be defined for every Access Point:



☑ Entry active
☑ Update management active

MAC address:	00A057FFFFFF
AP name:	AP-1
Location:	Headquarter
WLAN profile:	PROFILE-1
Mode WLAN ifc. 1:	2.4 GHz
Auto. chan. sel. ifc. 1:	
Mode WLAN ifc. 2:	5 GHz
Auto. chan. sel. ifc. 2:	
Encryption:	DTLS

802.11n

Double bandwidth:	Allow 40 MHz
Antenna grouping:	Auto

Fixed IP addresses

IP address:	0.0.0.0
IP parameter profile:	DHCP

LANconfig: WLAN-Controller ▶ AP config. ▶ Access-point table

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN management ▶ AP configuration ▶ Access points

- **Update management active**

  Activating update management for the access point enables the latest firmware and script versions to be uploaded automatically. All other settings are set under AP update.

- **MAC address**

  MAC address of each Access Point.

- **AP name**

  Name of the Access Point in managed mode.

- **Location**

  Location of the Access Point in managed mode.

- **WLAN profile**

  WLAN profile from the list of defined profiles ('WLAN profiles' → page 11-60).

- **WLAN interface 1**

  Frequency of the first WLAN module. This parameter can also be used to deactivate the WLAN module.

- **Auto. channel selection lfc 1**

  Access points automatically carry out channel selection for the frequency band available in the country of operation, assuming that no entry is made here.

  Enter the channels to be available for automatic selection by the first WLAN module. If just one channel is defined here, then this channel only will be used and no automatic selection takes place. For this reason you should ensure that the channels entered here are legal for use in the country of operation as defined. Invalid channels are ignored.

- **WLAN interface 2**

  Frequency of the second WLAN module. This parameter can also be used to deactivate the WLAN module.

- **Auto. channel selection lfc 2**

  Automatic channel selection for the second WLAN module.

Settings for the second WLAN module are ignored if the managed device has only one WLAN module.

- **Encryption**

  Encryption of communications over the control channel. Without encryption the control data is exchanged as plain text. In both cases authentication is by certificate.

- **Double bandwidth**

  LANCOM Access Points compliant with IEEE 802.11n optionally offer the activation of double the bandwidth.

- **Antenna grouping**

  Antenna grouping can be configured in order to optimize the gain from spacial multiplexing.

- **IP address**

  Here you specify the fixed IP address of the access point.

- **IP parameter profile**

  Here you specify the profile name used to reference the IP settings for the access point. If you retain the standard setting DHCP, the setting for the fixed IP address is ignored and the access point is forced to obtain its IP address via DHCP.

11.8.9 Station table (ACL table)

The station table defines which WLAN clients can associate with the WLAN networks of the LANCOM Wireless Routers and LANCOM Access Points which are centrally managed by the WLAN-Controller. Furthermore, the method offers a convenient way to assign an authentication passphrase and a VLAN ID to each WLAN client.

To use the station table, it is imperative that the RADIUS server is activated in the WLAN-Controller. As an alternative, requests can be forwarded to another RADIUS server. More information on RADIUS is available under 'RADIUS' → page 16-25.

For every logical WLAN in which WLAN clients are authenticated by RADIUS, the MAC check has to be activated.

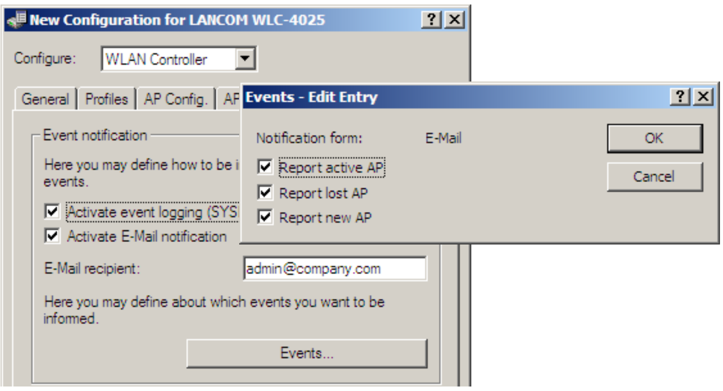
The ACL list is described under 'Access-control list' → page 11-26.

11.8.10 Options for the WLAN-Controller

The 'Options' area in the WLAN-Controller configuration is used to define notifications in case of events and to set various default values.

Event notification

Notification can take place via SYSLOG or e-mail. You can define the following parameters:



Configure: WLAN Controller

Here you may define how to be i events.

☑ Activate event logging (SYS

☑ Activate E-Mail notification

E-Mail recipient: admin@company.com

Here you may define about which events you want to be informed.

Notification form: E-Mail

☑ Report active AP

☑ Report lost AP

☑ Report new AP

LANconfig: WLAN-Controller ▶ Options ▶ Event notification

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN management ▶ Notification

- **SYSLOG**

  Activates notification by SYSLOG.

  - Possible values: On/off.

- **E-mail**

  Activates notification by e-mail.

  - Possible values: On/off.

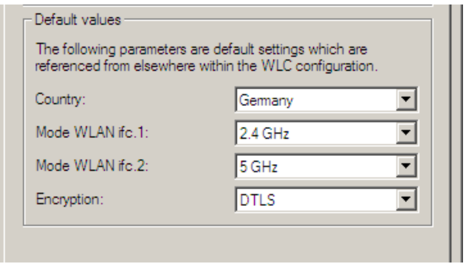
- **Events**

  Selects the events that trigger notification.

  - Possible values:
    - Active Access Point notification
    - Missing Access Point notification
    - New Access Point notification

Default parameters

For some parameters, default values can be defined centrally and these serve as reference default values for other parts of the configuration.



Default values

The following parameters are default settings which are referenced from elsewhere within the WLC configuration.

Country: Germany

Mode WLAN ifc.1: 2.4 GHz

Mode WLAN ifc.2: 5 GHz

Encryption: DTLS

LANconfig: WLAN-Controller ▶ Options ▶ Default parameters

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN management ▶ AP configuration

- **Country**

  The country in which the Access Point is to be operated. This information is used to define country-specific settings such as the permitted channels, etc.

- **WLAN interface 1**

  Frequency of the first WLAN module. This parameter can also be used to deactivate the WLAN module.

- **WLAN interface 2**

  Frequency of the second WLAN module. This parameter can also be used to deactivate the WLAN module.

- **Encryption**

  Encryption of communications over the control channel. Without encryption the control data is exchanged as plain text. In both cases authentication is by certificate.

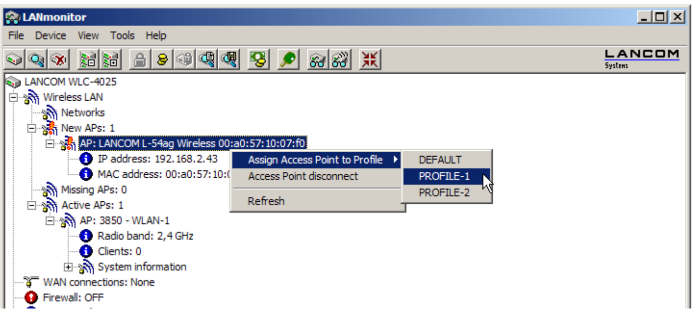
11.8.11 Accept new Access Points into the WLAN infrastructure manually

If you prefer not to accept Access Points into the WLAN infrastructure automatically (auto-accept, 'Automatically accept new APs (Auto-accept)' → page 11-59), you can accept Access Points manually.

Accepting Access Points via LANmonitor

It is especially easy to accept new Access Points with LANmonitor. A configuration is selected that will be assigned to the Access Point after transmission of a new certificate.

In LANmonitor, click on the new Access Point with the right-hand mouse key. From the context menu that pops up, you select the configuration which is to be assigned to the device.



LANCOM WLC-4025
Wireless LAN
Networks
New APs: 1
AP: LANCOM L-54ag Wireless 00:a0:57:10:07:f0
IP address: 192.168.2.43
MAC address: 00:a0:57:10:0
Missing APs: 0
Active APs: 1
AP: 3850 - WLAN-1
Radio band: 2,4 GHz
Clients: 0
System information
WAN connections: None
Firewall: OFF

> Assignment of the configuration causes the Access Point to be entered into the AP table in the WLAN-Controller. It takes a few seconds for the WLAN-Controller to assign a certificate to the Access Point and for this to become an active element in the central WLAN infrastructure. Due to this, the newly accepted Access Point is briefly signaled as a "Lost AP" by the red Lost AP LED, in the device's display, and in LANmonitor until assignment of the certificate is completed.

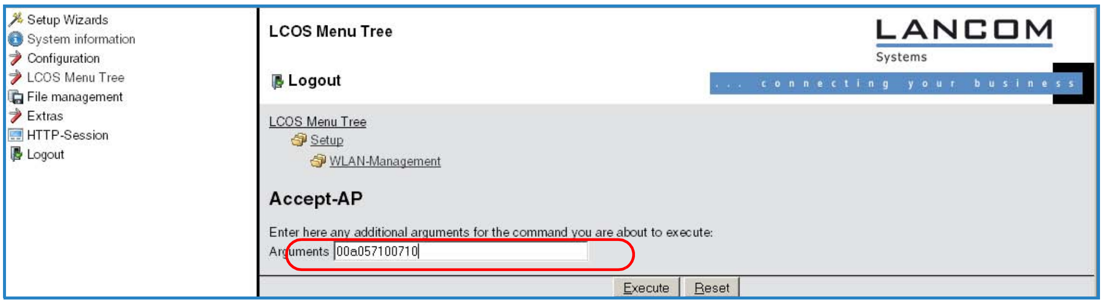
Accepting Access Points via WEBconfig with assignment of a certificate

New Access Points that do not have a valid certificate but do have an entry in the AP table can be manually accepted with WEBconfig.

① Open the LANCOM WLAN Controller configuration with WEBconfig.

② Under **LCOS menu tree** ▶ **Setup** ▶ **WLAN management** select the action **Accept AP**.

③ When requested for additional arguments, enter the MAC address of the Access Point for acceptance and confirm with **Execute**.



LCOS Menu Tree

Logout

LCOS Menu Tree
Setup
WLAN-Management

Accept-AP

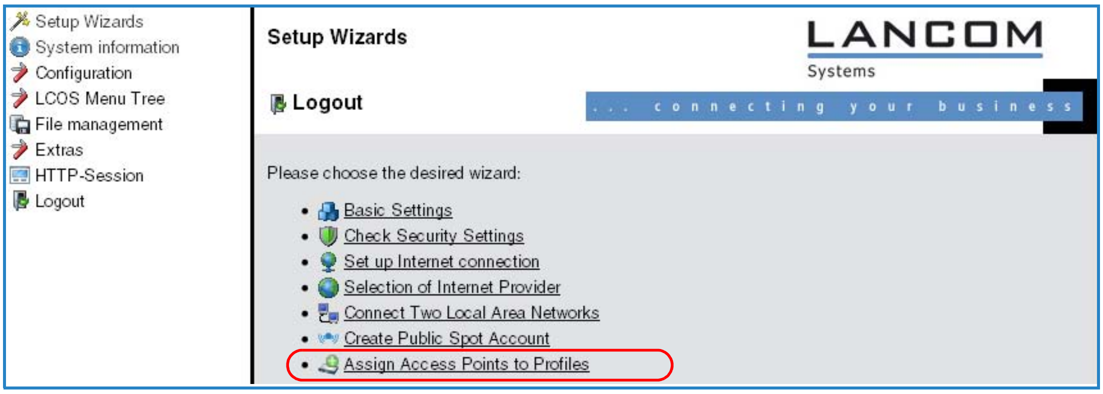
Enter here any additional arguments for the command you are about to execute:

Arguments 00a057100710

Accepting Access Points via WEBconfig with assignment of a certificate and configuration

New Access Points that do not have a valid certificate and do not have an entry in the AP table can be manually accepted by means of a wizard in WEBconfig. A configuration is selected that will be assigned to the Access Point after transmission of a new certificate.

① Open the LANCOM WLAN Controller configuration with WEBconfig and select the **Setup Wizards**.



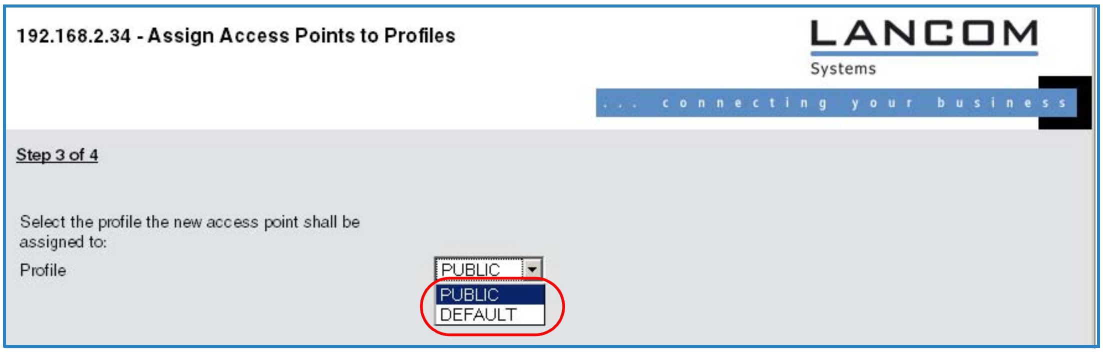
Setup Wizards

Logout

Please choose the desired wizard:

- Basic Settings
- Check Security Settings
- Set up Internet connection
- Selection of Internet Provider
- Connect Two Local Area Networks
- Create Public Spot Account
- Assign Access Points to Profiles

② Click on the link **Assign Access Point to Profiles** to start the wizard. Select the desired Access Point by means of its MAC address and choose the WLAN configuration that is to be assigned to the Access Point.



192.168.2.34 - Assign Access Points to Profiles

Step 3 of 4

Select the profile the new access point shall be assigned to:

Profile PUBLIC

Assignment of the configuration causes the Access Point to be entered into the AP table in the WLAN-Controller. It takes a few seconds for the WLAN-Controller to assign a certificate to the Access Point and for this to become an active element in the central WLAN infrastructure. Due to this, the newly accepted Access Point is briefly signaled as a "Lost AP" by the red Lost AP LED, in the device's display, and in LANmonitor until assignment of the certificate is completed.

11.8.12 Manually removing Access Points from the WLAN infrastructure

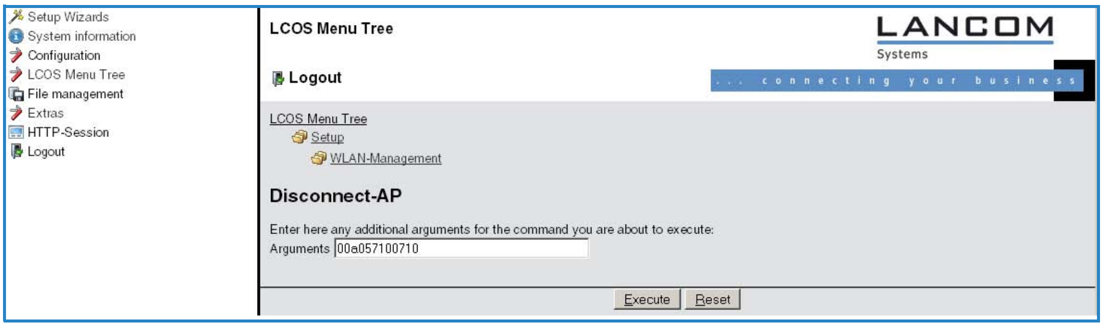
The following actions are required to remove an Access Point under management of the WLAN-Controller from the WLAN infrastructure:

① In the Access Point, switch the WLAN operating mode of the WLAN module from 'Managed' to 'Client' or 'Access Point'.

② In the WLAN-Controller, delete the configuration for the Access Point and/or deactivate 'Automatically provide APs with a default configuration'.

③ Disconnect the Access Point in WEBconfig by selecting **LCOS menu tree** ▶ **Setup** ▶ **WLAN-Management** and the action **Disconnect AP** or alternatively in LANmonitor.

④ When requested for additional arguments, enter the MAC address of the Access Point to be disconnected and confirm with **Execute**.



Disconnect-AP

Enter here any additional arguments for the command you are about to execute:

Arguments: 00a057100710

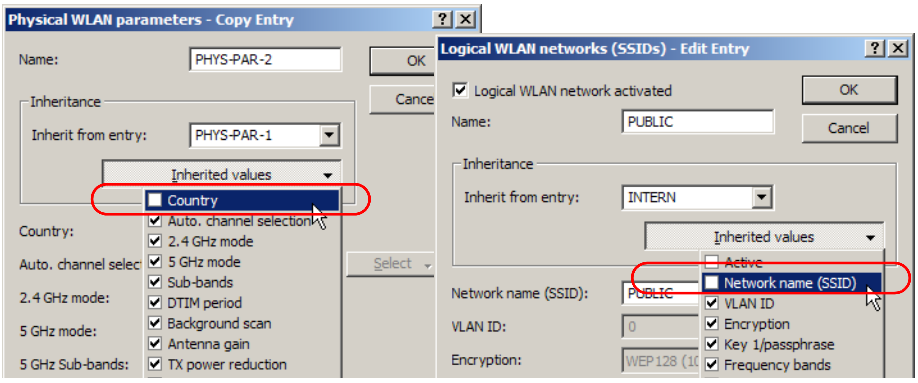
11.8.13 Inheritance of parameters

A LANCOM WLAN Controller is capable of managing a wide range of different Access Points at different locations. However, WLAN profiles include settings that are not equally suitable for every type of Access Point that can be managed. For example, there are differences between the country settings and the device properties.

In order to avoid having to maintain multiple redundant WLAN profiles to cater for countries or device types, it is possible to "inherit" selected properties from the logical WLAN networks and the physical WLAN parameters.

① You should initially generate the basic settings that are valid for the majority of the managed Access Points.

② You can then start to generate entries for the more specific values, e.g. physical settings for a certain country, or a logical WLAN network for public access by mobile clients.



Name: PHYS-PAR-2

Inherit from entry: PHYS-PAR-1

□ Country
☑ Auto. channel selection
☑ 2.4 GHz mode
☑ 5 GHz mode
☑ Sub-bands
☑ DTIM period
☑ Background scan
☑ Antenna gain
☑ TX power reduction

☑ Logical WLAN network activated

Name: PUBLIC

Inherit from entry: INTERN

□ Active
□ Network name (SSID)
☑ VLAN ID
☑ Encryption
☑ Key 1/passphrase
☑ Frequency bands

③ Select the entry from which the values are to be inherited and mark the values for inheritance. Parameters inherited in this way are displayed in the configuration dialog in gray and they cannot be edited.

④ Depending on the application, the WLAN settings collected in this way are then grouped into separate profiles, and these are then assigned to their respective Access Points.

Inheritance fundamentally allows chains over multiple stages (cascading). This means, for example, that country and device-specific parameters can be grouped for convenience.

Recursion is also possible—profile A inherits from profile B, and at the same time B inherits from A. However, the parameters available for inheritance are limited to one "inheritance direction" per parameter.

11.8.14 Backing up the certificates

At system startup, a LANCOM WLAN Controller generates the basic certificates for the assignment of certificates to the Access Points, including the root certificates for the CA (Certification Authority) and the RA (Registration Authority). Based on these two certificates, the WLAN-Controller issues device certificates for the Access Points.

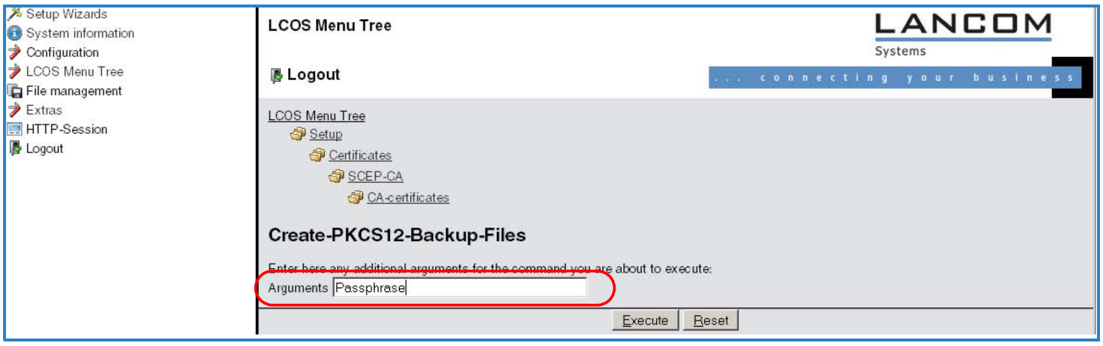
If multiple WLAN-Controllers are employed in parallel in the same WLAN infrastructure (for load balancing) or if a device is being replaced or reconfigured, the same root certificates should always be used to avoid problems operating the managed Access Points.

Create backups of the certificates

To restore the CA or RA, the relevant root certificates with private keys will be required as generated automatically when the LANCOM WLAN Controller was started. Furthermore the following files with information on issued device certificates should also be backed up ('Backing up and restoring further files from the SCEP-CA' → page 11-69). To ensure that this confidential information remains protected even when exported from the device, it is initially stored to a password-protected PCKS12 container.

① Open the configuration of the LANCOM WLAN Controller with WEBconfig under **LCOS menu tree** ▶ **Setup** ▶ **Certificates** ▶ **SCEP-CA** ▶ **CA certificates**.

② Select the command **Create PKCS12 backup files** and enter the passphrase for the PKCS12 container as the additional argument.



Create-PKCS12-Backup-Files

Enter here any additional arguments for the command you are about to execute:

Arguments: Passphrase

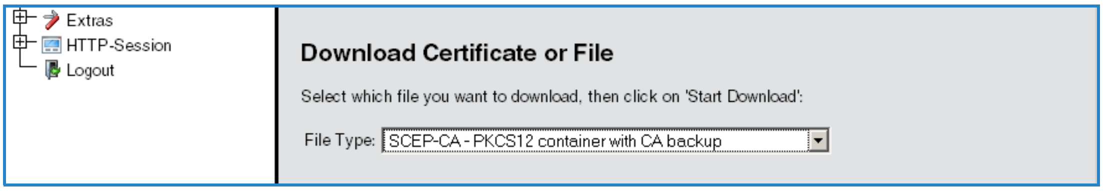
This command backs up the certificates and private keys to the PKCS12 files and these can then be downloaded from the device.

Downloading certificate backups from the device

① On the WEBconfig entry page select the command **Download certificate or file**.

② Select the two entries for SCEP-CA as data type one after the other and confirm with **Start download**:

- PKCS12 container with CA backup
- PKCS12 container with RA backup



Download Certificate or File

Select which file you want to download, then click on 'Start Download':

File Type: SCEP-CA - PKCS12 container with CA backup

The backup file is then stored to your data medium. The passphrase will be required is when uploading the backup to a LANCOM WLAN Controller.

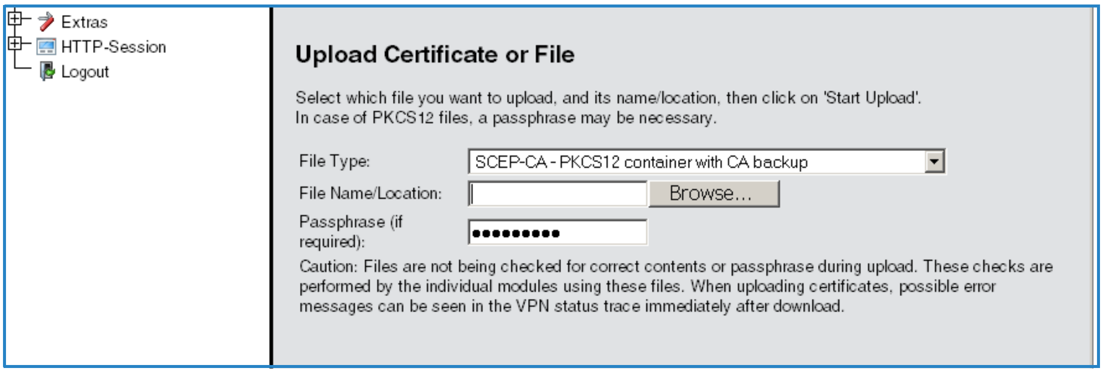
Uploading a certificate backup into the device

① On the WEBconfig entry page select the command **Upload certificate or file**.

② Select the two entries for SCEP-CA as data type one after the other:

- PKCS12 container with CA backup
- PKCS12 container with RA backup

③ For each upload, enter the file name, storage location, and the passphrase that was defined when the backup file was created. Confirm with **Start upload**:



Upload Certificate or File

Select which file you want to upload, and its name/location, then click on 'Start Upload'.
In case of PKCS12 files, a passphrase may be necessary.

File Type: SCEP-CA - PKCS12 container with CA backup
File Name/Location:
Passphrase (if required): ●●●●●●●●●●

Caution: Files are not being checked for correct contents or passphrase during upload. These checks are performed by the individual modules using these files. When uploading certificates, possible error messages can be seen in the VPN status trace immediately after download.

④ The file named controller_rootcert needs to be removed from the directory /Status/File-System/Contents after uploading the backup CA. Enter the following command at the command line interface:

```
cd /Status/File-System/Contents
del controller_rootcert
```

⑤ After that the reinit command has to be executed from the directory /Setup/Certificates/SCEP-Client:

```
cd /Setup/Certificates/SCEP-Client
do Reinit
```

11.8.15 Backing up and restoring further files from the SCEP-CA

To be able to fully restore the SCEP-CA, it is important to have the information on the device certificates issued for the individual Access Points by the SCEP-CA.

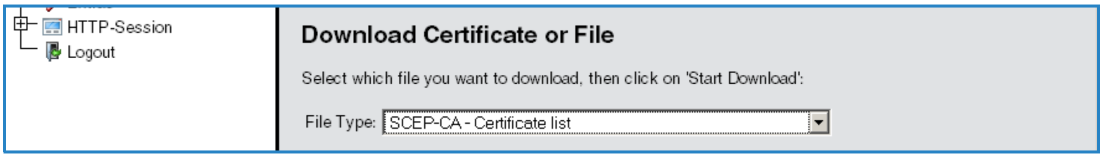
If the root certificates only were backed up, then any issued device certificates can no longer be revoked!

For this reason the following files have to be saved in addition to the certificates themselves:

- SCEP-CRL file: List of certificates issued and subsequently revoked by the SCEP-CA.
- SCEP certificate list: List of all certificates ever issued by the SCEP-CA.

① Select **File Management ▶ Download certificate or file** on the WEBconfig start page.

② Select the entries listed above as data type one after the other and then confirm with **Start download**:



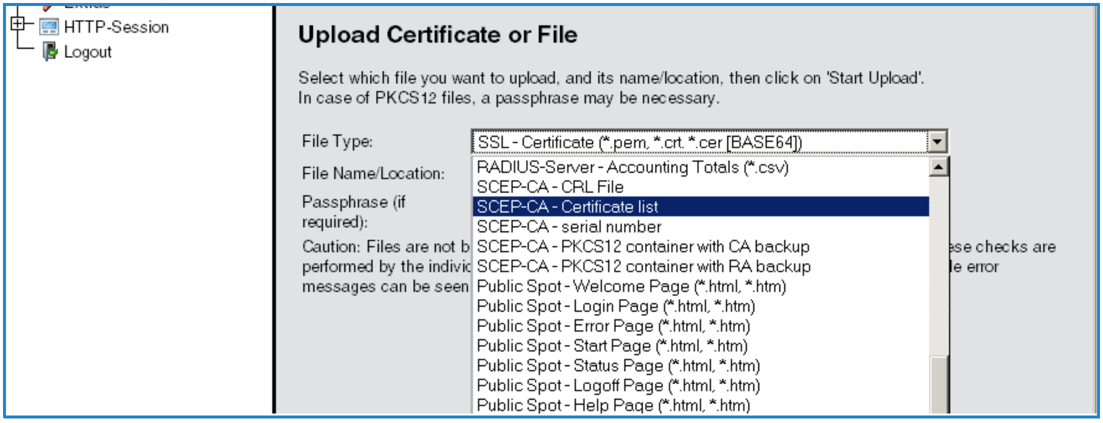
Download Certificate or File

Select which file you want to download, then click on 'Start Download'.

File Type: SCEP-CA - Certificate list

③ To upload these files to the device, go to the entry page of WEBconfig and select the command **Upload certificate or file**.

④ Select the entries listed above as data type one after the other, enter each file name and storage location and confirm with **Start upload**:


HTTP-Session
Logout
RADIUS-Server - Accounting Totals (*.csv)
SCEP-CA - CRL File
SCEP-CA - Certificate list
SCEP-CA - serial number
SCEP-CA - PKCS12 container with CA backup
SCEP-CA - PKCS12 container with RA backup
Public Spot - Welcome Page (*.html, *.htm)
Public Spot - Login Page (*.html, *.htm)
Public Spot - Error Page (*.html, *.htm)
Public Spot - Start Page (*.html, *.htm)
Public Spot - Status Page (*.html, *.htm)
Public Spot - Logoff Page (*.html, *.htm)
Public Spot - Help Page (*.html, *.htm)

Upload Certificate or File

Select which file you want to upload, and its name/location, then click on 'Start Upload'.
In case of PKCS12 files, a passphrase may be necessary.

File Type: SSL - Certificate (*.pem, *.crt, *.cer [BASE64])
File Name/Location:
Passphrase (if required):

Caution: Files are not b … se checks are performed by the indivic … le error messages can be seen

After uploading the new certificate list the expired certificates will be removed and a new CRL will be created. The CA will automatically reinitialize itself, if certificates and keys have been succsessfully extracted after uploading the certificate backup.

11.8.16 Load balancing between WLAN-Controllers

If multiple WLAN-Controllers are available in a network, the Access Points are automatically distributed evenly between the WLAN-Controllers.

At the beginning of communications, the Access Point sends a "Discovery Request Message" to find any available WLAN-Controllers.

- If the Access Point receives responses from primary and secondary WLAN-Controllers, then primary controllers are preferred.
- From the available WLAN-Controllers the Access Point selects the one with the lowest load, i.e. that with the lowest ratio of managed Access Points to the maximum possible Access Points.
- In case of two or more equally "good" WLAN-Controllers, the Access Point selects the nearest one in the network, i.e. that with the fastest response time.

In this way, e.g. by activating multiple WLAN-Controllers via automatic assignment of configurations ('Automatic provision of the default configuration' → page 11-60), all WLAN-Controllers can be "filled" with equal numbers of configurations from a portion of the Access Points.

11.8.17 Dynamic VLAN assignment

Larger WLAN infrastructures often require individual WLAN clients to be assigned to certain networks. Assuming that the WLAN clients are always within range of the same Access Points, then assignment can be realized via the SSID in connection with a particular IP network. If on the other hand the WLAN clients frequently change their position and logon to different Access Points then, depending on the configuration, they may find themselves in a different IP network.

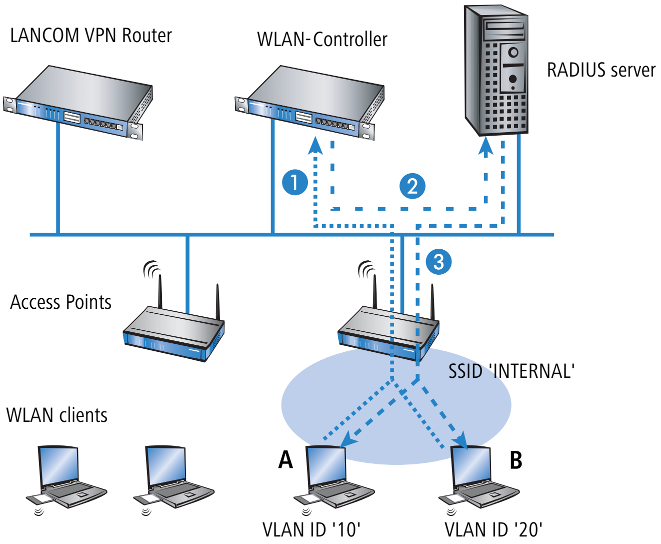
For WLAN clients to remain within a certain network **independent** of their current WLAN network, dynamically assigned VLANs can be used. Unlike the situation where VLAN IDs are statically configured for a certain SSID ('VLAN ID' → page 11-79), in this case a RADIUS server directly assigns the VLAN ID to the WLAN client.

Example:

- The WLAN clients of two employees log into an Access Point in the WPA-secured network with the SSID 'INTERNAL'. During registration, the RADIUS requests from the WLAN clients are directed to the Access Point. If the corresponding WLAN interface is in the operating mode 'managed' the RADIUS requests are automatically forwarded to the WLAN-Controller. This forwards the request in turn to the defined RADIUS server. The RADIUS server can check the access rights of the WLAN clients. It can also use the MAC address to assign a certain VLAN ID, for example for a certain department. The WLAN client in Marketing, for example, receives the VLAN ID '10' and WLAN client from Research & Development receives '20'. If no VLAN ID is specified for the user, the SSID's primary VLAN ID is used.
- The WLAN clients of the guests log into the same Access Point in the unsecured network with the SSID 'PUBLIC'. This SSID is statically bound to the VLAN ID '99' and leads the guests into a certain network. Static and dynamic VLAN assignment can be elegantly operated in parallel.

Assignment of the VLAN ID by the RADIUS server can be controlled by other criteria, such as a combination of user name and password, for example. In this way the unknown MAC address of a visitor to a company can be assigned a VLAN ID that permits guest access for Internet access only, for example, but that prohibits access to other network resources.

As an alternative to an external RADIUS server, WLAN clients can be assigned with a VLAN ID via the internal RADIUS server or the stations table in the LANCOM WLAN Controller ('Station table (ACL table)' → page 11-64).



① Activate VLAN tagging for the WLAN-Controller. This is done in the physical parameters of the profile by entering a value greater than '0' (’Management VLAN ID’ → page 11-62) for the management VLAN ID.

② For authentication via 802.1x, go to the encryption settings for the profile's logical WLAN network and choose a setting that triggers an authentication request.

③ To check the MAC addresses, activate the MAC check for the profile's logical WLAN network.

For the management of WLAN modules with a WLAN-Controller, a RADIUS server is required to operate authentication via 802.1x and MAC-address checks. The WLAN-Controller automatically defines itself as the RADIUS server in the Access Points that it is managing—all RADIUS requests sent to the Access Point are then directly forwarded to the WLAN-Controller, which can either process the requests itself or forward them to an external RADIUS server.

④ To forward RADIUS requests to another RADIUS server, use LANconfig to enter its address into the list of forwarding servers in the configuration area 'RADIUS servers' on the 'Forwarding' tab. Alternatively, external RADIUS servers can be entered in WEBconfig under **LCOS menu tree** ▶ **Setup** ▶ **RADIUS** ▶ **Server** ▶ **Forward server**. Also, set the standard realm and the empty realm to be able to react to different types of user information (with an unknown realm, or even without a realm).

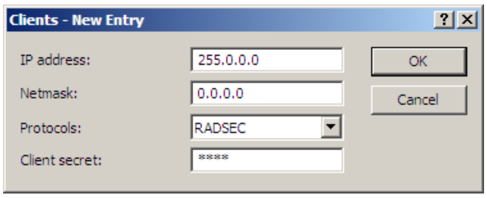
⑤ Configure the entries in the RADIUS server so that WLAN clients placing requests will be assigned the appropriate VLAN IDs as based on the identification of certain characteristics.

Further information about RADIUS is available in the documentation for your RADIUS server.

11.8.18 Checking WLAN clients with RADIUS (MAC filter)

To use RADIUS to authenticate WLAN clients and grant them WLAN access based on their MAC address, an external RADIUS server can be used, as can the internal user table in the LANCOM WLAN Controller.

In LANconfig enter the approved MAC addresses into the RADIUS database in the configuration area 'RADIUS servers' on the 'General' tab. Enter the MAC address as 'Name' and as 'Password' and select the authentication method 'All'.



Clients - New Entry

IP address: 255.0.0.0

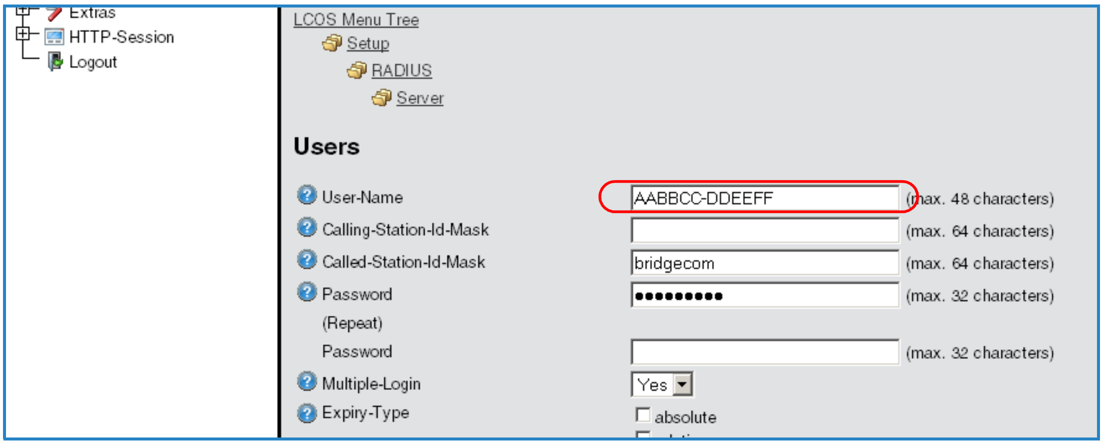
Netmask: 0.0.0.0

Protocols: RADSEC

Client secret: ****

Alternatively, approved MAC addresses can be entered in WEBconfig under **LCOS menu tree** ▶ **Setup** ▶ **RADIUS** ▶ **Server** ▶ **Users**.

The MAC address is entered as 'User name' **and** as 'Password' in the written form 'AABBCC-DDEEFF'.



Users

User-Name: AABBCC-DDEEFF (max. 48 characters)
Calling-Station-Id-Mask: (max. 64 characters)
Called-Station-Id-Mask: bridgecom (max. 64 characters)
Password: ●●●●●●●●● (max. 32 characters)
(Repeat) Password: (max. 32 characters)
Multiple-Login: Yes
Expiry-Type: □ absolute

11.8.19 Deactivating Access Points or permanently removing them from the WLAN infrastructure

Occasionally it is necessary to temporarily deactivate or even permanently remove a WLAN-Controller-managed Access Point.

Access Point deactivation

To deactivate an Access Point, set its corresponding entry in the AP table to 'inactive' or delete the entry from the table. In the Access Point, the WLAN modules in managed mode are switched off and the corresponding SSIDs are deleted.

The WLAN modules and the WLAN networks (SSIDs) are still switched off even if self-sufficient operation ('Self-sufficient operation' → page 11-61) is activated.

An Access Point deactivated in this way remains connected to the WLAN-Controller and the certificates are retained. The WLAN-Controller can reactivate the Access Point and its managed-mode WLAN modules at any time simply by activating the entry in the AP table or by making a new entry in the AP table along with the appropriate MAC address.

If the connection to a deactivated Access Point is broken (either unintentionally due to a failure or intentionally by the administrator) then the Access Point begins a new search for a suitable WLAN-Controller. Although the former WLAN-Controller can check the validity of the certificate, due to the fact that there is no (active) entry in the AP table, it is treated as a secondary WLAN-Controller by the Access Point. If the Access Point finds a primary WLAN-Controller then it will register with it.

Permanently removing Access Points from the WLAN infrastructure

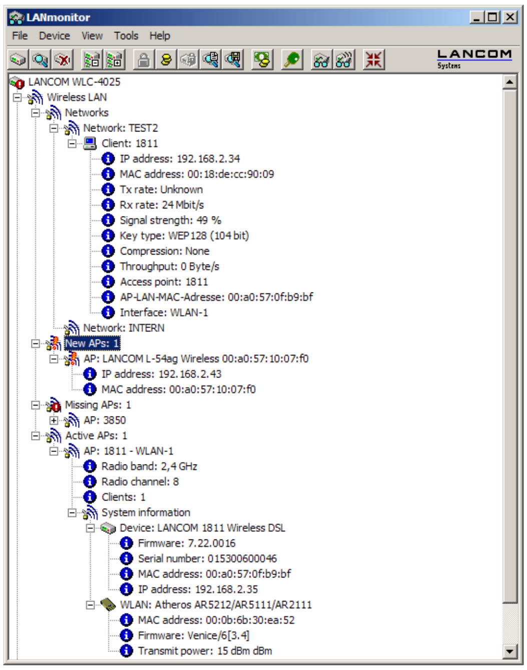
In order to permanently remove an Access Point from a centrally managed WLAN infrastructure, the certificates in the SCEP client have to be either deleted or revoked.

- If you have access to the Access Point, the certificates are quickly deleted by resetting the device.
- If the device has been stolen and consequently needs to be removed from the WLAN infrastructure, then the certificates in the WLAN-Controller's CA have to be revoked. This is done in WEBconfig by changing to **Status ▶ Certificates ▶ SCEP-CA ▶ Certificates** and accessing the **Certificate status table**. Here you delete the certificate for the MAC address of the Access Points which are to be removed from the WLAN infrastructure. The certificates are not actually deleted, but they are marked as expired.

In case of a backup solution featuring redundant WLAN-Controllers, the certificates have to be revoked in all of the WLAN-Controllers!

11.8.20 Displays and commands in LANmonitor

LANmonitor gives you a rapid overview of the LANCOM WLAN Controllers in your network and the Access Points within the WLAN infrastructure. LANmonitor displays the following information, among others:



```
LANCOM WLC-4025
⊟ Wireless LAN
    ⊟ Networks
        ⊟ Network: TEST2
            ⊟ Client: 1811
                IP address: 192.168.2.34
                MAC address: 00:18:de:cc:90:09
                Tx rate: Unknown
                Rx rate: 24 Mbit/s
                Signal strength: 49 %
                Key type: WEP128 (104 bit)
                Compression: None
                Throughput: 0 Byte/s
                Access point: 1811
                AP-LAN-MAC-Adresse: 00:a0:57:0f:b9:bf
                Interface: WLAN-1
          Network: INTERN
    ⊟ New APs: 1
        ⊟ AP: LANCOM L-54ag Wireless 00:a0:57:10:07:f0
            IP address: 192.168.2.43
            MAC address: 00:a0:57:10:07:f0
    ⊟ Missing APs: 1
        ⊞ AP: 3850
    ⊟ Active APs: 1
        ⊟ AP: 1811 - WLAN-1
            Radio band: 2,4 GHz
            Radio channel: 8
            Clients: 1
            ⊟ System information
                ⊟ Device: LANCOM 1811 Wireless DSL
                    Firmware: 7.22.0016
                    Serial number: 015300600046
                    MAC address: 00:a0:57:0f:b9:bf
                    IP address: 192.168.2.35
                ⊟ WLAN: Atheros AR5212/AR5111/AR2111
                    MAC address: 00:0b:6b:30:ea:52
                    Firmware: Venice/6[3.4]
                    Transmit power: 15 dBm dBm
```

- Active WLAN networks with the logged-on WLAN clients and the descriptor of the Access Points that the WLAN clients are associated with.
- Display of new Access Points with IP and MAC address
- Display of missing Access Points with IP and MAC address
- Display of managed Access Points with IP and MAC address, the utilized frequency band and channel

Using the right-hand mouse key, a context menu can be opened for the Access Points and the following commands are available:

- **Assign new Access Point to profile**

  Enables a new Access Point to be allocated to a profile and accepted into the WLAN infrastructure ('Accepting Access Points via LANmonitor' → page 11-65).

- **Disconnect Access Point**

  Breaks the connection between Access Point and WLAN-Controller. The Access Point then carries out a new search for a suitable WLAN-Controller. This command can be used after a backup event to disconnect Access Points from a backup controller and to redirect them to the correct WLAN-Controller.

- **Update**

  Updates LANmonitor's display.

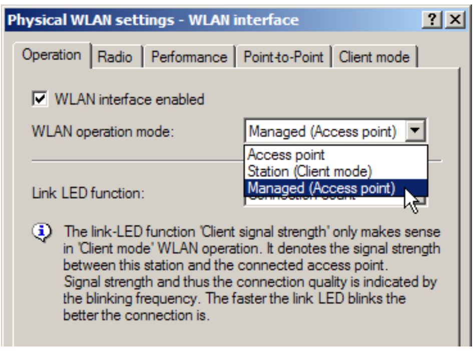
11.8.21 Configuring the Access Points

As of firmware version LCOS 7.20 there is a difference between LANCOM Access Points (e. g. the LANCOM L-54ag) and LANCOM Wireless Routers (e. g. the LANCOM 1811 Wireless) with regard to the ex-factory standard settings in the WLAN modules.

- When shipped, the WLAN modules in LANCOM Access Points are set to the 'Managed' operating mode. In this mode, LANCOM Access Points search for a central WLAN-Controller that can provide them with a configuration, and they remain in "search mode" until they discover a suitable WLAN-Controller or until the operating mode of the WLAN module is changed manually.
- When shipped, the WLAN modules in LANCOM Wireless Routers are set to the 'Access point' operating mode. In this mode, LANCOM Wireless Routers function as self-sufficient Access Points and use a configuration that is stored locally in the device. For integration into a WLAN infrastructure that is centrally managed by WLAN-Controllers, the operating mode of the WLAN modules in LANCOM Wireless Routers has to be switched into the 'Managed' mode.

The operating mode can be set separately for every WLAN module. For models with two WLAN modules, one module can work with a local configuration and the second module can be centrally managed with a WLAN-Controller.

For individual devices, the operating mode of the WLAN modules can be found in LANconfig under **Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Operation mode**:



☑ WLAN interface enabled

WLAN operation mode: Managed (Access point)

Link LED function:

The link-LED function 'Client signal strength' only makes sense in 'Client mode' WLAN operation. It denotes the signal strength between this station and the connected access point. Signal strength and thus the connection quality is indicated by the blinking frequency. The faster the link LED blinks the better the connection is.

If you need to change the operating mode for multiple devices, you can use a simple script on the devices with the following lines:

- `# Script (7.22 / 23.08.2007)`
- `lang English`
- `flash 0`
- `cd Setup/Interfaces/WLAN/Operational`
- `set WLAN-1 0 managed-AP 0`
- `# done`
- `exit`

11.8.22 Automatic RF optimization with LANCOM WLAN Controllers

Selecting the channel from the channel list defines a portion of the frequency band that an Access Point uses for its logical wireless LANs. All WLAN clients that need to connect to an Access Point have to use the same channel on the same frequency band. In the 2.4-GHz band channels 1 to 13 are available (depending on the country), and in the 5-GHz band channels 36 to 64 are available. On each of these channels, only one Access Point can actually transfer data. In order to operate another Access Point within radio range with maximum bandwidth, the Access Point must make use of a separate channel—otherwise all of the participating WLANs have to share the channel's bandwidth.

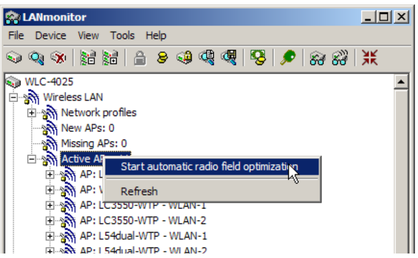
With a completely empty channel list, the access points could automatically select channels which overlap in some areas, so reducing signal quality. Similarly, the access points might select channels which the WLAN clients cannot use due to the country settings. To direct access points towards certain channels, the non-overlapping channels 1, 6, 11 can be activated in the channels list.

In larger installations with several Access Points it can be difficult to set a channel for every Access Point. With automatic radio-field (RF) optimization, the LANCOM WLAN Controllers provide an automatic method of setting the optimum channels for Access Points that work in the 2.4-GHz band.

WEBconfig: **Setup** ▶ **WLAN-management** ▶ **Start-automatic-radio-field-optimization**

Optimization can be initiated for a single Access Point by entering the MAC address as an argument for the action.

LANmonitor: Right-click on the list of active Access Points or on a specific device, and in the context menu select **Start automatic RF optimization**.



Optimization is then carried out in the following stages:

① The WLAN-Controller deletes the AP channel list in all of the Access Points in the 2.4-GHz range. Because the channel list for the Access Points is then empty, the channel list from their profile is assigned to them by means of a configuration update.

② The WLAN-Controller switches off all radio modules operating at 2.4 GHz.

③ The Access Points are switched on again one after the other. They are processed in the same order that they were registered with the WLAN-Controller.

④ Automatic calibration: After being switched on, the access point itself selects the most suitable channel from the list. To determine which channel is the best, the access point scans for interference to determine the signal strengths and channels occupied by other access points. Because the former list in the WLAN-Controller configuration was deleted, this is now the profile channel list. If the profile channel list is empty, then the Access Point has freedom of choice from the channels that are not occupied by other radio modules.

⑤ The selected channel is then communicated back to the WLAN-Controller and entered into the AP channel list there. For this reason, the Access Point receives the same channel the next time a connection is established. The AP channel list thus has a higher weighting than the profile channel list.

If an Access Point is equipped with multiple WLAN modules, this process is carried out separately for each WLAN module, one after the other.

11.9 Central firmware and script management

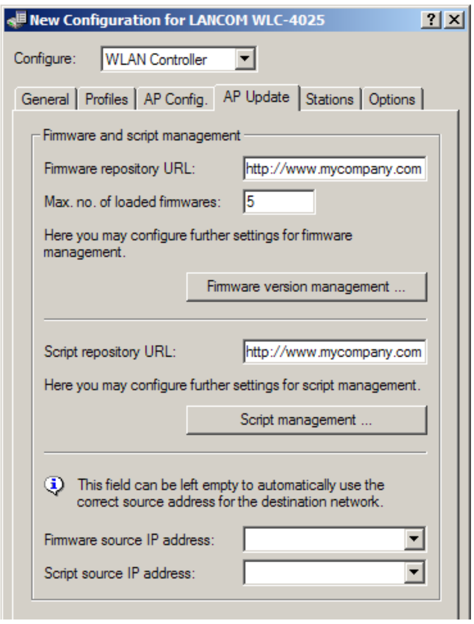
LANCOM WLAN Controllers allow the configurations of multiple LANCOM Wireless Routers and LANCOM Access Points to be managed from a central location in a consistent and convenient manner. With central firmware and script management, uploads of firmware and scripts can be automated for all of the WLAN devices.

To achieve this, the firmware and script files are stored on a Web server (firmware as *.upx files, scripts and *.lcs files). The WLAN-Controller checks once daily, or on user request, to compare the available files with those on the devices. Alternatively, this procedure can be handled by a cron job—overnight, for example. If an update can be carried out, or if the Access Point is not running the desired firmware version, then the WLAN-Controller downloads the file from the Web server and uploads it to the appropriate Wireless Routers and Access Points.

The configuration of firmware and script management provides precise control over the distribution of the files. It is possible, for example, to limit certain firmware versions to certain device types or MAC addresses.

An update can be carried out in two possible states:

- When a connection is established; the Access Point subsequently restarts automatically.
- If the Access Point is already connected, the device does **not** restart automatically. In this case the Access Point is manually restarted with the menu action "/Setup/WLAN-Management/Central-Firmware-Management/Reboot-updated-APs" or by a timed cron job.
- The action "/Setup/WLAN-Management/Central-Firmware-Management/Update-Firmware-and-Script-Information" updates the script and firmware directories.


New Configuration for LANCOM WLC-4025

Configure: WLAN Controller

Firmware and script management

Firmware repository URL: http://www.mycompany.com

Max. no. of loaded firmwares: 5

Here you may configure further settings for firmware management.

Script repository URL: http://www.mycompany.com

Here you may configure further settings for script management.

This field can be left empty to automatically use the correct source address for the destination network.

Firmware source IP address:

Script source IP address:

The parameters for configuration can be found under the following paths:

LANconfig: **WAN Controller ▶ AP Update**

WEBconfig: **Setup ▶ WLAN Management ▶ Central Firmware Management**

General settings for firmware management

- **Firmware URL**

  The path to the directory with the firmware files.

  - □ Possible values: URL in the form `Server/Directory` or `http://Server/Directory`
  - □ Default: Blank

- **Simultaneously loaded FW**

  The number of firmware versions loaded simultaneously into the main memory of the WLAN-Controller.

  ⓘ The firmware versions stored here are downloaded from the server just once and then used for all update processes.

  - □ Possible values: 1 to 10
  - □ Default: 5

- **Firmware sender IP address**

  This is where you can configure an optional sender address for use instead of the one automatically selected for the destination address.

  Possible values:

  - □ Name of a defined IP network.
  - □ 'INT' for the IP address in the first network with the setting 'Intranet'.
  - □ 'DMZ' for the IP address in the first network with the setting 'DMZ'.
  - □ Name of a loopback address.
  - □ Any other IP address.

  Default:

  - □ Blank

ⓘ If the list of IP networks or loopback addresses contains an entry named 'INT' or 'DMZ', the associated IP address of the IP network or the loopback address named 'INT' or 'DMZ' is used.

Firmware management table

Table with device type, MAC address and firmware version for the precise control of the firmware files in use.

- **Device types**

  Select here the type of device that the firmware version specified here is to be used for.

  - □ Possible values: All, or a selection from the list of available devices.
  - □ Default: All

- **MAC address**

  Select here the device (identified by its MAC address) that the firmware version specified here is to be used for.

  - □ Possible values: Valid MAC address
  - □ Default: Blank

- **Version**

  Firmware version that is to be used for the devices or device types specified here.

  - □ Possible values: Firmware version in the form `X.XX`
  - □ Default: Blank

General settings for script management

- **Script URL**

  The path to the directory with the script files.

  - □ Possible values: URL in the form `Server/Directory` or `http://Server/Directory`
  - □ Default: Blank

- **Script sender IP address**

  This is where you can configure an optional sender address for use instead of the one automatically selected for the destination address.

  Possible values:

  - □ Name of a defined IP network.

- □ 'INT' for the IP address in the first network with the setting 'Intranet'.
- □ 'DMZ' for the IP address in the first network with the setting 'DMZ'.
- □ Name of a loopback address.
- □ Any other IP address.

Default:

- □ Blank

If the list of IP networks or loopback addresses contains an entry named 'INT' or 'DMZ', the associated IP address of the IP network or the loopback address named 'INT' or 'DMZ' is used.

Script management table

Table with the name of the script file and a WLAN profile for allocating the script to a WLAN profile.

Configuring a Wireless Router and Access Point in the "Managed" mode is handled via WLAN profiles. A script can be used for setting those detailed parameters in managed devices that are not handled by the pre-defined parameters in a WLAN profile. Distribution is also handled by WLAN profiles to ensure that the Wireless Routers and Access Points with the same WLC configuration also use the same script.

As only one script file can be defined per WLAN profile, versioning is not possible here. However, when distributing a script to a Wireless Router or Access Point, an MD5 checksum of the script file is saved. This checksum allows the WLAN-Controller to determine whether the script file has to be transmitted again in case a new or altered script has the same file name.

- **Script file name**

  Name of the script file to be used.

  - □ Possible values: File name in the form *.lcs
  - □ Default: Blank

- **WLAN profile**

  Select here the WLAN profile that the script file specified here should be used for.

  - □ Possible values: Selection from the list of defined WLAN profiles.
  - □ Default: Blank

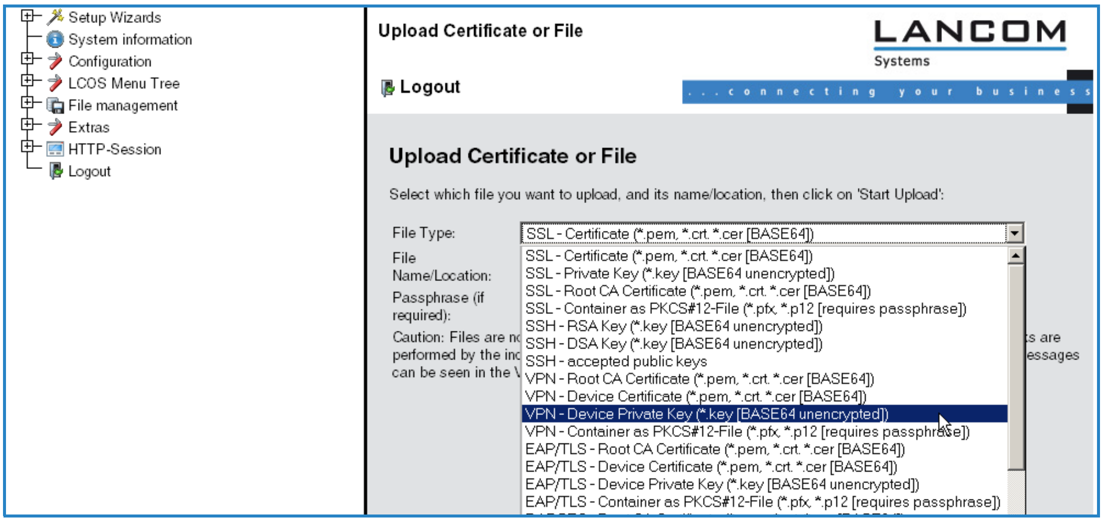
Internal script storage (script management without an HTTP server)

In contrast to firmware files, scripts involve only small volumes of data. The WLAN-Controller's internal script storage allows three scripts of up to 64KB each to be stored. If script requirements do not exceed this volume, an HTTP server does not need to be configured for this purpose.

Script files are simply loaded from the designated storage location using WEBconfig. After upload the list of available scripts must be updated with Configure/Wireless LAN/Central Firmware /Update Firmware and Script Information.

The internal scripts can be referenced from the script management table using the relevant names (WLC_Script_1.lcs, WLC_Script_2.lcs or WLC_Script_3.lcs).

Please be careful with upper and lower case letters when entering script names.


Setup Wizards
System information
Configuration
LCOS Menu Tree
File management
Extras
HTTP-Session
Logout
Upload Certificate or File
LANCOM
Systems
Logout
. . . c o n n e c t i n g   y o u r   b u s i n e s s
SSL - Certificate (*.pem, *.crt. *.cer [BASE64])
SSL - Private Key (*.key [BASE64 unencrypted])
SSL - Root CA Certificate (*.pem, *.crt. *.cer [BASE64])
SSL - Container as PKCS#12-File (*.pfx, *.p12 [requires passphrase])
SSH - RSA Key (*.key [BASE64 unencrypted])
SSH - DSA Key (*.key [BASE64 unencrypted])
SSH - accepted public keys
VPN - Root CA Certificate (*.pem, *.crt. *.cer [BASE64])
VPN - Device Certificate (*.pem, *.crt. *.cer [BASE64])
VPN - Device Private Key (*.key [BASE64 unencrypted])
VPN - Container as PKCS#12-File (*.pfx, *.p12 [requires passphrase])
EAP/TLS - Root CA Certificate (*.pem, *.crt. *.cer [BASE64])
EAP/TLS - Device Certificate (*.pem, *.crt. *.cer [BASE64])
EAP/TLS - Device Private Key (*.key [BASE64 unencrypted])
EAP/TLS - Container as PKCS#12-File (*.pfx, *.p12 [requires passphrase])

Upload Certificate or File

Select which file you want to upload, and its name/location, then click on 'Start Upload':

File Type: SSL - Certificate (*.pem, *.crt. *.cer [BASE64])

File Name/Location:

Passphrase (if required):

Caution: Files are nc ts are
performed by the inc essages
can be seen in the V

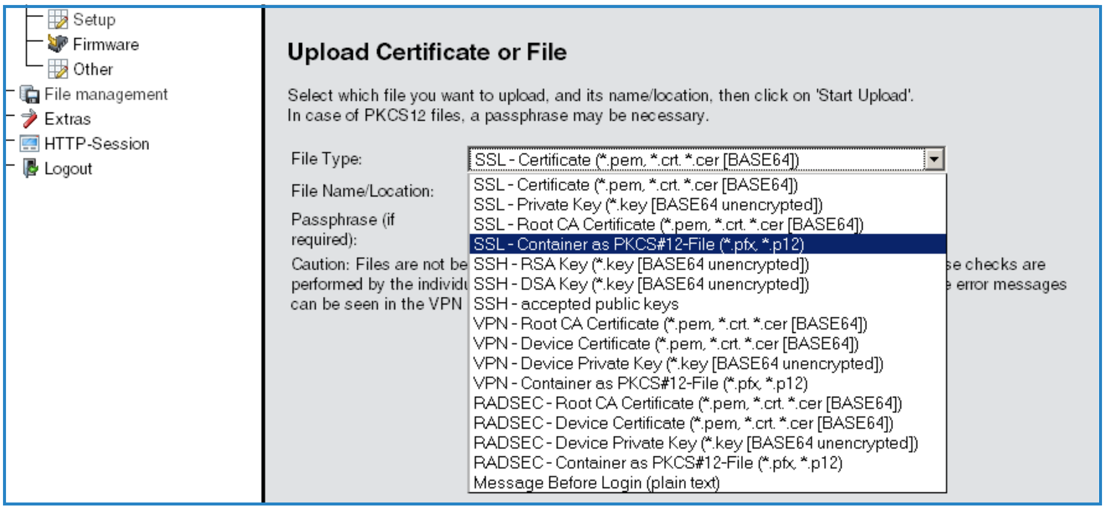
11.10 Multi-level certificates for PublicSpots

New with LCOS 7.6:

- Multi-level certificates for PublicSpots

SSL certificate chains can be loaded into the LANCOM as a PKCS#12 container. These certificate chains can be used for PublicSpot authentication pages by using the HTTPS server implemented in LCOS. Certificates from recognized trust centers are normally multi-level. Officially signed certificates in the PublicSpot are necessary to avoid certificate-related error messages from the browser when authenticating at a PublicSpot.

The certificate is loaded into the device for example by using File Management in WEBconfig to upload the individual files of the root CA certificate or a PKCS#12 container:


Setup
Firmware
Other
File management
Extras
HTTP-Session
Logout

Upload Certificate or File

Select which file you want to upload, and its name/location, then click on 'Start Upload'.
In case of PKCS12 files, a passphrase may be necessary.

File Type: SSL - Certificate (*.pem, *.crt, *.cer [BASE64])

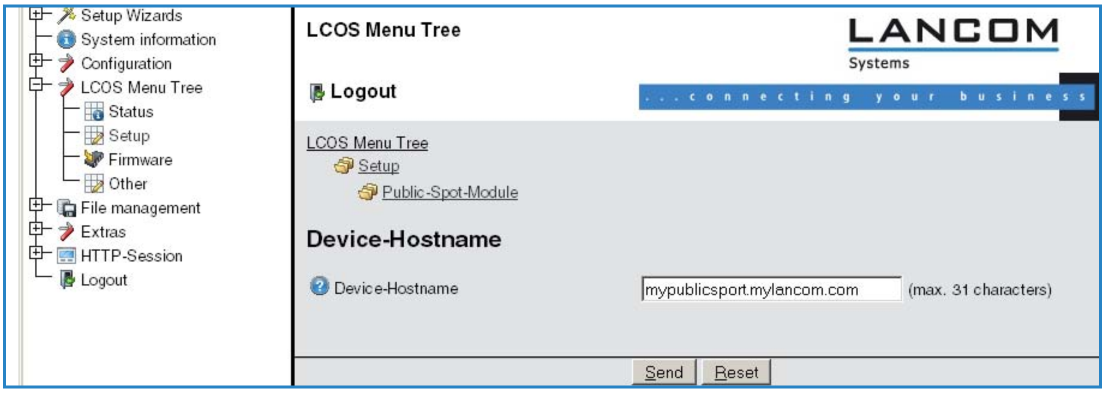
File Name/Location:

Passphrase (if required):

Caution: Files are not be … e checks are performed by the individu … e error messages can be seen in the VPN

SSL - Certificate (*.pem, *.crt, *.cer [BASE64])
SSL - Private Key (*.key [BASE64 unencrypted])
SSL - Root CA Certificate (*.pem, *.crt, *.cer [BASE64])
SSL - Container as PKCS#12-File (*.pfx, *.p12)
SSH - RSA Key (*.key [BASE64 unencrypted])
SSH - DSA Key (*.key [BASE64 unencrypted])
SSH - accepted public keys
VPN - Root CA Certificate (*.pem, *.crt, *.cer [BASE64])
VPN - Device Certificate (*.pem, *.crt, *.cer [BASE64])
VPN - Device Private Key (*.key [BASE64 unencrypted])
VPN - Container as PKCS#12-File (*.pfx, *.p12)
RADSEC - Root CA Certificate (*.pem, *.crt, *.cer [BASE64])
RADSEC - Device Certificate (*.pem, *.crt, *.cer [BASE64])
RADSEC - Device Private Key (*.key [BASE64 unencrypted])
RADSEC - Container as PKCS#12-File (*.pfx, *.p12)
Message Before Login (plain text)

Certificates are normally issues for DNS names, so the PublicSpot must specify the certificate's DNS name as the destination and not an internal IP address (LCOS Menu Tree/Setup/Public-Spot-Module/Device-Hostname). This name has to be resolved by the DNS server to provide the corresponding IP address of the PublicSpot.



LCOS Menu Tree

Logout

LCOS Menu Tree
Setup
Public-Spot-Module

Device-Hostname

Device-Hostname: mypublicsport.mylancom.com (max. 31 characters)

11.11 DFS 2: Non-use of channels for weather radar

With the DFS method (Dynamic Frequency Selection) as required for 5 GHz WLANs, an unused frequency is automatically selected, for example, to avoid interference from radar systems or to distribute WLAN devices as evenly as possible over the entire frequency band. Occasionally, however, signals from weather radar stations cannot be identified reliably.

For this reason the European Commission is extending the demands of standards ETSI EN 301 893 V1.3.1 and ETSI EN 310 893 V1.4.1 to additionally avoid the use of three channels (120, 124 and 128) in subband 2 of the 5 GHz band. These are not to be used for automatic channel selection. Methods for detecting weather radar signatures are currently under development.

11.12 Bandwidth limits in the WLAN

The bandwidths that are available can be limited so that they can be better distributed among several participants in the WLAN. This bandwidth limit is available for wireless ISPs, for example, who want to provide their customers with a defined bandwidth.

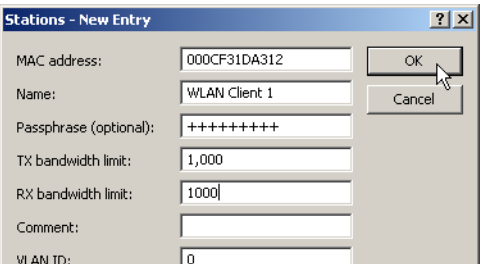
Unlike bandwidth management using QoS (Quality of Service), this procedure does not allow a minimum bandwidth, but an exactly defined maximum bandwidth instead. Even if more bandwidth were actually available due to low traffic from other network stations, only the bandwidth specified here is provided to the user.

The settings differentiate between operating a device as an access point or in client mode.

11.12.1 Operating as an access point

In the access point operating mode, the maximum permitted bandwidths can be specified in Tx and Rx direction for the WLAN clients that register with the access point. The values of the maximum Tx and Rx bandwidths are entered in kbps in the MAC access list. A value of '0' indicates that there is no intention to restrict the bandwidth in this transmission direction. The bandwidth that is actually provided is determined from the value that is entered here and the value that is transmitted by the client.

The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an access point, Rx stands for "Send data" and Tx stands for "Receive data".



MAC address: 000CF31DA312
Name: WLAN Client 1
Passphrase (optional): +++++++++
TX bandwidth limit: 1,000
RX bandwidth limit: 1000
Comment:
VLAN ID: 0

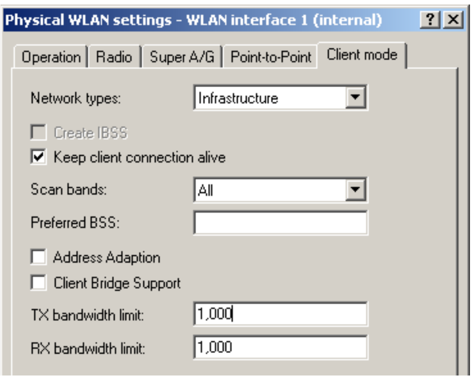
LANconfig: Wireless LAN ▶ Stations

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN ▶ Access list

11.12.2 Operating as a Client

If the device is operated as a WLAN client, the device can transmit its maximum bandwidth when it registers with the access point. The access point then provides the actual maximum bandwidths with proprietary limits for this client where necessary.

The significance of the Rx and Tx values depends on the device's operating mode. In this case, as a client, Tx stands for "Send data" and Rx stands for "Receive data".



Network types: Infrastructure
□ Create IBSS
☑ Keep client connection alive
Scan bands: All
Preferred BSS:
□ Address Adaption
□ Client Bridge Support
TX bandwidth limit: 1,000
RX bandwidth limit: 1,000

LANconfig: Interfaces ▶ Wireless LAN ▶ Physical WLAN Settings ▶ Client Mode

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN▶ Client modes

- **Comment**

  Comment on this entry.

- **VLAN ID**

  VLAN-ID for the WLAN client.

  - Possible values: 0 to 4094
  - Special values: 0: Switches the use of VLAN off.

12 Virtual LANs (VLANs)

12.1 What is a Virtual LAN?

The increasing availability of inexpensive layer 2 switches enables the setup of LANs much larger than in the past. Until now, smaller parts of a network had been combined with hubs. These individual segments (collision domains) had been united via routers to larger sections. Since a router represents always a border between two LANs, several LANs with own IP address ranges arose by this structure.

By using switches, it is possible to combine much more stations to one large LAN. By the specific control of data on the individual ports, the available bandwidth can be utilized much better than by using hubs, and the configuration and maintenance of routers within the network can omitted.

But also a network structure based on switches has disadvantages:

- Broadcasts are sent like hubs over the entire LAN, even if the respective data packets are only important for a certain segment of the LAN. A sufficient number of network stations can thus lead to a clear reduction of the available bandwidth in the LAN.
- The entire data traffic on the physical LAN is "public". Even if single segments are using different IP address ranges, each station of the LAN is theoretically able to tap data traffic from all logical networks on the Ethernet segment. The protection of individual LAN segments with Firewalls or routers increases again the requirements to network administration.

One possibility to resolve these problems are virtual LANs (VLANs), as described in IEEE 802.1p/q. By this concept, several virtual LANs are defined on a physical LAN, which do not obstruct each other, and which also do not receive or tap data traffic of the respective other VLANs on the physical Ethernet segment.

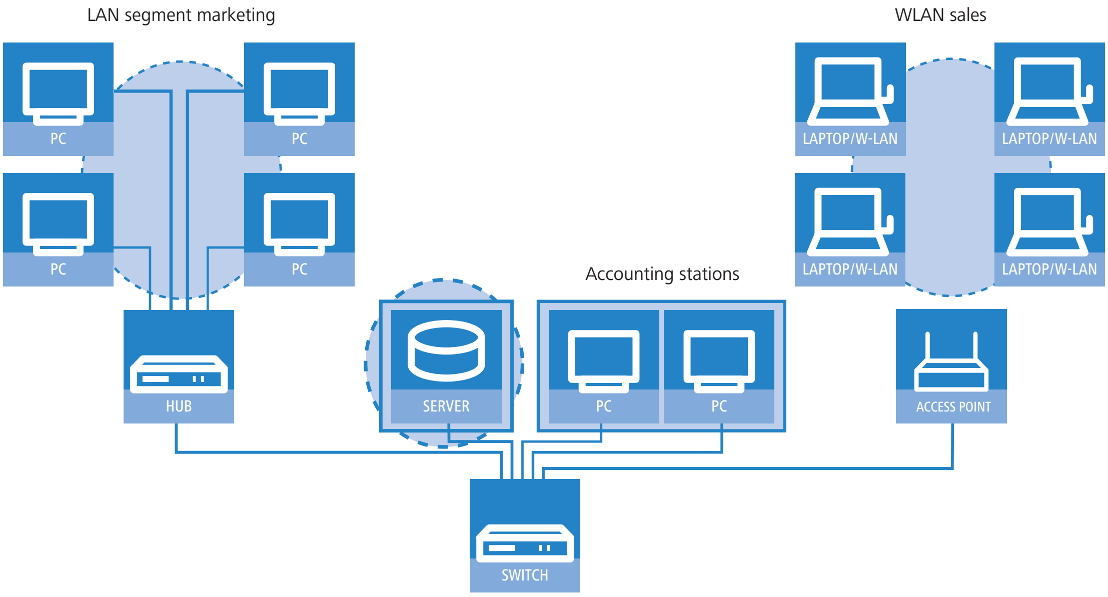
12.2 This is how a VLAN works

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.



12.2.1 Frame tagging

In order to shield or, if necessary, to priorities data traffic of a virtual LAN against the other network users, data packets must have an additional feature (a "tag"). That's why the respective process is also called "frame tagging".

Frame tagging must be realized such that the following requirements are fulfilled:

- Data packets with and without frame tagging must be able to exist in parallel on a physical LAN.
- Stations and switches in a LAN, which do not support VLAN technology, must ignore the data packets with frame tagging and/or treat them as "normal" data packets.

The tagging is realized by an additional field within the MAC frame. This field contains two important information for the virtual LAN:

- **VLAN ID**: A unique number describes the virtual LAN. This ID defines the belonging of data packets a logical (virtual) LAN. With this 12 bit value it is possible to define up to 4094 different VLANs (VLAN IDs "0" and "4095" are reserved resp. inadmissible).

VLAN ID "1" is used by many devices as the Default VLAN ID. Concerning unconfigured devices, all ports belong to this Default VLAN. However, this assignment can also be changed by configuration. ('The port table' → page 12-6).

- **Priority**: The priority of a VLAN-tagged data packet is indicated by a 3 bit value. "0" represents the lowest priority, "7" the highest one. Data packets without VLAN tag are treated with priority "0".

This additional field makes the MAC frames longer than actually allowed. These "overlong" packets can only be recognized and evaluated by VLAN-capable stations and switches. Frame tagging incidentally leads to the desired behavior for network users without VLAN support:

- Switches without VLAN support simply pass on these data packets and ignore the additional fields within the MAC frame.
- Stations without VLAN support are not able to recognize the protocol type due to the inserted VLAN tag and discard the packets silently.

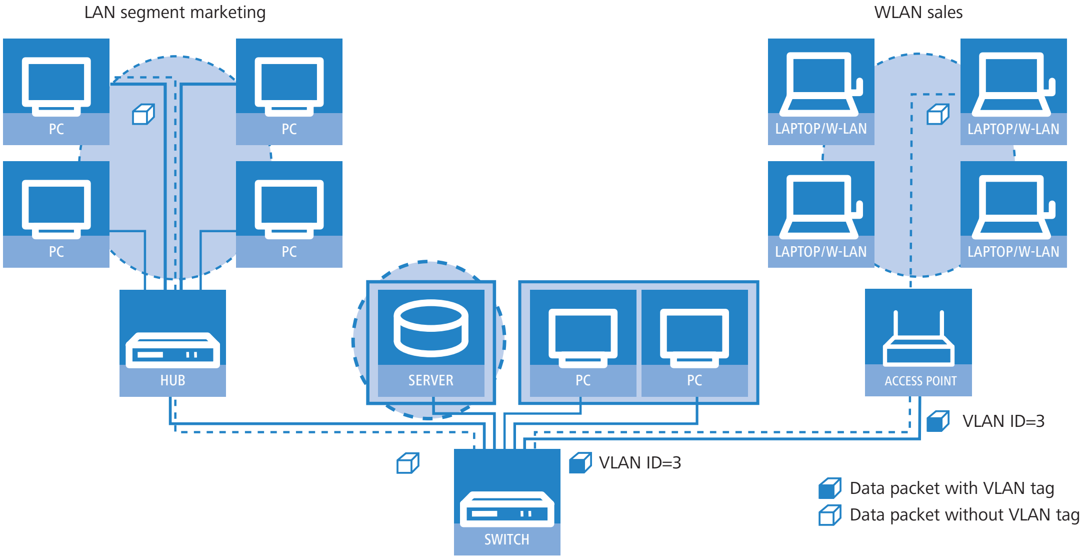
Older switches in the LAN are perhaps not able to pass on correctly the overlong frames between the individual ports and will reject the tagged packets.

12.2.2 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.

12.2.3 VLAN Q-in-Q tagging

VLANs compliant with IEEE302.1q are generally used to connect multiple networks that share a common physical medium but which are to be kept separate from one another. In some cases VLANs are operated on public networks that are operated by providers in order to keep the various company networks separate. Consequently VLAN tags may be used both in the LAN and over the WAN path—VLAN tagged LAN packets therefore require an additional VLAN tag for transmission over WAN. For control over VLAN tagging, the actions performed by each port can be defined separately.

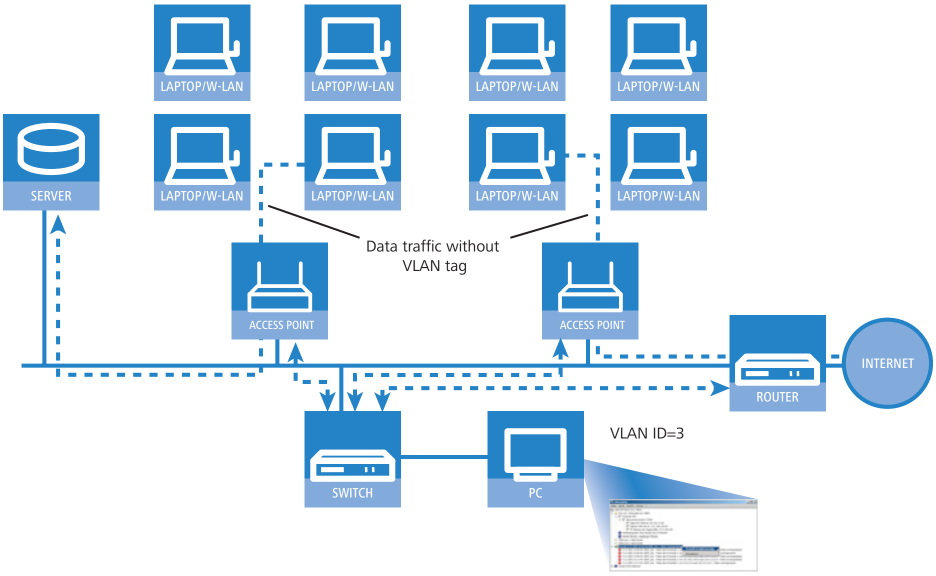
12.2.4 Application examples

Main application of virtual LANs is to install different logical networks on a physical Ethernet segment, whose data traffic is protected against the other logical networks.

The following sections present examples for the operation of virtual LANs on behalf of this background.

Management and user traffic on a LAN

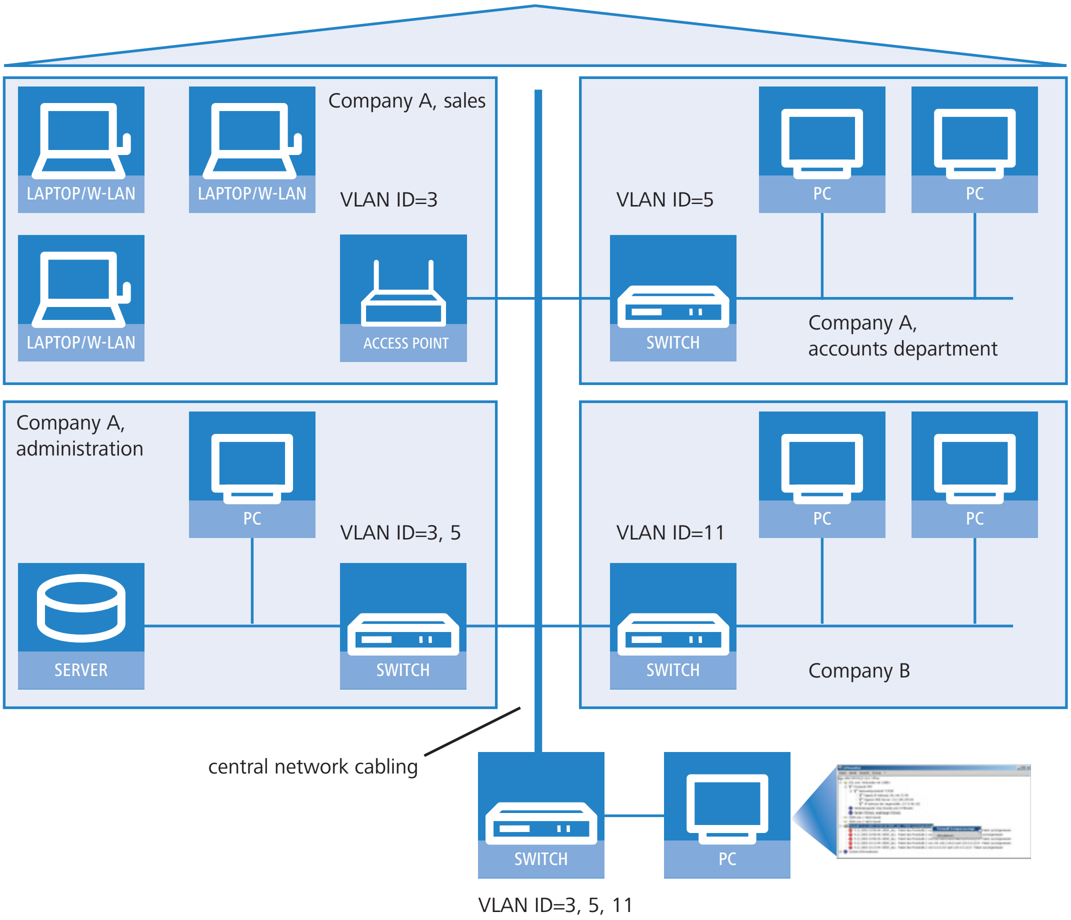
Several hot spots are installed on an university campus, so that students equipped with notebooks and WLAN cards have access to the Internet and to the server of the library. The hot spots are connected to the university LAN. Via this LAN the administrators also access the base stations to carry out several management tasks via SNMP.



By setting up a virtual LAN between the base stations and the administrator's switch, management data is shielded against all "public" traffic on the LAN.

Different organizations on one LAN

The flexibility of the modern world of work raises new challenges for administrators concerning planning and maintenance of network structures. The occupation of the rooms by leaseholders changes permanently in public office buildings, and also inside of a company, teams are often newly assembled. In both cases, the individual units must have an independent, protected LAN. But this task is very burdensome to realize by hardware changes, or even not at all, because e.g. only one single central cabling exists in the office building.



Virtual LANs enable to perform this task in a very smart way. Also when departments or companies change at a later time inside of the building, the network structure can be easily adjusted.

All network users in this example use the central Ethernet, which is, like the connected devices, supervised by a service provider. Company A has three departments on two floors. The sales department can communicate with the administration department via VLAN ID 3, the accounts department with the administration via VLAN ID 5. The networks of accounts department and sales do not see each other. Company B is also shielded by VLAN ID 11 against all other networks, only the service provider can access all devices for maintenance purposes.

12.3 Configuration of VLANs

The configuration of LANCOM Router 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.

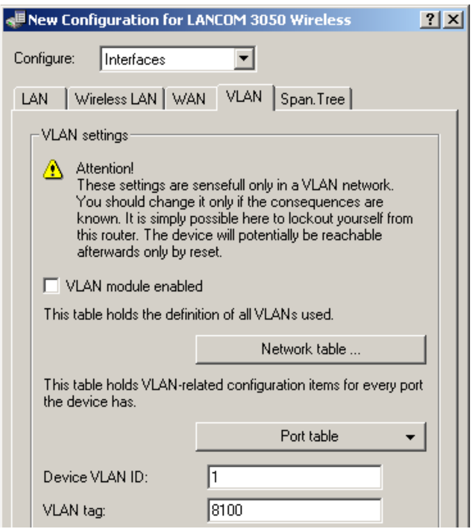
12.3.1 VLAN and ARF

In some cases it can suffice to configure the VLAN settings on the basis of the IP network (Advanced Routing and Forwarding, ARF). Here, a VLAN ID is defined for an IP network. All outbound packets from this network are tagged with this VLAN ID. Incoming packets have to be tagged with this VLAN ID in order for them to be assigned to the network. Please observe the relevant instructions in the section on ARF.

12.3.2 VLAN and WLAN Controllers

For large scale applications, LANCOM Access Points and LANCOM Wireless Routers can be managed from a central WLAN-Controller. The WLAN-Controller handles the definition of the wireless LAN networks (SSIDs) and it can assign a VLAN ID to these SSIDs. By assigning a VLAN ID to an SSID on the WLAN-Controller and the activation of the management VLAN (ID greater than 0), the VLAN module on the managed Access Point is activated automatically. Please also observe the instructions in the section on central WLAN management.

12.3.3 General settings



Configure: Interfaces

Attention!
These settings are sensefull only in a VLAN network. You should change it only if the consequences are known. It is simply possible here to lockout yourself from this router. The device will potentially be reachable afterwards only by reset.

□ VLAN module enabled

This table holds the definition of all VLANs used.

This table holds VLAN-related configuration items for every port the device has.

Device VLAN ID: 1

VLAN tag: 8100

LANconfig: interfaces ▶ VLAN

WEBconfig: LCOS menu tree ▶ Setup ▶ VLAN

To activate the VLAN module

You should only activate the VLAN module , if you are familiar with the effects of using VLAN.

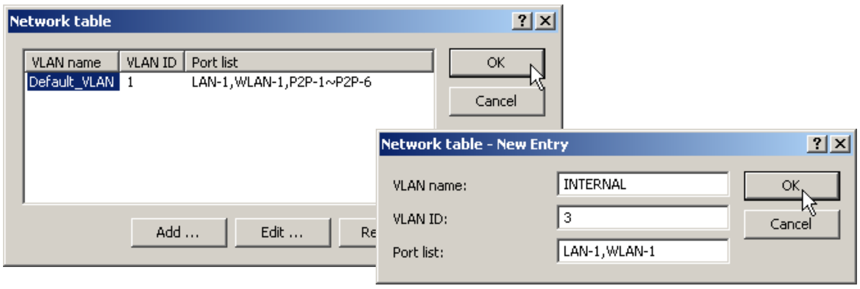
Wrong VLAN settings can obviate the access to the configuration of the device.

VLAN tagging mode

When transmitting VLAN tagged networks via provider networks that use VLAN themselves, providers sometimes use special VLAN tagging IDs. In order to set VLAN transmission on the LANCOM to accommodate this, the Ethernet2 type of the VLAN tag can be set as a 16-bit hexadecimal value as 'tag value' under `Setup/LAN Bridge/VLAN` or in LANconfig in the configuration area under 'Interfaces' using the 'VLAN' tab in the field 'VLAN tag'. The default is '8100' (802.1p/q VLAN tagging) other typical values for VLAN tagging could be '9100' or '9901'

12.3.4 The networktable

In the network table are those virtual LANs defined, in which the LANCOM should participate.



VLAN name	VLAN ID	Port list
Default_VLAN	1	LAN-1,WLAN-1,P2P-1~P2P-6

VLAN name: INTERNAL

VLAN ID: 3

Port list: LAN-1,WLAN-1

LANconfig: Interfaces ▶ VLAN ▶ VLAN table

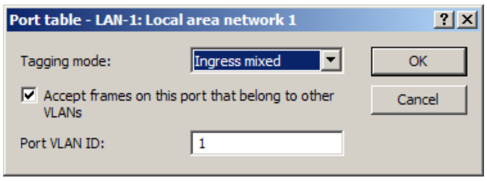
WEBconfig: LCOS menu tree ▶ Setup ▶ VLAN ▶ network table

- **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.
  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 first SSID of the first WLAN modul is named WLAN-1, the other SSIDs are WLAN-1-2 up to WLAN-1-8. If the device has two WLAN moduls the SSIDs are WLAN-2, WLAN-2-2 up to WLAN-2-8.

12.3.5 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 table - LAN-1: Local area network 1

Tagging mode: Ingress mixed

☑ Accept frames on this port that belong to other VLANs

Port VLAN ID: 1

LANconfig: Interfaces ▶ VLAN ▶ Port table

WEBconfig: LCOS menu tree ▶ Setup ▶ VLAN ▶ Port table

- **Port**: Name of the port, not editable.
- **Tagging mode**

  Controls the processing and assignment of VLAN tags at this port.

  - Never: Outbound packets are not given a VLAN tag at this port. Incoming packets are treated as though they have no VLAN tag. If incoming packets have a VLAN tag, it is ignored and treated as though it were part of the packet's payload. Incoming packets are always assigned to the VLAN defined for this port.
  - Unconditional: Outgoing packets at this port are always assigned with a VLAN tag, irrespective of whether they belong to the VLAN defined for this port or not. Incoming packets must have a VLAN tag, otherwise they will be dropped.
  - Mixed: Allows mixed operation of packets with and without VLAN tags at the port. Packets without a VLAN tag are assigned to the VLAN defined for this port. Outgoing packets are given a VLAN tag unless they belong to the VLAN defined for this port.
  - Ingress-mixed: Arriving (ingress) packets may or may not have a VLAN tag; outbound (egress) packets are never given a VLAN tag.
  - Default: Ingress mixed
- **Allow all VLANs (allows packets from other VLANs to enter this port)**

  This option defines whether tagged data packets with any VLAN ID should be accepted, even if the port is not a "member" of this VLAN.
- **Port VLAN ID**

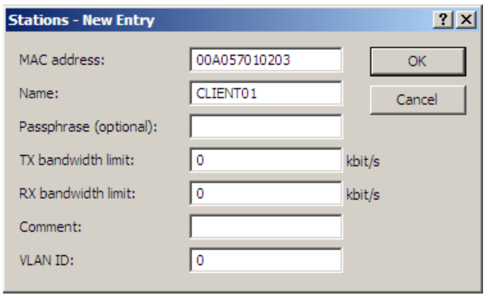
  This port ID has two functions:

  - Untagged packets received at this port in 'Mixed' or 'Ingress-mixed' mode are assigned to this VLAN, as are all ingress packets received in 'Never' mode.
  - In the 'Mixed' mode, this value determines whether outgoing packets receive a VLAN tag or not: Packets assigned to the VLAN defined for this port are given **no** VLAN tag; all others are given a VLAN tag.

12.4 Configurable VLAN IDs

12.4.1 Different VLAN IDs per WLAN client

VLANs are usually connected to a LAN interface on the LANCOM. Therefore, all packets that pass through this interface receive the same VLAN ID when the VLAN module is enabled. However, in some cases, administrators will want to assign different WLAN users to different VLANs.



Stations - New Entry

MAC address: 00A057010203

Name: CLIENT01

Passphrase (optional):

TX bandwidth limit: 0 kbit/s

RX bandwidth limit: 0 kbit/s

Comment:

VLAN ID: 0

LANconfig: Wireless-LAN ▶ Stations ▶ Stations

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN ▶ Access-List

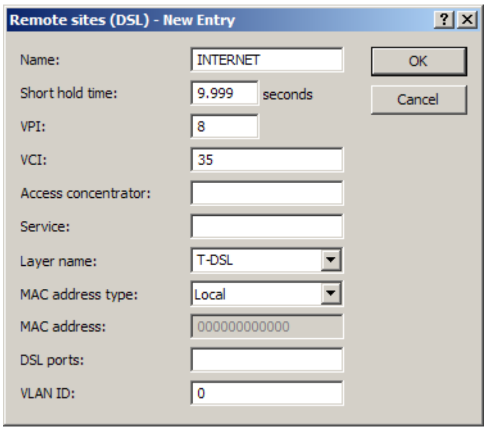
The client-specific VLAN ID can take on values from 0 to 4094. The default value of '0' stands for an unspecified VLAN ID. In such a case, the client will be assigned to the VLAN port of the logical WLAN.

The following requirements must be met in order to ensure successful client-specific VLAN assignment:

- VLAN operation must be enabled.
- The VLAN IDs that are to be assigned to the individual clients must be included in the VLAN network table.
- The LAN interfaces and all WLAN interfaces that are used by the clients must be assigned to the corresponding VLAN.

12.4.2 VLAN tags for DSL interfaces

Some DSL networks use VLAN tags in the same way as they are used in local networks to differentiate between logical networks on shared transmission media. The LANCOM Router can process these VLAN tags correctly if a VLAN ID is defined for each DSL remote site.



Remote sites (DSL) - New Entry

Name: INTERNET

Short hold time: 9.999 seconds

VPI: 8

VCI: 35

Access concentrator:

Service:

Layer name: T-DSL

MAC address type: Local

MAC address: 000000000000

DSL ports:

VLAN ID: 0

LANconfig: Communication ▶ Remote sites ▶ Remote sites (DSL)

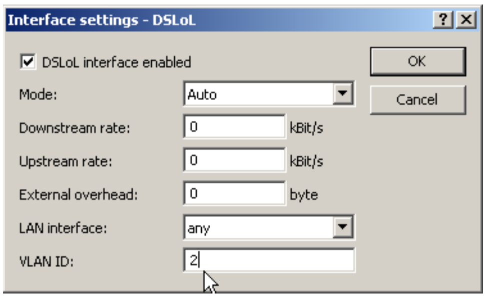
WEBconfig: LCOS menu tree ▶ Setup ▶ WAN ▶ DSL Broadband Peers

- **VLAN ID**

  ID used to explicitly identify the VLAN over the DSL connection.

12.4.3 Special VLAN ID for DSLoL interfaces

In order to better separate the data traffic on a DLSoL interface from other traffic, 'VLAN ID' can be set up for the DSLoL interface under `Setup/Interfaces/DSLoL` or in LANconfig in the configuration area 'Interfaces' using the 'WAN' tab under the interface settings for the DSLoL interface.



Interface settings - DSLoL

☑ DSLoL interface enabled

Mode: Auto

Downstream rate: 0 kBit/s

Upstream rate: 0 kBit/s

External overhead: 0 byte

LAN interface: any

VLAN ID: 2

12.5 VLAN tags on layer 2/3 in the Ethernet

12.5.1 Introduction

VLAN tags enable a simple form of QoS control even when using switches that cannot evaluate IP headers. The IEEE 802.1p standard defines a priority tag in the VLAN header with a length of 3 bits, which correspond to the first 3 bits of the DSCP fields (Differentiated Services Code Point - DiffServ) and/or the precedence in the TOS field (Type of Service). The processing of VLAN tagged packets requires that packets in the receive direction are regarded differently to packets in the send direction.

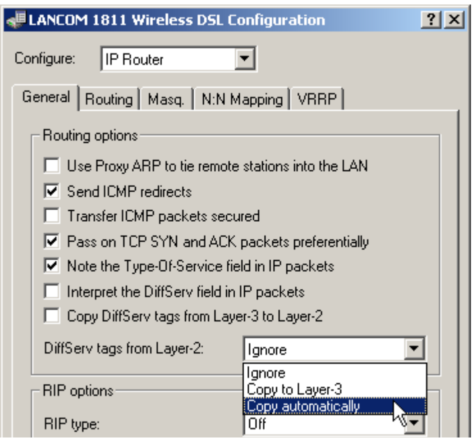
- Upon receipt of a tagged Ethernet packet, it may be processed in one of three ways:
  - The VLAN tag is ignored.
  - The VLAN tag is always copied to the DiffServ or TOS field.
  - The VLAN tag is copied to the DiffServ or TOS field if this is not marked already, i.e. the precedence is '000'.

- When a packet is transmitted over Ethernet, the VLAN tag can be set depending on the precedence. This should only happen if the recipient of the tag can understand it, i.e. tagged packets can be received. Tags are thus only set for packets which are sent to addresses from which the LANCOM already received tagged packets.

When a tagged packet is received, the tag is saved to the associated entry in the connection list. If a packet is to be sent with a precedence setting, then the VLAN ID recorded earlier is entered into the packet together with the precedence to form a VLAN tag. Where a connection causes other connections to be opened, e.g. with FTP or H.323, then the tag is inherited to the new entries.

12.5.2 Configuring VLAN tagging on layer 2/3

Configuring VLAN tagging on layer 2/3 involves the definition of the general routing settings and the behavior upon receipt and transmission of tagged packets.



LANCOM 1811 Wireless DSL Configuration

Configure: IP Router

Routing options

- ☐ Use Proxy ARP to tie remote stations into the LAN
- ☑ Send ICMP redirects
- ☐ Transfer ICMP packets secured
- ☑ Pass on TCP SYN and ACK packets preferentially
- ☑ Note the Type-Of-Service field in IP packets
- ☐ Interpret the DiffServ field in IP packets
- ☐ Copy DiffServ tags from Layer-3 to Layer-2

DiffServ tags from Layer-2: Ignore

RIP options

RIP type: Off

LANconfig: IP Router ▶ General

WEBconfig: LCOS menu tree ▶ Setup ▶ IP-Router ▶ Routing-Method

- **Routing method**
  - Normal: TOS/DiffServ field is ignored.
  - Type-Of-Service: The TOS/DiffServ field is regarded as a TOS field; the bits 'low delay' and 'high reliability' will be evaluated.
  - DiffServ: The TOS/DiffServ field is regarded as a DiffServ field. After evaluating the precedence, packets with the code points 'AFxx' are saved and packets with the code points 'EF' receive preferential treatment. All other packets are transmitted as normal.
- **DiffServ-Tags from Layer-2**

  The setting for Layer2-Layer3 tagging regulates the behavior when a data packet is received:
  - Off: VLAN tags are ignored.
  - On: Priority bits in the VLAN tag are always copied to the precedence of the DSCP.
  - Automatic: Priority bits in the VLAN tag are only copied to the DSCP precedence if this is '000'.
- **To copy DiffServ-Tags from Layer2 to Layer3**

  The setting for Layer3-Layer2 tagging regulates the behavior when a data packet is transmitted. If this option is activated, VLAN tags with priority bits originating from the DSCP precedence will be generated if the recipient has sent at least one tagged packet.

LANCOM reference manual part 5

- Voice over IP (VoIP)

Version: LCOS 7.6 with addendum 7.7 (see appendix)
(last update August 2009)

LANCOM
Systems

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

Subject to change without notice. No liability for technical errors or omissions.

Products from LANCOM Systems include software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

Products from LANCOM Systems include cryptographic software written by Eric Young (eay@cryptsoft.com).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

Products from LANCOM Systems contain open source software components which are available as source text and which are subject to special licenses and the copyright of their authors. In particular the firmware components are subject to the terms of the GNU General Public License, version 2 (GPL). The license agreement with the text of the GPL is available on the LANCOM CD in the relevant product's directory. On request, you can obtain the source texts and licensing details electronically from the LANCOM Systems GmbH FTP server.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen
Deutschland

www.lancom.de

Würselen, August 2009

110650/0809

Contents

13 Voice over IP (VoIP)

13.1 Introduction

The term Voice over IP (VoIP) refers to voice communications over computer networks based on the Internet protocol (IP). The core idea is to provide the functions of traditional telephony via cost-effective and wide-spread networking structures such as the Internet. VoIP itself is not a standard, rather it is a collective term for the various technologies (equipment, protocols, voice encoding, etc.) which make voice communications in IP networks possible.

Different terminology is used for telephony over a network (LAN or Internet) The terms "Voice over IP" or "IP telephony" are used as synonyms, although in actual fact they have different meanings.

- Strictly speaking, "Voice over IP" is merely a term for the technology of transmitting calls across data networks in real-time using the IP protocol (Internet protocol). The term is also used when the technology is implemented only in the provider's core networks, in what is known as the backbone
- The term "IP telephony" is used when the VoIP technology is also used in the terminal equipment, so that the call subscriber uses the IP network for telephony.
- "Internet telephony" is also used to describe telephony using VoIP over the Internet in general.

In the following, "Voice over IP" is usually used even to refer to IP telephony in accordance with general custom.

There are four basic types of terminal equipment that can be used for VoIP telephony:

- With software running on the PC, known as a "softphone".
- With an IP or VoIP telephone that is connected directly to the local network.
- With a conventional telephone that is connected to the local network by an adapter (analog telephone adapter, ATA).
- Via a VoIP gateway that converts telephone calls from telephones (analog and ISDN) to VoIP and can then communicate between the two "telephone worlds" like a PBX.

There is a basic difference between a VoIP connection being established between two pieces of terminal equipment that are connected directly to the data network (PC or IP telephone) and the situation where a subscriber in the land-line or mobile telephone network requires the conversion of the signaling, numbers and voice data. To differentiate the various connection variants, a device in the LAN has become known as a "PC", and a device in the land-line network has become known as a "phone".

PC-to-PC communication

With this application, the terminal equipment has to be integrated directly into the user's LAN. Examples are a PC, an IP telephone or a telephone that is connected to the LAN using an ATA.

Different software solutions are available for the PC, known as "softphones". Note that some of these programs can only communicate with users of the same software and not with softphones from other manufacturers. Communication is usually free of charge within the Internet. A current example is Skype, which uses its own protocol.

PC-to-phone and phone-to-PC communication

In this case, the call data has to be transmitted from the Internet to the landline network, usually using what are known as VoIP gateways. In general, these gateways are provided by providers and are subject to a fee.

VoIP routers offer another option that can switch VoIP calls to an ISDN line. Examples are different LANCOM VoIP Router types with an SIP gateway and ISDN interfaces. When the calls are transferred to the landline network, the usual telephone operator fees are charged.

So that the subscriber can even be called on a PC, he or she needs a VoIP telephone number that is usually provided by a provider.

VoIP providers usually only provide individual numbers and not complete number ranges with a switchboard number and extension numbers. This is why the numbers that are provided by public providers are not attractive to many business customers. When the LANCOM VoIP Router is used with a SIP gateway, previously-used numbers can be maintained; the functions of VoIP telephony can also be used.

13.2 VoIP implementation in the LANCOM VoIP Router

The main task of the VoIP implementation in the LANCOM VoIP Router is to connect telephone calls from different local interfaces (LAN, WLAN, ISDN) to the WAN connections that can be accessed by the router. This enables switching between the local interfaces (local call) as well as between WAN interfaces.

The basis for the implementation and switching is the SIP protocol. The calls over all interfaces are converted into SIP by the interface converter (this mainly concerns the ISDN interfaces). The ISDN-ISDN bridge function is a special case that is activated when ISDN protocols cannot be mapped in SIP, which is why a bit-transparent connection is created between an ISDN-TE (external ISDN connection) and an ISDN-NT (internal ISDN connection).

Furthermore, the bit-transparent connection is usually used for calls between multiple local ISDN interfaces to achieve the highest possible compatibility and quality.

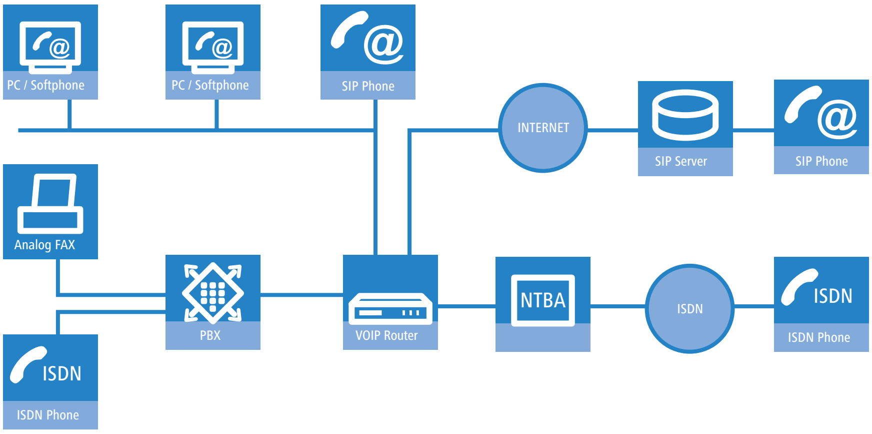
13.2.1 Example Applications

Voice over IP solutions offers advantages across a broad spectrum of applications, starting with small companies and extending to large corporations with extensive networks of subsidiaries. In the following section, we will demonstrate a number of examples.

Detailed information about configuration is available in the chapter 'Configuration of VoIP functions'.

Supplementing existing ISDN PBXs

VoIP functions can be conveniently added in to existing telephone structures by using a LANCOM VoIP Router. The LANCOM VoIP Router is simply connected between the public ISDN connection (e.g. ISDN NTBA) and the ISDN PBX.



Telephone calls over the PBX and its ISDN telephones remain possible just as before; the telephones remain available under the familiar telephone numbers. This application additionally offers the following options:

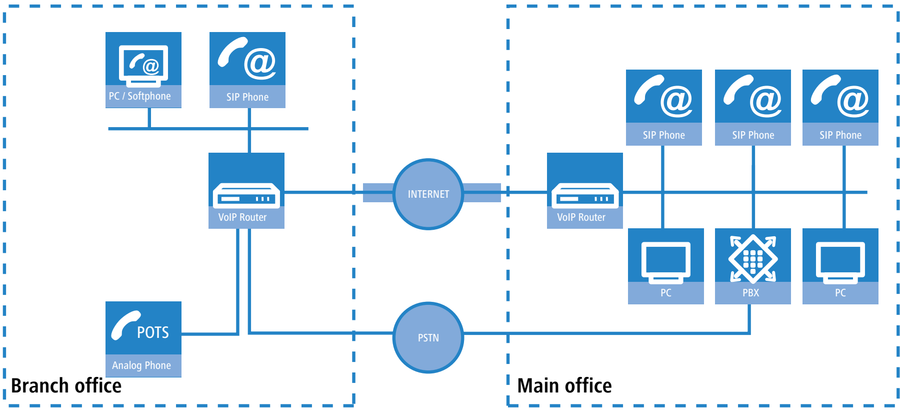
- In addition to the ISDN telephones, VoIP telephones or VoIP softphones can be included in the telephone infrastructure. VoIP subscribers in the internal LAN are also able to call external ISDN subscribers.
- The ISDN telephones continue to function, and additionally they can call all of the internal VoIP telephones and softphones in the LAN.
- Calls to external SIP subscribers who use the same Internet provider are often available at no cost.
- With the appropriate connection to a public SIP provider, any other SIP subscriber worldwide can be called, irrespective of the provider network. As an alternative to a direct ISDN connection, ISDN network subscribers can also be reached over a diversion via the SIP provider. The costs depend on the provider's particular tariff models. Frequently, long-distance and overseas calls via an SIP provider are significantly cheaper than the traditional telephone connection.

In this constellation, the LANCOM VoIP Router takes over the switching of the calls. The device can be individually configured, for example, to use the access codes to decide upon the switching of a call either via the ISDN interface, or via the Internet as a VoIP call.

Connecting subsidiaries or home offices to the headquarters

Many subsidiaries or home offices already have a connection to the network at headquarters over VPN. These connections are normally limited to conventional data transmission. By using VoIP, internal company calls can be made for free over the existing VPN connection and— thanks to the VPN encryption —these calls are secured against eavesdropping.

With a LANCOM VoIP Router located in the branch or home office, the two worlds of traditional and VoIP telephony can be united in a single telephone: A VoIP telephone or an existing ISDN telephone can be used for free telephone calls via VPN to the headquarters, or to make standard calls via ISDN.



The advantages of a telephone connection to headquarters:

- The configuration of telephone functions can be carried out centrally in the VoIP PBX at headquarters.
- Subscribers at their branch or home offices connect with the central PBX.
- Calls within the company network are free.
- Outgoing calls are automatically directed to the optimal line for cost optimization.

VoIP for companies through SIP trunking

One of the biggest hurdles for companies that fully migrate to VoIP is to maintain the existing telephone numbers. Normal provider SIP accounts come with a telephone number for the transition to the landline telephone network, but generally these numbers are selected from a pool of numbers available to the provider. However, for companies with a large number of telephone subscribers and numbers, it is of decisive importance that existing telephone and extension numbers are maintained after migrating to VoIP.

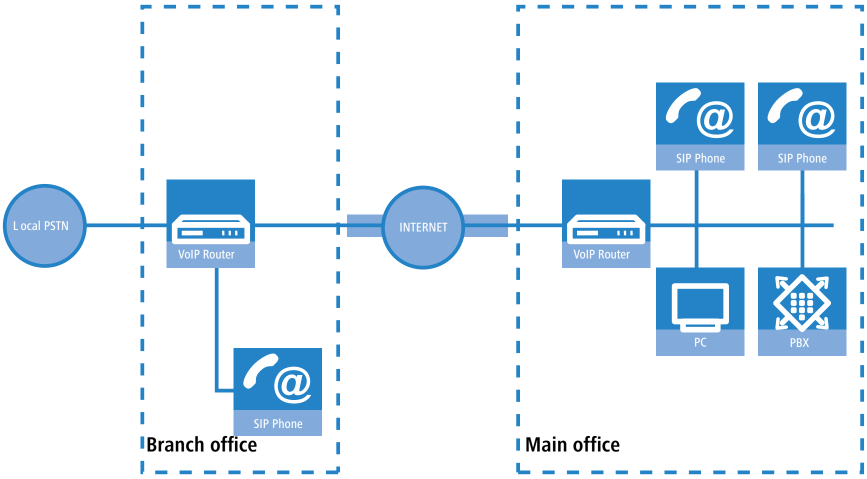
With the SIP trunking function, entire ranges of telephone numbers made up of external numbers and their associated extensions can be mapped by LANCOM VoIP Routers over a single connection to a SIP provider, assuming that the provider also supports Direct Dialing In (DDI) and can provide multiple connections simultaneously. Generally speaking, SIP providers that offer SIP trunking can acquire the existing telephone numbers from the former telecomms provider.

Connecting local ISDN lines with a remote SIP gateway

Companies with nation-wide and internationally distributed sites are often interconnected with VPN already. A LANCOM VoIP Router can be used not only to connect the SIP and ISDN telephones at a branch office to the SIP-PBX at headquarters; it can also integrate local ISDN networks into corporate communications with help of the "SIP Gateway" function.

The SIP gateway is active for outgoing and incoming calls.

- A company headquarters in New York can, for example, use a LANCOM VoIP Router with SIP gateway located at the Los Angeles branch office to telephone with customers and suppliers located in Los Angeles at local rates ("local break-out").
- For improved availability to customers located abroad, the New York headquarters can, for example, use a LANCOM VoIP Router with SIP gateway located at their sales office in Italy. Customers can then reach support or service numbers via a standard national telephone number. Calls from the local ISDN network are received and directed within the company network to the responsible employee. Call routing can be used which identifies the customer's calling number and automatically selects the appropriate connection to be used for forwarding the call.

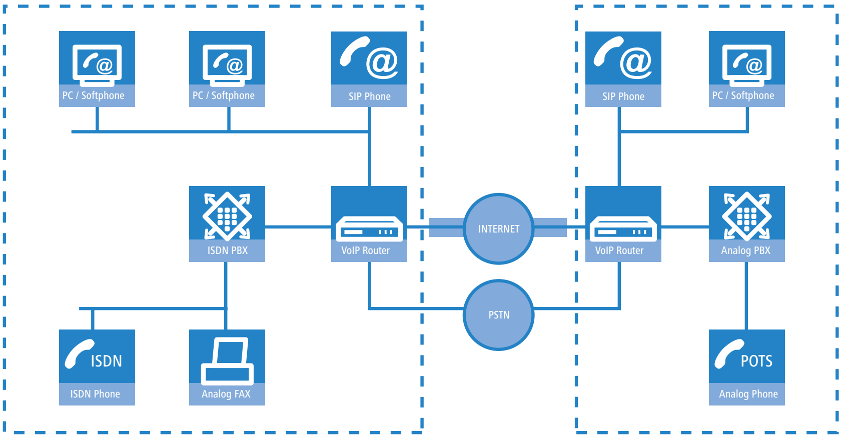


Advantages of the SIP gateway:

- The local ISDN connection at any site is available for use by any of the offices throughout the entire company.
- National and international long-distance calls can be mapped to local or regional calls, so saving costs.
- Automatic routing of incoming calls to the responsible employee.

Connecting sites without a SIP PBX

Companies with widely disperse offices and without their own SIP PBX can also take advantage of VoIP site-to-site connectivity. In this "Peer-to-Peer" scenario, a LANCOM VoIP Router has been implemented at both locations.



Along with data transfer via VPN, it is also possible to use VoIP functions between the two locations.

The advantages of peer-to-peer site-to-site connectivity

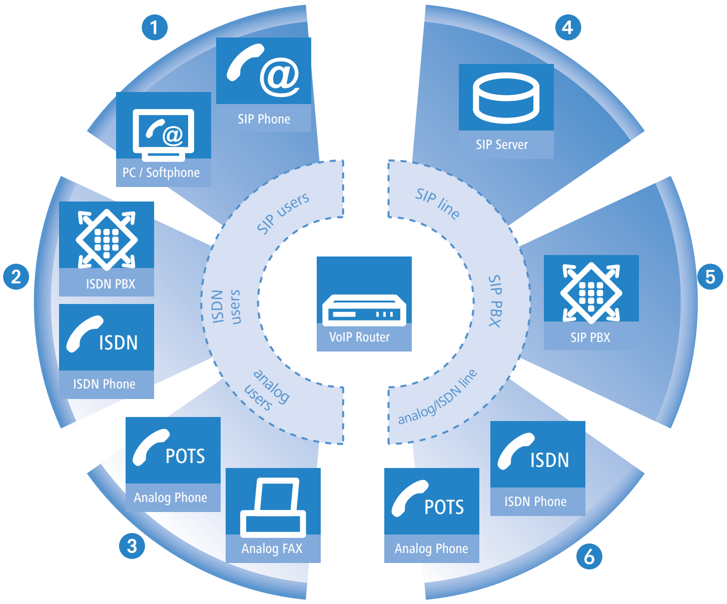
- ISDN PBXs at different locations can form a common internal telephone network.
- An SIP PBX is not necessary.
- Calls within the company network are at no charge.
- Outgoing calls are automatically directed to the optimal line for cost optimization.
- Incoming calls can be switched directly to the appropriate employee at a different location.

13.2.2 The central position of the LANCOM VoIP Router

LANCOM VoIP Router take up a central position in the switching of telephone calls between internal and external subscribers over the different channels of communication. Depending on the model and equipment, the devices interconnect the following communication participants and channels into a common telephone infrastructure.

1. Internal VoIP terminal devices connected to LAN, WLAN and DMZ, such as SIP telephones and SIP softphones
2. The internal ISDN infrastructure with ISDN PBX and ISDN telephones
3. Analog terminal devices, internally connected either into the ISDN network via a PBX with a/b ports, or alternatively into the VoIP network over an ATA (Analog Telephone Adapter).
4. External SIP providers and all of the external subscribers attainable via them
5. Upstream SIP PBXs with all of the internal and external subscribers attainable through it

6 The external ISDN world via ISDN NTBA or upstream ISDN PBX, and all of the external subscribers available via the land-line network



Users and lines

Telephony subscribers in internal areas can take part in voice communications and, in the LANCOM VoIP environment, are referred to as "users". The LANCOM differentiates between:

- ISDN users

  Devices connected over the ISDN network, including ISDN and analog devices connected to an upstream ISDN PBX.

  When connecting downstream PBXs to point-to-point lines, the number of possible ISDN subscribers is determined by the length of the extension number (DDI). In this case, all of the telephones and terminal equipment connected to the PBX can be mapped with a single ISDN user entry.

- SIP users

  SIP terminal devices connected over LAN, WLAN and DMZ and analog devices connected with an ATA.

The external paths of communication available to the users are known as "lines". The LANCOM differentiates between the following lines:

- ISDN

  A connection to an ISDN NTBA over the TE interface. The NT interface can additionally be used to connect ISDN terminal devices directly or via a downstream ISDN PBX.

- SIP lines

  There are three different types of SIP line:

  - □ A "Single account" line acts like a normal SIP account with a single telephone number. The internal users can all make use this account for making SIP calls, although only one call can be conducted at a time.

    Depending on the provider services, these lines can be used to reach subscribers in the provider networks, subscribers in other SIP networks (partner networks), or even land-line subscribers. Your own availability at your own telephone number or even solely with an SIP name over the Internet also differs from provider to provider.

  - □ A "trunk" line acts like an extended SIP account with a main external telephone number and multiple extension numbers. Internal users use this account in parallel and several calls can be made simultaneously (until the maximum available bandwidth is exhausted).

  - □ As a "SIP gateway" line, the LANCOM VoIP Router provides a remote SIP PBX with a transition to the local ISDN network. The SIP gateway is registered at the SIP PBX with a single number, although several calls can be conducted at once (until the maximum available bandwidth is exhausted). The connection between the SIP PBX and the LANCOM VoIP Router is normally established over a VPN connection.

- SIP PBXs

  Connections to upstream SIP PBXs. These lines are generally connections to large PBXs in the network at headquarters which can be reached via a VPN connection.

ⓘ The precise number of users and lines available varies between models and software options.

13.3 Call switching: Call routing

All calls between internal subscribers and subscribers who can be reached over external lines are handled as SIP calls by the LANCOM—even if the connection is between two ISDN subscribers.

The call router in the LANCOM VoIP Router switches the call. The switching relies mainly on the information in two tables:

- For telephone numbers arriving at the call router, rules in the call-routing table are able to alter these numbers if needed and can decide which line to use for a call.
- The table for the locally registered user provides information about which terminal device is available at which internal telephone number.

The bandwidth reservation, QoS settings and firewall settings that are necessary for reliable transmission of voice data are carried out automatically by the LANCOM.

- When establishing a connection, the LANCOM checks (under consideration of the permitted codecs) which **maximum** bandwidth will potentially be required.
  - This bandwidth is then automatically reserved by the QoS module upon initiation of the connection.
  - If negotiation shows that the maximum bandwidth is not available, the connection will not be made.
  - If negotiations between the terminal devices can agree upon a codec with lower bandwidth requirements, then the reserved bandwidth will be lowered accordingly.
- All packets from ISDN users are given a DiffServ marking by the LANCOM (with SIP users, the QoS marking is usually handled by the telephones or softphones).
  - SIP packets for signaling are marked as CS1.
  - RTP packets are marked as EF.
- The ports required for the transmissions are activated automatically.

13.3.1 SIP proxy and SIP gateway

The tasks involved in switching calls between the different lines of SIP and ISDN subscribers are handled by two functions in the LANCOM VoIP Router.

- SIP proxy

  A SIP proxy handles the switching between callers.
- SIP gateway

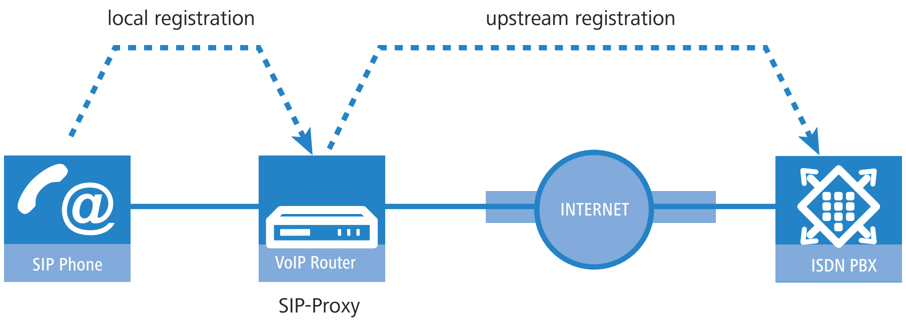
  The SIP gateway handles the conversion between IP-based telephony that uses the SIP protocol and other (telephone) networks, for example the ISDN network.

13.3.2 User registration at the SIP proxy

A LANCOM VoIP Router represents the central exchange for SIP calls between different subscribers who wish to communicate over different types of line. The task of switching in the LANCOM are handled by the SIP proxy. A telephone signals the SIP proxy that it needs to establish a connection, and the SIP proxy uses certain rules to decide which line is to be used for the connection. Conversely, incoming calls are assigned to a certain terminal device by the SIP proxy according to its rules.

For terminal devices to be able to take part in this switching, they must be registered with the SIP proxy. Where the registration is limited to call switching by the LANCOM, we refer to "local registration".

If other exchanges are involved, e.g. an SIP PBX at another location, then we refer to an upstream registration. In this case, the LANCOM accepts the request for registration and forwards it upstream. In this instance, the LANCOM is described as "transparent proxy".



The great advantage with this two-stage registration comes to bear in the backup event: If the connection to an upstream SIP PBX is not available, the SIP proxy can handle the user who is registered upstream as a local user and can then direct the calls over alternative lines.

Registration at the LANCOM VoIP Router (local registration)

For local registration at the LANCOM, it is initially sufficient for the user to send a valid VoIP domain to the SIP proxy. The internal VoIP domains of the LANCOM VoIP Router are valid, as are all domains entered in a SIP line.

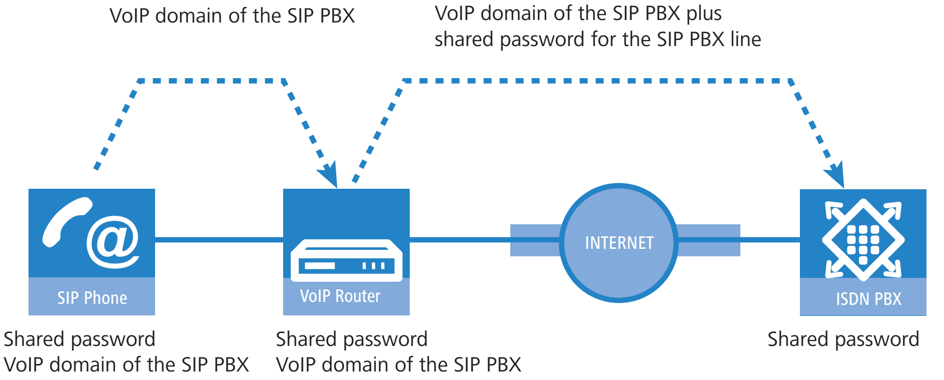
- For SIP terminal devices in the LAN (SIP telephone or SIP softphone), the domain is entered in the configuration. There is no need for an entry as a SIP user in the configuration of the LANCOM. This variant is known as "automatic registration".
- The domain cannot be entered into ISDN terminal equipment; instead, ISDN users have to be registered in the LANCOM configuration with a corresponding entry as an ISDN user (→ Dynamic ISDN users at point-to-point connections).
- To prevent unknown subscribers from registering, authentication at the SIP proxy can be set as a prerequisite to local registration (local authentication). In this case, an entry as a SIP or ISDN user in the LANCOM configuration is essential.

Automatic registration without entering a password is restricted to the SIP users in the LAN. SIP users in the WAN require an appropriate user entry and authentication by password.

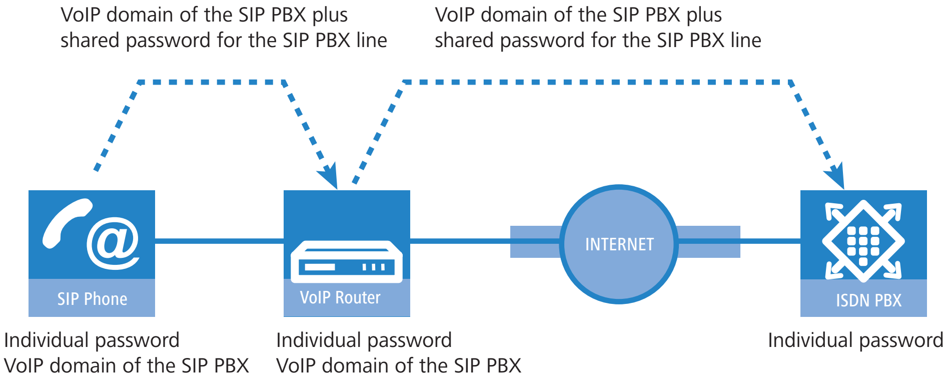
Registration at an upstream SIP PBX (upstream registration)

Generally, authentication by user and password is always required for registration at a SIP PBX. There are two possible ways of transmitting the authentication data to the SIP PBX:

- All SIP and ISDN users at the LANCOM VoIP Router end use the same shared access information. In this case, only the VoIP domain for the SIP PBX and the appropriate user ID are entered into the SIP terminal device. For ISDN users, the VoIP domain of the SIP PBX is entered into the LANCOM as an ISDN user. The SIP proxy recognizes the request for registration at the upstream SIP PBX if the domain communicated from the client agrees with a domain entered into the SIP PBX line. The proxy then forwards the registration data together with the shared password to the SIP PBX.


VoIP domain of the SIP PBX
VoIP domain of the SIP PBX plus shared password for the SIP PBX line
SIP Phone
VoIP Router
INTERNET
ISDN PBX
Shared password VoIP domain of the SIP PBX
Shared password VoIP domain of the SIP PBX
Shared password

- If SIP or ISDN users at the LANCOM VoIP Router are entered into the SIP PBX with different passwords, then the users have to enter their individual passwords upon registration. Consequently, each SIP or ISDN user has an entry into the LANCOM with the individual passwords, which are also entered into the SIP terminal devices. Users with shared and individual passwords can be managed in parallel.


VoIP domain of the SIP PBX plus shared password for the SIP PBX line
VoIP domain of the SIP PBX plus shared password for the SIP PBX line
SIP Phone
VoIP Router
INTERNET
ISDN PBX
Individual password VoIP domain of the SIP PBX
Individual password VoIP domain of the SIP PBX
Individual password

Particular aspects for ISDN users

Integrating ISDN terminal equipment into the LANCOM VoIP environment and the necessary steps for configuration depend upon the application at hand and, if applicable, upon the options available with a PBX. The main questions to be answered by the user are as follows:

- Can ISDN terminal devices telephone internally with SIP users?
- Are ISDN terminal devices available externally over SIP lines?
- Can ISDN terminal devices telephone externally over SIP lines?

To answer these questions, we differentiate between the following constellations:

- If ISDN terminal equipment can be reached over an ISDN TE interface on the LANCOM, it is described as "upstream". From the perspective of the LANCOM, the ISDN terminal devices are on an external line. This ISDN terminal equipment is normally not classified as being for local users, and so no entries for ISDN users are necessary.

  ISDN terminal equipment at an upstream ISDN PBX...

  - can make internal calls to SIP users if the corresponding telephone numbers are configured as internal MSNs in the ISDN PBX.
  - can receive internal calls from SIP users if the internal MSNs of the ISDN equipment are output to the ISDN line by the call-routing table, for example over a standard route.
  - can only make calls over SIP lines if the PBX is able to output certain call numbers over its internal ISDN bus. Otherwise, all calls not matching with its internal MSNs would be forwarded by the ISDN PBX to the public telephone network.
  - can only receive calls from an upstream SIP PBX if entered into the LANCOM as an ISDN user and registered as such with the SIP PBX.
- If ISDN terminal equipment can be reached over an ISDN NT interface on the LANCOM, it is described as "downstream". For the LANCOM, this is then a local subscriber that can be reached via the list of registered users. As ISDN terminal equipment cannot send domain information to register at the LANCOM, it must be entered as an ISDN user so that it can be recognized by the VoIP system.

  ISDN terminal equipment at a downstream ISDN PBX...

  - can make internal calls to SIP users by entering the character for an outside line as required by the PBX and then dialing the SIP user's internal number. The PBX then forwards the call to the SIP user's internal number—without the outside-line access code—over its external ISDN bus to the LANCOM.
  - can receive internal calls from SIP users as long as the entry for the ISDN user contains the correct allocation of the internal number to the appropriate MSN. The LANCOM takes a call to the ISDN user's internal number, translates it to the MSN, and outputs it to the allocated ISDN bus. The PBX receives the MSN as if it were an external call and forwards it to the corresponding ISDN terminal equipment.
  - can conduct incoming and outgoing calls over SIP and ISDN just like SIP users. Again, the outside-line code may be necessary for outgoing calls.

Dynamic ISDN users at point-to-point connections

When connecting downstream PBXs to a point-to-point interface of the LANCOM VoIP Router, the number of possible ISDN terminal devices is only limited by the length of the extension number. With three-figure extension numbers, almost 1000 terminal devices can be connected, all of which can be managed as ISDN users in the LANCOM VoIP Router.

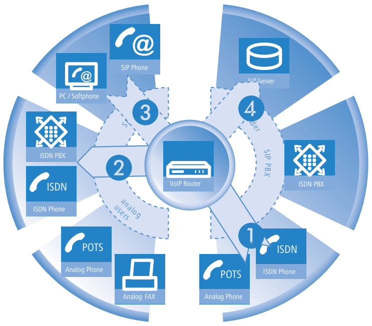
Through an ISDN user entry with a # character as a placeholder for the telephone numbers, all ISDN terminal devices with their respective extension numbers can be set up as dynamic ISDN users.

User entries that use # characters to map user groups cannot be used for registration at an upstream PBX. This registration always demands a specific entry for the individual ISDN user.

13.3.3 Number translation at network transitions

LANCOM VoIP Router switch calls between different telephone networks, e.g. the ISDN network, various SIP provider networks, and the internal telephone network. These networks generally have different ranges of numbers or even completely different conventions for addressing subscribers. Whereas the traditional land-line network uses numerical characters with country code and area access codes, the world of SIP allows alphanumerical names along with domain information.

The transition between these zones must guarantee the correct translation of "telephone numbers" so that the intended subscriber can be reached. For example, when a call from the land-line network arrives at a public MSN, the requested telephone number has to be translated to the ISDN user's internal number. This act of translation is known as "mapping". Mapping incorporates not only the **called** number, which represents the destination, but the **calling** number for the source as well.



Mapping the destination telephone number
1 external MSN from the ISDN network
2 internal telephone number of the ISDN user
Mapping the source telephone number
3 internal telephone number of the SIP user
4 external SIP telephone number in the SIP provider's network

Depending on the application at hand, both the called and the calling numbers have to be modified so that a return call can be made to the source number.

Call number translation at the transition to outside lines is primarily implemented by mapping entries in the ISDN and SIP lines and by rules in the call-routing table.

13.3.4 The Call Manager

The Call Manager has the central task of allocating the calls waiting to be switched to a certain line or to a certain user. The Call Manager makes this allocation by using the call-routing table and the list of registered users. The calls are switched in the following steps:

- Processing of called numbers (Calling Party ID)

  First of all there is a check to see whether a numeric or alphanumeric number is available. Typical dialing separators such as "()-/" and <blank> are removed. A leading "+" is left in place. In this case, the number is still treated as a numeric number. If the check reveals any other alphanumerical character, the number is treated as alphanumeric and remains unchanged.

- Resolving the call in the call routing table

  After processing the Called Party ID, the call is passed over to the call-routing table. Entries in the call-routing table consist of sets of conditions and instructions. The entries—with the exception of the default routes—are searched through and the first one that satisfies **all** of the conditions is executed.

- Resolution of the call with tables of local subscribers

  If no entry is found in the call-routing table, then the Call Manager searches through the list of local subscribers. Call routing considers all of the users known to the call router (registered SIP users, configured ISDN users). If an entry is found that agrees with the called number and that has the matching destination domain, then the call is delivered to the corresponding subscriber.

  If there is no local subscriber with matching number and destination domain, then the following cycle searches for an agreement between the number of the local subscriber and the called number; the destination domain is ignored.

- Resolution of the call with default entries in the call-routing table

  If the preceding cycles referring to the call-routing table and lists of local subscribers remain unsuccessful, then the waiting call is checked once again with the call-routing table. This pass only takes the default routes into account, however. The numbers and destination domains entered into the default routes are ignored. Only the source filters are processed, assuming that the default routes has these filters.

Specific examples of call-routing procedures can be found in the configuration examples described.

13.3.5 Making telephone calls with the LANCOM VoIP Router

Using the LANCOM VoIP Router opens up a variety of new possibilities for making telephone calls. Depending on the constellation of terminal equipment implemented (e.g. SIP or ISDN telephones, SIP or ISDN PBX systems) and, depending on the configuration for call routing in the LANCOM VoIP Router, certain information is critical for understanding the establishment of connections.

Automatic outside line access

Using the LANCOM VoIP Router and the enhancement with VoIP functionality within your telephone structure is designed to support the users' telephone behavior with the greatest possible convenience. One of the core aspects of this is the use of "spontaneous" or "automatic" outside line access, a feature that is familiar to users of standard PBX systems.

- Most PBX systems are configured in such a way that the telephone subscribers must dial a "0" before the desired telephone number in order to gain access to an outside line - that is, to carry out a telephone conversation via a public telephone network.

Without the "0" prefix, the number dialed is considered to be an internal number from another extension line on the private PBX.

- If "automatic outside line access" is set up, all numbers dialed are directed over the public telephone network. In this case, internal telephone calls to other extensions are not possible or only possible when a special symbol is dialed before the number.

When the telephone structure is extended with a LANCOM VoIP Router, a variety of new possibilities become available for connecting telephone terminal equipment. This includes the existing analog or ISDN telephones (where necessary, connected to the respective PBX) or VoIP terminal equipment such as SIP telephones or PCs with VoIP software.

As a new and central building block in the telephone structure, the LANCOM VoIP Router assumes many of the PBX tasks for connected terminal equipment. As such, you can also set up the automatic outside line access for the terminal equipment connected to the LANCOM VoIP Router directly for the ISDN or SIP subscriber groups, thereby adapting it to existing telephone behavior.

- When automatic outside line access is turned off, subscribers must dial a "0" before the desired number in order to carry out a telephone conversation via a public telephone network.

  All calls without a "0" preceding the number will be treated as calls to internal extensions within the private telephone network.

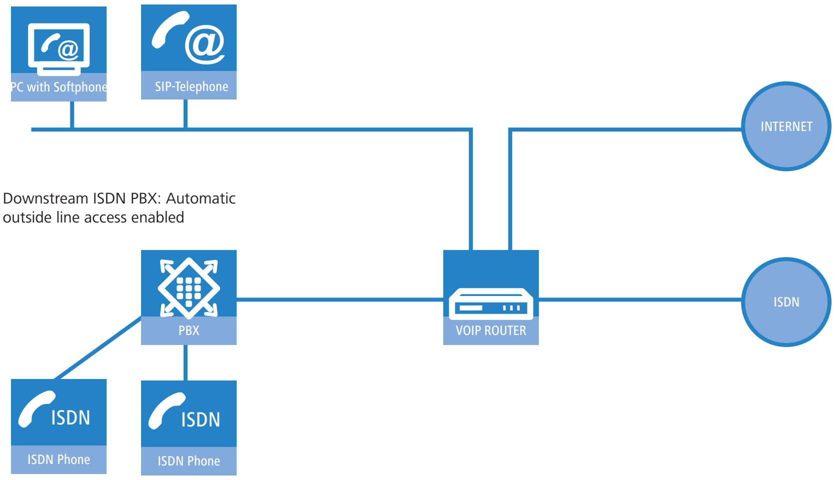
- If automatic outside line access is turned on, all numbers dialed will be directed over a public telephone network.

  For telephone calls to internal extensions, a special symbol or a specific number combination must be dialed before the number. With the standard settings, when automatic outside line access is enabled, a star * is activated as the identification symbol for an internal number. This setting can be adjusted to match the character that you are familiar with.

If you operate the LANCOM VoIP Router on the extension line of a PBX, it is recommended that outside line access for the router be configured in the same way as for the PBX so that the behavior remains the same from the user's perspective.

Example of a downstream PBX

A LANCOM VoIP Router is switched between the ISDN outside line and the existing ISDN PBX. In the PBX, automatic outside line access is enabled, the call router settings for the LANCOM VoIP Router decide whether or not a "0" must be dialed for outside line access for the connected ISDN and SIP subscribers.



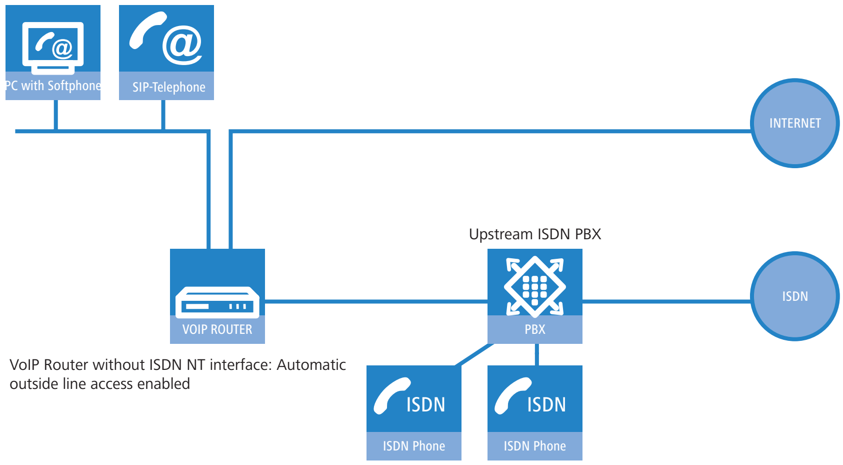
If the LANCOM VoIP Router in this constellation is not available, for example, due to a power outage, the ISDN connection for the downstream ISDN PBX is automatically "bridged" to the external ISDN connection (when life-line support is enabled). For a LANCOM VoIP Router **without** automatic outside line access, the ISDN subscribers should not dial a "0" before the number while the life-line support is active.

Example of an upstream PBX

A LANCOM VoIP Router is connected to an ISDN PBX extension line. In the LANCOM VoIP Router, automatic outside line access is enabled, the settings for the upstream PBX decide whether or not a "0" must be dialed for outside line access for the connected ISDN and SIP subscribers.

Dialing various numbering areas

When dialing other parties, the following numbering areas are available for use:



- **Internal numbers** are comparable to the extension line numbers for traditional PBX systems ("extension"). Subscribers can reach each other directly using these internal numbers without having to go through a public telephone network.

  The internal numbers must be unique for all subscribers within the private telephone network, this also includes any other PBX systems that may be connected!

  The internal subscribers can be reached by simply dialing the internal number without a "0" preceding it.

Depending on the settings for automatic outside line access ('Automatic outside line access' → page 13-9), a special preceding dialing signal may be required.

- Via **local telephone numbers** you can reach external parties who are in the same local telephone network as the LANCOM VoIP Router, i.e. users with the same area code as the public line for the LANCOM VoIP Router.

  In decentralized locations that extend beyond city or state boundaries, the physical location of the device is decisive, even if a central PBX is located at a different location. Therefore, for a LANCOM VoIP Router in London, all telephone subscribers in the local telephone network for London can be reached using local numbers, even if a SIP PBX connected via VPN can be reached in Manchester.

Depending on the settings for automatic outside line access ('Automatic outside line access' → page 13-9), a "0" prefix may be required.

- The **national and international numbers** behave in the same way as local numbers; here, the physical location of the devices is decisive for the assignment of corresponding access codes. Therefore, a LANCOM VoIP Router in Austria belongs to the national telephone network in Austria, even if there is a VPN connection to the SIP PBX at the headquarters in Germany.

Depending on the settings for automatic outside line access ('Automatic outside line access' → page 13-9), a "0" prefix may be required.

Special numbers

Certain special numbers (emergency numbers, toll-free or particularly expensive service numbers) can be subjected to special treatment by the call router.

- For example, this ensures that emergency numbers for the police or fire department are always secured, even if the subscribers do not dial the correct preceding dialing signal for outside line access.

  With the standard settings, the emergency numbers "110" and "112" are configured in such a way that they can be dialed correctly with or without the preceding "0".

- For toll-free numbers such as "0800", a direct connection via ISDN is usually selected in order to use the toll-free land-line to land-line connection.

Dialing using specific lines

With the LANCOM VoIP Router, other lines, in addition to the previously existing ISDN exchange lines, can be defined for voice communication, i.e. to a SIP PBX connected via VPN or to a public SIP provider via the Internet. Each time a connection is established, the call router decides which of the existing lines is to be used for the call based on pre-determined rules.

As an alternative to the automatic selection by the call router, you can direct individual calls to a certain line, for example when you want to call a party purposely via ISDN and not via the SIP PBX at the headquarters. For this purpose, the call router assigns specific code numbers to existing lines, such as "98" for ISDN or "97" for a SIP provider. The targeted call via this line is then initiated with the corresponding identifier:

- The call with "020 123456" is assigned to a corresponding line by the call router, e.g. via the SIP PBX at the headquarters.
- However, the call with "98 020 123456" is made directly via the ISDN connection by the call router.

13.3.6 Call hold, transfer call, connect call

LANCOM VoIP Routers support various services which are familiar to users of the ISDN network:

- With **call hold** the user can place an active call into a wait state. In this state, the user can for example make a call to another person.
- With **transfer call**, the user can switch to and fro between two connections. The user is only connected with one caller at a time, while the other caller is put on hold.
- With **connect call** the user switches an active call over to another call which is on hold. The two callers are then connected and the user is no longer involved in the call.

The services call hold, transfer call and connect call are available to all local SIP, ISDN and analog users, and also to subscribers at an upstream SIP PBX; however, they can only be initiated by a SIP user.

13.3.7 Transfer of DTMF tones

ISDN telephone networks introduced the possibility of transmitting information on which button was pushed on the telephone using DTMF tones (Dual Tone Multiple Frequency). With the help of DTMF tones, the telephone user can communicate with voice mailboxes and computer telephony systems, for example.

In VoIP applications, special mechanisms are required to assume the DTMF tone function. If, for example, during a telephone call, a button is pressed on a VoIP telephone or a VoIP softphone, this should trigger the same action as a call with an ISDN telephone.

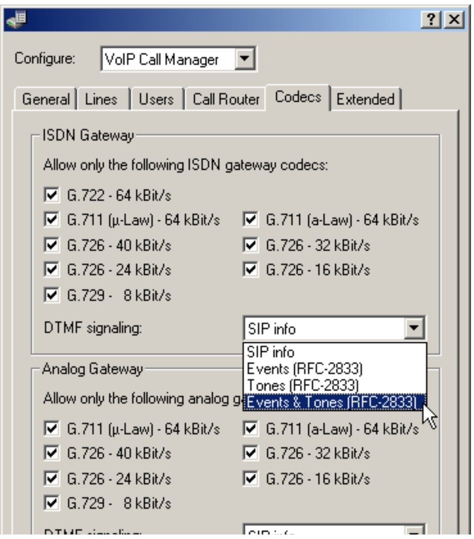
Generally, DTMF tones are transmitted in VoIP applications in one of two ways:

- In-band describes the transmission of the DTMF tones in the same data stream in which the voice data are transferred. However, this procedure is relatively unreliable because the DTMF tones in the IP datastream can easily be mistaken for voice data, particularly when using compression codecs.
- Out-of-band describes the transmission of the DTMF tones in a stream that runs parallel to the actual voice data. Two standards are generally used for out-of-band transmission:
  - SIP INFO (RFC 2976)
  - RC 2833 (RTP payload for DTMF digits)

  Both variations can wrap information, e.g. on buttons pressed, their tone frequency and the length of time the button was pressed into the signaling datastream. In addition, events that should be transmitted with DTMF tones can also be transmitted in cleartext in the SIP data.

DTMF signaling configuration

When configuring DTMF signaling, the type of transmission to be used for the DTMF tones must be set:



Configure: VoIP Call Manager

ISDN Gateway

Allow only the following ISDN gateway codecs:

☑ G.722 - 64 kBit/s
☑ G.711 (µ-Law) - 64 kBit/s ☑ G.711 (a-Law) - 64 kBit/s
☑ G.726 - 40 kBit/s ☑ G.726 - 32 kBit/s
☑ G.726 - 24 kBit/s ☑ G.726 - 16 kBit/s
☑ G.729 - 8 kBit/s

DTMF signaling: SIP info

Analog Gateway

Allow only the following analog g

☑ G.711 (µ-Law) - 64 kBit/s ☑ G.711 (a-Law) - 64 kBit/s
☑ G.726 - 40 kBit/s ☑ G.726 - 32 kBit/s
☑ G.726 - 24 kBit/s ☑ G.726 - 16 kBit/s
☑ G.729 - 8 kBit/s

LANconfig: VoIP Call Manager ▶ Extended

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ General

13.3.8 Transfer toll information to the internal ISDN buses

LANCOM VoIP Routers support two variants of the AOC (Advice Of Charge) service:

- AOC-D refers to the transmission of charge information during the call.
- AOC-E refers to the transmission of charge information at the end of the call.

LANCOM VoIP Routers transmit charge information from both types of AOC service between internal and external buses. AOC-D charge information can be converted into a metering pulse for analog users at the internal analog interfaces if the corresponding option has been activated.

13.3.9 Supporting digital calls

LANCOM VoIP Routers support digital calls, e.g. when using Group 4 fax machines or when using ISDN terminal equipment for dialing in to particular networks. To direct these calls over an ISDN interface of the LANCOM VoIP Router, destination numbers can be given special prefixes ('Dialing using specific lines' → page 13-11).

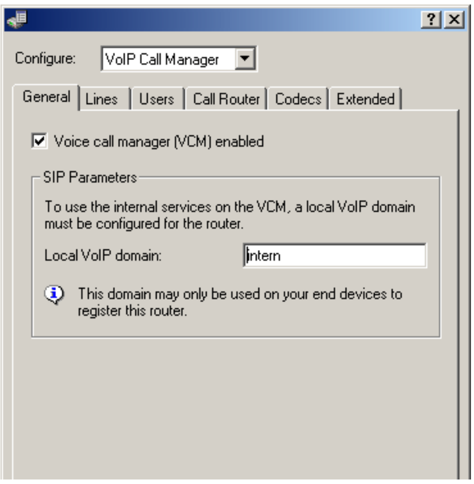
13.4 Configuration of VoIP parameters

Changes with LCOS 7.6:

- Entry of the following parameter for SIP, ISDN and analog users:
  - CLIR
- Entry of the following parameters for SIP providers and SIP-PBX lines:
  - Local port number
  - (Re-) registration
  - Line monitoring
  - Monitoring interval
  - Trusted
  - Privacy method
- Entry of the following parameters for analog lines:
  - Caller-ID signaling
  - Caller-ID transmission requirements

13.4.1 General settings

LANconfig: VoiP Call Manager ▶ General



☑ Voice call manager (VCM) enabled

SIP Parameters

To use the internal services on the VCM, a local VoIP domain must be configured for the router.

Local VoIP domain: intern

This domain may only be used on your end devices to register this router.

- **Voice Call Manager (VCM) activated**

  Switches the Voice Call Manager between active / not active

- **Domain**

  Name of the domain in which the connected telephones and the LANCOM Wireless Router are operated.

  - Terminal devices working in the same domain register as local subscribers at the LANCOM Wireless Router and make use of the SIP proxy.
  - Terminal devices working with the other domain of an active SIP PBX line register themselves as subscribers at an upstream PBX.

- **Create a SYSLOG message for each call**
  Each time a call is made with the LANCOM VoIP Router a SYSLOG message is created.

Please note that to use this function, the appropriate SYSLOG settings have to be made ('SYSLOG' → page 5-9).

- **Send an e-mail for each call**
  Each time a call is made with the LANCOM VoIP Router an e-mail is sent to the defined address.

Please note that to use this function, an SMTP account must have been set up.

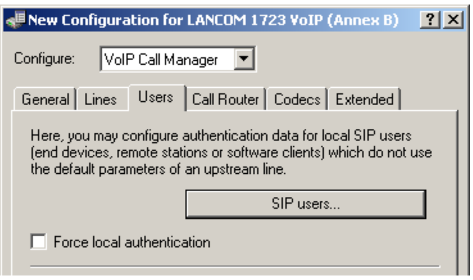
13.4.2 Configuration of users

Local users are the terminal equipment/telephones that are connected to the LANCOM VoIP Router. There is a difference between:

- SIP users: Users who are connected to the LAN by means of a SIP telephone. For the user configuration, it does not matter whether the LAN is connected directly to LANCOM, or whether it is connected via a VPN (over the Internet).
- ISDN users: Users who are connected by ISDN. They use the SIP gateway to telephone using the VoIP function.
- Analog users: Users who are connected via analog interfaces. They use the SIP gateway to telephone using the VoIP function.

General settings for all SIP users

LANconfig: VoiP Call Manager ▶ Users



Here, you may configure authentication data for local SIP users (end devices, remote stations or software clients) which do not use the default parameters of an upstream line.

□ Force local authentication

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ General

- **Force local authentication**
  The SIP proxy usually accepts a registration from all SIP users who register themselves with a valid domain. If local authentication is forced, only those subscribers who are saved in one of the user tables with relevant access information can register with the SIP proxy.

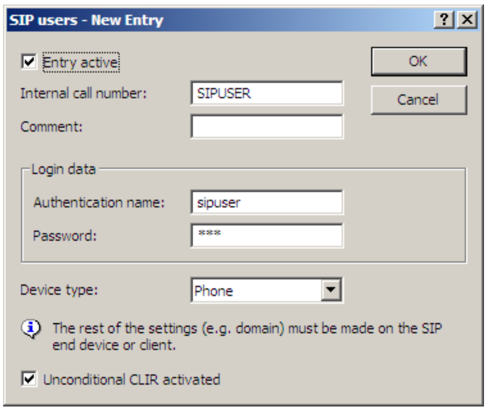
Automatic registration without entering a password is restricted to the SIP users in the LAN. SIP users from the WAN as well as ISDN and analog users must always be authenticated by a user entry with password.

SIP users

Depending on the model, different numbers of SIP users can be created. You cannot create more than the maximum number of users permitted; similarly, duplicate names or called numbers are not permitted.

The domain that is used by the SIP subscriber is usually configured in the terminal equipment itself.

LANconfig: VoiP Call Manager ▶ Users ▶ SIP users


SIP users - New Entry

☑ Entry active

Internal call number: SIPUSER

Comment:

Login data

Authentication name: sipuser

Password: ***

Device type: Phone

The rest of the settings (e.g. domain) must be made on the SIP end device or client.

☑ Unconditional CLIR activated

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ Users ▶ SIP users

The following parameters can be used to define a SIP user:

- **Number/Name**

  Telephone number of the SIP telephone or name of the user (SIP URI).

- **Auth-Name**

  Name for authentication at the SIP proxy, and also to any upstream SIP PBX when the user's domain is the same as the domain of a SIP PBX line. This name is required if registration is mandatory (e.g. when logging in to an upstream SIP PBX or when "Force local authentication" is set for local users).

- **Secret**

  Password for authentication to the SIP proxy, and also to any upstream SIP PBX, when the user's domain is the same as the domain of a SIP PBX line. It is possible for users to log in to the local SIP proxy without authentication ("Force local authentication" is deactivated for SIP users) and where applicable to an upstream SIP PBX using a shared password ("Standard password" on the SIP PBX line).

- **Device type**

  Type of device connected.

- **CLIR**

  Switches the transmission of the calling-line identifier on/off.

- **Active**

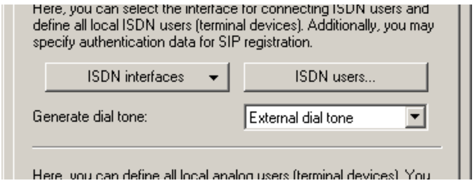
  Activates or deactivates the entry.

- **Comment**

  Comment on this entry

General settings for all ISDN users

LANconfig: VoiP Call Manager ▶ Users


Here, you can select the interface for connecting ISDN users and define all local ISDN users (terminal devices). Additionally, you may specify authentication data for SIP registration.

Generate dial tone: External dial tone

Here, you can define all local analog users (terminal devices). You

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ General

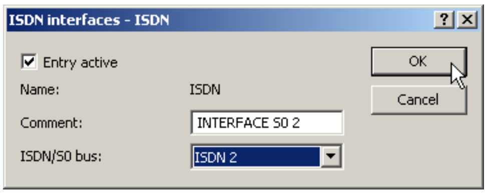
- **Generate dial tone**

  The dial tone determines the noise an ISDN user hears after lifting up the receiver. The "internal dial tone" is the same as the tone that a user hears at a PBX without spontaneous outside-line access (three short tones followed by a pause). The "external dial tone" is thus the same as the tone that indicates an external line when the receiver is lifted (constant tone without any interruptions). If necessary, adapt the dial tone for the users with spontaneous outside-line access to simulate the behavior of a standard outside line.

ISDN interfaces

For users who are connected by an ISDN line, the interface that is used is configured globally. An ISDN T interface (external) or even an ISDN TE interface (internal) can be configured. The latter is the case if users of an upstream PBX are to be managed as local users.

LANconfig: VoiP Call Manager ▶ Users ▶ ISDN interfaces



ISDN interfaces - ISDN

☑ Entry active

Name: ISDN

Comment: INTERFACE S0 2

ISDN/S0 bus: ISDN 2

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ Users ▶ Interfaces

- **ISDN interface**

  Interface to which the ISDN subscribers are connected.

- **Entry active**

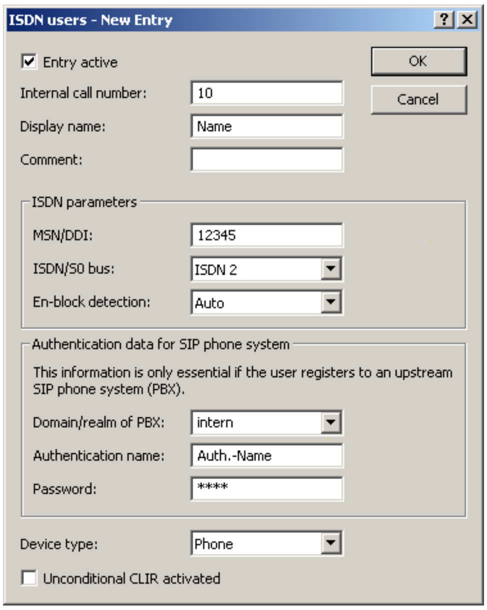
  Interface is active / not active.

- **Comment**

  Comment on the ISDN interface

ISDN users

LANconfig: VoiP Call Manager ▶ Users ▶ ISDN users



ISDN users - New Entry

☑ Entry active

Internal call number: 10

Display name: Name

Comment:

ISDN parameters

MSN/DDI: 12345

ISDN/S0 bus: ISDN 2

En-block detection: Auto

Authentication data for SIP phone system

This information is only essential if the user registers to an upstream SIP phone system (PBX).

Domain/realm of PBX: intern

Authentication name: Auth.-Name

Password: ****

Device type: Phone

☐ Unconditional CLIR activated

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ Users ▶ ISDN users

- **Number/Name**

  Internal number of the ISDN telephone or name of the user (SIP URI).

By using the # character as a placeholder, entire groups of numbers (e.g. when using extension numbers at a point-to-point connection) can be addressed via a single entry. With the number '#' and the DDI '#', for example, extension numbers can be converted into internal telephone numbers without making any changes. With the call number '3#' and the DDI '#', for example, an incoming call for extension '55' is forwarded to the internal number '355', and for outgoing calls from the internal number '377', the extension number '77' will be used.

User entries that use # characters to map user groups cannot be used for registration at an upstream PBX. This registration always demands a specific entry for the individual ISDN user.

- **Ifc**

  ISDN interface that should be used to establish the connection.

- **MSN/DDI**

  Internal MSN that is used for this user on the internal ISDN bus.

  - MSN: Number of the telephone connection if it is a point-to-multipoint connection.
  - DDI (Direct Dialing in): Telephone extension number if the connection is configured as a point-to-point line.

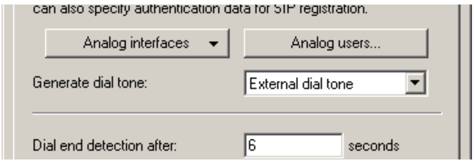
By using the # character as a placeholder, entire groups of call numbers, e.g. when using extension numbers, can be addressed via a single entry.

User entries that use # characters to map user groups cannot be used for registration at an upstream PBX. This registration always demands a specific entry for the individual ISDN user.

- **Auth-Name**
  Name for authentication at any upstream SIP PBX when the user's domain is the same as the domain of a SIP PBX line.
- **Display name**
  Name for display on the telephone being called.
- **Secret**
  Password for authentication as a SIP user at any upstream SIP PBX when the user's domain is the same as the domain of a SIP PBX line. It is possible for ISDN users to log in to an upstream SIP PBX using a shared password ("Standard password" on the SIP PBX line).
- **Domain**
  Domain of an upstream SIP PBX when the ISDN user is to be logged in as a SIP user. The domain must be configured for a SIP PBX line in order for upstream login to be performed.
- **Device type**
  Type of device connected.
- **DialCompl**
  En-block dial detection.
- **CLIR**
  Switches the transmission of the calling-line identifier on/off.
- **Active**
  Activates or deactivates the entry.
- **Comment**
  Comment on this entry.

General settings for all analog users

LANconfig: VoiP Call Manager ▶ Users


can also specify authentication data for SIP registration.

Generate dial tone: External dial tone

Dial end detection after: 6 seconds

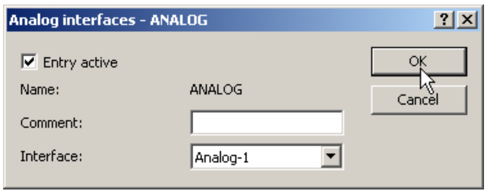
WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ General

- **Generate dial tone**
  The dial tone determines the noise an analog user hears after lifting up the receiver. The "internal dial tone" is the same as the tone that a user hears at a PBX without spontaneous outside-line access (three short tones followed by a pause). The "external dial tone" is thus the same as the tone that indicates an external line when the receiver is lifted (constant tone without any interruptions). If necessary, adapt the dial tone for the users with spontaneous outside-line access to simulate the behavior of a standard outside line.

Analog interfaces

The internal analog interfaces (a/b ports) require configuration if they are to be used by local users (connection of terminal equipment).

LANconfig: VoiP Call Manager ▶ Users ▶ Analog interfaces


Analog interfaces - ANALOG

☑ Entry active

Name: ANALOG

Comment:

Interface: Analog-1

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ Users ▶ Interfaces

- **Interface**

  An internal interface to which the analog subscribers are connected.

- **Entry active**

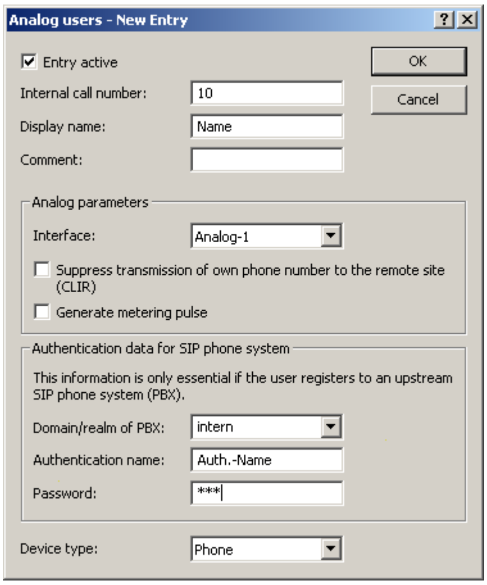
  Interface is active / not active.

- **Comment**

  Comment about analog interface

Analog users

LANconfig: VoiP Call Manager ▶ Users ▶ Analog users



Analog users - New Entry

☑ Entry active

Internal call number: 10

Display name: Name

Comment:

Analog parameters

Interface: Analog-1

☐ Suppress transmission of own phone number to the remote site (CLIR)

☐ Generate metering pulse

Authentication data for SIP phone system

This information is only essential if the user registers to an upstream SIP phone system (PBX).

Domain/realm of PBX: intern

Authentication name: Auth.-Name

Password: ***

Device type: Phone

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ Users ▶ Analog users

- **Number/Name**

  Internal number of the analog telephone or name of the user (SIP URI).

- **Auth-Name**

  Name for authentication at any upstream SIP PBX when the user's domain is the same as the domain of a SIP PBX line.

- **Display name**

  Name for display on the telephone being called.

- **Secret**

  Password for authentication as a SIP user to any upstream SIP PBX when the analog user's domain is the same as the domain of a SIP PBX line. It is possible for ISDN users to log in to an upstream SIP PBX using a shared password ("Standard password" on the SIP PBX line).

- **Ifc**

  Analog interface that should be used to establish the connection.

- **CLIR**

  Switches the transmission of the calling-line identifier on/off.

- **Metering pulse**

  The metering pulse is used in analog telephone networks to inform callers of the costs of their calls. With appropriate terminal equipment (e.g. telephone with charge display), the metering pulse is filtered out from the overall signal and this information is converted to display the call charge.

ⓘ This option allows the metering pulse to be passed on to the analog user/equipment. It is possible for charge information from the ISDN telephone network to be transferred to an ISDN line and converted into an analog metering pulse.

- **Domain**

  Domain of an upstream SIP PBX when the analog user is to be logged in as a SIP user. The domain must be configured for a SIP PBX line in order for upstream login to be performed.

- **Device type**

  Type of device connected.

The type determines whether an analog connection should be converted into SIP T.38, where applicable. Selecting "Fax" or "Telephone/Fax" activates fax signal recognition that could result in an impairment of the connection quality for telephones. Therefore please select the corresponding type of device connected in order to ensure optimum quality.

- **Active**

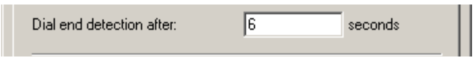
  Activates or deactivates the entry.

- **Comment**

  Comment on this entry

General settings for all SIP, ISDN and analog users

LANconfig: VoiP Call Manager ▶ Users



Dial end detection after: 6 seconds

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ General

- **Dial end detection after**

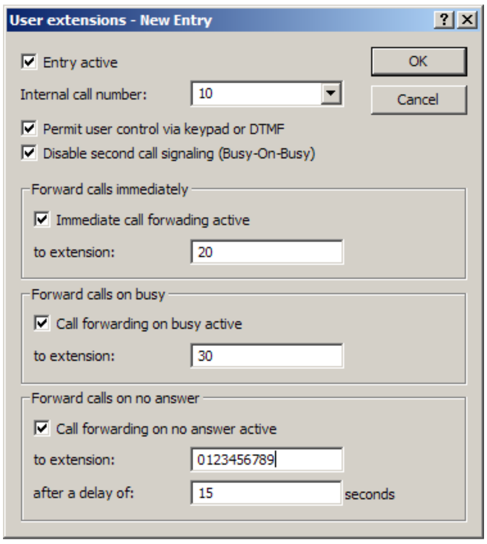
  When dialing from an ISDN telephone, this time period is waited until the called number is considered as complete and sent to the call router.

  Special values: With a dial delay of '0', a '#' has to be entered at the end of the called number. Entering the '#' character after the called number manually reduces the dial delay.

User settings

The following parameters are available for configuring user settings in the LANCOM:

LANconfig: VoiP Call Manager ▶ Users ▶ User settings



User extensions - New Entry

☑ Entry active

Internal call number: 10

☑ Permit user control via keypad or DTMF

☑ Disable second call signaling (Busy-On-Busy)

Forward calls immediately

☑ Immediate call forwarding active

to extension: 20

Forward calls on busy

☑ Call forwarding on busy active

to extension: 30

Forward calls on no answer

☑ Call forwarding on no answer active

to extension: 0123456789

after a delay of: 15 seconds

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ Users ▶ Extensions

- **Entry active**

  Activates or deactivates the entry.

- **Internal telephone number**

  The call forwarding applies to this telephone number or SIP-ID.

Call forwarding can be set up for all local users (SIP, ISDN or analog).

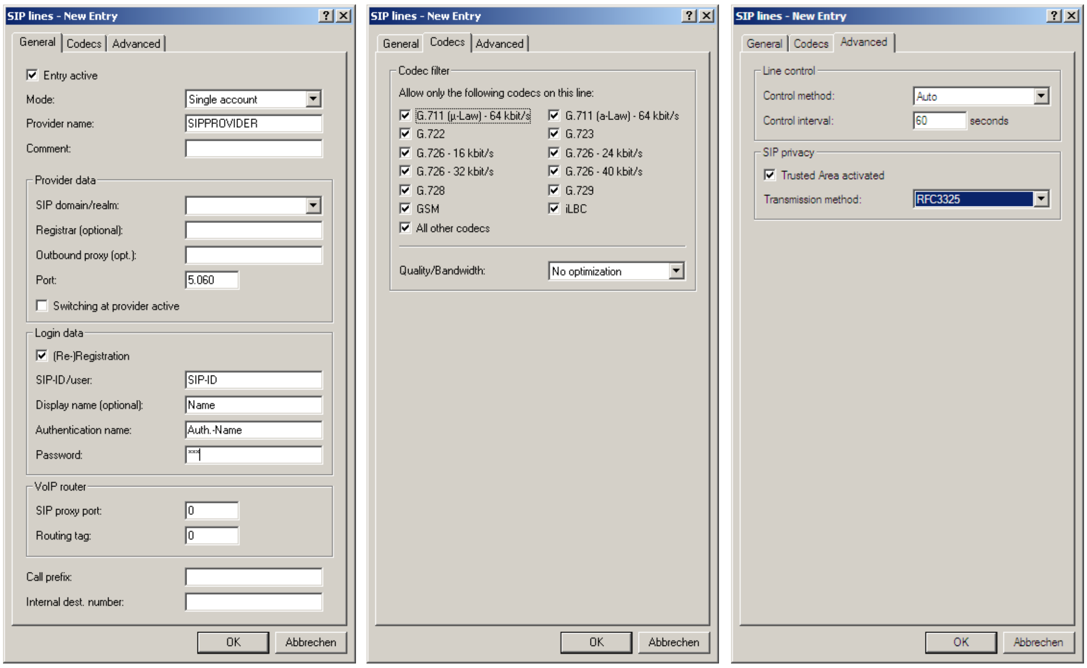
- **Enabling user control via keypad or DTMF**
  This activates or deactivates the option for users to configure their settings via the telephone.
- **Busy on busy**
  Prevents a second call from being connected to a terminal device, irrespective of whether CW (call-waiting indication) is active on the device or not; i.e. there is no "call waiting" signal. The second caller hears an engaged tone. This also applies where an internal telephone number supports multiple logins and just one of the possible terminal devices is already in use.
- **Call-forwarding unconditional (CFU)**
  Activates or deactivates the immediate forwarding of calls (CFU).
- **to number**
  Target for immediate unconditional call forwarding
- **Call-forwarding on busy (CFB)**
  Activates or deactivates call forwarding on busy.
- **to number**
  Target for call forwarding on busy.
- **Call forwarding, no reply (CFNR)**
  Activates or deactivates the delayed forwarding of call (after waiting for no reply).
- **to number**
  Target for call forwarding no reply.
- **Delay**
  Wait time for call forwarding on no reply. After this time period the call is forwarded to the target number if the subscriber does not pick up the phone.

13.4.3 Line configuration

SIP provider line

The device uses these lines to register with other SIP remote stations (usually SIP providers or remote gateways at SIP PBXs). The connection is made either over the Internet or a VPN tunnel.

LANconfig: VoIP Call Manager ▶ Lines ▶ SIP lines



☑ Entry active
Mode: Single account
Provider name: SIPPROVIDER
Comment:
Provider data
SIP domain/realm:
Registrar (optional):
Outbound proxy (opt.):
Port: 5.060
☐ Switching at provider active
Login data
☑ (Re-)Registration
SIP-ID/user: SIP-ID
Display name (optional): Name
Authentication name: Auth.-Name
Password: ***
VoIP router
SIP proxy port: 0
Routing tag: 0
Call prefix:
Internal dest. number:

Codec filter
Allow only the following codecs on this line:
☑ G.711 (µ-Law) - 64 kbit/s ☑ G.711 (a-Law) - 64 kbit/s
☑ G.722 ☑ G.723
☑ G.726 - 16 kbit/s ☑ G.726 - 24 kbit/s
☑ G.726 - 32 kbit/s ☑ G.726 - 40 kbit/s
☑ G.728 ☑ G.729
☑ GSM ☑ iLBC
☑ All other codecs
Quality/Bandwidth: No optimization

Line control
Control method: Auto
Control interval: 60 seconds
SIP privacy
☑ Trusted Area activated
Transmission method: RFC3325

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ Lines ▶ SIP provider

- **Name**
  Name of the line; may not be identical to another line that is configured in the device.
- **Mode**
  This selection determines the operating mode of the SIP line.

Possible values:

- Single account mode: Externally, the line behaves like a typical SIP account with a single public number. The number is registered with the service provider, the registration is refreshed at regular intervals (when (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number is replaced (masked) by the registered number. Incoming calls are sent to the configured internal target number. The maximum number of simultaneous connections is either set by the provider or it depends on the available bandwidth and the codecs being used.

  Table for number translation:

Single account	SIP number incoming to the line	SIP number sent from the line
Outgoing call	"From:"	The number registered at the provider (User ID)
Incoming call	"To:"	User ID

- Trunk mode: Externally, the line acts like an extended SIP account with a main external telephone number and multiple extension numbers. The SIP ID is registered as the main external number with the service provider and the registration is refreshed at regular intervals (when (re-)registration has been activated for this SIP provider line). For outgoing calls, the switchboard number acts as a prefix placed in front of each calling number (sender; SIP: "From:") . For incoming calls, the prefix is removed from the target number (SIP: "To:"). The remaining digits are used as the internal extension number. In case of error (prefix not found, target equals prefix) the call is forwarded to the internal target number as configured. The maximum number of connections at any one time is limited only by the available bandwidth.

  Table for number translation:

Trunk	SIP number incoming to the line	SIP number sent from the line
Outgoing call	"From:"	Switchboard number (User-ID) + "From:"
Incoming call	Switchboard number (User-ID) + "To:"	"To:" As internal extension

- Gateway mode: Externally the line behaves like a typical SIP account with a single public number, the SIP ID. The number (SIP ID) is registered with the service provider and the registration is refreshed at regular intervals (when (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number (sender) is replaced (masked) by the registered number (SIP ID in SIP: "From:") and transmitted in a separate field (SIP: "Contact:") . For incoming calls the dialed number (target) is not modified. The maximum number of connections at any one time is limited only by the available bandwidth.

  Table for number translation:

Gateway	SIP number incoming to the line	SIP number sent from the line
Outgoing call	"From:"	The number registered at the provider (User ID)
	"From:"	"Contact:"
Incoming call	"To:"	"To:"

- Link mode: Externally, the line behaves like a typical SIP account with a single public number (SIP ID). The number is registered with the service provider, the registration is refreshed at regular intervals (when (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number (sender; SIP: "From:") is not "From:") is not modified. For incoming calls, the dialed number (target; SIP: "To:") is not modified. The maximum number of connections at any one time is limited only by the available bandwidth.

  Table for number translation:

Link	SIP number incoming to the line	SIP number sent from the line
Outgoing call	"From:"	"From:"
Incoming call	"To:"	"To:"

- **Domain**

  SIP domain/realm of the upstream device. Provided the remote device supports DNS service records for SIP, this setting is sufficient to determine the proxy, outbound proxy, port and registrar automatically. This is generally the case for typical SIP provider services.

- **Rtg tag**

  Routing tag for selecting a certain route in the routing table for connections to this SIP provider.

- **Port**

  TCP/UDP port that the SIP provider uses as the target port for SIP packets.

ℹ This port has to be activated in the firewall for the connection to work.

- **User ID**

  Telephone number of the SIP account or name of the user (SIP URI).

ℹ For a SIP trunking account, the switchboard number is entered here. For incoming calls, any numerals after the switchboard number are interpreted as extension numbers (DDI) and these are passed to the call router. For outgoing calls, DDI numbers received from the call router are combined with the switchboard number.

This access data is used to register the line (single account, trunk, link, gateway), but not the individual local users with their individual registration details. If individual users (SIP, ISDN, analog) are to register with an upstream device using the data stored there or on the terminal device, then the line type "SIP PBX line" should be selected.

- **Auth-Name**

  Name for authentication to the upstream SIP device (provider/SIP PBX).

ℹ This access data is used to register the line (single account, trunk, link, gateway), but not the individual local users with their individual registration details. If individual users (SIP, ISDN, analog) are to register with an upstream device using the data stored there or on the terminal device, then the line type "SIP PBX line" should be selected.

- **Display name**

  Name for display on the telephone being called.

ℹ Normally this value should not be set as incoming calls have a display name set by the SIP provider, and outgoing calls are set with the local client or call source (which may be overwritten by the user settings for display name, if applicable). This settings is often used to transmit additional information (such as the original calling number when calls are forwarded) that may be useful for the person called.

In the case of single-line SIP accounts, some providers require an entry that is identical to the display name defined in the registration details, or the SIP ID (e.g. T-Online).

This access data is used to register the line (single account, trunk, link, gateway), but not the individual local users with their individual registration details. If individual users (SIP, ISDN, analog) are to register with an upstream device using the data stored there or on the terminal device, then the line type "SIP PBX line" should be selected.

- **Secret**

  The password for authentication at the SIP registrar and SIP proxy at the provider. For lines without (re-)registration, the password may be omitted under certain circumstances.

ℹ This access data is used to register the line (single account, trunk, link, gateway), but not the individual local users with their individual registration details. If individual users (SIP, ISDN, analog) are to register with an upstream device using the data stored there or on the terminal device, then the line type "SIP PBX line" should be selected.

- **Registrar**

  The SIP registrar is the point at the SIP provider that accepts the login with the authentication data for this account.

ℹ This field can remain empty unless the SIP provider specifies otherwise. The registrar is then determined by sending DNS SRV requests to the configured SIP domain/realm (this is often not the case for SIP services in a corporate network/VPN, i.e. the value must be explicitly set).

- **Outb-proxy**

  The SIP provider's outbound proxy accepts all SIP signaling originating from the LANCOM device for the duration of the connection.

ⓘ This field can remain empty unless the SIP provider specifies otherwise. The outbound proxy is then determined by sending DNS SRV requests to the configured SIP domain/realm (this is often not the case for SIP services in a corporate network/VPN, i.e. the value must be explicitly set).

- **Cln prefix**

  The call prefix is a number placed in front of the caller number (CLI; SIP "From:") for all incoming calls on this SIP provider line in order to generate unique telephone numbers for return calls.

  For example; a number can be added, which the call router analyzes (and subsequently removes) to select the line to be used for the return call.

- **Number/Name**

  The effect of this field depends upon the mode set for the line:

  - If the line is set to "Single account" mode, all incoming calls on this line with this number as the target (SIP: "To:") and transferred to the call router.
  - If the mode is set to "Trunk", the target number is determined by removing the trunk's switchboard number. If an error occurs, the call will be supplemented with the number entered in this field (SIP: "To:") and transferred to the call router.
  - If mode is set to "Gateway" or "Link" the value entered in this field has no effect.

- **Codecs**

  While the connection is being established, the terminal equipment negotiates the codecs that are to be used for voice-data compression. Use the codec filter to restrict the codecs that are permitted and to permit only certain codecs.

ⓘ If no common the codecs can be agreed upon, no connection is made.

- **Codec order**

  This parameter influences the order in which the codecs are presented during connection establishment.

- **Refer**

  Call switching (connect call) between two remote subscribers can be handled by the device itself (media proxy) or it can be passed on to the exchange at the provider if both subscribers can be reached on this SIP provider line (otherwise the media proxy in the LANCOM device assumes responsibility for switching the media streams, for example when connecting between two SIP providers).

ⓘ An overview of the main SIP providers supporting this function is available in the Support area of our Internet site.

- **Local port number**

  This is the port used by the LANCOM proxy to communicate with the provider.

ⓘ If line (re-)registration is deactivated, the local port has to be defined with a fixed value, and this also has to be entered at the provider end as the destination port (e.g. when using an unregistered trunk in the company VPN). This ensures that both ends can send SIP signaling.

- **(Re-) registration**

  This activates the (repeated) registration of the SIP provider line. Registration can also be used for line monitoring.

ⓘ To use (re-) registration, the line monitoring method must correspondingly be set to "Register" or "Automatic". Registration is repeated after the monitoring interval has expired. If the provider's SIP registrar suggests a different interval, the suggested value is used automatically.

- **Line monitoring**

  Specifies the line monitoring method. Line monitoring checks if a SIP provider line is available. The Call Router can make use of the monitoring status to initiate a change to a backup line. The monitoring method sets the way in which the status is checked.

  Possible values:

  - Auto: The method is set automatically.
  - Disabled: No monitoring; the line is always reported as being available. This setting does not allow the actual line availability to be monitored.

  - Register: Monitoring by means of register requests during the registration process. This setting also requires "(Re-)registration" to be activated for this line.
  - Options: Monitoring via Options Requests. This involves regular polling of the remote station. Depending on the response the line is considered to be available or unavailable. This setting is well suited for e. g. lines without registration.

- **Monitoring interval**

  The monitoring interval in seconds. This value affects the line monitoring with register request and also the option request. The monitoring interval must be set to at least 60 seconds. This defines the time period that passes before the monitoring method is used again. If (re-) registration is activated, the monitoring interval is also used as the time interval before the next registration.

ⓘ If the remote station responds to an option request with a different suggested value for the monitoring interval, this is accepted and subsequently applied.

- **Trusted**

  Specifies the remote station on this line (provider) as "Trusted Area". In this trusted area, the caller ID is not concealed from the caller, even if this is requested by the settings on the line (CLIR) or in the device. In the event of a connection over a trusted line, the Caller ID is first transmitted in accordance with the selected privacy policy and is only removed in the final exchange before the remote subscriber. This means, for example, that Caller ID can be used for billing purposes within the trusted area. This function is interesting for providers using a VoIP router to extend their own managed networks all the way to the connection for the VoIP equipment.

ⓘ Please note that not all providers support this function.

- **Privacy method**

  Specifies the method used for transmitting the caller ID in the separate SIP-header field.

- **Active**

  Activates or deactivates the entry.

- **Comment**

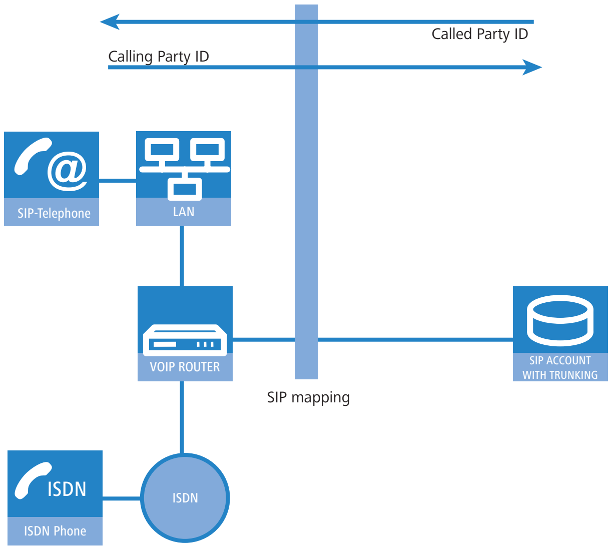
  Comment on this entry.

SIP mapping

The entries made under SIP mapping establish a series of rules for number translation to SIP lines in the trunk or gateway mode.

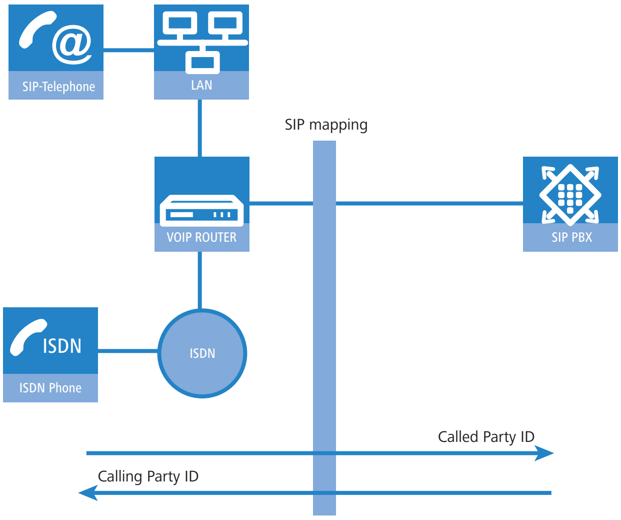
- A SIP line in trunk mode is used for mediating between internal numbers and the range of telephone numbers offered by a SIP account.
  - For incoming calls, the destination number (called party ID) is modified. The internal number is used if the called party ID matches with the external telephone number.
  - For outgoing calls, the calling party ID is modified. The external number is used if the calling party ID matches with the internal telephone number.

ⓘ For SIP mapping on trunk lines, only the extension (DDI) is mapped. The extension is interpreted as those numerals which follow the switchboard number (SIP ID or SIP line).

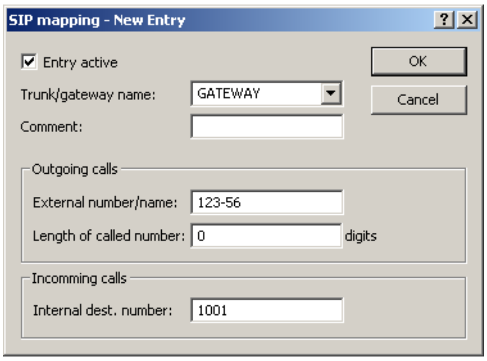


- For a SIP line in gateway mode, the telephone number plan of the upstream SIP PBX is adapted to the internal numbers in the call router.
  - For incoming calls (from the SIP line), the calling party ID is modified. The internal number is used if the calling party ID matches with the external telephone number.
  - For outgoing calls (to the upstream PBX), the destination number (called party ID) is modified. The external number is used if the called party ID matches with the internal telephone number.

For SIP mapping to gateway lines, the full telephone number is mapped.
Depending on the configuration, the call number arriving at the ISDN interface can be subjected to further mapping (ISDN mapping).



LANconfig: VoIP Call Manager ▶ Lines ▶ SIP mapping


SIP mapping - New Entry

☑ Entry active

Trunk/gateway name: GATEWAY

Comment:

Outgoing calls

External number/name: 123-56

Length of called number: 0 digits

Incomming calls

Internal dest. number: 1001

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ Lines ▶ SIP provider ▶ Mapping

- **Trunk/gateway name**

  Name of the line which is the target of the call number mapping.

- **Comment**

  Comment about this rule.

- **External number / name**

  Call number within the range of those used by the SIP trunk account or upstream SIP PBX.

- **Length of called number**

  This value defines the number of numerals required for a called number to be regarded as complete. It only applies to SIP gateway lines with entries that end in a # symbol.

  For an outgoing call, the external called number generated from this entry is automatically regarded as complete according to the defined number of numerals, and then forwarded. This process speeds up the dialing process. Alternatively, the called number is regarded as complete when:

  - The user concludes the dialed number with a # symbol, or
  - a precisely matching entry was found in the SIP mapping table without a # symbol, or
  - the wait time expires.

Setting the length of called number to '0' deactivates premature dialing from the length of called number.

- **Internal destination number**

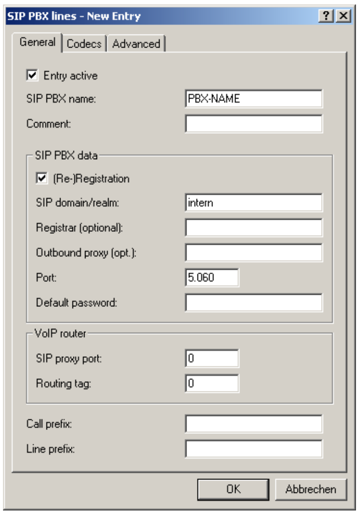
  Called number inside the range of the LANCOM VoIP Router.

Using the # symbol as a placeholder allows blocks of numbers to be captured by one rule.

SIP PBX line

These lines are used to configure connections to upstream SIP PBXs, which are usually connected via VPN.

LANconfig: VoIP Call Manager ▶ Lines ▶ SIP PBX lines



☑ Entry active

SIP PBX name: PBX-NAME

Comment:

SIP PBX data

☑ (Re-)Registration

SIP domain/realm: intern

Registrar (optional):

Outbound proxy (opt.):

Port: 5.060

Default password:

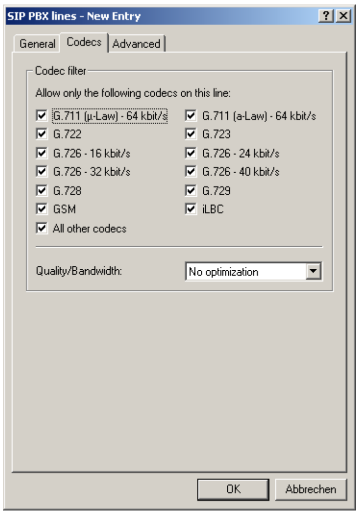
VoIP router

SIP proxy port: 0

Routing tag: 0

Call prefix:

Line prefix:



Codec filter

Allow only the following codecs on this line:

☑ G.711 (µ-Law) - 64 kbit/s ☑ G.711 (a-Law) - 64 kbit/s

☑ G.722 ☑ G.723

☑ G.726 - 16 kbit/s ☑ G.726 - 24 kbit/s

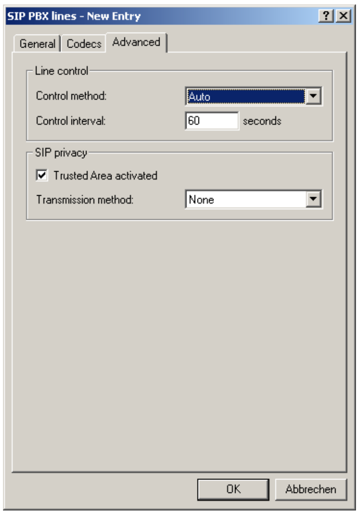
☑ G.726 - 32 kbit/s ☑ G.726 - 40 kbit/s

☑ G.728 ☑ G.729

☑ GSM ☑ iLBC

☑ All other codecs

Quality/Bandwidth: No optimization



Line control

Control method: Auto

Control interval: 60 seconds

SIP privacy

☑ Trusted Area activated

Transmission method: None

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ Lines ▶ SIP PBX

- **Name**

  Name of the line; may not be identical to another line that is configured in the device.

- **Domain**

  SIP domain/realm of the upstream SIP PBX.

- **Rtg tag**

  Routing tag for selecting a certain route in the routing table for connections to this SIP PBX.

- **Port**

  TCP/UDP port of the upstream SIP PBX to which the LANCOM device sends the SIP packets.

ⓘ This port has to be activated in the firewall for the connection to work.

- **Secret**

  Shared password for registering with the SIP PBX. This password is only required (a) when SIP subscribers have to log in to the PBX who have not been set up as SIP users with their own access data in the SIP user list or (b) when local SIP authentication is not forced. This means that SIP users can register with the LANCOM device without a password and can log in to the upstream SIP PBX with a shared password if the SIP user's domain is the same as the domain of a SIP PBX line.

- **Registrar**

  The SIP registrar is the point that accepts the login with the configured authentication data for this account in the SIP PBX.

- **Cln prefix**

  The call prefix is a number placed in front of the caller number (CLI; SIP "From:") for all incoming calls on this SIP PBX line in order to generate unique telephone numbers for return calls.

  For example; a number can be added, which the call router analyzes (and subsequently removes) to select the line to be used for the return call.

- **Line prefix**

  With outgoing calls using this line, this prefix is placed in front of the calling number to create a complete telephone number that is valid for this line. With incoming calls this prefix is removed, if present.

- **Codecs**

  While the connection is being established, the terminal equipment concerned negotiate which codecs are to be used to compress the voice data. Use the codec filter to restrict the codecs that are permitted and to permit only certain codecs.

ⓘ If no common the codecs can be agreed upon, no connection is made.

- **Codec order**

  This parameter influences the order in which the codecs are presented during connection establishment.

- **Local port number**

  This is the port used by the LANCOM proxy to communicate with the upstream SIP PBX.

ⓘ If line (re-)registration is deactivated, the local port has to be defined with a fixed value, and this also has to be entered into the SIP PBX to ensure that both ends can send SIP signaling.

- **(Re-) registration**

  This activates the (repeated) registration of the SIP PBX line. Registration can also be used for line monitoring.

ⓘ To use (re-) registration, the line monitoring method must correspondingly be set to "Register" or "Automatic". Registration is repeated after the monitoring interval has expired. If the SIP registrar in the SIP PBX suggests a different interval, the suggested value is used automatically.

- **Line monitoring**

  Specifies the line monitoring method. Line monitoring checks if a SIP PBX line is available. The Call Router can make use of the monitoring status to initiate a change to a backup line. The monitoring method sets the way in which the status is checked.

- **Monitoring interval**

  The monitoring interval in seconds. This value affects the line monitoring with register request and also the option request. The monitoring interval must be set to at least 60 seconds. This defines the time period that passes before the monitoring method is used again. If (re-) registration is activated, the monitoring interval is also used as the time interval before the next registration.

ⓘ If the remote station responds to an option request with a different suggested value for the monitoring interval, this is accepted and subsequently applied.

- **Trusted**

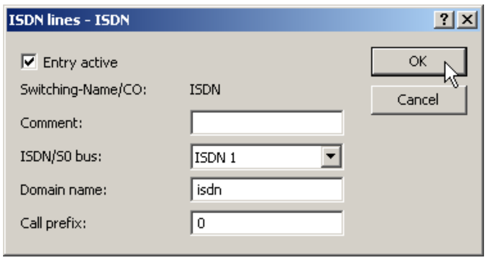
  Specifies the remote station on this line (provider) as "Trusted Area". In this trusted area, the caller ID is not concealed from the caller, even if this is requested by the settings on the line (CLIR) or in the device. In the event of a connection over a trusted line, the Caller ID is first transmitted in accordance with the selected privacy policy and is only removed in the final exchange before the remote subscriber. This means, for example, that Caller ID can be used for billing purposes within the trusted area. This function is interesting for providers using a VoIP router to extend their own managed networks all the way to the connection for the VoIP equipment.

Please note that not all providers support this function.

- **Privacy method**
  Specifies the method used for transmitting the caller information in the separate SIP field.
- **Active**
  Activates or deactivates the entry.
- **Comment**
  Comment on this entry.

ISDN lines

LANconfig: VoIP Call Manager ▶ Lines ▶ ISDN lines


ISDN lines - ISDN

☑ Entry active

Switching-Name/CO: ISDN

Comment:

ISDN/S0 bus: ISDN 1

Domain name: isdn

Call prefix: 0

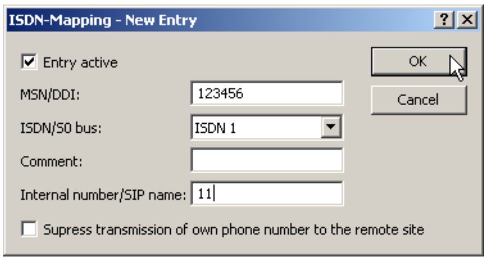
WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ Lines ▶ ISDN

- **Switching name/CO**
  Name of the line; may not be identical to another line that is configured in the device.
- **ISDN/S_0 bus, Ifc**
  ISDN interface(s) with which the LANCOM Wireless Router is connected to the ISDN network. The line entered here are usually configured as ISDN-TE.
- **Domain name, Domain**
  Domain in which the calls from/to the ISDN line are managed in LANCOM's SIP world.
- **Call prefix, Cln-Prefix**
  With incoming calls using this line, this prefix is placed in front of the calling number so that the correct line is automatically selected for a return call.
- **Entry active, Active**
  Line is active / not active.
- **Comment**
  Comment on the line

ISDN mapping

ISDN mapping assigns external ISDN telephone numbers (MSN or DDI) to the telephone numbers that are used internally.

LANconfig: VoIP Call Manager ▶ Lines ▶ ISDN mapping


ISDN-Mapping - New Entry

☑ Entry active

MSN/DDI: 123456

ISDN/S0 bus: ISDN 1

Comment:

Internal number/SIP name: 11

☐ Supress transmission of own phone number to the remote site

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ Lines ▶ ISDN ▶ Mapping

- **MSN/DDI**

  External telephone number of the connection in the ISDN network.

  For incoming calls that are directed to this number, the corresponding internal telephone number is entered as the destination number. For outgoing calls, this number is transmitted as the caller's number, unless this has been suppressed.

  - MSN: Number of the telephone connection
  - DDI (Direct Dialing in): Telephone extension number if the connection is configured as a point-to-point line.

By using the # character as a placeholder, entire groups of call numbers, e.g. when using extension numbers, can be addressed via a single entry.

- **ISDN/S$_0$ bus, Ifc**

  ISDN interface(s) used for connecting terminal devices to the LANCOM Wireless Router. These line have to be configured as ISDN-NT.

- **Telephone number/SIP name, Number/Name**

  Internal telephone number of the ISDN telephone or name of the user (SIP URL).

  For incoming calls, this is the SIP name or internal telephone number of the telephone to which the call from this interface is switched with the corresponding MSN/DDI. For outgoing calls, the SIP name is replaced by the MSN/DDI of the corresponding entry.

By using the # character as a placeholder, entire groups of call numbers, e.g. when using extension numbers, can be addressed via a single entry.

- **Hide your telephone number from the person called, CLIR**

  The display of your telephone number is suppressed so the person called cannot see it.

- **Entry active, Active**

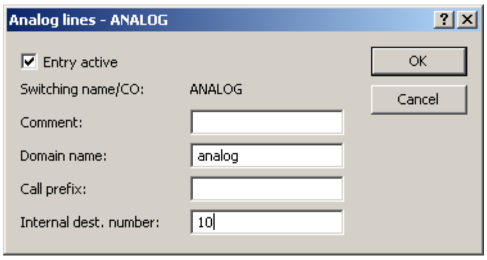
  External telephone number is active / not active.

- **Comment**

  Comment on the external telephone number.

Analog line

LANconfig: VoIP Call Manager ▶ Lines ▶ Analog lines



Analog lines - ANALOG

☑ Entry active

Switching name/CO: ANALOG

Comment:

Domain name: analog

Call prefix:

Internal dest. number: 10

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ Lines ▶ Analog

- **Name**

  Name of the line; may not be identical to another line that is configured in the device.

- **Domain**

  The analog line's domain name used for addressing in SIP.

- **Cln prefix**

  The call prefix is a number placed in front of the caller number (CLI; SIP "From:") for all incoming calls on this analog line in order to generate unique telephone numbers for return calls.

  For example; a number can be added, which the call router analyzes (and subsequently removes) to select the line to be used for the return call.

- **Number/Name**

  Internal number/SIP URI that each call on this analog line is given as call destination. This number can differ from the telco's actual call number for the analog connection (mapping).

Here you can, for example, enter the telephone number for a group that is to receive incoming calls. This allows you to flexibly control which telephones ring for incoming calls, or to transfer calls to a mobile phone number or answering machine after a certain time.

- **Active**

  Activates or deactivates the entry.
- **Comment**

  Comment on this entry.
- **Caller-ID signaling**

  Providers of analog telephone connections support various services including Caller ID transmission, i.e. the caller's number is shown in the display of the telephone being called. This service is also known as Calling Line Identification Presentation (CLIP). Depending on the country and provider, two different methods of modulation are used to transfer the caller ID over the analog line (FSK or DTMF).
- **Caller-ID transmission requirements**

  Apart from selecting the modulation method, different countries and providers also have different time delays in the signaling of the Caller ID over analog lines The telephone being called expects the Caller ID at a certain time, and so providers should set up their systems accordingly.

  Possible values:

  - □ Default: This setting causes the standard value for the country where the device is operated to be taken.
  - □ During ringing: The Caller ID is transmitted while the phone is ringing, between the first and second ring.
  - □ RP AS: Transmission of the Caller ID is not connected with the ringing but is transferred via a special "alarm signal". This alarm signal is a ringing impulse (Ringing Pulse Alerting Signal, RP-AS). The Caller ID can be transferred after the ringing impulse.
  - □ Line reversal: Transmission of the Caller ID is not connected with the ringing but is transferred via a special "alarm signal". The alarm signal is sent by a brief reversal of polarity in the line (line reversal). The Caller ID can be transferred after the line reversal.

13.5 Call Manager Configuration

The Call Manager manages and connects the various subscribers and lines described above with one other. The Call Manager's main task is to determine the correct target subscriber for each call and to select a suitable line for this subscriber. To be able to meet this task, the Call Manager mainly uses two table areas:

- The call routing table
- The tables of local subscribers

As the Call Manager usually switches between internal and external telephone networks with different number ranges, the Call Manager often has to change the numbers that are called, and this is known as number translation.

In the world of VoIP telephony, both numbers and names (such as "anyone@company.com") can be used. Although the following description refers to telephone numbers, this also includes telephone names unless specified otherwise.

The procedure known from internal extension lines is used, whereby connections to external subscribers start with a preceding "0". The Call Manager processes calls to and from all registered subscribers and lines.

13.5.1 Process of call routing

The calls are switched in the following steps:

- Processing the calling number (Calling Party ID)

  First of all there is a check to see whether a numeric or alphanumeric number is available. Typical dialing separators such as "()-/" and <blank> are removed. A leading "+" is left in place. In this case, the number is still treated as a numeric number. If the check reveals any other alphanumerical character, the number is treated as alphanumeric and remains unchanged.
- Resolving the call in the call routing table

  After processing the Called Party ID, the call is passed over to the call-routing table. The entries in the call routing table consist of records of conditions and instructions ('Call-routing table parameters' → page 13-32). The entries are searched through and the first one that satisfies **all** of the conditions is executed.
- Resolution of the call with tables of local subscribers

If no entry is found in the call-routing table, then the Call Manager searches through the list of local subscribers. If an entry is found here matching the number that is called, and that also has the appropriate destination domain, then the call is delivered to the corresponding subscriber.

If no local subscriber is found for whom the number and destination domain match, another pass is made where it suffices for the telephone number of the local subscriber to match the called number; the destination domain is not considered.

- Resolution of the call with default entries in the call-routing table

  If the previous passes through the call routing table and the lists with the local subscribers were unsuccessful, the call is checked again in the call routing table. This pass only takes the default routes into account, however. It does not include the numbers and destination domains that were entered in the default routes. Only the source filters are processed, assuming that the default routes has these filters.

The procedure described here only considers the call numbers as processed by the Call Router. Mapping to the ISDN or SIP line can also alter the number.

13.5.2 Handling the calling party ID

The configuration options for the call router offer numerous options for manipulating the telephone numbers that are used to establish the connection. The call router usually connects different "telephone worlds" (internal and external, SIP and ISDN) that use completely different telephone number ranges. So that the subscribers can communicate successfully with each other, the telephone numbers at the interfaces have to be configured in such a way that, on the one hand, the required subscriber is reached via the correct line and, on the other hand, a return call (automatically upon "engaged", where applicable) can be placed successfully. To enable this return call, the calling number (calling party ID) has to be **after** the processing by the Call Manager, directly before it is delivered to the relevant subscriber.

Handling outgoing calls

The telephone numbers of outgoing calls are converted depending on the line that is used:

- SIP lines

  The treatment of the calling-party ID on SIP lines depends upon the line's operating mode:

  - Single account: In the case of an outgoing call over a SIP line, the calling party ID is converted to the number that was entered for the SIP line (SIP ID).
  - Trunk and gateway: Please observe the information in section 'SIP mapping' → page 13-24.

- SIP PBX lines

  In the case of an outgoing call over a SIP PBX line, the subscriber is registered at the upstream SIP PBX and is part of the telephone number range there. This is why the calling party ID—which represents the internal telephone number or "extension" of the subscriber in this case—is passed unchanged to the SIP PBX line.

- ISDN lines

  In the case of an outgoing call over an ISDN point-to-multipoint connection, the calling party ID is converted to the MSN that is entered for the subscriber (or the internal telephone number) in the ISDN mapping table.

  If this does not contain an entry for the number that is currently calling, no calling party ID is sent. Similarly, no calling party ID is sent if CLIR (Calling Line Identifier Restriction) is activated.

Handling incoming calls

The telephone numbers of incoming calls are converted differently depending on the SIP or ISDN subscriber criteria and whether automatic outside line access is active or not.

The calling party ID is changed depending on the following parameters:

- The prefix ("call prefix" or "Cln-Prefix") that is stored for the **line** (default: <blank>).
- The prefix for internal connections with destination ISDN users ("internal ISDN prefix" or "Intern-Cln-Prefix" - default: '99').
- The prefix for internal connections with destination SIP users ("internal SIP prefix" or "Intern-Cln-Prefix" - default: '99').
- The prefix for external connections with destination ISDN users ("external ISDN prefix" or "Extern-Cln-Prefix" - default: <blank>).
- The prefix for external connections with destination SIP users ("external SIP prefix" or "Extern-Cln-Prefix" - default: <blank>).

The activation of automatic outside line access is taken into account by configuring the prefixes appropriately:

- If automatic outside line access is activated, the internal prefixes are typically set to the dial character that is used to reach the internal subscriber, usually '99' or '*'.
- Without automatic outside line access, the external prefixes are typically set to '0'.

The calling party ID is only extended if the incoming call has a calling party ID. If the calling party ID is blank, no prefix is attached.

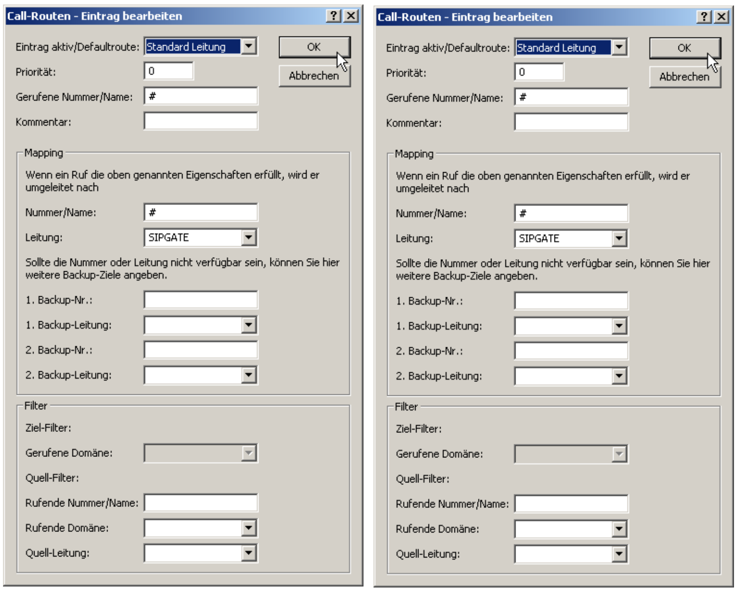
It is changed as follows:

- With internal connections, the internal subscriber prefix (SIP or ISDN) is placed in front of the calling party ID.
- With external connections, depending on the (line) call prefix, the following decision is made:
  - (Line) call prefix blank: The external subscriber prefix (SIP or ISDN) is placed in front of the calling party ID.
  - (Line) call prefix not blank: The internal subscriber prefix (SIP or ISDN) **and** the (line) call prefix is placed in front the calling party ID.

> A call is regarded as external if it comes from a "line". If this line is a SIP PBX line, then the call is only external if the incoming calling party ID is preceded by a "0".

13.5.3 Call-routing table parameters

LANconfig: VoiP Call Manager ▶ Call router



Eintrag aktiv/Defaultroute: Standard Leitung
Priorität: 0
Gerufene Nummer/Name: #
Kommentar:

Mapping
Wenn ein Ruf die oben genannten Eigenschaften erfüllt, wird er umgeleitet nach
Nummer/Name: #
Leitung: SIPGATE
Sollte die Nummer oder Leitung nicht verfügbar sein, können Sie hier weitere Backup-Ziele angeben.
1. Backup-Nr.:
1. Backup-Leitung:
2. Backup-Nr.:
2. Backup-Leitung:

Filter
Ziel-Filter:
Gerufene Domäne:
Quell-Filter:
Rufende Nummer/Name:
Rufende Domäne:
Quell-Leitung:

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ Call router

An entry in the call routing table consists of:

- Conditions that have to be met so that the entry is "considered" appropriate. This includes:
  - Information about which subscriber is to be called; called number/name (Called Party ID), called domain (if appropriate).
  - Information about the calling subscriber; calling number/name, calling domain, source line through which the call enters LANCOM VoIP Router.
- Instructions regarding the procedure for the call:
  - How is the telephone number converted and changed for further processing?
  - Which line should used to place the call (destination line)?
  - Which backup lines should be used if the destination line is not available?

The entries are searched row by row; the first suitable entry is performed. This is why the special entries should be configured first of all, then the general entries.

If an entry is found in the call routing table with the destination line "RESTART", then the complete pass starts again with the new, converted called party ID. The entry for the source line (calling line) is deleted for the next pass.

Both the call routing table and the local subscriber table can contain and process alphanumeric names where this makes sense.

- **Active entry/default route, active**

  The routing entry can be activated, deactivated, or marked as a default entry. All calls that can be resolved using the first passes but not using the call routing table or local subscriber table are then automatically resolved using these default entries. You can use any destination name and destination domain; only the source filters that are set are considered

- **Priority of the entry, Prio**

  The Call Manager sorts all entries with the same priority automatically, so that the table can be processed through logically from top to bottom. With some entries, however, the sequence of the entries has to be specified (for the telephone number translation, for example). The entries with the highest priority are automatically sorted to the top.

- **Called number/name, Called ID**

  The called party name or destination telephone number (without domain information) that is called.

  The # character is used as a placeholder for any character strings. All characters in front of the # are removed, the remaining characters are used in the "Number/name" field instead of the # character to further establish the connection.

  Example: The call routing table contains entry '00049#' as the called number/name and '00#' as the number/name. For all calls with a preceding '0' for outside-line access and the complete dialing code for Germany, only the leading '0' for the outside-line access and the leading '0' for the local area dialing code are retained as the number/name; the country ID is removed. So '00049 2405 123456' becomes '0 02405 123456'.

  Independently of this, an alphanumeric number can also be specified.

- **Number/name, Dest-ID**

  This telephone number is used to continue with establishing the connection. If no connection can be established using this telephone number and the corresponding line, then the backup telephone numbers with their associated lines are used

  At least one of "Number/name", "1st backup no." or "2nd backup no." has to be filled in. They are evaluated in this sequence. A blank field is skipped.

- **Line, Dest-Line**

  The connection is established using the destination line. Normal destination lines can be:

  □ ISDN

  □ All defined SIP lines.

  The following special functions can be entered as a destination line:

  □ REJECT highlights a blocked telephone number.

  □ USER forwards the call to local SIP or ISDN subscribers.

  □ RESTART starts a new pass through the call routing table with the previously formed "number/name". The former "source line" is deleted.

This field has to be completed, otherwise the entry is not used.

- **2. Number, Dest-ID-2**

  This telephone number is used to establish the connection further if nothing is entered in "number/name" or the corresponding "line" is not available. If no connection can be established using this telephone number and the corresponding line, then the third telephone number and the third line is used.

- **2. Line, Dest-Line-2**

  The connection is established using this line if the second number is used to establish the connection. The same lines can be dialed as for "line".

- **3. Number, Dest-ID-3**

  Similar to the second number.

- **3. Line, Dest-Line-3**

  Similar to the second line.

- **Called domain, Cld Domain**

  This entry filters the called domain, the "Called Party Domain". The call router entry is only considered to match if the Called Party Domain for the call matches the domain that is entered here. If nothing is specified, any destination domain is accepted.

  The following can be entered as called domains:

  □ ISDN

  □ The internal VoIP domain of LANCOM Wireless Router.

  □ All domains entered for the SIP and SIP-PBX lines.

- **Calling number/name, Calling ID**

  This entry filters the calling number/name, the "calling party ID". It is specified as an internal number or as a national or international telephone number. The domain is not specified. No "0" or other character for a line ID is prefixed; the ID is used as if it comes from the line or from internal telephone calls.

  The call router entry is only evaluated as matching if the Calling Party ID for the call matches the number that is entered here. After "#", any characters can be accepted. If nothing is specified here, any Calling Party ID is accepted.

  The following special functions can be entered as a calling number:

  - LOCAL restricts to internal telephone numbers (without a leading "0").
  - EMPTY can be used for Calling Party IDs that are not specified.

- **Calling domain, Cln Domain**

  This entry filters the calling domain. The call router entry is only considered to match if the Calling Domain for the call matches the domain that is entered here. If nothing is specified, each calling domain is accepted.

  The following can be entered as calling domains:

  - ISDN
  - The internal VoIP domain of LANCOM Wireless Router.
  - All domains entered for the SIP and SIP-PBX lines.

  SIP telephones usually have several line keys, for which different domains can be configured. With this filter, telephone calls are handled depending on the selection that is made using different line keys.

- **Source line, Src-Line**

  This entry filters the source line. The call router entry is only considered to match if the source line for the call matches the line that is entered here. If nothing is specified, any calling line is accepted.

  The following can be entered as the source line:

  - USER.ISDN for calls from a local ISDN subscriber
  - USER.SIP for calls from a local SIP subscriber
  - USER# for calls from a local subscriber in general
  - All ISDN, SIP and SIP-PBX lines that are entered.

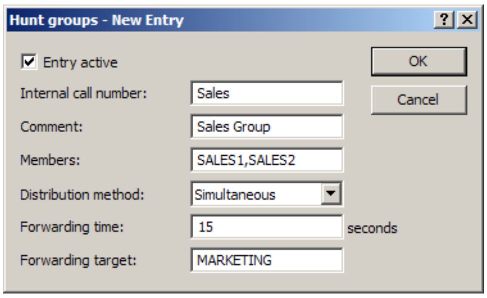
- **Comment**

  Comment on the current routing entry

Hunt-group functions

The following parameters are available in the LANCOM for configuring hunt-group functions:

LANconfigVoIP Call Manager ▶ Call router ▶ Hunt groups



☑ Entry active

Internal call number:	Sales
Comment:	Sales Group
Members:	SALES1,SALES2
Distribution method:	Simultaneous
Forwarding time:	15 seconds
Forwarding target:	MARKETING

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ Groups

- **Entry active**

  Activates or deactivates the entry.

  - Default: Active

- **Internal telephone number**

  The hunt group is available under this telephone number or SIP-ID.

  - Possible values: Maximum 64 alphanumerical characters.

The names of hunt groups may not coincide with the names of users (SIP, ISDN, analog).

- **Comment**

  Comment on the defined entry (64 characters)

- **Members**

  Comma-separated list of the members of the hunt group. Members can be users, hunt groups or external telephone numbers, and so there is no limit on scaling.

  - □ Possible members: Users, hunt groups, external telephone numbers
  - □ Possible values: Maximum 128 alphanumerical characters.

A hunt group may not contain itself or any parents in the hierarchical system—recursion through user entries is not possible. However, loops to parents in the structure can be set up via the 'Forwarding target' → page 13-35.

- **Forwarding method**

  Set the type of call distribution:

  - □ Simultaneous: The call is signaled to all group members at once. If a member picks up the call within the call-forwarding time, the call is no longer signaled to other group members. If nobody accepts the call within the forwarding time, then the call is switched to its forwarding target.
  - □ Sequential: The call is directed to one member of the group after the other. If a group member does not accept the call within the forwarding time, then the call is switched to the next member of the group. If nobody in the group accepts the call within the forwarding time, then the call is switched to its forwarding target.

- **Forwarding time**

  If an incoming call is not picked up by a group member within the forwarding time, then the call is forwarded according to the distribution method selected:

  - □ In case of simultaneous call distribution, the call is forwarded to the forwarding target.
  - □ In case of sequential call distribution, the call is forwarded to the next group member in line. If the group member is the last one, then the call is redirected to its forwarding target.
  - □ Possible values: Max. 255 seconds.
  - □ Default: 0 seconds
  - □ Significant values: 0 seconds. The call is forwarded immediately to the forwarding target (temporarily jumps a hunt group in a hierarchy).

If all members of the group are busy or unavailable, then the call is redirected to the forwarding target without waiting for the forwarding-time to expire.

- **Forwarding target**

  If none of the group members accepts the call within the forwarding time, then the call is switched to the forwarding target entered here. Forwarding targets can be users, hunt groups or external telephone numbers. Only one forwarding target can be entered.

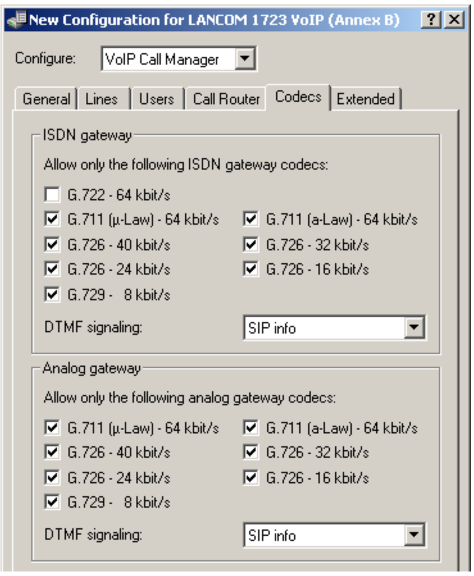
  - □ Possible targets: Users, hunt groups, external telephone numbers
  - □ Possible values: Maximum 64 alphanumerical characters.

If no forwarding target is defined, then the call is rejected as soon as the member list has been worked through, or if all members are busy or unavailable.

The forwarding target only becomes active once the group's forwarding time has expired or if no members are available. Here, too, redirection to a higher level of the hunt-group structure is possible, unlike with the 'Members' → page 13-35 entry.

13.5.4 Codecs

LANconfig: VoiP Call Manager ▶ Codecs



New Configuration for LANCOM 1723 VoIP (Annex B)

Configure: VoIP Call Manager

ISDN gateway

Allow only the following ISDN gateway codecs:

- □ G.722 - 64 kbit/s
- ☑ G.711 (µ-Law) - 64 kbit/s
- ☑ G.711 (a-Law) - 64 kbit/s
- ☑ G.726 - 40 kbit/s
- ☑ G.726 - 32 kbit/s
- ☑ G.726 - 24 kbit/s
- ☑ G.726 - 16 kbit/s
- ☑ G.729 - 8 kbit/s

DTMF signaling: SIP info

Analog gateway

Allow only the following analog gateway codecs:

- ☑ G.711 (µ-Law) - 64 kbit/s
- ☑ G.711 (a-Law) - 64 kbit/s
- ☑ G.726 - 40 kbit/s
- ☑ G.726 - 32 kbit/s
- ☑ G.726 - 24 kbit/s
- ☑ G.726 - 16 kbit/s
- ☑ G.729 - 8 kbit/s

DTMF signaling: SIP info

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ General ▶ ISDN gateway codecs

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ General ▶ Analog gateway codecs

- **ISDN gateway**

  During connection establishment, the ISDN terminal devices negotiate which codecs are to be used to compress the voice data. Use the codec filter to restrict the codecs that are permitted and to permit only certain codecs.

- **Analog gateway**

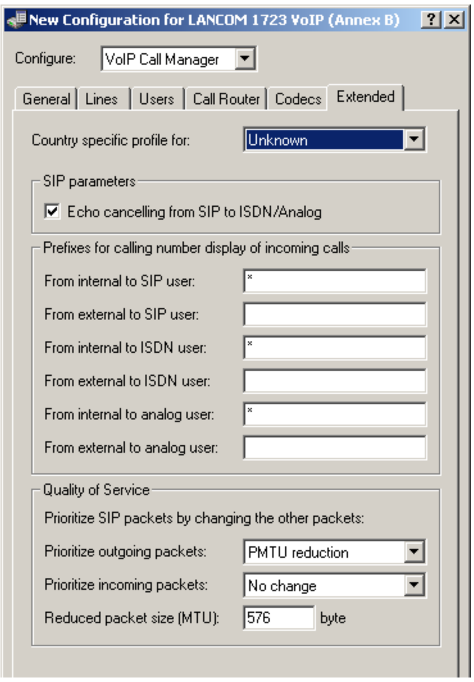
  Use the codec filter to restrict the codecs that are permitted for analog terminal equipment and to permit only certain codecs.

- **DTMF signaling**
  - SIP info: Transmits the DTMF tones according to the SIP info standard
  - Events (RFC 2833): Transmits the events in cleartext according to the RFC 2833 standard
  - Tones (RFC 2833): Transmits the tones according to the RFC 2833 standard
  - Events&tones (RFC 2833): Transmits the events in cleartext and tones according to the RFC 2833 standard

The DTMF signaling settings must match the SIP provider requirements. Defective DTMF signaling settings could make it impossible to establish a connection via the SIP provider.

13.5.5 Extended settings

LANconfig: VoiP Call Manager ▶ Extended



New Configuration for LANCOM 1723 VoIP (Annex B)

Configure: VoIP Call Manager

Country specific profile for: Unknown

SIP parameters

☑ Echo cancelling from SIP to ISDN/Analog

Prefixes for calling number display of incoming calls

From internal to SIP user: *

From external to SIP user:

From internal to ISDN user: *

From external to ISDN user:

From internal to analog user: *

From external to analog user:

Quality of Service

Prioritize SIP packets by changing the other packets:

Prioritize outgoing packets: PMTU reduction

Prioritize incoming packets: No change

Reduced packet size (MTU): 576 byte

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ General ▶ ISDN gateway codecs

- **Echo canceling from SIP to ISDN**

  Activates the echo canceling of remote echoes. With an echo that is too strong, subscribers can hear their own voices after a short delay. Activating this option reduces the ISDN echo at the SIP > ISDN gateway.

- **Prefix from internal to SIP user**

  This prefix is added to the calling party ID, if available, for an incoming, **internal** call if the call is directed to a SIP user.

A call is regarded as external if it comes from a "line". If this line is a SIP PBX line, then the call is only external if the incoming calling party ID is preceded by a "0". All other calls are regarded as internal.

For more information about handling the calling party ID, see 'Handling the calling party ID' → page 13-31.

- **Prefix from external to SIP user**

  This prefix is added to the calling party ID, if available, for an incoming, **external** call if the call is directed to a SIP user.

- **Prefix from internal to ISDN user**

  This prefix is added to the calling party ID, if available, for an incoming, **internal** call if the call is directed to an ISDN user. If a line prefix is defined, this is placed in front of the whole of the called number.

- **Prefix from external to ISDN user**

  This prefix is added to the calling party ID, if available, for an incoming, **external** call if the call is directed to an ISDN user. If a line prefix is defined, this is placed in front of the whole of the called number.

- **Prefix from internal to analog user**

  This prefix is added to the calling party ID, if available, for an incoming, **internal** call if the call is directed to a analog user. If a line prefix is defined, this is placed in front of the whole of the called number.

- **Prefix from external to analog user**

  This prefix is added to the calling party ID, if available, for an incoming, **external** call if the call is directed to a analog user. If a line prefix is defined, this is placed in front of the whole of the called number.

- **Prefer outgoing packets**

  Depending on the audio codec that is used for SIP calls, sufficient bandwidth through the firewall is reserved (provided sufficient bandwidth is available). To control the firewall, you can configure how the remaining data packets that do not belong to the SIP data stream are handled.

  ▷ **PMTU reduction**

  The subscribers of the data connection are informed that they should only send data packets up to a certain length (Path Maximum Transmission Unit, PMTU).

- ▷ **Fragmentation**

  The LANCOM Wireless Router reduces the data packets by fragmenting them to the required length.
- ▷ **No change**

  The length of the data packets is not changed by the VoIP operation.

For more information, see the description of PMTU and fragmenting with regard to quality of service ('Reducing the packet length' → page 9-5).

- **Prefer incoming packets**

  Similar to the outgoing data packets, you configure how non-VoIP data packets are handled when bandwidth is reserved for SIP data.

  - ▷ **PMTU reduction**

    The subscribers of the data connection are informed that they should only send data packets up to a certain length (Path Maximum Transmission Unit, PMTU).
  - ▷ **No change**

    The length of the data packets is not changed by the VoIP operation.
- **Reduced packet size**

  This parameter specifies the packet size that should be used for PMTU adjustment or fragmentation while the SIP data have priority.

13.6 PBX functions for LANCOM VoIP Router

LANCOM VoIP Routers can provide small companies or subsidiaries with all of the functions of a classical private branch exchange (PBX).

- Telephony functions such as call hold, swap, connect or transfer
- Hunt group function with flexible call distribution and cascading of hunt groups
- Multiple logins to use various telephones under one telephone number

! Please note that the extent to which features such as connect call and automatic call transfer (redirection) are supported by SIP providers can differ enormously. It is impossible to guarantee that this function will work properly with all combinations of SIP devices and SIP providers. We recommend that you use LANCOM VP-100 and LANCOM Advanced VoIP Client terminal equipment.

13.6.1 Connect and forward call

The integration of SIP telephones and VoIP routers into existing telephone structures means that we have to take a fresh look at familiar functions such as transferring calls. Call transfer means that a call that has already been placed (routed) is redirected to a new destination either spontaneously by the user (connect call) or by automatic call forwarding set up in advance. SIP-based VoIP telephony uses processes which are fundamentally different to technologies used until now. For example, ISDN and analog terminal devices require a telephone exchange that usually has to continue to manage the connection after transfer. SIP telephones can transfer calls without any need of a telephone exchange: The devices make a connection over the shortest possible route and the call router stops its management function immediately after the connection has been established. The SIP exchange is also able to handle signaling over SIP and the actual data transfer over RTP in different ways.

Due to the differences arising from the various types of terminal device, the easiest way to understand call transfer in a LANCOM VoIP Router is to consider different scenarios and to explain the terminology.

Active and passive transfer

When looking at the technical details, it is important to consider the end from which call transfer is initiated. "Local" users are all SIP, ISDN or analog users who are accessible via the LANCOM VoIP Router in their own LAN. "External" users are those accessible via a line (SIP account, SIP trunk, SIP PBX, ISDN or analog).

- Active: A local subscriber initiates call transfer
- Passive: An external subscriber initiates call transfer

Call transfer with and without consulting

A subscriber transferring a call can either directly hand over an active call to a third subscriber (unattended call transfer), or a separate call can be made to a third subscriber to communicate the call and then transfer it (attended call transfer).

Charges for calls when transferring to external users

The transfer of a call from an external caller to a third party who is also external carries the risk that charges will arise for the ongoing call, even though the initiating subscriber has ended the call.

The LANCOM VoIP Router's job during call transfer

Irrespective of the terminal devices involved in the call transfer, a LANCOM VoIP Router can take over a variety of tasks:

- Passthrough: Both subscribers in the call transfer are on the same side of the connection, e.g. transfer from a local to a local subscriber.
- Delegate: The call transfer is not handled by the LANCOM VoIP Router itself but by an upstream exchange, e.g. in a VoIP PBX that is accessible via a PBX line.
- Switching: The LANCOM VoIP Router handles the signaling and the data transfer between subscribers.

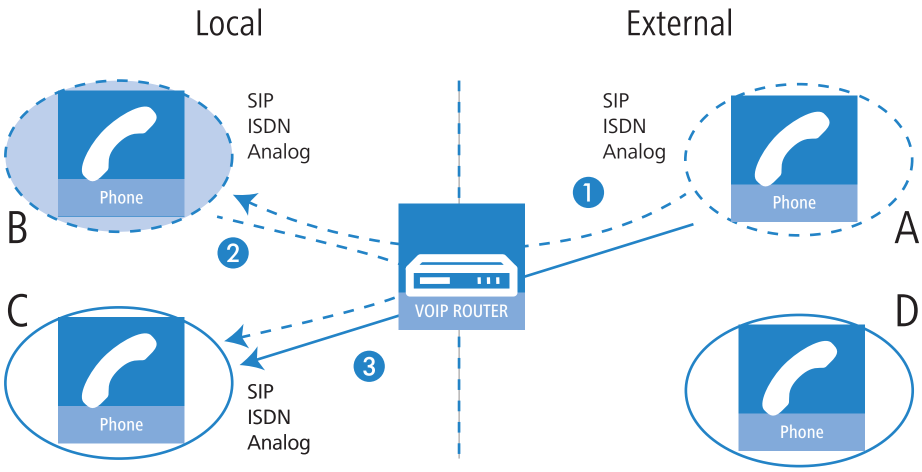
Active forwarding to local users

① An external user **A** makes a call to an internal user **B** (SIP, ISDN or analog).

② **B** makes an additional call to a local user **C**. These two users can call each other directly, and so the LANCOM VoIP Router only handles the signaling via SIP; the data transfer via RTP takes the shortest possible route.

③ The local user **B** then transfers the call (with consultation) to **C**.

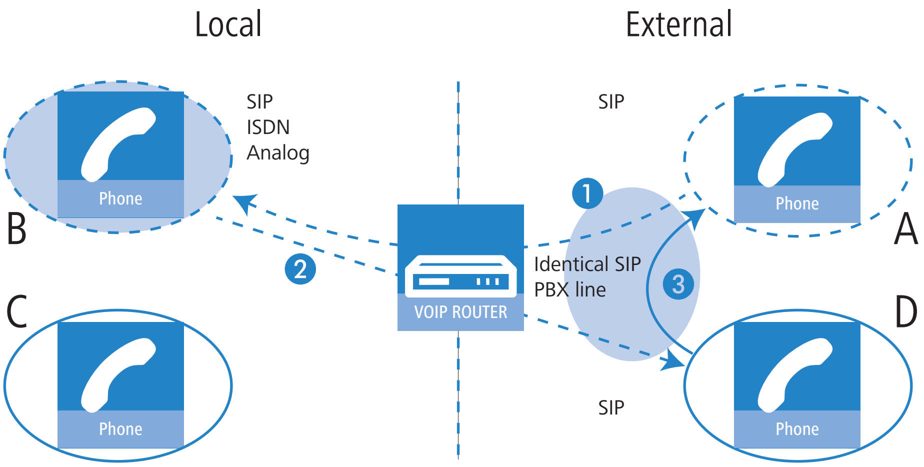
④ The LANCOM VoIP Router manages the call transfer.



In case of SIP at the external subscriber, this requires that Transfer in SIP (re-invites) is fully supported.

Active transfer to external SIP users

1. An external SIP user **A** makes a call to an internal user **B** (SIP, ISDN or analog).
2. **B** makes an additional call to an external user **D**.
3. If the two external SIP users **A** and **D** can be accessed over the same SIP line, the LANCOM VoIP Router delegates the management of the call transfer to the upstream provider.

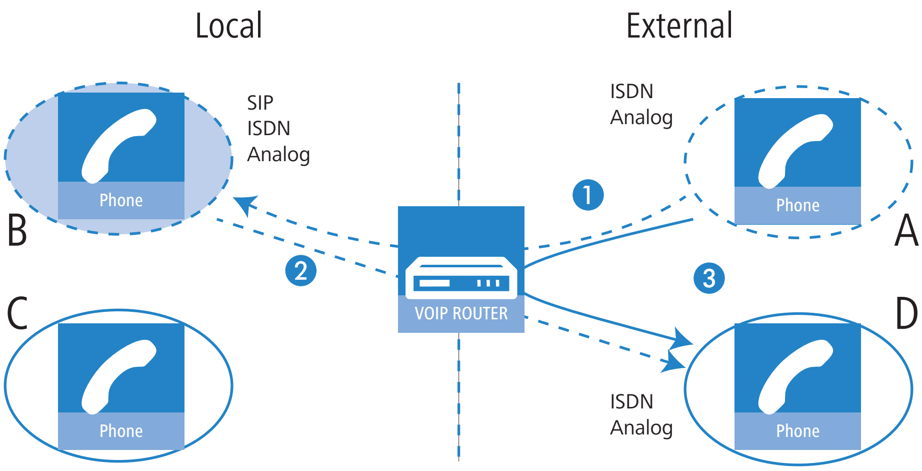


Requires that the VoIP PBX fully supports Transfers in SIP (re-invites).

Active transfer to external ISDN or analog users

In some cases upstream exchanges do not support the delegation of call-transfer functions to external ISDN or analog users, often due to the unclear situation about who carries the call charges. For this reason, call transfer between external subscribers is always handled by the LANCOM VoIP Router.

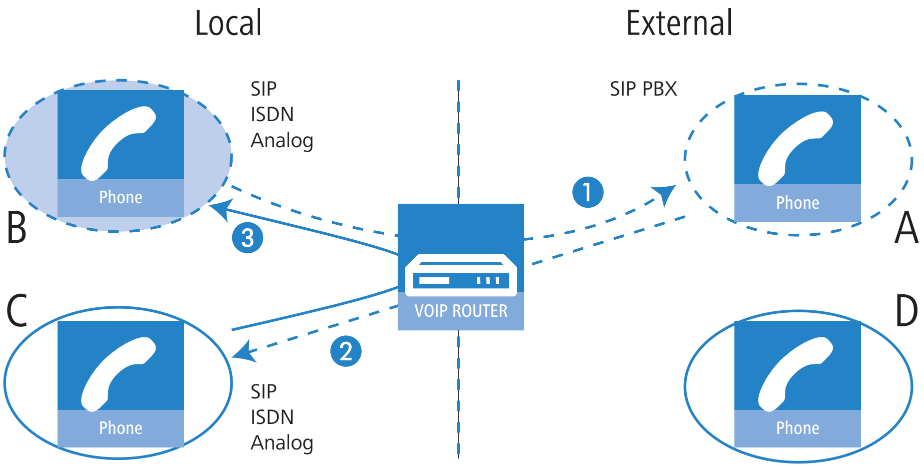
1. An external subscriber **A** (external SIP, ISDN or analog) calls an internal user **B** (SIP, ISDN or analog).
2. **B** makes a further call to an external subscriber **D** (ISDN or analog).
3. The local user **B** then transfers the call (with consultation) to **A**.
4. If the two external users **A** and **D** use different protocols (SIP, ISDN or analog) then the LANCOM VoIP Router handles the management and conversion of the data.
5. If both external users **A** and **D** use SIP the LANCOM VoIP Router cannot enable the call transfer.



ⓘ Requires that the VoIP PBX fully supports Transfers in SIP (re-invites).

Passive forwarding between local users

1. An internal user **B** (SIP, ISDN or analog) calls an external user **A** (at a SIP PBX line).
2. **A** makes an additional call to a local user **C**.
3. The external user **A** then transfers the call to **C**.
4. The LANCOM VoIP Router manages the call transfer. If the connected subscribers **B** and **C** are internal users, the LANCOM VoIP Router controls the SIP data for signaling only and enables RTP-based data transfer over the shortest possible route directly between the SIP users.

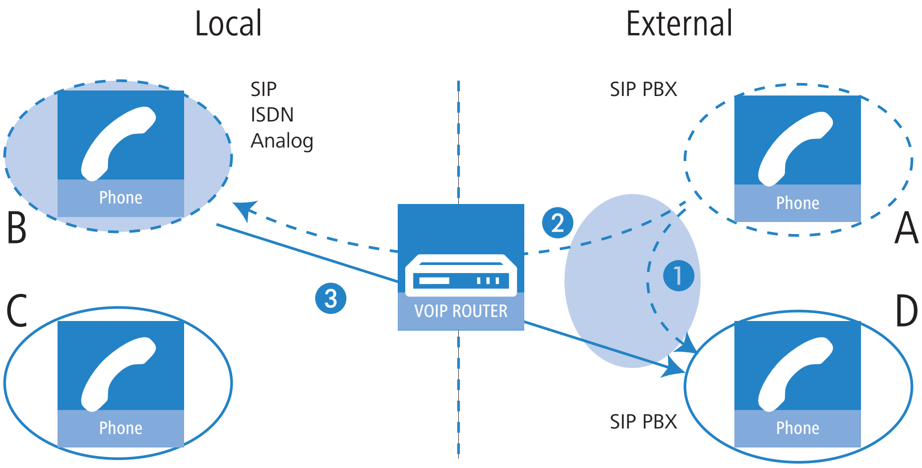


Requires that the VoIP PBX fully supports Transfers in SIP (re-invites).

Passive transfer from local to external users

1. An external user **A** (at a SIP PBX line) makes a call to an internal user **B** (SIP, ISDN or analog).
2. **A** makes an additional call to an external user **D** (who is also a subscriber to the same SIP PBX line as **A**).
3. The external user **A** then transfers the call from **B** to **D**. To do this, the LANCOM VoIP Router has to open an external connection to D.

The LANCOM VoIP Router can only establish this connection if D can be accessed over the same SIP PBX line as **A**, i.e. if external call forwarding is permitted.



Requires that the VoIP PBX fully supports Transfers in SIP (re-invites).

13.6.2 Spontaneous call management by the user

Functions for spontaneous call management

Calls can be managed on an individual basis and the LANCOM VoIP Router supports the services known from the ISDN network:

- With **call hold** the user can place an active call into a wait state. In this state, the user can for example make a call to another person.
- Establishing an additional call while a call is on hold is referred to as **consulting**. This call can be ended again and the conversation with the call on hold continued.
- With **transfer call**, the user can switch to and fro between two connections. The user is only connected with one caller at a time, while the other caller is put on hold.
- With **call swap** the user switches an active call over to another call which is on hold. The two callers are then connected and the user is no longer involved in the call. A subscriber transferring a call can either directly hand over an active call to a third subscriber (unattended call transfer), or a separate call can be made to a third subscriber to communicate the call and then transfer it (attended call transfer).

Using spontaneous call management with various telephones

SIP telephones and SIP softphones generally feature special keys or menu entries to manage calls. Depending on the model or program, different terms may be used the the functions are as follows:

- HOLD: Places an active call into a wait mode or swaps between two active calls. On ISDN and analog telephones this function is often referred to as the F-key/Flash/Call hold. Flash function (F key).
- HANG UP: End the current call.
- SWAP: Swap between two active calls (depending on the ISDN telephone, this may be initiated by a display-menu entry, a special key, or the "F" key).
- CONNECT: Initiates the call's transfer (can be triggered by "hanging-up" with an active call and a call on hold)*.

These functions can be used to manage calls as follows:

Holding/consulting and continuing with calls	SIP	ISDN	Analog
To place a call on hold, press the Flash/Call hold key (or 'F' on analog phones). The caller can no longer hear you and you can initiate a second call by dialing a telephone number (consulting).	HOLD	HOLD or F	R
To continue with a call which is on hold, press the Flash/Call hold key again (or 'F 2').	HOLD	HOLD or F	F 2
If the consultation call has not yet been picked up, you can stop the consulting by hanging up the handset on a SIP or ISDN telephone*. You can stop the consultation call with the appropriate menu function of the telephone (e.g. 'Cancel') or 'F 1' (analog).*	HANG UP	HANG UP	HANG UP

Swap call	SIP	ISDN	Analog
To open a second line during a call, first press the Flash/Call hold key (or 'F' on analog phones). The other caller can no longer hear you.	HOLD	HOLD or F	R
Dial the number for the second caller while the first call is on hold. If you cannot reach the second caller, you can return to the call which is on hold by pressing the hold key (or 'R').	123456789	123456789	123456789
As soon as two simultaneous connections are open, you can use the hold key (or swap key for ISDN phones, 'R' and '2' for analog phones) to swap to-and-fro between the two connections. You will be connected to one of the other callers; the other caller is placed on hold.	HOLD	SWAP	F 2
To end an active call, hang up the handset on SIP or ISDN telephones, and on analog phones press 'R 1'. The call which is on hold is not automatically reactivated, but it will be signaled (ringing phone) for a period of 15 seconds.	END or HANG UP*	END or HANG UP*	F 1

Call transfer, consult	SIP	ISDN	Analog
To open a second line during a call, first press the Flash/Call hold key (or 'F' on analog phones). The other caller can no longer hear you.	HOLD	HOLD or F	R
Dial the number for the second caller while the first call is on hold. If you cannot reach the second caller, you can return to the call which is on hold by pressing the hold key.	123456789	123456789	123456789
As soon as you have established two simultaneous connections you can connect the two callers with the connect key (or 'R' and '4' on analog phones) or by hanging up the handset.* Optionally you can switch between the two lines as often as you like before transferring. Call transfer always connects the active call and the call on hold.	CONNECT or HANG UP*	CONNECT or HANG UP*	R 4 or HANG UP
You have no more active calls. You can either hang up or make a new call.	HANG UP 123456789	HANG UP 123456789	HANG UP 123456789

Call transfer, blind	SIP	ISDN	Analog
To open a second line during a call, first press the Flash/Call hold key. The other caller can no longer hear you.	HOLD	HOLD	HOLD
Dial the number for the second caller while the first call is on hold.	123456789	123456789	123456789
Press the connect key (or 'R' and '4' on analog phones) or hang-up the handset before the second connection has been established.* The two callers will now be connected "in the background".	CONNECT or HANG UP*	CONNECT or HANG UP*	R 4 or HANG UP
You have no more active calls. You can either hang up or make a new call.	HANG UP 123456789	HANG UP 123456789	HANG UP 123456789

! *In some cases, SIP or ISDN telephones can be configured so that hanging-up the handset either causes the consultation or active call or be terminated, or a call transfer is triggered ("Connect").

13.6.3 Configure permanent call forwarding

Along with spontaneous call transfers as controlled by a subscriber during a call, it is often useful to set up a permanent call forwarding ("redirect calls"). For example, a call should be forwarded when a line is busy, if there is no answer within a certain period, or in case of absence (e.g. vacation).

There are two possibilities for configuring permanent call forwarding.

- Via the telephone or terminal device itself with the aid of control characters
- In the configuration of the LANCOM VoIP Router by means of the management tools (LANconfig, WEBconfig or telnet)

i If permanent call forwarding is activated by both methods, then the behavior of the call forwarding follows the last respective action.

Triggering call forwarding

The following events can be used as a trigger or condition of the permanently configured call transfers:

- CFU, call-forwarding unconditional
- CFB, call forwarding on busy
- Delayed call forwarding, CFNR (call forwarding no reply); CFNA (call forwarding no answer)
- No call transfer

All types of call forwarding can be used in parallel with your own target telephone numbers. If multiple call-forwarding conditions are active, the following priority applies:

1. CFU
2. CFB
3. CFNR

If, for example, call forwarding on busy is activated and a corresponding target number has been defined, then the call will be forwarded to this target before referring to a target as defined for forwarding on busy.

If the incoming call has already been forwarded from another telephone number, then forwarding will not take place again, so as to avoid endless call-forwarding queues.

Configuring user settings in the LANconfig see 'User settings' → page 13-19

Configuring user settings with the telephone with character strings

For the configuration of user settings with the telephone, the various technologies (SIP, ISDN, analog) each offer specific possibilities. With ISDN telephones, call forwarding can be controlled by the functional protocol in the ISDN signaling or via so-called keypads (character stings). For analog telephones the same character strings are transferred by DTMF. The SIP protocol provides another option with its REFER method that is supported by most SIP phones and SIP softphones. However, call forwarding can only be controlled by the terminal device. To enable a uniform behavior for users in mixed infrastructures, the LANCOM VoIP Router offer an additional variant of call forwarding for SIP phones, as is presented here in comparison with ISDN and analog telephones.

Immediate call forwarding	SIP	ISDN	Analog
Switch on and define target for call forwarding	*21*TargetNo#	*21*TargetNo*MSN#	*21*TargetNo#
Switch off	#21#	#21#*MSN	#21#
Switch off temporarily, maintain call-forwarding target	#22#	#22*MSN#	#22#
Switch on again, maintain defined call-forwarding target	*22#	*22*MSN#	*22#

Call forwarding on busy	SIP	ISDN	Analog
Switch on and define target for call forwarding	*67*TargetNo#	*67*TargetNo*MSN#	*67*TargetNo#
Switch off	#67#	#67*MSN#	#67#

Call-forwarding on no reply	SIP	ISDN	Analog
Switch on and define target for call forwarding	*61*TargetNo#	*61*TargetNo*MSN#	*61*TargetNo#
Switch off	#61#	#61*MSN#	#61#

Please note the following when using character stings to configure call forwarding:

1. Some ISDN telephones feature special keys or menu entries to configure call forwarding, and these can be used as an alternative to the listed character strings. Refer to the documentation from the corresponding manufacturers.

13.6.4 Fax via T.38 – Fax over IP (FoIP)

The migration of telephone infrastructure towards VoIP also increases the demand for fax devices to communicate over VoIP. Even in the age of e-mail, fax transmissions continue to be highly important in legal respects as legally binding documents such as contracts and invoices can be far more easily handled by fax than with the alternative of e-mails with digital signature. The integration of fax devices into VoIP infrastructure can be implemented in two ways:

- Fax messages are transmitted via landline just like a conventional fax.
- The transmission takes place over an Internet connection. Options for this are as follows:

- □ The fax signals are transmitted like voice data over a VoIP connection, referred to as "fax over VoIP". Fax transmission should only make use of the G.711 codec for compression, as other codecs are inferior at converting fax tones, which are designed for analog networks, into digital VoIP data. Due to the highly sensitive nature of fax connections, this method can only be used with high-quality connections, whereby the transmission speed is sub-optimal.
- □ For example, with the "store-and-forward" principle (ITU-T.37), fax messages are passed from the fax machine to a gateway that stores and converts the fax document. In a second step the fax is transmitted to the destination for conversion back into a fax format. Alternatively fax messages can be sent by e-mail (fax-to-mail and mail-to-fax). Solutions of this type may not meet the legal requirements mentioned above, due to the fact that there is no direct connection between transmitter and receiver.
- □ With "real-time routing" of fax messages, on the other hand, a direct connection is established between the two fax machines and all data is transferred in real time. The fax machines are connected virtually over the Internet. Communication between the two fax machines follows the ITU-T.38 standard for converting standard fax signals. This variant is also known as Fax over IP (FoIP). The fax messages are not transferred as acoustic signals via VoIP, but rather in a special protocol, the IFP (Internet Facsimile Protocol), that embeds the signals in UDP/TCP packets.

To enable fax transmissions with T.38, either the fax machines themselves have to support the T.38 standard, or they must be interconnected over the Internet via fax gateways. LANCOM VoIP Routers and LANCOM Routers with the LANCOM VoIP Advanced Option or LANCOM VoIP Basic Option support the T.38 standard and are thus suitable for operation as fax gateways in VoIP infrastructure.

The fax machines are connected to the LANCOM VoIP Routers by means of a suitable interface. The fax gateway in the LANCOM VoIP Router handles the conversion of the signals for transmission and reception of fax messages:

- Demodulation of incoming T.30 fax signals
- Conversion of T.30 fax signals into T.38 IFP packets
- Transmission of IFP packets between transmitting and receiving gateways
- Conversion of T.38 IFP packets into T.30 fax signals
- Modulation of T.30 fax signals and transmission to the fax machine

With the device type "fax" or "telephone/fax" is selected in the analog or ISDN user settings the LANCOM VoIP Router automatically recognizes a fax for transmission and it attempts to transmit via F.38/FoIP. If the remote site does not support this method, the LANCOM VoIP Router automatically uses the fax over VoIP-version using G.711 compression.

Successful transmission of fax via FoIP requires that the VoIP infrastructure also supports the T.38 standard. For example, where a public SIP provider is involved, this provider also has to offer T.38 support.

13.6.5 Hunt groups with call distribution

Introduction

Calls are normally intended for an individual or their telephone number. Occasionally it is not important to speak to a particular individual, but to anybody in a certain department or with a certain function. In this case, telephone infrastructure collects multiple users into hunt groups where they can all be reached under a single shared telephone number. The group call function can then follow certain rules to distribute or forward incoming calls to the call group.

Call distribution

A hunt group consists of two or more users, or even other hunt groups, as potential destinations for an incoming call. Hunt groups are comparable to local users and have their own number and, as such, they can be used as a target number in the call router.

Incoming calls can be distributed by a variety of methods, allowing different scenarios to be realized.

- Calls are signaled to all group members at the same time (simultaneous)
- Calls are signaled to one member of the group after the other, in a set order (sequential)

Along with the members of the hunt group and distribution method, also to be defined are a call-forwarding time and and call-forwarding target, all of which control the call-distribution procedure. The forwarding time determines the time period during which the dialed user can answer a signaled call. The forwarding target defines where the call is to be forwarded to (user, group, internal or external call number) for the case that none of the group members picks up the call within the forwarding time—if no forwarding target is defined, then the call is rejected.

Cascading of hunt groups

The defined hunt groups can themselves be members of a higher-level hunt group, just as hunt groups can be entered as the forwarding target for a higher-level hunt group. These options enable the establishment of a cascaded hunt-group structure which can form highly complex scenarios by using a multitude of branches. These branches represent the hunt groups and the end points are the users themselves. The following rules apply to structures of this type:

- If a hunt group is used as a member, then this lower-level hunting group causes a new "branch" in the structure to open up when that member receives a call.
- When a lower-level hunt group opens, certain parameters that have been defined, e.g. forwarding time, etc., apply.
- This branch from the lower-level group only remains open for as long as the member in the upper-level hunt group is being signaled according to the settings. If the next member in the upper-level hunt group is reached, then the entire branch along with all of its other sub-branches is closed. The system does not wait until all possible combinations along the branch have been tried out. It is thus possible that there are members defined in a lower-level hunt group who cannot be reached because of settings in the upper-level groups.
- If a member of a hunt group picks up the call, all open branches are closed and all attempts to reach forwarding targets are stopped.
- If a call remains unanswered after signaling all of the members of an (upper or lower-level) hunt group, then the call is passed on the the call-forwarding target. This means that any call-forwarding times which may be running in the upper-level hunt groups are ended. In this case the call "jumps" out of the hunt-group structure and is given a new target.

Example: The following hunt groups have been defined:

Group telephone number	Comment	Members	Forwarding method	Forwarding time	Forwarding target
100	Entire company	200, 300, 400	Simultaneous	10	ext. Telephone number
200	Service Dept.	201 to 209	Simultaneous	10	100
300	Marketing Dept.	301 to 309	Sequential	10	200
400	Sales Dept.	409	Sequential	15	100
410	Sales Europe group	411, 412, 413, 414, 415	Sequential	10	400
420	Sales America group	421, 422, 410	Sequential	30	400
430	Sales Asia group	431, 432, 410	Sequential	30	400

Each department or group has users who use the final digits in the telephone number, i.e. 411 to 419 for the Sales Europe staff and 409 for the Sales team secretary. Only the group call numbers are communicated externally because all staff members tend to travel frequently on business. The purpose of the hunt-group structure is to connect each customer with a competent staff member in the shortest possible time.

An incoming call directed to the telephone number 420 for a Sales America team member is handled as follows:

1. The call is signaled to the users 421 and 422 in this group for 30 seconds each. If there is no answer, then the hunt group 410 is activated for 30 seconds—a member of the Sales Europe team should take care of the customer when Sales America no team members are available.

2. In the Sales Europe team, the call are distributed to each number for 10 seconds. The hunt group has five members, but with a forwarding time of just 10 seconds, not all of the users can be signaled: The branch is only opened for a maximum of 30 seconds by the upper-level group, in this case 420. This is a way of limiting the maximum waiting time for a customer. If the first three signaled members of the lower-level group 410 do not answer, then the call jumps back to the upper-level hunt group 420.

3. There is still nobody available in the upper-level hunt group 420, and so the call is directed to the call-forwarding target 400.

4. Hunt group 400 directs the call to the team secretary 409. If here nobody answers for 15 seconds then the call-forwarding target 100 is used, which addresses the entire company.

5. Hunt group 100 calls all of the numbers in the hunt groups 200, 300 and 400 simultaneously. If even then nobody answers within 10 seconds, then the hunt group forwards the call to an external telephone number, for example a 24/7 call center.

Configuring hunt-group functions , see 'Hunt-group functions' → page 13-34

13.6.6 Multi-login

For subscribers using multiple terminal devices, e.g. a softphone on PC and a "normal" telephone on the desktop, multiple SIP, ISDN or analog telephones all using the same internal telephone number can log on to the LANCOM VoIP Router. Multi-login telephones behave like a single user in a hunt group with 'simultaneous' call distribution:

1. Incoming calls are signaled **simultaneously at all** telephones with this internal number.
2. As soon as a call is picked up at one of the telephones, signaling at the other devices stops.
3. Other incoming calls are signaled at all telephones. If one of the telephones is 'busy', then the entire multi-login group is taken to be 'busy'.
4. Outgoing calls can be made from every telephone without limitation.
5. For a multi-login group only one call forwarding setting (call redirection) can be configured. This applies to all telephones and can be set from any telephone.

To use multi-login, multiple telephones can be set to have the same internal telephone number.

13.7 VoIP media proxy – Optimized management for SIP connections

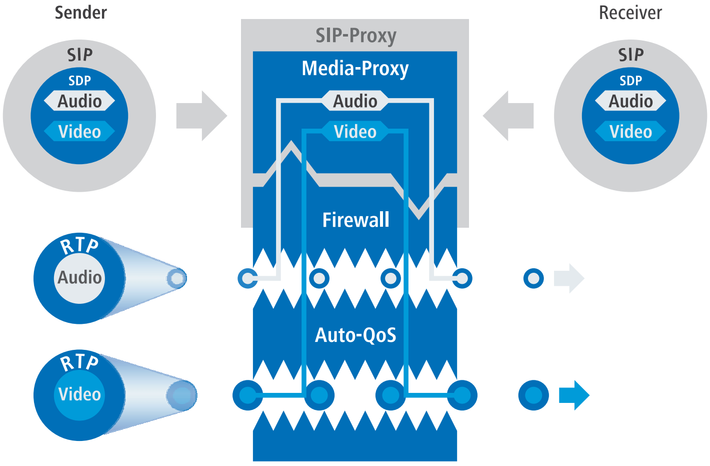
When connecting or forwarding calls between remote subscribers over different SIP lines, the SIP proxy in the LANCOM VoIP Router attempts to connect the two callers by means of a REFER or a Re-INVITE. The two external subscribers are not always able to reach one another directly and so the connection may fail. This is because the SIP providers do not make the necessary adaptations, e.g. translation of the target IP addresses. To improve performance in these situations, the SIP proxy in the LANCOM VoIP Routers has been additionally equipped with a media proxy.

The media proxy helps to establish connections and forward calls between subscribers who are reachable over different types of telephone line (e.g. SIP PBX line and SIP provider line). The media streams, generally RTP connections, remain unchanged. The media proxy changes the ports and IP addresses in the data packets and it adapts special media end points to the corresponding target networks (ARF networks, interface and IP address).

Multiple media streams in one SIP connection

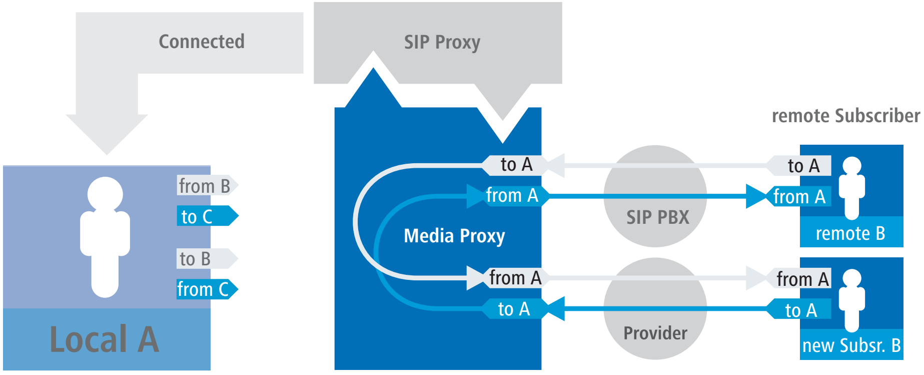
The SIP protocol can negotiate multiple data streams in a session, e.g. separate media streams for audio and video. Each stream is handled separately. A data stream initially terminates at the media proxy and continues from the "other side". This provides the data stream with end points at the LAN and WAN sides of the media proxy.

All of the connection information in the direction of the SIP provider can be maintained and all of the necessary changes to IP addresses, ports, etc., are handled by the media proxy.



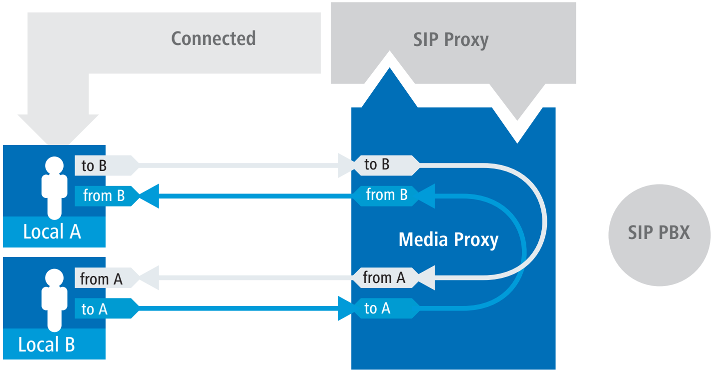
The data streams are all fed through the firewall individually, which enables a differentiated control of the QoS settings, among other things.

Connection management by the media proxy enables all subscribers to be connected to one another, whatever type of line they are using. This makes it possible to connect between SIP, ISDN and analog subscribers, something that a pure SIP connection is not capable of. Furthermore, the monitoring of individual media streams in the firewall allows certain types of application to be permitted or prevented depending on the connection's end point.



Management of media streams in case of an upstream SIP PBX

Even for two subscribers in the same network behind the LANCOM VoIP Router, when connected to an upstream SIP PBX the media proxy generates data streams with separate media end points on the LAN side and on the WAN side (towards the SIP PBX).



In this case it is not necessary to pass the media streams through the upstream PBX, so the SIP signaling helps the LANCOM VoIP Router to make a new decision on the path to be taken by the connection data. Using the end points in the media proxy the data streams can be connected directly, making a diversion via the SIP PBX unnecessary.

This decision is also made again in the media proxy if a local and an external subscriber are connected in such a way that, ultimately, two local subscribers are connected to one another. The media proxy re-assigns the end points when making the connection, so enabling the direct transmission of the data streams between the local participants.

Managing the media streams in the firewall

The media streams are monitored in the firewall as a matter of principle. A firewall rule is generated for each media stream (audio, video). This rule opens a connection for the corresponding IP addresses and ports for each side (LAN-WAN) and carries out a translation according to the IP-port relationships as specified by the media proxy.

Automatic QoS rules for media streams

The QoS mechanism in the firewall reserves the maximum possible amount of connection bandwidth as agreed during the SDP negotiation (SDP, Session Description Protocol) and the packets are prioritized accordingly.

Handling subscribers using different codecs

When connecting different subscribers, the situation can arise where the codecs available to the subscribers do not match together—there are no common codecs due to the SDP negotiation.

The following situations are to be observed here:

- Connections with different media streams, e.g. a video-telephone call (audio + video) and a traditional telephone call (audio only): This connection will be rejected with the message "Codec mismatch".
- Similar media types (audio-audio, video-video) with codecs that do not match: This connection will be rejected with the message "Codec mismatch".

The media proxy can only connect different subscribers if the media type and the codec type match.

13.8 SIP-ID as switchboard number with trunk lines

Until now, SIP trunk lines were given the SIP ID as the switchboard number, which was adapted to suit the telephone number. However, this method is not supported by all trunk-line suppliers.

For this reason LCOS 7.52 and later provides the SIP mapping table that, like ISDN mapping, explicitly defines how telephone numbers are to be processed.

0123456789# -> #

This allows the extension numbers of the trunk to be translated 1:1 to the internal telephone numbers.

If you have until now used a trunk with automatic switchboard-number translation and you update to LCOS 7.52, then it is imperative that you make a corresponding entry in the SIP mapping table.

13.9 Switching at the SIP provider

When switching external SIP connections, the Call Router in the LANCOM VoIP Router generally manages the connection for the full duration of the call. This means that the Call Router retains control over a call even when two external subscribers have been connected to one another and the local subscriber on the LANCOM VoIP Router side has ended the call. In this case, the LANCOM VoIP Router takes up bandwidth for connecting the two external subscribers.

If the connections to the two external subscribers both run via the same SIP provider, an alternative is available whereby call switching is transferred to the provider. The LANCOM VoIP Router no longer takes up the bandwidth.

LANconfig: **VoIP-Call-Manager ▶ Lines ▶ SIP lines**

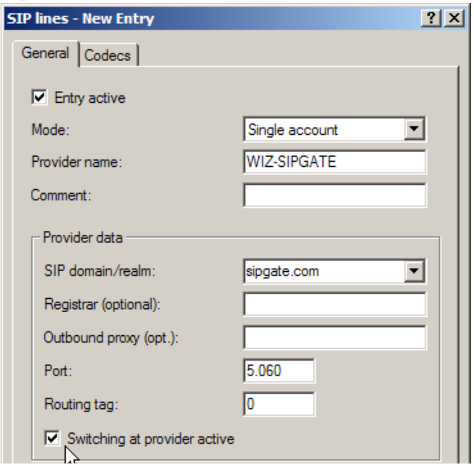
WEBconfig: **Setup ▶ Voice-Call-Manager ▶ Lines ▶ SIP-Provider ▶ Lines**

- **Activate switching at provider (Refer-forwarding)**

  With this option activated, a REFER is forwarded to the provider when two external lines are connected, and the provider then handles the call transfer. The advantage of this is that the LANCOM VoIP Router no longer requires the bandwidth.

  - Possible values: On, off
  - Default: Off

Switching at the provider will only work if both connections are routed via the same provider line.



☑ Entry active

Mode: Single account

Provider name: WIZ-SIPGATE

Comment:

Provider data

SIP domain/realm: sipgate.com

Registrar (optional):

Outbound proxy (opt.):

Port: 5.060

Routing tag: 0

☑ Switching at provider active

13.10 Handling canonical telephone numbers

Canonical telephone numbers (familiar from mobile phones and starting with '+') were formerly automatically reformatted into standard telephone numbers. '+' was converted to '00'.

As of LCOS 7.52 automatic conversion can be disabled and canonical numbers can be processed directly in the call-routing table. For example, a dedicated line can be defined for canonical numbers.

- WebConfig: **Setup ▶ Voice-Call-Manager ▶ General**
- **Convert-Canonicals**

  Activates or deactivates the conversion of canonical numbers into standard telephone numbers.

  - Possible values: Yes, No
  - Default: Yes

13.11 Processing Destination Domains

As the VoIP implementation in the LANCOM VoIP Router handles all calls as SIP calls, telephone numbers and SIP subscribers contain domain information. Furthermore, SIP numbers can also contain alphanumeric characters.

The SIP domains are used in LCOS as follows:

- When SIP subscribers register at upstream PBXs or at the LANCOM VoIP Router itself.
- When SIP subscribers establish a connection.

LCOS supports the following defined domains:

- ISDN for the ISDN interfaces
- All domains that are entered for the lines

13.11.1 Registration at upstream exchanges

Local SIP subscribers can only register using the domains that are known. The subscribers authenticate themselves at the local LANCOM VoIP Router with their user name and password. This excludes domains that correspond to an upstream SIP PBX. These registrations are authenticated in the upstream SIP PBX.

If a subscriber tries to register with an unknown domain, then this may be accepted as a local registration ('Force local authentication' → page 13-14).

13.11.2 Switching internal calls

For internal connections, internal numbers are generally assigned unambiguously. However, SIP telephones, for example, can register with several "lines", such as '1011@provider.com' and '1011@isdn.com', so that a line can be assigned specifically to the required connection.

With internal switching, an attempt is made to find a subscriber whose number and domain match. Only if this was not successful is the call placed using the destination number only. The domain remains unchanged.

For example, calls that are incoming via ISDN (from <calling pty id>@isdn) are switched to subscriber 1011 (to 1011@isdn). The call to the SIP telephone is displayed on the ISDN line key. If there is no such subscriber with such a domain, then the call is delivered to the first known subscriber '1011'.

13.12 ISDN interface configuration

LANCOM VoIP Router routers feature several ISDN interfaces with which they can be connected to ISDN exchange lines, or with which ISDN terminal equipment can be connected to them.

- ISDN TE interface ("external ISDN connection"): An ISDN interface in TE mode for connection to the ISDN bus of an upstream ISDN PBX or to an ISDN NTBA. This ISDN interface can be used for backup connections over ISDN or as a dial-in interface for remote sites.
- ISDN NT interface ("internal ISDN connection"): With its ISDN interface in NT mode, the LANCOM VoIP Router itself provides an internal ISDN bus. This ISDN interface can be used to connect ISDN PBXs or ISDN telephones.

The factory settings have the ISDN interfaces marked with ☒ set to TE mode and the ISDN interfaces marked with ☎ set to NT mode. These ISDN settings can be altered according to your requirements:

- Multiple TE interfaces provide, for example, up to eight B channels as a backup or for dial-in.
- With multiple NT interfaces, for example, a downstream ISDN PBX can be provided with up to eight B channels.

Depending on the combination of ISDN interfaces in TE and NT mode, the hardware must be set up with the functions for bus termination, life-line support and power relay, and the software must be set up with the appropriate protocol. The setting for the protocol allows for the type of ISDN connection to be used (point-to-multipoint or point-to-point).

13.12.1 Point-to-multipoint and point-to-point connections

LANCOM VoIP Routers support point-to-multipoint and point-to-point connections:

- Point-to-multipoint connection (point-to-multipoint): Up to 8 ISDN terminal devices can be connected to this type of connection. Terminal equipment can include ISDN telephones and ISDN PBXs, which can be used for connecting yet more equipment. As an alternative, a LANCOM VoIP Router can be connected to a point-to-multipoint connection.
- Point-to-point connection (point-to-point): This type of device is suitable for the connection of one ISDN device only, generally an ISDN PBX. As an alternative, a LANCOM VoIP Router can be connected to a point-to-point connection.

To connect a LANCOM VoIP Router, the interface that is used is set up for the type of line in use.

Equipment connected to an ISDN connection can be addressed in two ways:

- The devices are addressed with a multiple subscriber number (MSN) that is linked to the ISDN connection and cannot be influenced.
- Terminal devices are addressed via a Direct Dialing In-Number (DDI). However, only the switchboard number is associated with the telephone line; the extension numbers that address the individual terminal devices can be chosen at will and are merely suffixes to the switchboard number. The switchboard number, extension and area selection code (not including the leading zero) can be at the most 11 characters long.

> The terms "point-to-multipoint connection" and "point-to-point connection" are used in many countries to describe the technical implementation of point-to-multipoint with MSN and point-to-point with DDI. Other countries may use different types of connection and other combinations of protocol and call-number type, or even different names. Please refer to your telephone network operator for the technical specifications of your ISDN connection.

13.12.2 Bus termination, life-line support and power relay

The hardware function modes of the ISDN interfaces are set by DIP switches on the underside of the LANCOM VoIP Router.

- **Bus termination** is obligatory with an ISDN interface in NT mode.

  Bus termination is generally deactivated for ISDN interfaces in TE mode. If the LANCOM VoIP Router is the last device at a longer ISDN bus and this itself is not terminated, it may be advantageous to activate the bus termination for an ISDN interface in TE mode.

> The supplied adapter must be used if a connection is to be made to an ISDN interface which is set differently to its default settings. This adapter serves to cross-over the contacts in the ISDN interface. Not using the adapter can cause damage to both the LANCOM VoIP Router and to the devices connected with it!

Not for all LANCOM VoIP Router

- If **life-line support** is activated, the interfaces ISDN 1 and ISDN 2 are bridged if the device is unavailable due to a power outage or if the ISDN 2 interface is switched off (default: on). The life-line support is used when the device is connected to an external ISDN line over a TE interface with the simultaneous operation of ISDN terminal devices at the internal ISDN connection of an NT interface. If bridged, the ISDN devices can then use the external ISDN bus directly.

  To activate life-line support, all four DIP switches (3 to 6) must be up; to deactivate, all four DIP switches must be down.

> Life-line support is to be deactivated when both ISDN interfaces are to be operated in the same mode, i.e. as two TE or two NT interfaces. The interfaces are not to be bridged in case of power failure when being operated in this manner!

- The **ISDN power relay** means that the bus voltage of an external ISDN bus at ISDN 1 is switched through to the terminal equipment connected to another ISDN bus. As a consequence, ISDN equipment operated at the internal ISDN bus of the LANCOM VoIP Router can be operated without its own power supply.

> Be sure to deactivate the ISDN power relay if both ISDN interfaces are to be operated in TE mode, such as when both ISDN interfaces are connected to an ISDN NTBA, for example. A power relay in this situation would result in a short-circuit which would damage the device and the ISDN NTBAs!

> Further information about settings for life-line support and ISDN power relay can be found in the user manual for your LANCOM VoIP Router.

13.12.3 Protocol setting

Parameters for the ISDN interfaces are entered into LANconfig in the configuration area 'Interfaces' on the 'WAN' tab. Under WEBconfig, Telnet or SSH client you will find the settings for the ISDN interface parameters under `Setup/Interfaces/WAN`.

Select the protocol for each ISDN interface according to its application and the ISDN connection type: Point-to-multipoint and point-to-point connections can be used in various combinations at a LANCOM VoIP Router. The following options are available:

- **Automatic** for automatic selection of the operating mode (only in TE mode)
- **DSS1 TE (Euro ISDN)** for connection to a point-to-multipoint ISDN bus.
- **DSS1 TE point-to-point** for connection to a point-to-point ISDN bus.
- **1TR6 TE (German ISDN)** for connection an ISDN bus which uses this protocol (in Germany only).
- **DSS1 NT (Euro ISDN)** to provide point-to-multipoint ISDN interfaces

- **DSS1 NT reverse** to provide point-to-multipoint interfaces while maintaining the ISDN timing of the connected ISDN line, please refer to 'ISDN connection timing'
- **DSS1 NT (point-to-point)** to provide point-to-point ISDN interfaces
- **DSS1 NT point-to-point reverse** to provide point-to-point interfaces while maintaining the ISDN timing of the connected ISDN line, please refer to 'ISDN connection timing'
- **DSS1 timing** to maintain the ISDN timing of the connected ISDN line, please refer to 'ISDN connection timing'
- **Off**

NT mode operation always has to be set manually.

If an ISDN device is attached to an ISDN interface that is set to auto and is not recognized properly, set the required protocol manually.

13.12.4 ISDN connection timing

To ensure trouble-free transmission, all of the components in the ISDN system (LANCOM VoIP Router, upstream and downstream ISDN PBXs and ISDN terminal devices) have to use the same ISDN timing. In the LANCOM VoIP Router, an ISDN interface in TE mode can take on the timing of the ISDN line. The TE interface enables the device itself to behave like a terminal device. In NT mode, the LANCOM VoIP Router can pass on the on this timing over the ISDN interfaces to any connected terminal equipment or downstream ISDN PBXs. The NT interface enables the device itself to behave like an exchange.

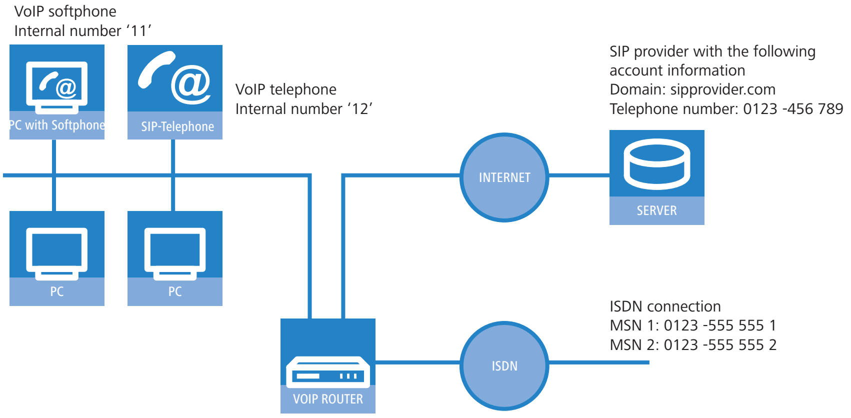
There are various ISDN interface settings to define the ISDN interface which is to supply the LANCOM VoIP Router with the ISDN timing to be passed on to the devices at the NT interfaces.

- **Automatic**: If no interface has been manually selected for the timing, the device automatically searches for a TE interface that is supplying a timing. To ensure that the timing is synchronous, the TE connectors constantly try to keep the connection activated. This ensures that the timing continues to be supplied even if one of multiple TE lines should be shut off. If none of the TE connectors supply a timing, then the timing system runs "freely" and uses the internal timing of the LANCOM VoIP Router.
- **DSS1 timing**: This setting takes on the ISDN timing from the connection for use by the LANCOM VoIP Router and further devices connected over the NT interface. In this way, the timing can be switched through in parallel to an existing ISDN PBX at a point-to-point connection. Apart from passing on the ISDN timing, the interface is not active.
- **DSS1 NT reverse** or **DSS1 NT point-to-point reverse**: When all ISDN interfaces are operated in NT mode, the timing system runs "freely" because there is no TE interface to take on the ISDN timing. If in this case the ISDN connections are connected, for example, to an ISDN PBX which is being supplied with ISDN timing from another source, then interference to the transmission may arise because the timing of the LANCOM VoIP Router is not synchronous to that of the PBX. In such cases, the reverse setting allows the ISDN timing to be taken from an NT-mode interface, so ensuring that the LANCOM VoIP Router runs synchronously with the overall system.

13.13 Configuration examples

13.13.1 VoIP telephony for stand-alone use

This example shows how to configure a LANCOM which is used as a central device for Internet connectivity and VoIP telephony at a new site.



Destination

- Internal telephony with SIP telephones and SIP softphones.
- Access to internal terminal equipment via the MSNs.
- External telephony via the SIP provider with backup over ISDN.
- Calls to emergency and special numbers via ISDN.

Requirements

- LANCOM connected to the LAN and WAN, an ISDN TE interface is linked to the ISDN NTBA. The Internet connection has been set up.
- A dialing plan with a unique internal telephone number for all terminal equipment to be connected, here, for example, the number '11' for the VoIP softphone and the number '12' for the VoIP telephone.
- A SIP provider account.

Using the information during configuration

The following table provides a summary of the information required for configuration and where it can be entered. SIP terminal equipment parameters can be entered using the SIP telephone keypad, the corresponding configuration software, or the softphone configuration menu.

	LANCOM	SIP terminal equipment
Internal VoIP domain	✔	✔
Internal numbers	✔	✔
External SIP telephone number	✔	
Access information for SIP account	✔	
External ISDN telephone numbers (MSNs)	✔	
Country and local area code	✔	

Configuring the LANCOM

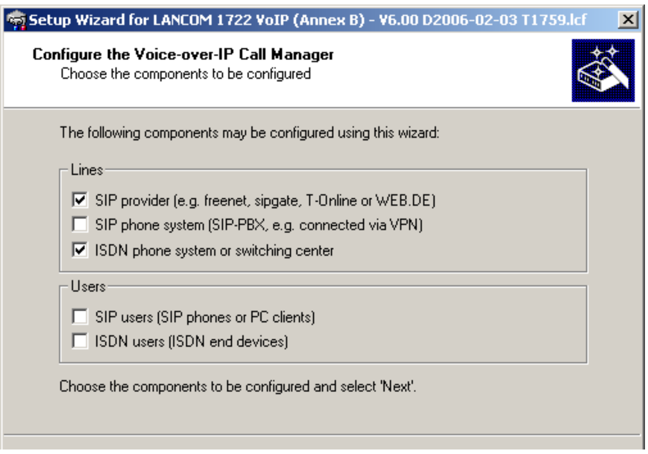
When configuring the LANCOM, the following steps must be carried out:

- Set up the line to the SIP provider
- Enabling the ISDN interface and assigning MSNs to the internal numbers

In this example, it is not necessary to configure SIP users: The SIP users are registered at the LANCOM with the settings created in the terminal equipment (softphone and VoIP telephone).

Detailed instructions on configuring the LANCOM:

① Under LANconfig, start the setup wizard for configuring the VoIP Call Manager. Enable the options 'SIP phone system', 'ISDN phone system' and 'ISDN users'.



Setup Wizard for LANCOM 1722 VoIP (Annex B) - V6.00 D2006-02-03 T1759.lcf

Configure the Voice-over-IP Call Manager
Choose the components to be configured

The following components may be configured using this wizard:

Lines
☑ SIP provider (e.g. freenet, sipgate, T-Online or WEB.DE)
□ SIP phone system (SIP-PBX, e.g. connected via VPN)
☑ ISDN phone system or switching center

Users
□ SIP users (SIP phones or PC clients)
□ ISDN users (ISDN end devices)

Choose the components to be configured and select 'Next'.

② Enter a unique domain for the local VoIP domain which describes the local VoIP range for the site (e.g. 'mycompany.internal'.)

③ Configure the line leading to the SIP provider, for example with the name 'SIPPROVIDER' with the following values:

- □ Internal standard number: All calls that come in through the SIP provider are forwarded to this internal number. Enter an internal number from your dialing plan here, e.g. '11'.
- □ SIP domain/realm: You received this domain from your SIP provider; it is usually entered in the format 'sipdomain.tld' without the part that designates a specific server.
- □ Registrar (FQDN / IP) (optional):
- □ Outbound proxy (optional)

The server description is generally not required; the DNS query for the SIP domain returns this information. Enter a server designation here only if your provider has informed you of the corresponding addresses.

- □ SIP ID / user: Enter the SIP number with local area code here, providing that the SIP provider does not require any other information.
- □ Display name (optional): The display name is only required if the SIP provider verifies this during registration. If you enter a display name here, then this name will be displayed at the remote site. If the field remains empty, then the display name for the corresponding internal user is transmitted.
- □ Authentication name (optional): Special authentication names are not supported by all SIP providers. In many cases, the authentication name is the same as the SIP ID or the user name. Complete this field only if your SIP provider has issued you a special authentication name.
- □ Password: Enter the password for SIP access here.

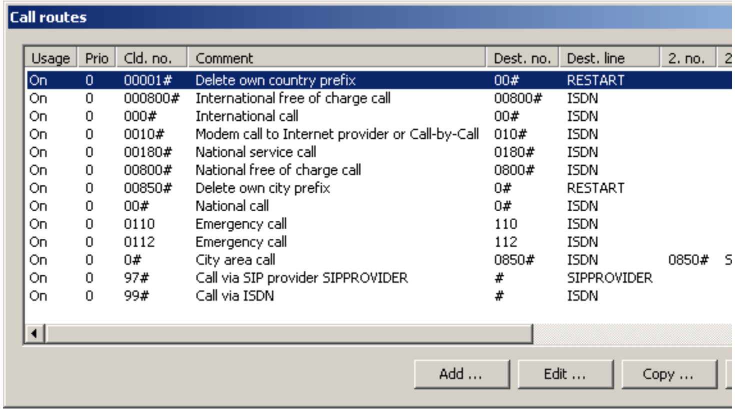
This description applies to a "user-defined configuration". If you select a special SIP provider from the list, then some of the parameters will be pre-configured automatically.

④ Configure an ISDN line for VoIP telephony use. For every MSN on your ISDN connection, make an assignment to an internal number within your telephone number plan during ISDN mapping.

- □ MSN 1 '555 555 1' ▶ internal number '11'
- □ MSN 2 '555 555 2' ▶ internal number '12'

⑤ Enter the local and national area code for the device's location. Using this information, the Voice Call Manager can decide whether or not outgoing calls are local calls, national or international long distance calls.

⑥ Based upon the entries made so far, the LANconfig creates a suggestion for the call routing table which you can adapt to fit your requirements as follows:

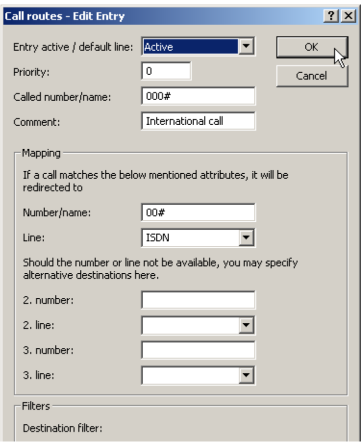


Call routes

Usage	Prio	Cld. no.	Comment	Dest. no.	Dest. line	2. no.	2
On	0	00001#	Delete own country prefix	00#	RESTART		
On	0	000800#	International free of charge call	00800#	ISDN		
On	0	000#	International call	00#	ISDN		
On	0	0010#	Modem call to Internet provider or Call-by-Call	010#	ISDN		
On	0	00180#	National service call	0180#	ISDN		
On	0	00800#	National free of charge call	0800#	ISDN		
On	0	00850#	Delete own city prefix	0#	RESTART		
On	0	00#	National call	0#	ISDN		
On	0	0110	Emergency call	110	ISDN		
On	0	0112	Emergency call	112	ISDN		
On	0	0#	City area call	0850#	ISDN	0850#	S
On	0	97#	Call via SIP provider SIPPROVIDER	#	SIPPROVIDER		
On	0	99#	Call via ISDN	#	ISDN		

The # sign is a placeholder for any character string. The entry '0#' is therefore suitable for all numbers dialed that have at least one '0' preceding them.

This suggested call routing table would place all external calls over the ISDN line. The SIP line is set up as a backup for international and national long distance calls and local calls that are not in the list of special or emergency numbers.



Call routes - Edit Entry

Entry active / default line: Active

Priority: 0

Called number/name: 000#

Comment: International call

Mapping

If a call matches the below mentioned attributes, it will be redirected to

Number/name: 00#

Line: ISDN

Should the number or line not be available, you may specify alternative destinations here.

2. number:

2. line:

3. number:

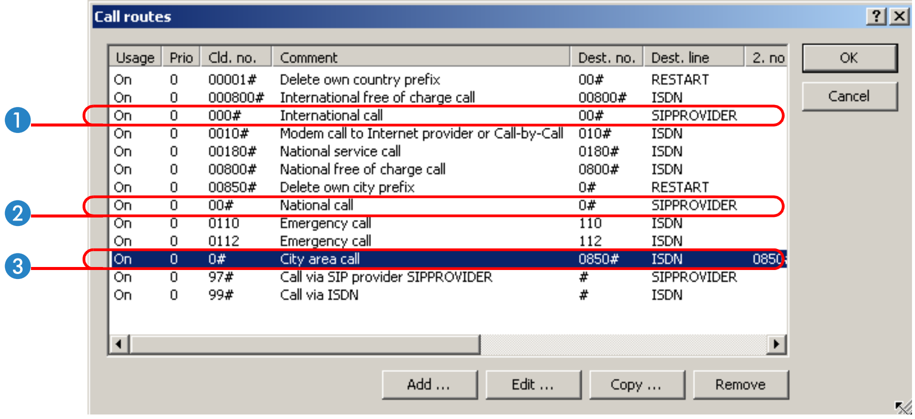
3. line:

Filters

Destination filter:

In order to channel calls to special destinations, such as international and national long distance calls, over the SIP provider, double-click on the corresponding entry in the table and switch the line used from 'ISDN' to 'SIPPROVIDER'. Don't forget to switch the backup line from SIP to ISDN, if necessary!

After being adapted for international ❶ and national ❷ long distance, the call routing table should appear as follows:



Call routes

Usage	Prio	Cld. no.	Comment	Dest. no.	Dest. line	2. no
On	0	00001#	Delete own country prefix	00#	RESTART	
On	0	000800#	International free of charge call	00800#	ISDN	
On	0	000#	International call	00#	SIPPROVIDER	
On	0	0010#	Modem call to Internet provider or Call-by-Call	010#	ISDN	
On	0	00180#	National service call	0180#	ISDN	
On	0	00800#	National free of charge call	0800#	ISDN	
On	0	00850#	Delete own city prefix	0#	RESTART	
On	0	00#	National call	0#	SIPPROVIDER	
On	0	0110	Emergency call	110	ISDN	
On	0	0112	Emergency call	112	ISDN	
On	0	0#	City area call	0850#	ISDN	0850
On	0	97#	Call via SIP provider SIPPROVIDER	#	SIPPROVIDER	
On	0	99#	Call via ISDN	#	ISDN	

Configuring the VoIP terminal equipment

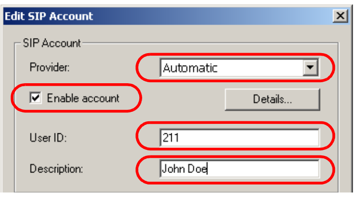
Enter the registration information for the first SIP user in the softphone (example for LANCOM Advanced VPN Client).

Defining the SIP account in the LANCOM Advanced VPN Client to register at the LANCOM VoIP Router or at a PBX

Enter the registration information for the first SIP user in the LANCOM Advanced VPN Client.

① On the ' SIP accounts' tab, use the **Add** button to create a new SIP account.

② For the provider setting, leave the entry as 'Custom' and activate the new account.



Edit SIP Account

SIP Account

Provider: Automatic

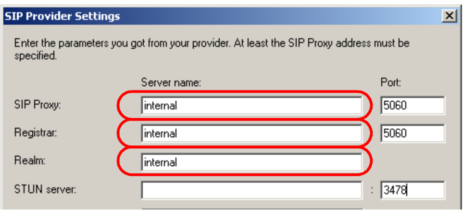
☑ Enable account

User ID: 211

Description: John Doe

③ For the 'User ID' enter the internal telephone number to be used by LANCOM Advanced VPN Client for taking calls and, optionally, enter a name for your phone under 'Description'; this name will be displayed on the other phone at the other end of the connection.

④ With the button **Details**, open the dialog for the advanced settings and enter the following data:



SIP Provider Settings

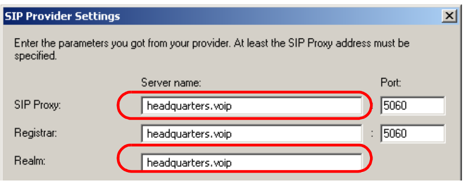
Enter the parameters you got from your provider. At least the SIP Proxy address must be specified.

	Server name:	Port:
SIP Proxy:	internal	5060
Registrar:	internal	5060
Realm:	internal	
STUN server:		3478

- □ As the 'SIP proxy' and 'Registrar', enter the internal VoIP domain for your LANCOM VoIP Router (default: 'internal') if this also acts as the DNS server for the client; if not, enter the LAN IP address.
- □ 'Realm' is always the internal VoIP domain.

With this information, the LANCOM Advanced VPN Client can register locally at a LANCOM VoIP Router and use the telephone lines defined there.

⑤ If the LANCOM Advanced VPN Client is to registering not only with the LANCOM VoIP Router locally, but an upstream SIP PBX (e.g. at Headquarters) as well, then enter under 'SIP proxy', 'Registrar' and, under 'Realm', enter the VoIP domain of the SIP PBX at Headquarters. On the LANCOM VoIP Router, an appropriate SIP-PBX line has to be configured with the same domain, and the router has to be the DNS server for the LANCOM Advanced VPN Client.

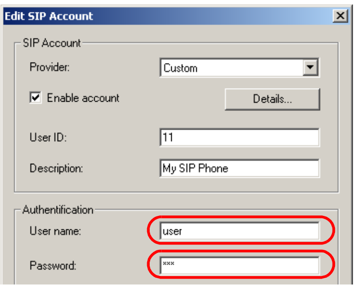


SIP Provider Settings

Enter the parameters you got from your provider. At least the SIP Proxy address must be specified.

	Server name:	Port:
SIP Proxy:	headquarters.voip	5060
Registrar:	headquarters.voip	5060
Realm:	headquarters.voip	

⑥ Enter the SIP-account user name and password for logging in to the SIP PBX.



Edit SIP Account

SIP Account

Provider: Custom

☑ Enable account

User ID: 11

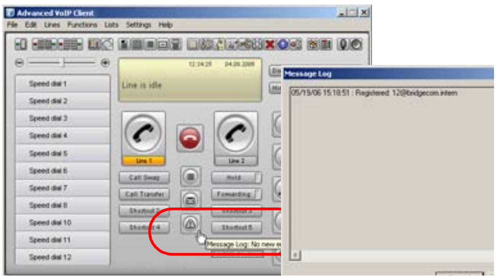
Description: My SIP Phone

Authentification

User name: user

Password: ***

⑦ You can check if the registration was successful by looking at the list of recent messages (via button or menu).



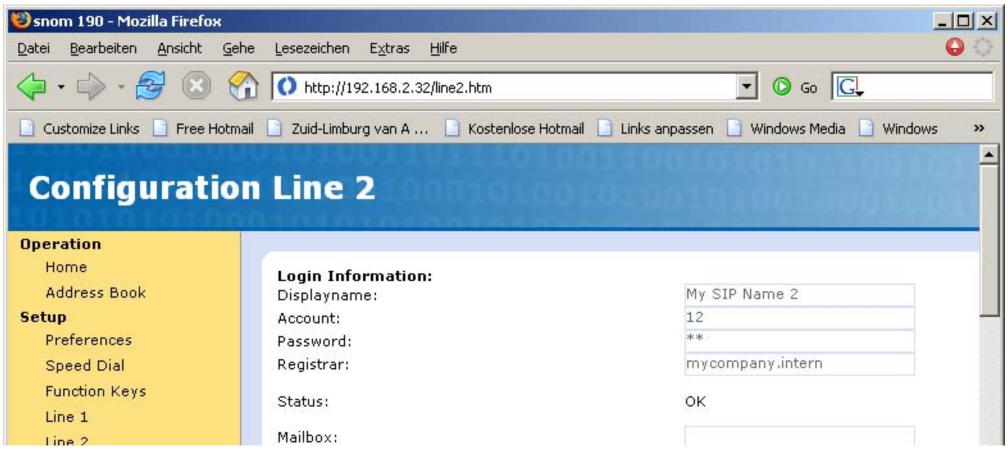
Message Log

05/19/06 15:18:51 : Registered 12@bridgecom.intern

On the tab 'Location' enter your international country code and local code, each without their leading zero(s), and enter the national and international prefixes (e.g. '0' and '00'). The field 'Public line access prefix' is for the character your PBX or LANCOM VoIP Router uses to access an outside line (e.g. '0' or '*').

Enter the registration data for the second SIP user in the VoIP telephone (example for Snom 190).

① From the **Setup** menu, select one of the possible lines, e.g. 'Line 2'.


snom 190 - Mozilla Firefox
Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe
http://192.168.2.32/line2.htm
Go
Customize Links Free Hotmail Zuid-Limburg van A ... Kostenlose Hotmail Links anpassen Windows Media Windows
Operation
Home
Address Book
Setup
Preferences
Speed Dial
Function Keys
Line 1
Line 2

Configuration Line 2

Login Information:

Displayname: My SIP Name 2

Account: 12

Password: **

Registrar: mycompany.intern

Status: OK

Mailbox:

② Enter the following values:

- □ Registrar: Internal VoIP domain for the LANCOM.
- □ Account: Internal number for the user.
- □ Displayname: Name of the user as it is to be displayed at the remote site.

If you use another softphone or VoIP telephone, please consult the documentation for this device for information on configuring the software.

Call routing procedure on outgoing calls

On outgoing calls, the Call Manager first searches the call routing table from top to bottom. If the Call Router cannot find a matching entry there, it uses the list of registered users:

	User	dials	correct call route	correct user	mapping, number in use	Destination line
①	VoIP telephone	11	None	VoIP softphone	11	Internal
②	VoIP telephone	0 555 555	❸ 0#		0241#: 0241 555 555	ISDN
③	VoIP telephone	0 0123 666 666	❷ 00#		0#: 0123 666 666	SIP provider

① The Call Router cannot find a an entry that corresponds to '11' in the call routing table. Now it searches the list of registered users and finds the internal SIP user there.

For call routing, not just the users configured in the LANCOM, but all of the users that are actually registered on the Call Router are used. The SIP users can register themselves as long as they are not entered in the in the LANCOM. The entry for the internal VoIP domain on the LANCOM is sufficient for registration, assuming that local authentication is not required.

② The entry ❸ in the call routing table depicted above matches the number dialed. The call router removes the '0' outside-line access prefix, completes the area code for the local telephone network and completes the call to '0241 555 555' using the ISDN line.

The area code for the local telephone network is added on because calls via SIP providers usually require the area code to be dialed.

③ The entry ❷ in the call routing table is suitable here. The call router removes the '0' prefix for access to the outside line and completes the call to '0123 555 555' via the SIP line. If the SIP line is not available, then the call is made over the ISDN line.

Call routing procedure on incoming calls

For incoming calls, the telephone network exchange removes the prefix from the number dialed (destination number). Therefore, the LANCOM only receives the number itself, which may be treated differently depending on the source:

- Numbers from the ISDN network are translated with the ISDN mapping table to the internal number which is entered for the receiving MSN.

- Calls from a SIP network are converted to the internal destination number that is entered for the respective SIP line.

With the altered number, the Call Manager begins to search the call routing table from top to bottom. If the Call Router cannot find a matching entry there, the call is forwarded directly to the internal number:

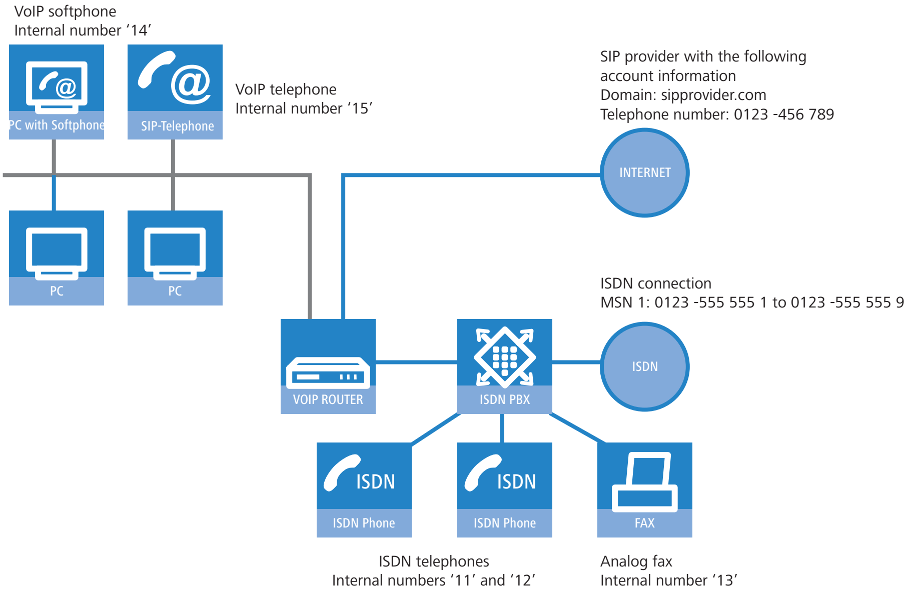
	Remote site dials	Call router receives	Assigned via	number in use	correct call route	Destination line
①	0 123 456 789	456 789	internal destination number for SIP line	11	None	Internal
②	0 123 555 555 1	555 555 1	ISDN mapping	11	None	Internal
③	0 123 555 555 2	555 555 2	ISDN mapping	12	None	Internal

13.13.2 Using VoIP telephony to extend the upstream ISDN PBX

This example shows how to configure a LANCOM when an upstream ISDN PBX is enhanced with VoIP telephony capability. Until now, the MSNs '11' to '13' for the ISDN connection have been used for two ISDN telephones and one analog fax.

The PBX is configured so that subscribers dial '0' to access an outside line.

The LANCOM is operated on an ISDN PBX extension line.



Destination

- Internal telephony with ISDN and SIP telephones and SIP softphones.
- External telephony with VoIP terminal equipment via the SIP provider with backup over ISDN.
- External telephony with ISDN terminal equipment in the PBX. Depending on the functionality of the ISDN PBX, ISDN terminal equipment can also use the SIP lines in the LANCOM VoIP Router ('Configuring ISDN PBX' → page 13-62).
- Accessing internal terminal equipment (ISDN and SIP) via the MSNs.
- Calls to emergency and special numbers via ISDN.

Requirements

- LANCOM connected to the LAN and WAN, an ISDN TE interface is linked to the extension interface on the ISDN PBX. The Internet connection has been set up.
- A dialing plan with a unique internal telephone number for each piece of terminal equipment to be connected. In general, the numbers used are predetermined by the PBX, which often only allows certain number ranges.
- A SIP provider account.

Using the information during configuration

Dialing plans with ISDN PBX systems.

When crossing from the ISDN network to the internal subscribers, the ISDN PBX converts the external MSNs to internal MSNs. When operating a LANCOM VoIP Router at the extension interface of the ISDN PBX, there is another conversion of the internal MSNs to the internal numbers of the VoIP range. For reasons of clarity, we recommend using congruent internal MSNs/numbers for terminal equipment for all connections.

The following table provides a summary of the information required for configuration and where it can be entered. SIP terminal equipment parameters can be entered using the SIP telephone keypad, the corresponding configuration software, or the softphone configuration menu.

	LANCOM	SIP terminal equipment	ISDN PBX	ISDN terminal equipment
Internal VoIP domain	✓	✓		
Internal numbers	✓	✓	✓	✓
External SIP telephone number	✓			
Access information for SIP account	✓			
External ISDN telephone numbers (MSNs)			✓	
Country and local area code	✓			

Configuring the LANCOM

When configuring the LANCOM, the following steps must be carried out:

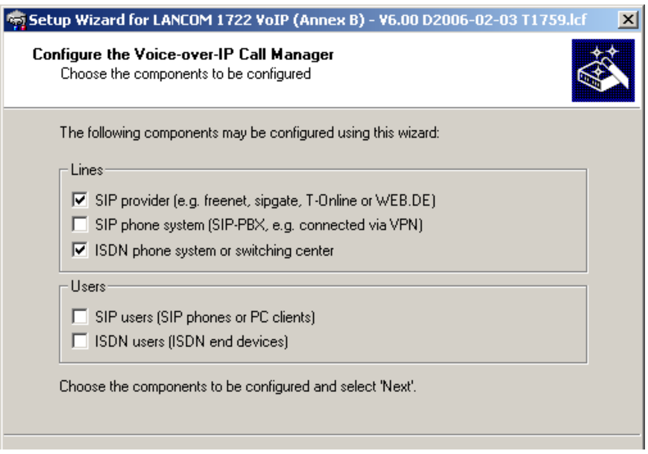
- Set up the line to the SIP provider
- Enabling the ISDN interface and assigning internal MSNs in the PBX to the internal numbers of the LANCOM VoIP Router
- Adapt the call routing table

In this example, it is not necessary to configure SIP or ISDN users:

- The SIP users are registered at the LANCOM with the settings created in the terminal equipment (softphone and VoIP telephone).
- The ISDN devices can be reached via a corresponding entry in the call routing table.

Detailed instructions on configuring the LANCOM:

① Under LANconfig, start the setup wizard for configuring the VoIP Call Manager. Enable the options 'SIP phone system', 'ISDN phone system' and 'ISDN users'.



Setup Wizard for LANCOM 1722 VoIP (Annex B) - V6.00 D2006-02-03 T1759.lcf

Configure the Voice-over-IP Call Manager
Choose the components to be configured

The following components may be configured using this wizard:

Lines
- ☑ SIP provider (e.g. freenet, sipgate, T-Online or WEB.DE)
- ☐ SIP phone system (SIP-PBX, e.g. connected via VPN)
- ☑ ISDN phone system or switching center

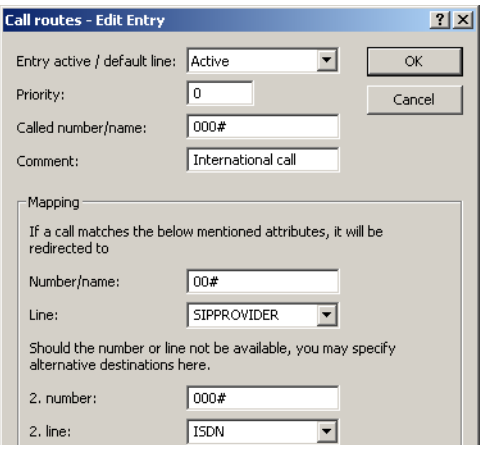
Users
- ☐ SIP users (SIP phones or PC clients)
- ☐ ISDN users (ISDN end devices)

Choose the components to be configured and select 'Next'.

② Configure the device as described in the preceding examples:

- Unique local VoIP domains
- one line to a SIP provider
- ISDN line

③ Adapt the suggested call routing table in order to direct calls to special numbers automatically over the SIP provider's line. The following example shows the entry for international calls.



Call routes - Edit Entry

Entry active / default line: Active

Priority: 0

Called number/name: 000#

Comment: International call

Mapping

If a call matches the below mentioned attributes, it will be redirected to

Number/name: 00#

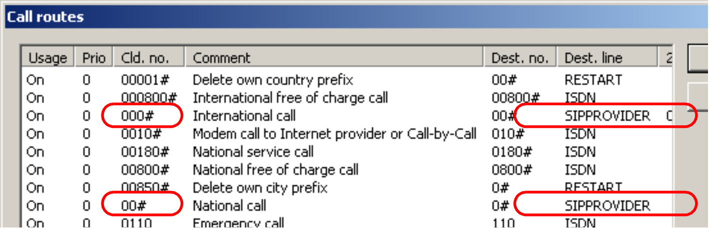
Line: SIPPROVIDER

Should the number or line not be available, you may specify alternative destinations here.

2. number: 000#

2. line: ISDN

After being adapted, the call routing table should appear as follows:



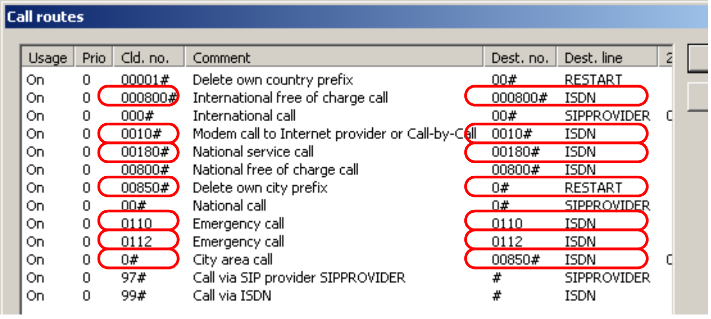
Call routes

Usage	Prio	Cld. no.	Comment	Dest. no.	Dest. line	2
On	0	00001#	Delete own country prefix	00#	RESTART	
On	0	000800#	International free of charge call	00800#	ISDN	
On	0	000#	International call	00#	SIPPROVIDER	C
On	0	0010#	Modem call to Internet provider or Call-by-Call	010#	ISDN	
On	0	00180#	National service call	0180#	ISDN	
On	0	00800#	National free of charge call	0800#	ISDN	
On	0	00850#	Delete own city prefix	0#	RESTART	
On	0	00#	National call	0#	SIPPROVIDER	
On	0	0110	Emergency call	110	ISDN	

Therefore, for every long distance call, the '0' preceding the number is removed, the call is made via the SIP provider.

④ For all ISDN calls, however, the '0' may not be removed from the destination number because the upstream ISDN PBX requires the '0' to access an outside line! Therefore, adapt the destination number for all entries with the target line 'ISDN'.

After being adapted, the call routing table should appear as follows:

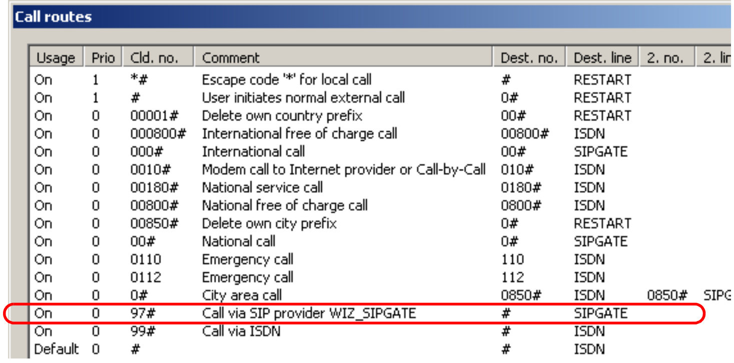


Call routes

Usage	Prio	Cld. no.	Comment	Dest. no.	Dest. line	2
On	0	00001#	Delete own country prefix	00#	RESTART	
On	0	000800#	International free of charge call	000800#	ISDN	
On	0	000#	International call	00#	SIPPROVIDER	C
On	0	0010#	Modem call to Internet provider or Call-by-Call	0010#	ISDN	
On	0	00180#	National service call	00180#	ISDN	
On	0	00800#	National free of charge call	00800#	ISDN	
On	0	00850#	Delete own city prefix	0#	RESTART	
On	0	00#	National call	0#	SIPPROVIDER	
On	0	0110	Emergency call	0110	ISDN	
On	0	0112	Emergency call	0112	ISDN	
On	0	0#	City area call	00850#	ISDN	C
On	0	97#	Call via SIP provider SIPPROVIDER	#	SIPPROVIDER	
On	0	99#	Call via ISDN	#	ISDN	

⑤ In order to allow the ISDN subscribers to be contacted internally by the VoIP users, a standard route is also set up which directs all calls that have not yet been resolved to the ISDN line without changing the numbers.

After being adapted, the call routing table should appear as follows:



Call routes

Usage	Prio	Cld. no.	Comment	Dest. no.	Dest. line	2. no.	2. lir
On	1	*#	Escape code '*' for local call	#	RESTART		
On	1	#	User initiates normal external call	0#	RESTART		
On	0	00001#	Delete own country prefix	00#	RESTART		
On	0	000800#	International free of charge call	00800#	ISDN		
On	0	000#	International call	00#	SIPGATE		
On	0	0010#	Modem call to Internet provider or Call-by-Call	010#	ISDN		
On	0	00180#	National service call	0180#	ISDN		
On	0	00800#	National free of charge call	0800#	ISDN		
On	0	00850#	Delete own city prefix	0#	RESTART		
On	0	00#	National call	0#	SIPGATE		
On	0	0110	Emergency call	110	ISDN		
On	0	0112	Emergency call	112	ISDN		
On	0	0#	City area call	0850#	ISDN	0850#	SIPG
On	0	97#	Call via SIP provider WIZ_SIPGATE	#	SIPGATE		
On	0	99#	Call via ISDN	#	ISDN		
Default	0	#		#	ISDN		

This call routing table is only valid for PBX systems in which the subscribers have to dial '0' to access an outside line. If the PBX uses another mechanism for accessing an outside line, then the table must be adapted accordingly.

Configuring the VoIP terminal equipment

The VoIP terminal equipment is configured as described in the preceding examples with internal VoIP domains and internal numbers for the local site.

Configuring ISDN PBX

When configuring the PBX, external MSNs are assigned to internal MSNs. For every VoIP terminal device, a free internal MSN is linked to an external MSN.

External and internal calls from ISDN terminal devices into VoIP telephony

First, the ISDN terminal devices forward the desired destination number to the ISDN PBX when the call is being established. If the number is an internal number/MSN, then the PBX directs the call to the internal ISDN bus. The SIP terminal equipment connected to the LANCOM can therefore only be reached via an internal call when the PBX knows the internal number for the VoIP user.

If your PBX is able to direct external numbers to the internal ISDN bus, then the ISDN terminal devices can also use the lines configured in the LANCOM, such as the SIP provider line, for outgoing external calls.

Configuring the ISDN terminal equipment

Configuring the ISDN terminal equipment is generally limited to entering the internal MSN used in the PBX.

Call routing procedure on outgoing calls

	User	dials	correct call route	correct user	mapping, number in use	Destination line
①	VoIP telephone	14	None	VoIP softphone	14	Internal
②	VoIP telephone	11	❸ # (Standard)		#: 11	ISDN
③	ISDN telephone	14	■ PBX	VoIP softphone	14	Internal
④	VoIP telephone	0 555 555	❷ 0#		00241#: 0 555 555	ISDN
⑤	ISDN telephone	0 555 555	■ PBX		555 555	ISDN outside line
⑥	VoIP telephone	0 0123 666 666	❶ 00#		0#: 0123 666 666	SIP provider

① Internal call between two VoIP terminal devices.

② Internal call from VoIP to ISDN. In the first pass (without the standard routes), the number '11' does not match any of the routes. Similarly, no matching entry can be found in the list of registered users. In the second pass, the standard route meets '#' (entry ❸ in the call routing table depicted above) and directs the call to the ISDN line **unchanged**. The PBX receives the call on its internal ISDN bus, recognizes the called number as an internal MSN and again forwards the call to the internal ISDN bus to which the respective ISDN terminal device is connected.

③ Internal call from ISDN to VoIP. The ISDN PBX recognizes the destination number '14' as an internal MSN and directs the call to the corresponding internal ISDN bus. The Call Router receives the call to '14', does not find a matching entry in the call routing table but does find an entry in the list of registered users.

④ External call from the VoIP into the local telephone network. The entry ❷ in the call routing table depicted above matches the number dialed. The Call Router completes the area code for the local telephone network and sends the call out to the ISDN line. Only now does the SIP PBX removes the '0' outside-line access prefix and completes the call to '0241 555 555' via the ISDN outside line.

⑤ External call from ISDN into the local telephone network. The ISDN PBX recognizes the destination number as an external destination, removes the '0' outside-line access prefix and completes the call to '555 555' via the ISDN outside line.

⑥ External call from VoIP into the national telephone network. The entry ❶ fits in the call routing table here. The call router removes the '0' prefix for access to the outside line and completes the call to '0123 555 555' via the SIP line. If the SIP line is not available, then the call is made over the ISDN line. In this case, the '0' is not removed from the destination number in order to gain access to an outside line through the PBX.

Call routing procedure on incoming calls

	Remote site dials	Call router receives	Assigned via	number in use	correct call route	Destination line
①	0 123 456 789	456 789	internal destination number for SIP line	11	None	ISDN
②	0 123 555 555 1		ISDN PBX	11		Internal
③	0 123 555 555 4	14	■ ISDN PBX ■ List of local users	14	None	Internal

① The incoming call for the SIP line number is directed to the Call Router along with the internal destination number that has been configured. The Call Router cannot find a matching entry in the call routing table, but it can find a registered user with the matching internal number. Since the user is an ISDN user, the Call Router directs the call to the ISDN line. The PBX receives the number '11' and can determine this call to be an internal call for the connected ISDN telephone.

② The incoming calls to the MSNs for the connected ISDN terminal equipment can be assigned directly by the PBX itself, the Call Router is not involved here.

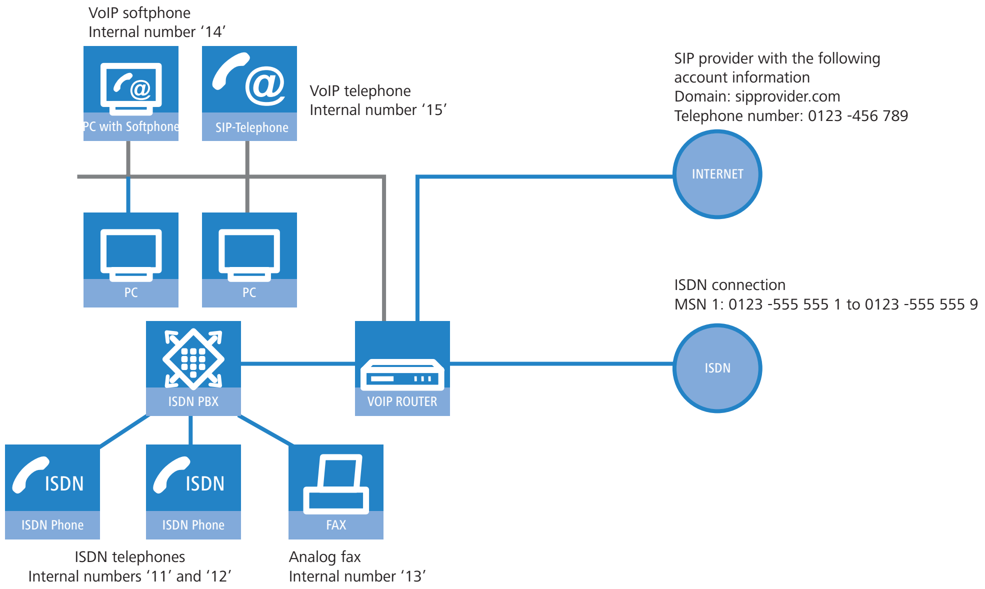
③ The PBX directs incoming calls to the MSNs for the connected VoIP terminal equipment to the internal ISDN bus with the internal MSN. The Call Router receives these calls as if they were internal calls and forwards them to the appropriate user since no corresponding entry can be found in the call routing table here either.

13.13.3 Using VoIP telephony to extend the downstream ISDN PBX

This example shows how to configure a LANCOM when a downstream ISDN PBX is enhanced with VoIP telephony capability. Until now, the MSNs '11' to '13' for the ISDN connection have been used for two ISDN telephones and one analog fax. The LANCOM will now be switched between the public ISDN connection and the ISDN PBX.

The PBX is configured to allow subscribers to receive immediate access to an outside line when they pick up the receiver.

This ISDN PBX is operated as a downstream PBX on the ISDN NT interface of the LANCOM.



Destination

- Internal telephony with ISDN and SIP telephones and SIP softphones.
- External telephony with ISDN and SIP terminal equipment over ISDN.
- Accessing internal terminal equipment (ISDN and SIP) via the MSNs.

Requirements

- LANCOM connected to the LAN and WAN, an ISDN NT interface is linked to the outside exchange line on the ISDN PBX. The Internet connection has been set up.

- A dialing plan with a unique internal telephone number for each piece of terminal equipment to be connected. In general, the numbers used are predetermined by the PBX, which often only allows certain number ranges.
- A SIP provider account.

Using the information during configuration

Dialing plans with ISDN PBX systems.

When crossing from the ISDN network to the internal subscribers, the ISDN PBX converts the external MSNs to internal MSNs. When operating a LANCOM VoIP Router at the extension interface of the ISDN PBX, there is another conversion of the internal MSNs to the internal numbers of the VoIP range. For reasons of clarity, we recommend using congruent internal MSNs/numbers for terminal equipment for all connections.

The following table provides a summary of the information required for configuration and where it can be entered. SIP terminal equipment parameters can be entered using the SIP telephone keypad, the corresponding configuration software, or the softphone configuration menu.

	LANCOM	SIP terminal equipment	ISDN PBX	ISDN terminal equipment
Internal VoIP domain	✔	✔		
Internal numbers	✔	✔	✔	✔
External SIP telephone number	✔			
Access information for SIP account	✔			
External ISDN telephone numbers (MSNs)	✔			
Country and local area code	✔			

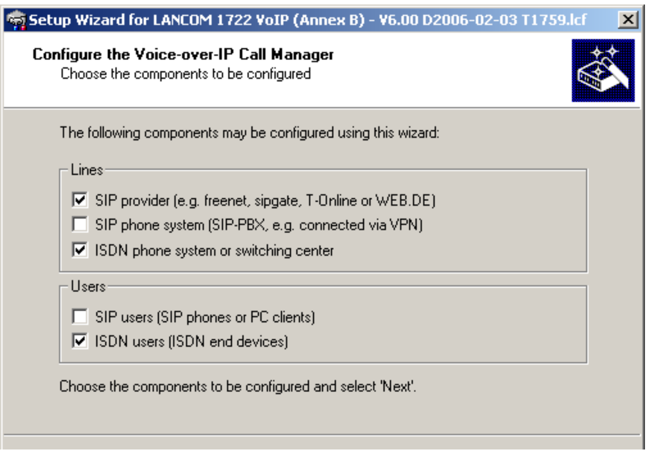
Configuring the LANCOM

When configuring the LANCOM, the following steps must be carried out:

- Set up the line to the SIP provider
- Enabling the ISDN interface and assigning MSNs to the internal numbers in the LANCOM VoIP Router
- Creating ISDN users
- Adapt the call routing table

Detailed instructions on configuring the LANCOM:

① Under LANconfig, start the setup wizard for configuring the VoIP Call Manager. Enable the options 'SIP provider', 'ISDN phone system' and 'ISDN users'.



Setup Wizard for LANCOM 1722 VoIP (Annex B) - V6.00 D2006-02-03 T1759.lcf

Configure the Voice-over-IP Call Manager
Choose the components to be configured

The following components may be configured using this wizard:

Lines
☑ SIP provider (e.g. freenet, sipgate, T-Online or WEB.DE)
☐ SIP phone system (SIP-PBX, e.g. connected via VPN)
☑ ISDN phone system or switching center

Users
☐ SIP users (SIP phones or PC clients)
☑ ISDN users (ISDN end devices)

Choose the components to be configured and select 'Next'.

② Configure the device as described in the preceding examples:

- □ Unique local VoIP domains
- □ one line to a SIP provider

③ Enable the external ISDN outside line and the internal ISDN bus in order to use the VoIP functionality. Enter all external MSNs for the ISDN outside line in the ISDN mapping table with their assignment to the internal numbers in the VoIP range.

④ Enter all connected ISDN terminal devices as ISDN users with the following values:

- □ Telephone number / SIP name: This number will be assigned to the ISDN terminal device as an "internal number". The telephone structure will remain clear if you use the same internal number for a terminal device here as it uses in its own ISDN environment.
- □ MSN/DDI: Enter the external MSNs for the ISDN outside line here; this will also be assigned to the terminal device by the ISDN PBX.

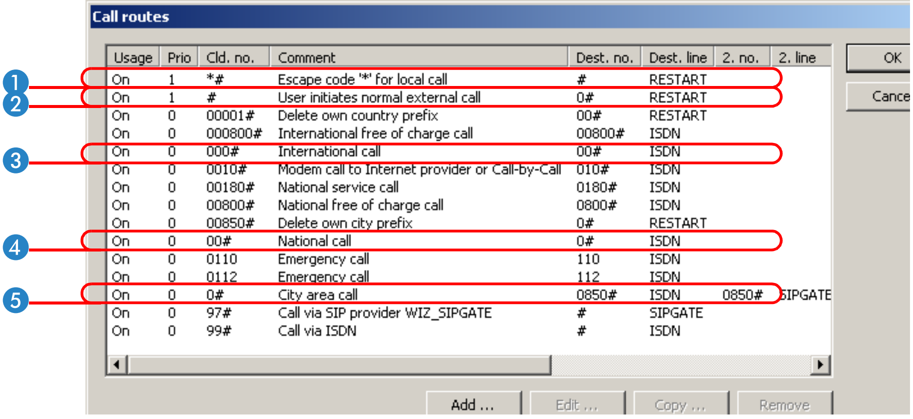
⑤ Enable spontaneous outside line access for ISDN and SIP users in order to keep the subscribers' telephone behavior as consistent as possible.

⑥ The call routing table suggested by the setup wizard automatically allows spontaneous outside line access for ISDN and SIP users ❶ and ❷.

Routes for spontaneous outside line access

Entering the source line 'USER' is not visible in the screenshot. Using this filter, the route will only be in effect for calls that originate from a local user. The destination line 'RESTART' prompts a new pass through the call routing table, whereby the source line is deleted. Due to the missing source line, the route does not match this call during the second pass.

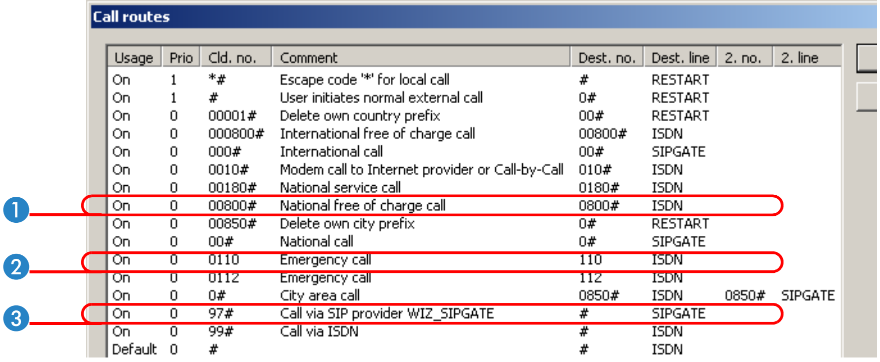
As a result of both of these routes, any stars '*' that might have preceded the numbers are removed before each call from a local user. For all other calls from local users, the number is preceded with a '0', as it is automatically assumed that the user is trying to establish an outside connection.



Usage	Prio	Cld. no.	Comment	Dest. no.	Dest. line	2. no.	2. line
On	1	*#	Escape code '*' for local call	#	RESTART		
On	1	#	User initiates normal external call	0#	RESTART		
On	0	00001#	Delete own country prefix	00#	RESTART		
On	0	000800#	International free of charge call	00800#	ISDN		
On	0	000#	International call	00#	ISDN		
On	0	0010#	Modem call to Internet provider or Call-by-Call	010#	ISDN		
On	0	00180#	National service call	0180#	ISDN		
On	0	00800#	National free of charge call	0800#	ISDN		
On	0	00850#	Delete own city prefix	0#	RESTART		
On	0	00#	National call	0#	ISDN		
On	0	0110	Emergency call	110	ISDN		
On	0	0112	Emergency call	112	ISDN		
On	0	0#	City area call	0850#	ISDN	0850#	SIPGATE
On	0	97#	Call via SIP provider WIZ_SIPGATE	#	SIPGATE		
On	0	99#	Call via ISDN	#	ISDN		

The other routes are used to carry out international ❸ and national ❹ long distance calls as well as local calls ❺ as standard over the ISDN line. The Call Router removes the preceding zeros from the number again and sends the call out to the ISDN line.

In order to channel calls to special destinations, such as international and national long distance calls, over the SIP provider and not over ISDN, double-click on the corresponding entry in the table and switch the line used form 'ISDN' to 'SIPPROVIDER'. Don't forget to switch the backup line from SIP to ISDN, if necessary!



Usage	Prio	Cld. no.	Comment	Dest. no.	Dest. line	2. no.	2. line
On	1	*#	Escape code '*' for local call	#	RESTART		
On	1	#	User initiates normal external call	0#	RESTART		
On	0	00001#	Delete own country prefix	00#	RESTART		
On	0	000800#	International free of charge call	00800#	ISDN		
On	0	000#	International call	00#	SIPGATE		
On	0	0010#	Modem call to Internet provider or Call-by-Call	010#	ISDN		
On	0	00180#	National service call	0180#	ISDN		
On	0	00800#	National free of charge call	0800#	ISDN		
On	0	00850#	Delete own city prefix	0#	RESTART		
On	0	00#	National call	0#	SIPGATE		
On	0	0110	Emergency call	110	ISDN		
On	0	0112	Emergency call	112	ISDN		
On	0	0#	City area call	0850#	ISDN	0850#	SIPGATE
On	0	97#	Call via SIP provider WIZ_SIPGATE	#	SIPGATE		
On	0	99#	Call via ISDN	#	ISDN		
Default	0	#		#	ISDN		

This call routing table is only valid for PBX systems that forward the special character star '*' for internal calls on their external ISDN bus. If the PBX processes this character in a different manner, then the table must be adapted accordingly.

Configuring the VoIP terminal equipment

The VoIP terminal equipment is configured as described in the preceding examples with internal VoIP domains and internal numbers for the local site.

Configuring ISDN PBX

When configuring the PBX, external MSNs are assigned to internal MSNs. For every VoIP terminal device, a free internal MSN is linked to an external MSN. The internal number for the SIP user can be used as an external MSN for the VoIP terminal equipment in the PBX.

Configuring the ISDN terminal equipment

Configuring the ISDN terminal equipment is generally limited to entering the internal MSN used in the PBX.

Call routing procedure on outgoing calls

	User	dials	correct call route	correct user	mapping, number in use	Destination line
①	VoIP telephone	*14	❶ *#	VoIP softphone	#: 14	Internal
②	VoIP telephone	*11	❶ *#	ISDN users	#: 11	ISDN

① Internal call between two VoIP terminal devices. On the first pass, only the star is removed from the number, the source line is deleted. During the second pass, no other route matches this call but the Call Router finds a matching entry for a SIP user in the list of registered users and can complete the call.

② Internal call from VoIP to ISDN. On the first pass, the star is removed from the number again, the source line is deleted. During the second pass, no other route matches this call but the Call Router finds a matching entry for an ISDN user in the list of registered users and establishes the call via the ISDN interface configured for this user. The destination number is replaced by the MSN entered for this user '555 555 1' . The PBX receives the call to '555 555 1' on its external ISDN bus and again determines that this is an external MSN and can channel the call to the corresponding ISDN telephone.

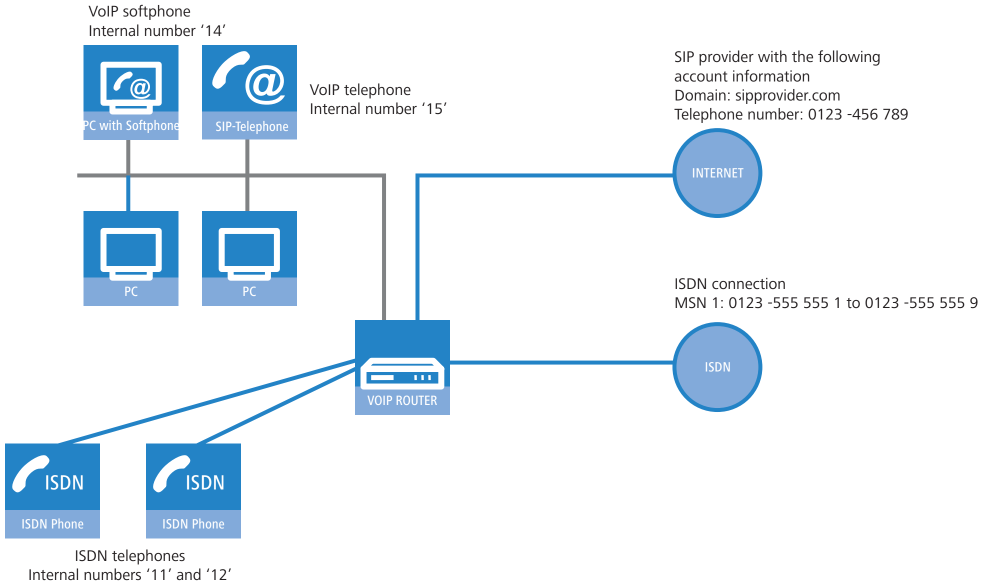
Call routing procedure on incoming calls

	Remote site dials	Call router receives	Assigned via	number in use	correct call route	Destination line
①	0 123 555 555 1	555 555 1	■ ISDN mapping table ■ List of local ISDN users	11		ISDN NT

① The incoming call via the number to the MSNs for the connected ISDN terminal equipment is converted into an internal number by the ISDN mapping table and passed on to the Call Router. The Call Router cannot find a matching entry in the call routing table, but it can find a registered user with the matching internal number. Since the user is an ISDN user, the Call Router directs the call to the ISDN line with the MSN entered for this user, '555 555 1'. The PBX receives the call to '555 555 1' on its external ISDN bus and again determines that this is an external MSN and can channel the call to the corresponding ISDN telephone.

13.13.4 Using VoIP telephony to supplement existing ISDN telephones

This example shows how to configure a LANCOM when the ISDN telephones used unit now are to be enhanced with VoIP telephony. The external MSNs '555 555 1' and '555 555 2' on the ISDN bus at the NTBA were used for two ISDN telephones until now. The LANCOM will now be switched between the public ISDN connection and the internal ISDN bus connected to the ISDN telephones.



Destination

- Internal telephony with ISDN and SIP telephones and SIP softphones.
- External telephony with ISDN and SIP terminal equipment over ISDN.
- Accessing internal terminal equipment (ISDN and SIP) via the MSNs.

Requirements

- LANCOM connected to LAN and WAN, an ISDN NT interface connected to the ISDN telephone, an ISDN TE interface connected to the ISDN outside line (NTBA). The Internet connection has been set up.
- A dialing plan with a unique internal telephone number for each piece of terminal equipment to be connected.
- A SIP provider account.

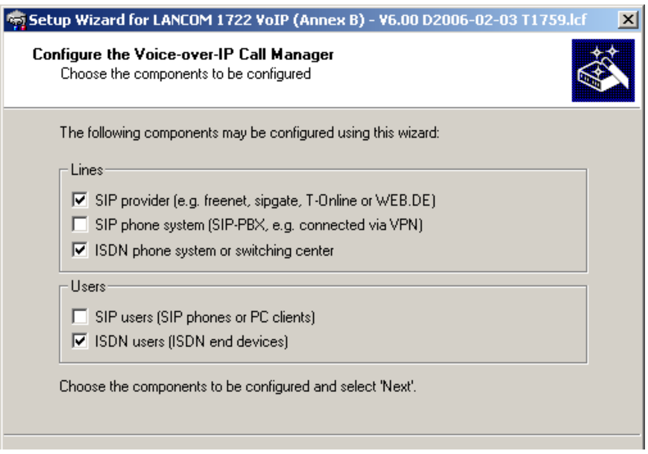
Configuring the LANCOM

When configuring the LANCOM, the following steps must be carried out:

- Set up the line to the SIP provider
- Enabling the ISDN interface and assigning MSNs to the internal numbers in the LANCOM VoIP Router
- Creating ISDN users
- Adapt the call routing table

Detailed instructions on configuring the LANCOM:

① Under LANconfig, start the setup wizard for configuring the VoIP Call Manager. Enable the options 'SIP provider', 'ISDN phone system' and 'ISDN users'.


Setup Wizard for LANCOM 1722 VoIP (Annex B) - V6.00 D2006-02-03 T1759.lcf

Configure the Voice-over-IP Call Manager

Choose the components to be configured

The following components may be configured using this wizard:

Lines

☑ SIP provider (e.g. freenet, sipgate, T-Online or WEB.DE)

☐ SIP phone system (SIP-PBX, e.g. connected via VPN)

☑ ISDN phone system or switching center

Users

☐ SIP users (SIP phones or PC clients)

☑ ISDN users (ISDN end devices)

Choose the components to be configured and select 'Next'.

② Configure the device as described in the preceding examples:

- □ Unique local VoIP domains
- □ one line to a SIP provider

③ Enable the external ISDN outside line and the internal ISDN bus in order to use the VoIP functionality. Enter all external MSNs for the ISDN outside line in the ISDN mapping table with their assignment to the internal numbers in the VoIP range.

④ Enter all connected ISDN terminal devices as ISDN users with the following values:

- □ Telephone number / SIP name: This number will be assigned to the ISDN terminal device as an "internal number". The telephone structure will remain clear if you use the same internal number for a terminal device here as it uses in its own ISDN environment.
- □ MSN/DDI: Here, enter the external MSN of the ISDN outside line which was formerly entered into the ISDN telephone.

Assigning external MSNs to internal telephone numbers

In this example, the external MSNs and the internal telephones will be assigned "crossed over":

- ■ In the ISDN mapping table, the external MSN '555 555 1' is assigned to the internal telephone number '11', for example. An external call to '555 555 1' will be switched by the LANCOM as a call to '11'.
- ■ By assigning the MSN '555 555 1' to the internal telephone number of the ISDN user '11', the call will be directed over the internal ISDN bus of the LANCOM with the target telephone number '555 555 1'.

Because the ISDN telephone "listens" out for its own MSN, exactly as it used to before implementing the LANCOM VoIP Router, the call is placed to the correct telephone.

Should the LANCOM VoIP Router fail due to a power outage, the life-line support and power relay over the ISDN bus, if activated, enable the connected telephones to continue to function.

⑤ Enable spontaneous outside line access for ISDN and SIP users in order to keep the subscribers' telephone behavior as consistent as possible.

⑥ The continued configuration and changes to the call routing table are carried out just as in the example 'Using VoIP telephony to extend the downstream ISDN PBX'.

Configuring the VoIP terminal equipment

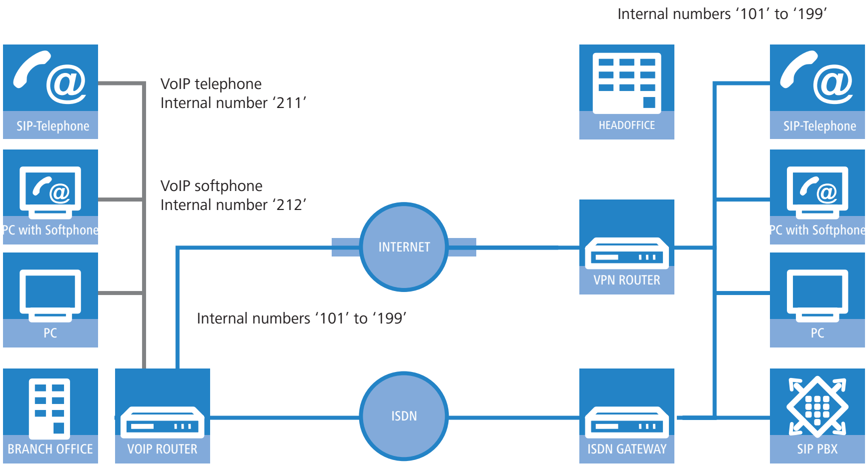
The VoIP terminal equipment is configured as described in the preceding examples with internal VoIP domains and internal numbers for the local site.

Configuring the ISDN telephones

Configuring the ISDN terminal equipment is generally limited to entering the external MSN. As a rule, the MSNs were already entered into the ISDN telephones before, and so no changes should be necessary.

13.13.5 Connecting to an upstream SIP PBX

In this example, a branch office network will be connected to the headquarters network over VPN. In addition to data transfer, the telephone structure in the branch office is also connected to the central SIP PBX. A LANCOM VoIP Router is used in the branch office network and a LANCOM VPN router, for example, could act as the VPN end point at the headquarters. The telephony subscribers at the headquarters receive internal extensions from the number range '101' to '199'; for each of the branch offices, a 10-digit block from the 200 range is reserved - in this example, '211' to '219'.



Destination

- Internal telephony between all locations.
- External telephony from the branch office via the SIP PBX at the headquarters with backup over ISDN.
- Calls from the branch office into the local telephone network via ISDN.
- Calls to emergency and special numbers via ISDN.

Requirements

- LANCOM connected to the LAN and WAN, an ISDN TE interface is linked to the ISDN NTBA.
- The Internet connection has been set up by means of a VPN tunnel, as has the network connection between the two locations. All terminal devices can contact each other with the IP addresses used.
- A dialing plan with a unique internal telephone number for each piece of terminal equipment to be connected.
- A SIP provider account.

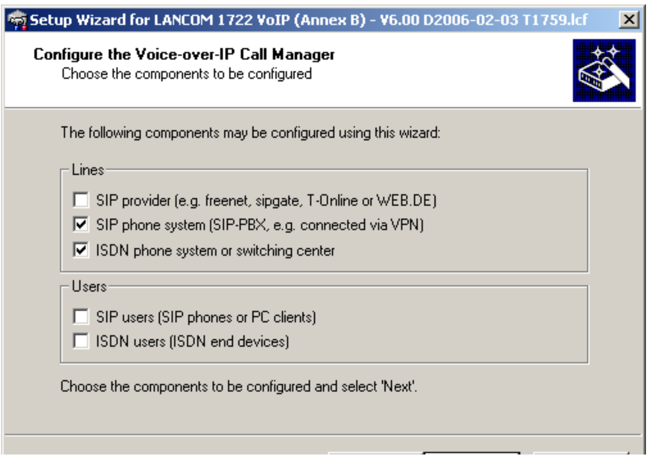
Configuring the LANCOM

The following table provides a summary of the information required for configuration and where it can be entered. Basically, all that is needed is a SIP PBX line for each location that is correspondingly setup at the remote location

	LANCOM	SIP terminal equipment	SIP PBX
	Branch office	Branch office	Headquarters
Internal VoIP domain	mycompany.BRANCH01	mycompany.HQ	mycompany.HQ
Internal SIP subscriber numbers at the branch office		✓	✓
External ISDN telephone numbers (MSNs)	✓		
Country and local area code	✓		
SIP PBX line	HQ		
SIP PBX domains	mycompany.HQ		
SIP PBX registration password	✓		✓
Call route	■ Called number '2#' ■ Destination line 'LOCATION_B' ■ Destination number ''2#'		

Detailed instructions on configuring the LANCOM:

① Under LANconfig, start the setup wizard for configuring the VoIP Call Manager. Enable the options 'SIP phone system', 'ISDN phone system' and 'ISDN users'.



Setup Wizard for LANCOM 1722 VoIP (Annex B) - V6.00 D2006-02-03 T1759.lcf

Configure the Voice-over-IP Call Manager

Choose the components to be configured

The following components may be configured using this wizard:

Lines

☐ SIP provider (e.g. freenet, sipgate, T-Online or WEB.DE)

☑ SIP phone system (SIP-PBX, e.g. connected via VPN)

☑ ISDN phone system or switching center

Users

☐ SIP users (SIP phones or PC clients)

☐ ISDN users (ISDN end devices)

Choose the components to be configured and select 'Next'.

② Configure the device as described in the preceding examples:

- □ ISDN line with MSN mapping
- □ Area and country code for each location

③ Enter a unique domain for the local VoIP domain which describes the local VoIP range for the branch office, e.g. 'mycompany.BRANCH01' for the first branch.

④ Configure the line leading to the SIP PBX with the following values:

- □ SIP PBX line name: Unique name for the line leading to the SIP PBX, e.g. 'HQ' for "Headquarters".
- □ PBX SIP domain/realm: Internal VoIP domain or SIP PBX, e.g. 'mycompany.HQ'.
- □ Registrar (FQDN or IP) (optional): SIP PBX address in the headquarters network, in the event that the device cannot be identified via DNS resolution of the VoIP domain (PBX SIP domain/realm).

Use the SIP PBX IP address from the private IP address range at the headquarters that can be reached via VPN here.

- □ Outbound proxy (optional): It is generally not necessary to designate the outbound proxy. Only enter a server designation here should the SIP PBX require your corresponding addresses.
- □ Shared PBX password: This password is used by all SIP users when registering at the SIP PBX.

Shared or user-dependent SIP PBX password

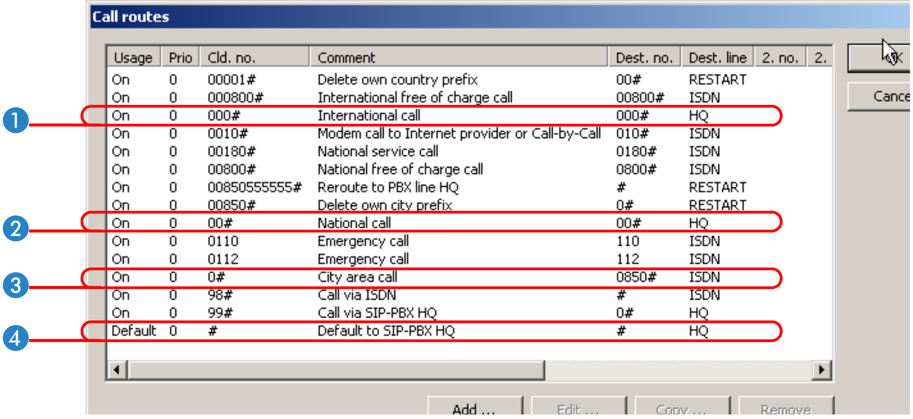
If registration with a shared password is not desired, then an individual password can be used for each SIP user. In this case, each SIP user is configured with its own password in the LANCOM.

- □ Public PBX number: Here, enter the number at which the SIP PBX is to be be reached over the public telephone network from the location of the LANCOM. The number is entered with the **necessary** prefixes, but without an extension number. For example, if the SIP PBX is located in London and the LANCOM is in Birmingham, then the public PBX number is '020 12345'.

⑤ The call routing table suggested by the setup wizard automatically allows international ❶ and national ❷ long distance calls to be made via the SIP PBX at the headquarters.

In addition, a **standard route** ❹ is used in order to conduct calls from the LANCOM VoIP range to internal SIP PBX numbers via the corresponding SIP PBX lines.

This special entry is only used during the second pass in the call routing table, after the first pass found no corresponding entry for "normal" routes and if no matching internal number was found in the list of local users.



Usage	Prio	Cld. no.	Comment	Dest. no.	Dest. line	2. no.	2.
On	0	00001#	Delete own country prefix	00#	RESTART		
On	0	000800#	International free of charge call	00800#	ISDN		
On	0	000#	International call	000#	HQ		
On	0	0010#	Modem call to Internet provider or Call-by-Call	010#	ISDN		
On	0	00180#	National service call	0180#	ISDN		
On	0	00800#	National free of charge call	0800#	ISDN		
On	0	00850555555#	Reroute to PBX line HQ	#	RESTART		
On	0	00850#	Delete own city prefix	0#	RESTART		
On	0	00#	National call	00#	HQ		
On	0	0110	Emergency call	110	ISDN		
On	0	0112	Emergency call	112	ISDN		
On	0	0#	City area call	0850#	ISDN		
On	0	98#	Call via ISDN	#	ISDN		
On	0	99#	Call via SIP-PBX HQ	0#	HQ		
Default	0	#	Default to SIP-PBX HQ	#	HQ		

Configuring the VoIP terminal equipment

The VoIP terminal equipment is configured as described in the preceding examples. However, here, the SIP PBX VoIP domain and the internal numbers configured in the SIP PBX are used.

Automatic SIP user registration with the LANCOM and the SIP PBX.

By using the SIP PBX domain with VoIP terminal equipment, the user is registered in two ways:

- Since registration takes place with a valid domain defined in the LANCOM, terminal devices are registered as "local users".
- Since the domain that is used does not correspond to the LANCOM's own VoIP domain, a simultaneous attempt is made at registering with the upstream SIP PBX. If the password used corresponds to the password stored in the SIP PBX for this user, then the registration on the SIP PBX will be successful.

Configuring the SIP PBX

In the SIP PBX, all users from the branch office network are entered with their own internal number. For this purpose, either the shared password is entered or a separate password is assigned for each user ('Shared or user-dependent SIP PBX password' → page 13-70).

Call routing procedure on outgoing calls

	User	dials	correct call route	correct user	mapping, number in use	Destination line
①	Branch VoIP telephone	212	None	VoIP softphone	212	Internal
②	Branch VoIP telephone	199	❹ #	SIP subscribers at the headquarters	#: 199	SIP PBX
③	Branch VoIP telephone	0 555 555	❸ 0#		0241#: 0241 555 555	ISDN
④	Branch VoIP telephone	0 0123 666 666	❷ 00#		00#: 0123 666 666	SIP PBX

① Internal call between two VoIP terminal devices at the branch office. The number dialed, '212', does not match any of the routes listed in the call routing table. Therefore, the call router searches the local user list, finds the correct entry there and can forward the call internally.

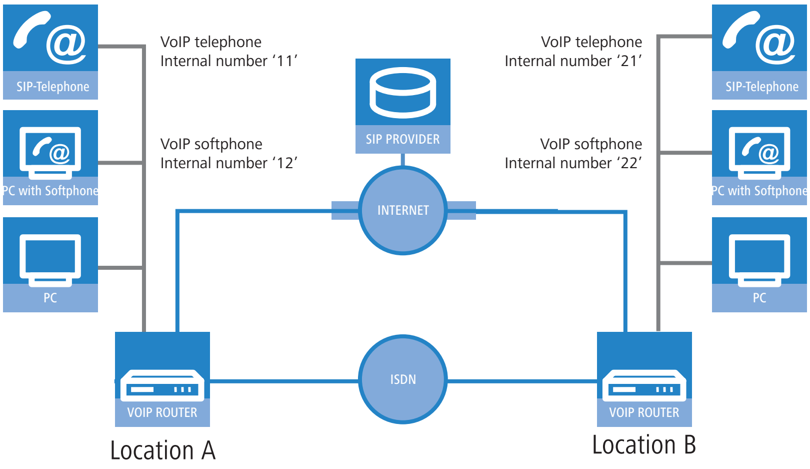
② Internal call between a VoIP terminal device at the branch office and the internal subscriber '199' at the headquarters. The number dialed, '199', does not match any of the routes listed in the call routing table during the first pass. Similarly, no matching entry can be found in the local user list. In the second pass through the call routing table, the standard routes are considered too. The route with the number called '#' ❹ corresponds to all calls which could not be assigned earlier. The call to '199' is therefore carried out over the SIP PBX line.

③ External call from the branch office into the local telephone network. The number dialed, '0 555,555', matches the route '0#' ❸ in the call routing table. The call router removes the '0' outside-line access prefix, completes the area code for the local telephone network and completes the call to '0241 555 555' using the ISDN line.

④ External call from the branch office into a national telephone network. The number dialed, '0 0123 555 555', matches the route '00#' ❷ in the call routing table. The call router sends the call out to the SIP PBX line **unchanged**. Only now does the SIP PBX removes the '0' outside-line access prefix and completes the call to '0123 555 555' via the ISDN outside line.

13.13.6 VoIP connectivity for locations without a SIP PBX

Companies with widely disperse offices and without their own SIP PBX can also take advantage of VoIP site-to-site connectivity. In this "Peer-to-Peer" scenario, a LANCOM VoIP Router has been implemented at both locations.



Destination

- Internal telephony at and between both locations.
- External telephony via the SIP provider with backup over ISDN.
- Calls to emergency and special numbers via ISDN.

Requirements

- LANCOM connected to the LAN and WAN, an ISDN TE interface is linked to the ISDN NTBA.
- The Internet connection has been set up by means of a VPN tunnel, as has the network connection between the two locations. All terminal devices can contact each other with the IP addresses used.

- A dialing plan with a unique internal telephone number for each piece of terminal equipment to be connected. For each site, a separate number range is used; in this example, the internal numbers for location A begin with a '1' and the internal numbers for location B begin with a '2'.
- Each site has a SIP provider account.

Configuring the LANCOM

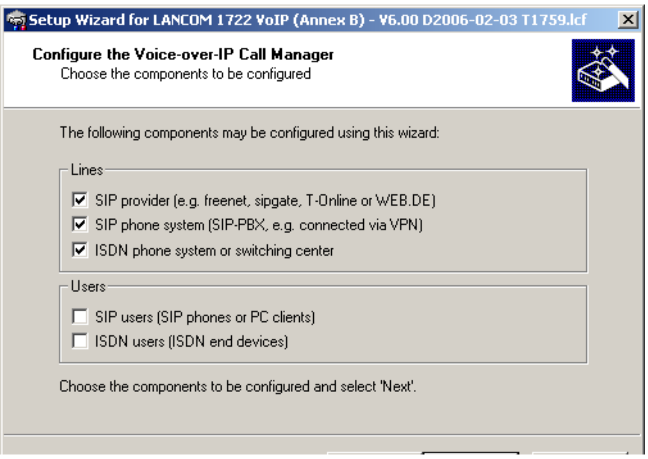
The following table provides a summary of the information required for configuration and where it can be entered. Basically, all that is needed is a SIP PBX line for each location that is correspondingly setup at the remote location

	LANCOM Location A	SIP terminal equipment location A	LANCOM Location B	SIP terminal equipment location B
Internal VoIP domain	location_A.internal	location_A.internal	location_B.internal	location_B.internal
Internal numbers		10 to 19		20 to 29
External SIP telephone number	✓		✓	
Access information for SIP account	✓		✓	
External ISDN telephone numbers (MSNs)	✓		✓	
Country and local area code	✓		✓	
SIP PBX line	LOCATION_B		LOCATION_A	
SIP PBX domains	location_B.internal		location_A.internal	
Call route	■ Called number '2#' ■ Destination line 'LOCATION_B' ■ Destination number ''2#'		■ Called number '1#' ■ Destination line 'LOCATION_A' ■ Destination number ''1#'	

Although SIP PBX lines are the subject of the configuration presented here, you can still use this function even without a PBX.

Detailed instructions on configuring the LANCOM:

① Under LANconfig, start the setup wizard for configuring the VoIP Call Manager. Enable the options 'SIP phone system', 'ISDN phone system' and 'ISDN users'.



Setup Wizard for LANCOM 1722 VoIP (Annex B) - V6.00 D2006-02-03 T1759.lcf

Configure the Voice-over-IP Call Manager

Choose the components to be configured

The following components may be configured using this wizard:

Lines

☑ SIP provider (e.g. freenet, sipgate, T-Online or WEB.DE)

☑ SIP phone system (SIP-PBX, e.g. connected via VPN)

☑ ISDN phone system or switching center

Users

☐ SIP users (SIP phones or PC clients)

☐ ISDN users (ISDN end devices)

Choose the components to be configured and select 'Next'.

② Configure the device as described in the preceding examples:

- □ one line to a SIP provider
- □ ISDN line with MSN mapping
- □ Area and country code for each location

③ Enter a unique domain for the local VoIP domain which describes the local VoIP range for the site. Both sites use **different** VoIP domains, e.g. 'location_A.internal' or 'location_B.internal'.

④ Configure the line leading to the SIP PBX with the following values:

- □ SIP PBX line name: Unique name for the line leading to the remote site.
- □ PBX SIP domain/realm: Internal VoIP domain for the remote site.

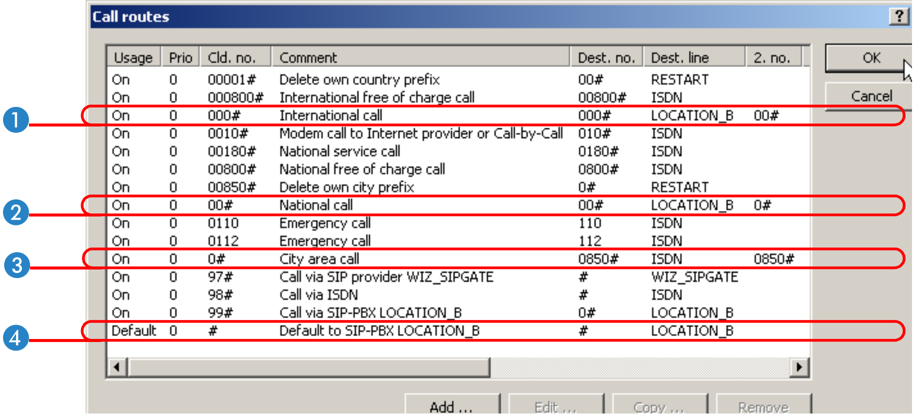
- □ Registrar (FQDN or IP): Address for the LANCOM at the remote site, in the event that the device cannot be identified via DNS resolution of the VoIP domain (PBX SIP domain/realm).

Use the private IP address that can be reached via VPN for the LANCOM here, not the public IP.

- □ Leave the field for the shared password empty when registering to the SIP PBX.
- □ Leave the field for the public PBX number empty.

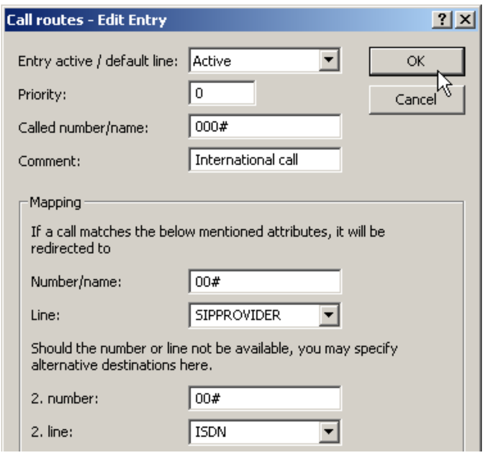
⑤ The call routing table suggested by the setup wizard automatically allows international ❶ and national ❷ long distance calls to be made via remote site's line, local calls ❸ are routed via ISDN.

In addition, a **standard route** ❹ directs all numbers which cannot be resolved to the remote location's line.



Usage	Prio	Cld. no.	Comment	Dest. no.	Dest. line	2. no.
On	0	00001#	Delete own country prefix	00#	RESTART	
On	0	000800#	International free of charge call	00800#	ISDN	
On	0	000#	International call	000#	LOCATION_B	00#
On	0	0010#	Modem call to Internet provider or Call-by-Call	010#	ISDN	
On	0	00180#	National service call	0180#	ISDN	
On	0	00800#	National free of charge call	0800#	ISDN	
On	0	00850#	Delete own city prefix	0#	RESTART	
On	0	00#	National call	00#	LOCATION_B	0#
On	0	0110	Emergency call	110	ISDN	
On	0	0112	Emergency call	112	ISDN	
On	0	0#	City area call	0850#	ISDN	0850#
On	0	97#	Call via SIP provider WIZ_SIPGATE	#	WIZ_SIPGATE	
On	0	98#	Call via ISDN	#	ISDN	
On	0	99#	Call via SIP-PBX LOCATION_B	0#	LOCATION_B	
Default	0	#	Default to SIP-PBX LOCATION_B	#	LOCATION_B	

⑥ Adapt the suggested call routing table in order to make international and national long distance calls via the SIP provider line with backup over ISDN. When doing so, please observe that the '0' preceding the number must be removed.



Entry active / default line:	Active
Priority:	0
Called number/name:	000#
Comment:	International call

Mapping

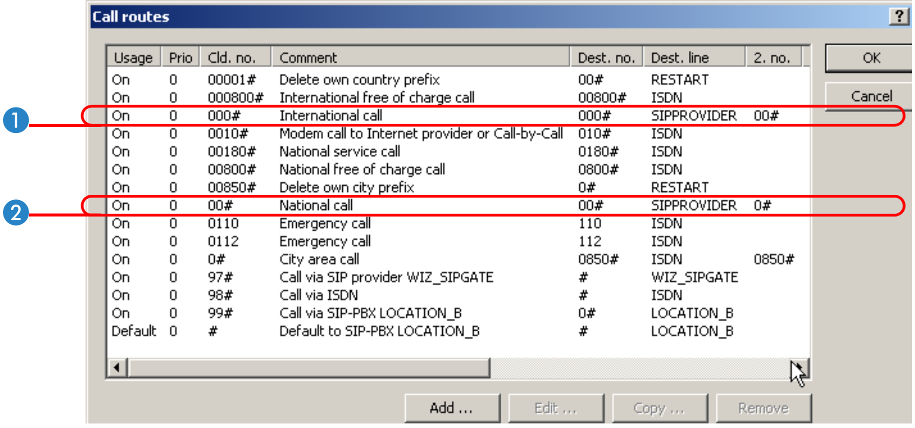
If a call matches the below mentioned attributes, it will be redirected to

Number/name:	00#
Line:	SIPPROVIDER

Should the number or line not be available, you may specify alternative destinations here.

2. number:	00#
2. line:	ISDN

After being adapted for international ❶ and national ❷ long distance, the call routing table should appear as follows:



Usage	Prio	Cld. no.	Comment	Dest. no.	Dest. line	2. no.
On	0	00001#	Delete own country prefix	00#	RESTART	
On	0	000800#	International free of charge call	00800#	ISDN	
On	0	000#	International call	000#	SIPPROVIDER	00#
On	0	0010#	Modem call to Internet provider or Call-by-Call	010#	ISDN	
On	0	00180#	National service call	0180#	ISDN	
On	0	00800#	National free of charge call	0800#	ISDN	
On	0	00850#	Delete own city prefix	0#	RESTART	
On	0	00#	National call	00#	SIPPROVIDER	0#
On	0	0110	Emergency call	110	ISDN	
On	0	0112	Emergency call	112	ISDN	
On	0	0#	City area call	0850#	ISDN	0850#
On	0	97#	Call via SIP provider WIZ_SIPGATE	#	WIZ_SIPGATE	
On	0	98#	Call via ISDN	#	ISDN	
On	0	99#	Call via SIP-PBX LOCATION_B	0#	LOCATION_B	
Default	0	#	Default to SIP-PBX LOCATION_B	#	LOCATION_B	

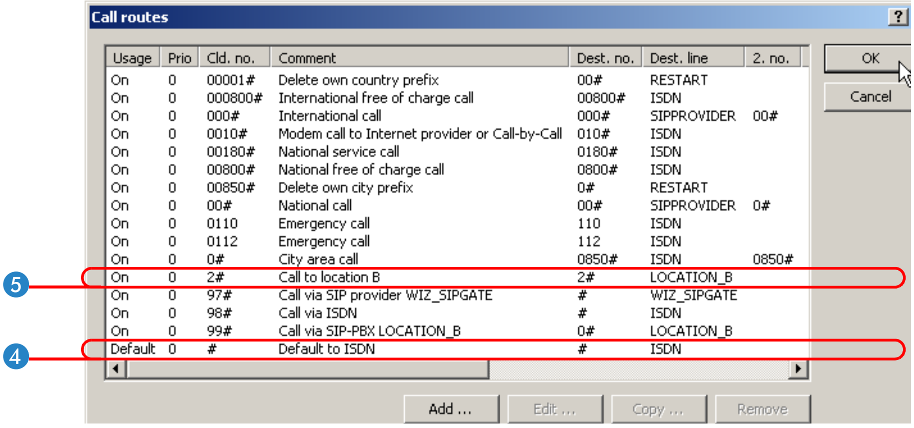
⑦ In this state, all calls that cannot be resolved by the call routing table and which do not have a corresponding entry in the local user list are automatically forwarded to the remote site.

If this is not desired, for example, where more than two sites are connected in this way, an additional entry can detect only the internal calls to a particular site. For this, make a new entry (for the number range '20' to '29' at location B) in the call routing table ⑤ with the following values:

- □ Called number / name: e.g. '2#' for all numbers that begin with a 2.
- □ Number / name: The number called is remains unchanged and is used as a destination number, i.e. here, also '2#'.
- □ Line: Enter the SIP PBX line for the remote location here, i.e. 'LOCATION_B'.

In doing so, the standard route ④ is adjusted so that all numbers which cannot be resolved are transmitted via ISDN.

After being adapted, the call routing table should appear as follows:



Usage	Prio	Cld. no.	Comment	Dest. no.	Dest. line	2. no.
On	0	00001#	Delete own country prefix	00#	RESTART	
On	0	000800#	International free of charge call	00800#	ISDN	
On	0	000#	International call	000#	SIPPROVIDER	00#
On	0	0010#	Modem call to Internet provider or Call-by-Call	010#	ISDN	
On	0	00180#	National service call	0180#	ISDN	
On	0	00800#	National free of charge call	0800#	ISDN	
On	0	00850#	Delete own city prefix	0#	RESTART	
On	0	00#	National call	00#	SIPPROVIDER	0#
On	0	0110	Emergency call	110	ISDN	
On	0	0112	Emergency call	112	ISDN	
On	0	0#	City area call	0850#	ISDN	0850#
On	0	2#	Call to location B	2#	LOCATION_B	
On	0	97#	Call via SIP provider WIZ_SIPGATE	#	WIZ_SIPGATE	
On	0	98#	Call via ISDN	#	ISDN	
On	0	99#	Call via SIP-PBX LOCATION_B	0#	LOCATION_B	
Default	0	#	Default to ISDN	#	ISDN	

This entry for 'LOCATION_B' is placed well down toward the end of the call routing table so as not to affect the more general rules. However, for interaction with the other routes, verify that only the internal numbers for the remote site are directed to the respective line.

Configuring the VoIP terminal equipment

The VoIP terminal equipment is configured as described in the preceding examples with internal VoIP domains and internal numbers for the local site.

Call routing procedure on outgoing calls

For this application, most calls take place as described in the preceding examples. Internal calls between locations are resolved as follows:

	User	dials	correct call route	correct user	mapping, number in use	Destination line
①	VoIP telephone location A	21	2#	none	21	LOCATION_B

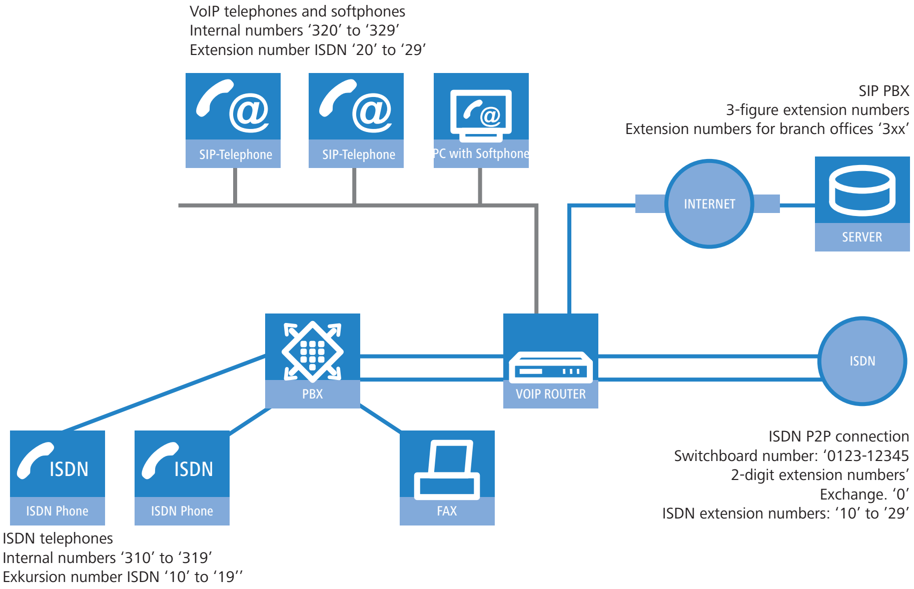
① Internal call between two VoIP terminal devices at locations A and B. The number dialed '21' matches the route ⑤ '2#' in the call routing table. The call router sends the call out over the line to the remote SIP PBX without changing the number.

13.13.7 The LANCOM VoIP Router at a P2P (point-to-point) connection

Many companies use a point-to-point ISDN connection instead of the more common point-to-multipoint connection. Point-to-point connections offer two significant advantages:

- Because extension numbers can be used (DDI – Direct Dialing In), all terminal devices can be directly reached via a common external switchboard number plus an extension number as a suffix.
- A larger number of B channels can be used with the same range of telephone numbers, whereas with a point-to-multipoint connection there are only two B channels, typically supporting up to 10 telephone numbers.

ISDN P2P connections are available either as a basic rate interface (BRI) with two B channels or as a primary rate interface (PRI) typically with 30 B channels. LANCOM VoIP Routers support the ISDN basic rate interface only. To be able to use more than four B channels, a P2P connection can be switched to multiple basic rate interfaces with the same range of telephone numbers.


VoIP telephones and softphones
Internal numbers ’320’ to ’329’
Extension number ISDN ’20’ to ’29’
SIP-Telephone
SIP-Telephone
PC with Softphone
SIP PBX
3-figure extension numbers
Extension numbers for branch offices ’3xx’
INTERNET
SERVER
PBX
VOIP ROUTER
ISDN
ISDN
ISDN Phone
ISDN
ISDN Phone
FAX
ISDN P2P connection
Switchboard number: ’0123-12345
2-digit extension numbers’
Exchange. ’0’
ISDN extension numbers: ’10’ to ’29’
ISDN telephones
Internal numbers ’310’ to ’319’
Exkursion number ISDN ’10’ to ’19’’

Objectives in implementing the LANCOM VoIP Router

- Connecting additional SIP devices at the branch office.
- Internal calls to users based at the headquarters and other branch offices via the SIP PBX located at the headquarters (using VPN connection).

Requirements

- LANCOM connected to LAN and WAN (via DSL/ADSL), ISDN-TE interface(s) are connected to the ISDN P2P connection, ISDN-NT interface(s) are connected to an ISDN PBX.
- The Internet connection has been set up by means of a VPN tunnel, as has the network connection between the two locations. All terminal devices can contact each other with the IP addresses used.
- A dialing plan with a unique internal telephone number for each piece of terminal equipment to be connected.

Configuring the LANCOM

The configuration of the SIP client or connection to the SIP PBX as a SIP PBX line named 'HQ' has already been described in other example applications and, here, is assumed to be familiar to you. The SIP PBX at headquarters uses the SIP domain 'mycompany.HQ' and the branch office has the internal domain 'mycompany.BRANCH01'.

This is how the LANCOM is configured for operation at a point-to-point line:

① The ISDN mapping table translates the DDI (extension numbers) to the internal numbers for processing as SIP calls.

MSN/DDI	ISDN/S0 Bus	Internal number	Comment
0	ISDN1, ISDN2	300	Maps DDI '0' to internal number '300'
#	ISDN1, ISDN2	3#	Adds the prefix '3' to all other DDI '0' for the internal numbers

Both entries in this example apply to the ISDN interfaces 1 and 2, which are connected to the ISDN line. The activation of two ISDN interfaces makes four B channels available for use. If both B channels of an ISDN interface are engaged, there is an automatic attempt to redirect calls to another ISDN interface with free B channels.

② Based on the ISDN user entries, the internal numbers are translated back to the DDI numbers.

Internal number	MSN/DDI	ISDN/S0 Bus	Comment
300	0	ISDN3, ISDN4	Maps internal number '300' to DDI '0'. Useful if the exchange is on the ISDN PBX.
31#	1#	ISDN3, ISDN4	Removes the leading '3' from all internal numbers beginning with '3'.

With the second entry, all ISDN terminal devices with the ISDN extension numbers '10' to '19' are made known to be ISDN users in the VoIP system. A single entry here suffices for all subscribers. All ISDN users then use the same data to register at the SIP PBX.

ISDN users entered with the # symbol can only be reached from the SIP PBX if this does not require users to register. For ISDN users to register, separate entries in the ISDN user list are required.

Both entries in this example apply to the ISDN interfaces 3 and 4, which are connected to the ISDN PBX. Here, too, the four B channels of the two interfaces can be used "dynamically" for the connection between the ISDN PBX and the LANCOM VoIP Router.

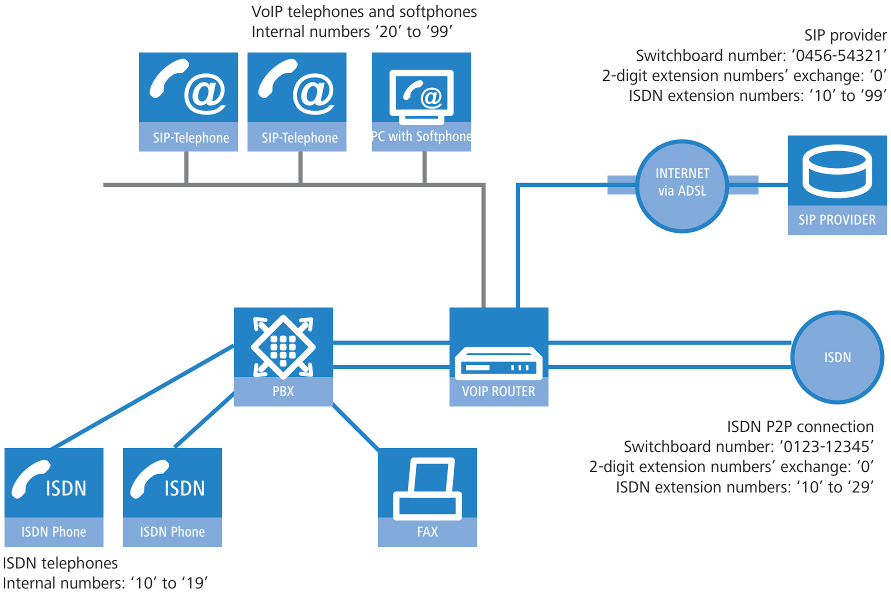
③ Routing of calls is governed by the call routing table. If you use the LANconfig Wizard, the call-routing table is preset so that all outgoing calls from ISDN and SIP devices are conducted via the SIP PBX with the exception of local calls and calls to service numbers, such as 0800 numbers.

13.13.8 SIP trunking

In telecommunications jargon, trunking is the process by which several lines or connections are combined into one shared line. In the world of VoIP, SIP providers are increasingly offering products which provide the ability to make several calls simultaneously using a single account. Together with the possibility of being able to contact SIP participants via a shared switchboard number with individual extensions (DDIs), these types of accounts are also becoming attractive for business customers.

There are two possible options when using a SIP account with trunking:

- The customer retains his previous ISDN connection, along with any corresponding telephone numbers from the telephone company, and sets up an additional account having a separate number range with a SIP provider.
- The customer ports the numbers used thus far from the telephone company to the SIP provider and from then on uses the same numbers using SIP.


VoIP telephones and softphones
Internal numbers '20' to '99'
SIP-Telephone
SIP-Telephone
PC with Softphone
SIP provider
Switchboard number: '0456-54321'
2-digit extension numbers' exchange: '0'
ISDN extension numbers: '10' to '99'
INTERNET via ADSL
SIP PROVIDER
PBX
VOIP ROUTER
ISDN
ISDN P2P connection
Switchboard number: '0123-12345'
2-digit extension numbers' exchange: '0'
ISDN extension numbers: '10' to '29'
ISDN
ISDN Phone
ISDN
ISDN Phone
FAX
ISDN telephones
Internal numbers: '10' to '19'

In this example we will take a look at a company planning to add a SIP trunking account, with up to 100 extension numbers, to its current ISDN point-to-point line having 20 extensions. The ISDN terminal devices with point-to-point line extensions used thus far can be retained. All new employees are to be issued with a SIP telephone with an extension via the SIP account.

Unique extensions are used since staff members have to be able to call each other internally. In order to migrate smoothly towards SIP, all ISDN terminal devices are to be contactable using **both** extension number and switchboard number of the SIP account. So an ISDN telephone should react in the same way for calls to '0123-12345 12' as it does for calls to '0456-54321 12'.

With the exception of emergency calls and service numbers, such as "0800" numbers, out-going calls are generally made using the SIP account. The signaling of SIP telephone numbers to call parties is paving the way for the medium-term discontinuation of ISDN telephone numbers.

Objectives in implementing the LANCOM VoIP Router

- Connection of additional SIP terminal devices
- Internal calls between ISDN and SIP terminal devices.
- Continuation of availability using ISDN telephone numbers used thus far.
- Low-cost calls by using a shared SIP account.

Requirements

- LANCOM connected to LAN and WAN (via DSL/ADSL), ISDN-TE interface(s) are connected to the ISDN P2P connection, ISDN-NT interface(s) are connected to an ISDN PBX.
- The Internet connection has been set up. All terminal devices can contact each other with the IP addresses used.
- A dialing plan with a unique internal telephone number for each piece of terminal equipment to be connected.

Configuring the LANCOM

This is how the LANCOM is configured for operation at a point-to-point line:

① The LANCOM is configured for operation at a point-to-point line by adding two simple entries in the ISDN mapping table and in the list of ISDN users.

ISDN mapping table

MSN/DDI	ISDN/S0 Bus	Internal number	Comment
#	ISDN1, ISDN2	#	Outputs the unchanged DDI as an internal telephone number.

ISDN user list

Internal number	MSN/DDI	ISDN/S0 Bus	Comment
#	#	ISDN3, ISDN4	Outputs the unchanged internal number as a DDI.

② When configuring SIP clients, just the internal VoIP domain of the LANCOM VoIP Router and the associated internal number are entered. The extension numbers previously used for the ISDN terminal devices remain unallocated.

③ A SIP provider line is created for the SIP account. The 'Trunk' option is selected as the mode for this line.

④ Routing of calls is governed by the call routing table. When using the Wizards available with LANconfig, the call routing table is pre-configured such that all out-going calls from ISDN and SIP devices are made using the SIP trunk account (with the exception of local calls and calls to service numbers such as the emergency services or "0800" numbers).

Process of call routing

In this example, call routing benefits from the unique internal telephone numbers.

- With in-coming calls, regardless of whether they are via ISDN or SIP, only the DDI is passed on to the LANCOM VoIP Router. Since the DDI and internal numbers are the same in this example, an extension number can be used to put through calls to locally registered SIP users or to dynamic ISDN users.

ⓘ If the reported DDIs can not, or should not, be used directly as internal numbers, corresponding telephone number translations are defined in the ISDN and SIP mapping tables, see 'ISDN mapping' → page 13-28 and 'SIP mapping' → page 13-24..

- With out-going calls, the decision as to whether calls are made using ISDN or SIP may be controlled from the call routing table. In the default setting after using the Wizards, SIP is taken to be the normal destination line (with the exception of local calls and special numbers). Local calls, for example, may be switched to SIP by changing an entry in the call routing table.

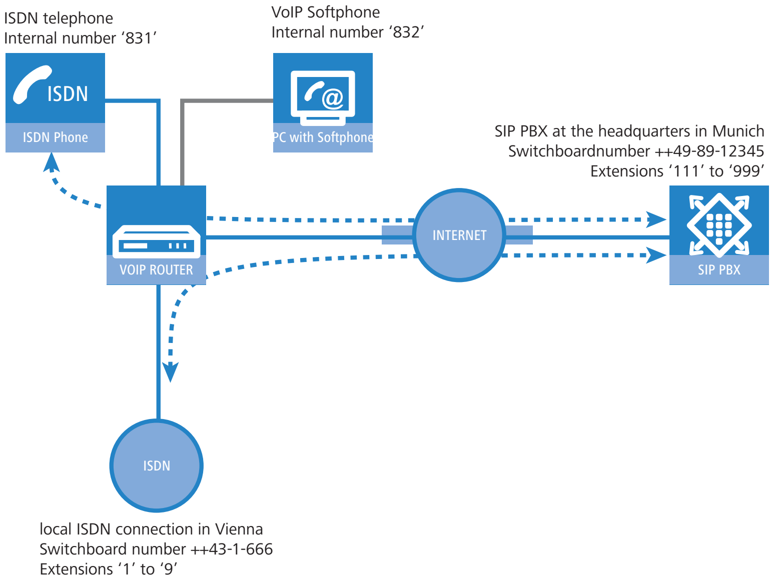
ⓘ In this case, the SIP number is displayed at the subscribers on the other side of the connection, even if the call originates from an ISDN terminal device.

13.13.9 Remote gateway

Distributed company structures usually provide ISDN connections at branch offices to allow staff local access to the telephone network using appropriate ISDN terminal devices.

- A connection from the local ISDN terminal devices to a SIP PBX at the headquarters can easily be set up using a LANCOM VoIP Router.
- Furthermore, the "Remote Gateway" function can be used to connect both the terminal devices and the local ISDN connections to the central PBX. Benefits of the remote gateway:
  - □ The local ISDN connections are made available to all users in the company network. Calls to the local ISDN network can be made from anywhere as local calls (even from beyond state boundaries).

- □ All calls, even those made by local users into their "own" telephone network, can be made via the SIP PBX, consequently facilitating central administration and logging.


ISDN telephone
Internal number ‘831’
VoIP Softphone
Internal number ‘832’
ISDN
ISDN Phone
PC with Softphone
SIP PBX at the headquarters in Munich
Switchboardnumber ++49-89-12345
Extensions ‘111’ to ‘999’
INTERNET
VOIP ROUTER
SIP PBX
ISDN
local ISDN connection in Vienna
Switchboard number ++43-1-666
Extensions ‘1’ to ‘9’

In this example we'll take a look at a company headquartered in Munich. The branch office in Vienna should be in a position to call the headquarters using the internal numbers. "83“ numbers are taken from the headquarter's number range and are reserved for Vienna for this purpose. The sales and support departments at the company headquarters should also be contactable from Austria as a local, or national long-distance call from Vienna. The purchasing department would also like to be able to contact suppliers in Austria using national long-distance calls.

Objectives in implementing the LANCOM VoIP Router

- Internal calls to users based at the headquarters and other branch offices via the SIP PBX located at the headquarters (using VPN connection).
- Integration of the local ISDN interface into the telephone structure of the organization.

Requirements

- LANCOM Connected to LAN and WAN (via DSL/ADSL), ISDN-TE interface(s) are connected to the ISDN connection, ISDN-NT interface(s) are connected to an ISDN PBX or the ISDN terminal devices.
- The Internet connection has been set up by means of a VPN tunnel, as has the network connection between the two locations. All terminal devices can contact each other with the IP addresses used.
- A dialing plan with a unique internal telephone number for each piece of terminal equipment to be connected.

Configuring the LANCOM

The following steps are involved when configuring the LANCOM VoIP Router:

- An entry is created for each ISDN user so that the terminal equipment can register with the upstream SIP PBX.
- For SIP clients, this registration information is entered in the VoIP telephone or the softphone.
- The connection to the SIP PBX, as a SIP-PBX line with the name 'HQ', has already been described in other application examples and familiarity with it is assumed from here on.
- In addition to this connection, a further connection "Gateway“ needs to be made to the SIP PBX, which helps in making the local ISDN connection known to the upstream SIP PBX.
- The connection between the local ISDN connection and the remote SIP PBX is made using the entries in the call-routing table.

This is how the LANCOM is configured for operation as a remote gateway:

① In the ISDN mapping table, local DDIs (extension numbers) are converted to internal telephone numbers for processing as SIP calls.

MSN/DDI	ISDN/S0 Bus	Internal number	Comment
#	ISDN1, ISDN2	#	All DDIs pending at the ISDN interfaces are switched further without being changed.

② A new entry is created in the list of SIP provider connections with the following information:

- Name of the connection: 'GW.HQ'
- Mode: Gateway
- SIP domain: SIP domain of the headquarters 'mycompany.HQ'
- SIP ID: Account name for the SIP gateway in the SIP PBX located at the headquarters
- Authentication name and password: Registration data for the SIP gateway

③ Additional entries are created in the call-routing table to switch calls between the headquarters and the local ISDN connection:

Called number	Destination number	Source line	Destination line	Comment
#	83#	ISDN	GW.HQ	Forwards all in-going calls arriving at the LANCOM VoIP Router over ISDN to the headquarters via the gateway. The DDI is preceded by '83' so as to map correctly to the internal numbers.
9	555	ISDN	GW.HQ	Forwards all in-going calls arriving at the LANCOM VoIP Router over ISDN to the headquarters via the gateway. 555' is used as the number for support.
0043#	0#	GW.HQ	ISDN	Forwards all out-going calls from the headquarters to the Austrian national network to the local ISDN connection (without country code).
#	#			Forwards all other calls without change.

Call routing procedure on outgoing calls

	User	dials	Call router receives	Call router sends	Assigned via	Source line	Destination line
①	ISDN network D	089-12345-831	831	831	■ List of local ISDN users	GW.HQ	Internal
②	ISDN network A	666-1	1	831	■ Call routing table ■ List of local ISDN users	ISDN	GW.HQ
③	ISDN network A	666-9	9	555	■ Call routing table	ISDN	GW.HQ
④	SIP exchange	0043-662-33333	0043-662-33333	0662-33333	■ Call routing table	GW.HQ	ISDN

① Call from customer in Hamburg to staff in Vienna. The customer dials the number of the Munich headquarters using the correct extension '089-12345-831'. Because the ISDN user is registered with the internal telephone number, the PBX at the headquarters receives only the DDI '831' and passed it on via the SIP PBX line. The LANCOM VoIP Router receives '831', locates a matching entry in the list of locally registered users and is able to connect the call.

② Call from customer in Vienna to the branch office in Vienna. The customer dials the number of the branch office in Vienna using the correct extension '666-1'.

- The LANCOM VoIP Router receives the DDI '1' and is not able to locate a matching entry in the list of locally registered users. Using the call-routing table, the telephone number is changed to '831' and forwarded on to the PBX in Munich via the SIP gateway connection. The PBX recognizes the registered ISDN user with the internal telephone number '831' and passes the call back to the LANCOM VoIP Router via the SIP PBX line.
- The LANCOM VoIP Router then receives '831', locates a matching entry in the list of locally registered users and is able to connect the call.

③ Call from customer in Salzburg to the support number in Vienna. The customer dials the number of the branch office in Vienna using the correct extension '666-9'. The call is automatically put through to the internal support number '555' using the call routing table.

④ Call from employee in Munich to customer in Salzburg. The employee dials '0043-662-33333'. The PBX in Munich is configured such that all calls to Austria are forwarded via the SIP gateway connection to the LANCOM VoIP Router. The call router receives the complete number, drops the country code as per the routing table having source line 'GW.HQ' and forwards the remaining number to the ISDN line.

ⓘ Here the call number from Munich is displayed at the remote site.

13.14 Diagnosis of VoiP connections

13.14.1 SIP traces

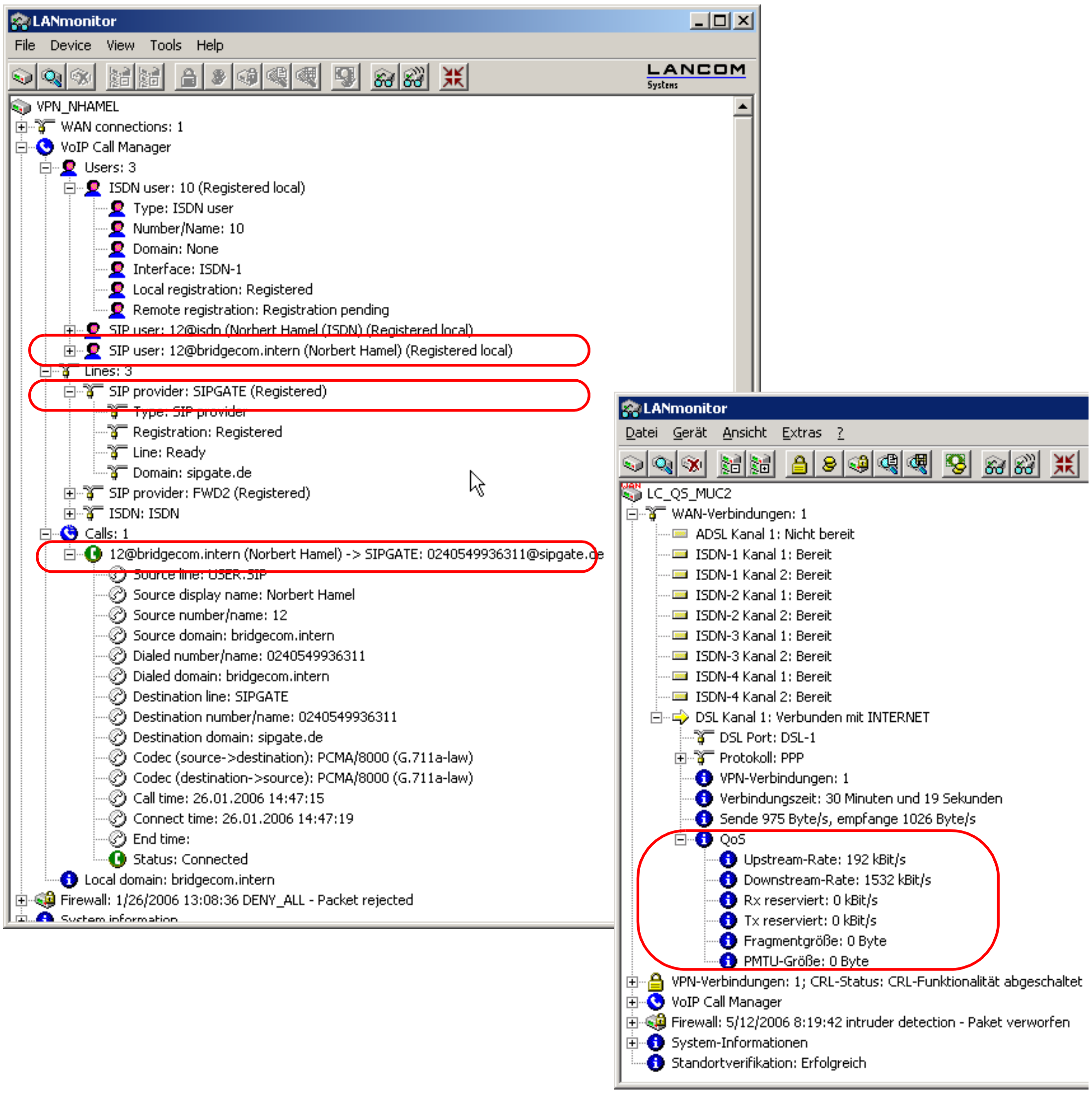
Trace output can be used to check the internal processes in LANCOM devices during or after configuration. A SIP trace displays all of the SIP information which is exchanged between a LANCOM VoIP Router and a SIP provider or upstream SIP PBX. The SIP trace is activated with the following command:

```
trace + sip-packet
```

13.14.2 Connection diagnosis with LANmonitor

LANmonitor displays a wealth of information about calls switched in the LANCOM:

- Information about the registered users.
- Information about the lines available.
- Information about current calls, including the translation of telephone numbers and domains by the Call Manager.
- Information about the fixed and automatic QoS bandwidth reservations and settings.



```
VPN_NHAMEL
  WAN connections: 1
  VoIP Call Manager
    Users: 3
      ISDN user: 10 (Registered local)
        Type: ISDN user
        Number/Name: 10
        Domain: None
        Interface: ISDN-1
        Local registration: Registered
        Remote registration: Registration pending
      SIP user: 12@isdn (Norbert Hamel (ISDN) (Registered local)
      SIP user: 12@bridgecom.intern (Norbert Hamel) (Registered local)
    Lines: 3
      SIP provider: SIPGATE (Registered)
        Type: SIP provider
        Registration: Registered
        Line: Ready
        Domain: sipgate.de
      SIP provider: FWD2 (Registered)
      ISDN: ISDN
    Calls: 1
      12@bridgecom.intern (Norbert Hamel) -> SIPGATE: 0240549936311@sipgate.de
        Source line: USER.SIP
        Source display name: Norbert Hamel
        Source number/name: 12
        Source domain: bridgecom.intern
        Dialed number/name: 0240549936311
        Dialed domain: bridgecom.intern
        Destination line: SIPGATE
        Destination number/name: 0240549936311
        Destination domain: sipgate.de
        Codec (source->destination): PCMA/8000 (G.711a-law)
        Codec (destination->source): PCMA/8000 (G.711a-law)
        Call time: 26.01.2006 14:47:15
        Connect time: 26.01.2006 14:47:19
        End time:
        Status: Connected
    Local domain: bridgecom.intern
  Firewall: 1/26/2006 13:08:36 DENY_ALL - Packet rejected
  System information
```

```
LC_QS_MUC2
  WAN-Verbindungen: 1
    ADSL Kanal 1: Nicht bereit
    ISDN-1 Kanal 1: Bereit
    ISDN-1 Kanal 2: Bereit
    ISDN-2 Kanal 1: Bereit
    ISDN-2 Kanal 2: Bereit
    ISDN-3 Kanal 1: Bereit
    ISDN-3 Kanal 2: Bereit
    ISDN-4 Kanal 1: Bereit
    ISDN-4 Kanal 2: Bereit
    DSL Kanal 1: Verbunden mit INTERNET
      DSL Port: DSL-1
      Protokoll: PPP
      VPN-Verbindungen: 1
      Verbindungszeit: 30 Minuten und 19 Sekunden
      Sende 975 Byte/s, empfange 1026 Byte/s
      QoS
        Upstream-Rate: 192 kBit/s
        Downstream-Rate: 1532 kBit/s
        Rx reserviert: 0 kBit/s
        Tx reserviert: 0 kBit/s
        Fragmentgröße: 0 Byte
        PMTU-Größe: 0 Byte
  VPN-Verbindungen: 1; CRL-Status: CRL-Funktionalität abgeschaltet
  VoIP Call Manager
  Firewall: 5/12/2006 8:19:42 intruder detection - Paket verworfen
  System-Informationen
  Standortverifikation: Erfolgreich
```

LANCOM reference manual part 6

- Backup Solutions
- Office Communication with LANCAPI
- More Services

Version: LCOS 7.6 with addendum 7.7 (see appendix)
(last update August 2009)

LANCOM
Systems

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

Subject to change without notice. No liability for technical errors or omissions.

Products from LANCOM Systems include software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

Products from LANCOM Systems include cryptographic software written by Eric Young (eay@cryptsoft.com).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

Products from LANCOM Systems contain open source software components which are available as source text and which are subject to special licenses and the copyright of their authors. In particular the firmware components are subject to the terms of the GNU General Public License, version 2 (GPL). The license agreement with the text of the GPL is available on the LANCOM CD in the relevant product's directory. On request, you can obtain the source texts and licensing details electronically from the LANCOM Systems GmbH FTP server.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen
Deutschland

www.lancom.de

Würselen, August 2009

110650/0809

Contents

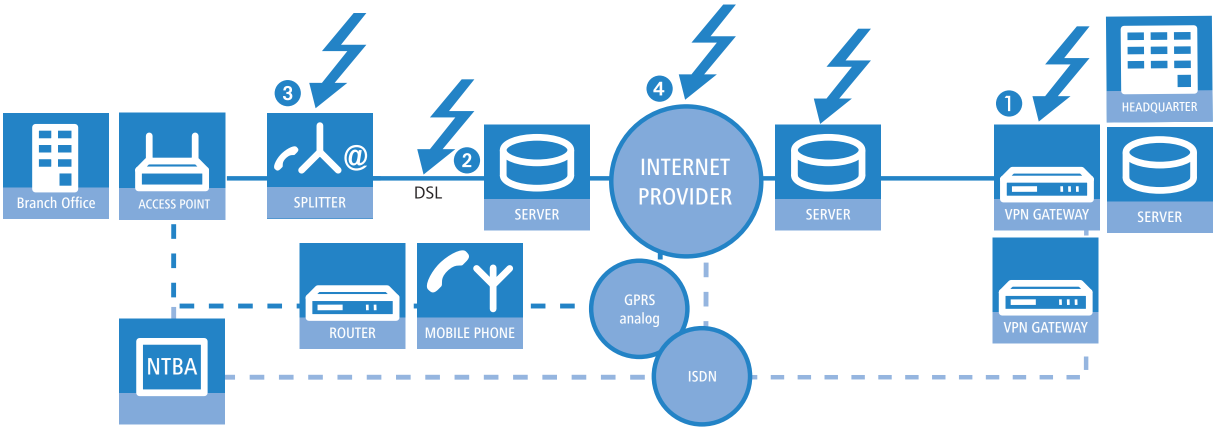
14 High availability – backup solutions

14.1 High availability for networks

Networked cooperation between several offices or even between continents has become an everyday part of modern business. The paths of communication between headquarters, subsidiaries and field workers increasingly rely upon public infrastructures. VPN has become established as the de facto standard for cost-effective and secure enterprise communications over the Internet.

However, many of important elements in these network structures remain susceptible to failure which could have severe consequences for business operations:

- The remote Internet gateway ➊ itself can fail.
- The physical lines for the connection to the Internet or to a remote network can fail:
  - The Internet-access cable between the site and the provider ➋ could fail; after damage from construction work, for example.
  - The DSL connection ➌ may fail, while the ISDN connection remains functional.
- The provider's network ➍ may be disturbed or even fail.



Internet routers and access points from LANCOM offer a range of security and backup functions that can be used for the protection of your network from disturbance.

14.1.1 How is a network-connection disturbance detected?

The first stage in protecting a network connection from the effects of a disturbance is to detect the disturbance itself. The following methods are available to check the connections:

- Check the PPP connection to the provider with PPP LCP echo monitoring.
- Check if remote stations can be contacted via name or IP address with ICMP polling (ping from end to end).
- Check the tunnel end points with "dead peer detection" (DPD).

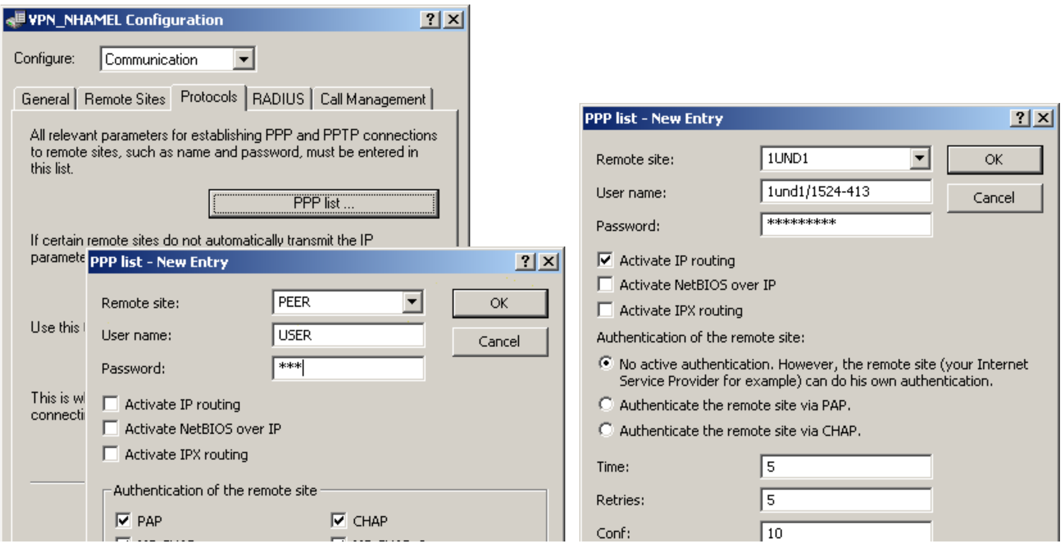
PPP LCP echo monitoring

The method checks the PPP connection to a certain remote site with regular LCP requests. This method is typically used to check the connection to the Internet provider. LCP requests are directly sent to the access server.

In the PPP list, a time interval for the transmission of LCP requests to the remote site is defined for this connection. Further, for the event that LCP replies are missed, the number of retries before the transmission of a new LCP request is defined. Should the transmitter not receive any reply to the retries, the line is considered to have failed.

- **Time:** The time entered into the PPP list must be multiplied by the factor 10 to arrive at the actual interval between two LCP requests. Entering the time as "5" means that an LCP request will be prompted every 50 seconds.
- **Retries:** If no reply to an LCP request is received then the remote site will be checked in shorter intervals. The device then tries to reach the remote site once a second. The number of retries defines how many times these attempts are repeated. Entering "5" under retries means that the LCP request will be repeated 5 times before the connection is considered to have failed.

PPP LCP monitoring only checks the PPP connection path as far as the Internet provider.



VPN_NHAMEL Configuration

Configure: Communication

General | Remote Sites | Protocols | RADIUS | Call Management

All relevant parameters for establishing PPP and PPTP connections to remote sites, such as name and password, must be entered in this list.

PPP list ...

If certain remote sites do not automatically transmit the IP paramete

Use this

This is w
connecti

PPP list - New Entry

Remote site: PEER

User name: USER

Password: ***

OK

Cancel

☐ Activate IP routing

☐ Activate NetBIOS over IP

☐ Activate IPX routing

Authentication of the remote site

☑ PAP ☑ CHAP

PPP list - New Entry

Remote site: 1UND1

User name: 1und1/1524-413

Password: *********

OK

Cancel

☑ 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.

Time: 5

Retries: 5

Conf: 10

LANconfig: Communication ▶ Protocols ▶ PPP list

WEBconfig: LCOS menu tree ▶ Setup ▶ WAN ▶ PPP list

ICMP polling

Similar to LCP monitoring, ICMP polling transmits regular requests to a remote site. Ping commands are transmitted and the answers to them are monitored. Unlike LCP monitoring, the target site for ICMP pings can be freely defined. Pinging a router in a remote network thus provides monitoring for the entire connection and not just the section to the Internet provider.

A ping interval is defined for the remote site in the polling table. Further, for the event that replies are missed, the number of retries before the transmission of a new LCP request is defined. Should the transmitter not receive any reply to the retries, the target for the ping requests is classified as unavailable.

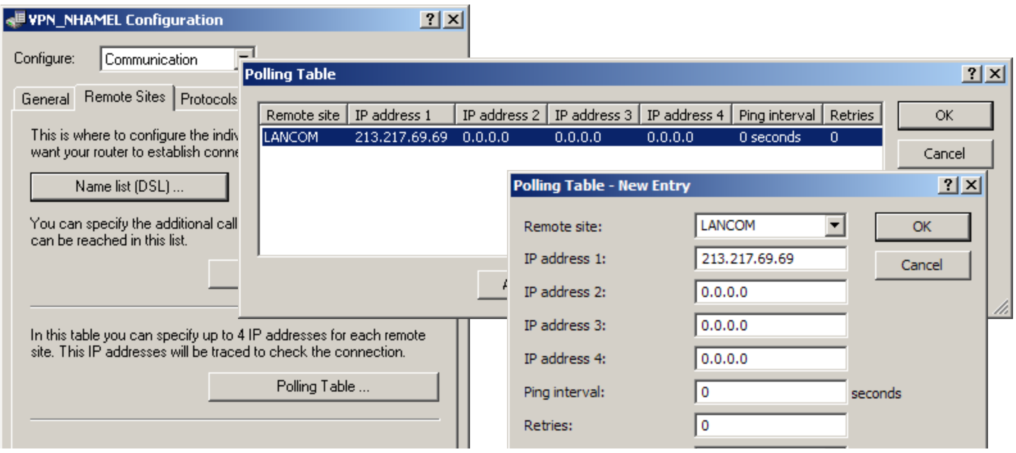
Up to four different IP addresses can be entered for each remote site that will be checked in the remote network in parallel. Only if all of the IP addresses are unavailable is the connection considered to have failed.

With the ICMP polling, an entire connection can be monitored from end to end.

- **Name of the remote site**
- **IP address 1-4:** IP addresses for targeting with ICMP requests to check the remote site.

If no IP address is entered for a remote site that can be checked with a ping, then the IP address of the DNS server that was determined during the PPP negotiation will be checked instead.

- **Ping interval:** The time entered into the polling table defines the time interval between ping requests. If the value "0" is entered, then the standard value of 30 seconds applies.
- **Retries:** If no reply to a ping is received then the remote site will be checked in shorter intervals. The device then tried to reach the remote site once a second. The number of retries defines how many times these attempts are repeated. If the value "0" is entered, then the standard value of 5 retries applies.



VPN_NHAMEL Configuration

Configure: Communication

General | Remote Sites | Protocols

This is where to configure the indiv
want your router to establish conne

Name list (DSL) ...

You can specify the additional call
can be reached in this list.

In this table you can specify up to 4 IP addresses for each remote site. This IP addresses will be traced to check the connection.

Polling Table ...

Polling Table

Remote site	IP address 1	IP address 2	IP address 3	IP address 4	Ping interval	Retries
LANCOM	213.217.69.69	0.0.0.0	0.0.0.0	0.0.0.0	0 seconds	0

OK

Cancel

Polling Table - New Entry

Remote site: LANCOM

IP address 1: 213.217.69.69

IP address 2: 0.0.0.0

IP address 3: 0.0.0.0

IP address 4: 0.0.0.0

Ping interval: 0 seconds

Retries: 0

OK

Cancel

LANconfig: Communication ▶ Remote sites ▶ Polling table

WEBconfig: LCOS menu tree ▶ Setup ▶ WAN ▶ Polling table

Dead peer detection (DPD)

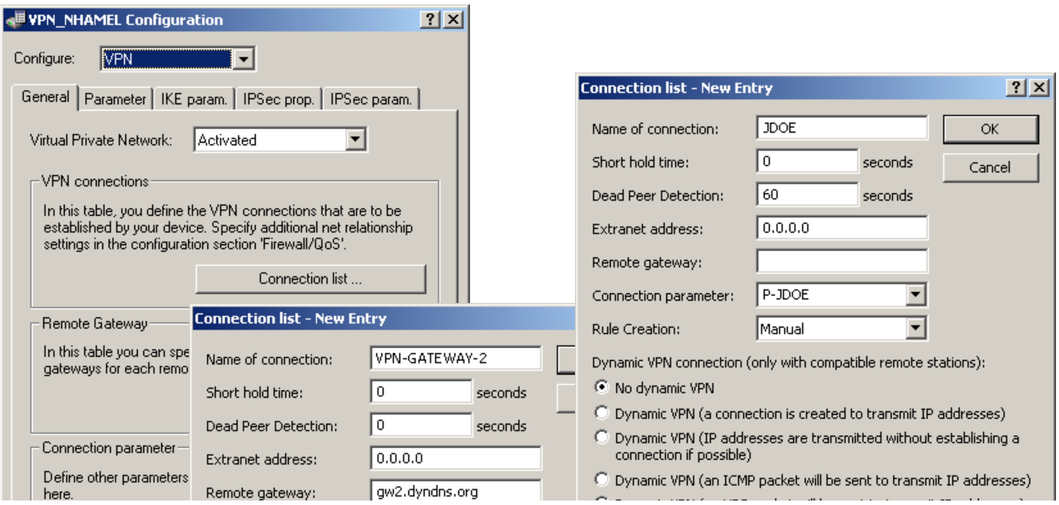
This method of connection monitoring is used when VPN clients dial-in to a VPN gateway. This is designed to ensure that a client is logged out if there is an interruption to the VPN connection, for example when the Internet connection is interrupted briefly. If the line were not to be monitored, then the VPN gateway would continue to list the client as logged-on. This would prevent the client from logging in again as, for example, the WLANmonitor prevents single serial numbers from multiple simultaneous log-ins.

For the same reason, without line monitoring a user with the same "identity" (user name) would be prevented from dialling in because the associated user would still be in the list for the logged-in client.

With dead peer detection, the gateway and client regularly exchange "keep alive" packets. If no replies are received, the gateway will log out the client so that this identity can be registered anew once the VPN connection has been re-established. The DPD time for VPN clients is typically set to 60 seconds.

Configuration with LANconfig

The dead peer detection is set up with LANconfig in the configuration area 'VPN' on the 'General' tab in the 'Connection list'.



Configure: VPN

Virtual Private Network: Activated

VPN connections

In this table, you define the VPN connections that are to be established by your device. Specify additional net relationship settings in the configuration section 'Firewall/QoS'.

In this table you can spe gateways for each remo

Define other parameters here.

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 list - New Entry

Name of connection: JDOE

Short hold time: 0 seconds

Dead Peer Detection: 60 seconds

Extranet address: 0.0.0.0

Remote gateway:

Connection parameter: P-JDOE

Rule Creation: Manual

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)

LANconfig: VPN ▶ General ▶ Connection list

WEBconfig: LCOS menu tree ▶ Setup ▶ VPN ▶ VPN-Peers

14.1.2 High-availability of lines – backup connections

If there is a disturbance to the connection with the Internet provider or to a remote network, a backup line can act as a temporary replacement for the normal data line. This requires the existence of a second physical connection which can be used to contact the remote site. Examples of backup lines are typically:

- An ISDN line as a backup for DSL Internet access
- An ISDN line as a backup for VPN network coupling
- A modem connection (GSM or analog) as a backup for DSL or ISDN lines and VPN connections

Configuration of the backup connection

The following steps are necessary to define a backup connection:

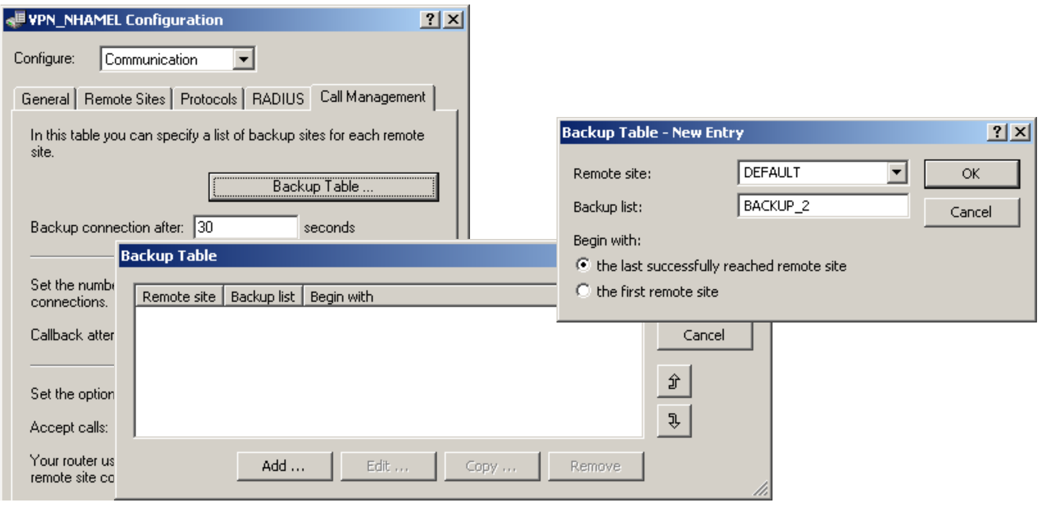
① The backup connection requires the appropriate WAN interface to be set up so that the remote site can be reached via this alternative route. If, for example, the ISDN line is to serve as the backup connection, then the remote site is set up as an ISDN remote site (along with the necessary entries in the communications layers and in the PPP list).

② If the connection to the remote site cannot be checked with LCP requests, the monitoring of the connection should be initiated with an entry in the polling table.

③ Assignment of the new backup connection to the remote site which is to be backed up. This entry is made in the backup table. Dedicated entries in the routing table are not required for a backup connection. The backup connection automatically takes over the source and target networks from the remote site that routes the data under normal operating conditions.

A remote site can be assigned with multiple backup lines in the backup table. In the case of backup, the system decides which backup line is to be used first:

- The last remote site that was reached successfully
- The first remote site in the list



Configure: Communication

In this table you can specify a list of backup sites for each remote site.

Backup connection after: 30 seconds

Remote site: DEFAULT

Backup list: BACKUP_2

Begin with:

● the last successfully reached remote site

○ the first remote site

LANconfig: Communication ▶ Call management ▶ Backup table

WEBconfig: LCOS menu tree ▶ Setup ▶ WAN ▶ Backup table

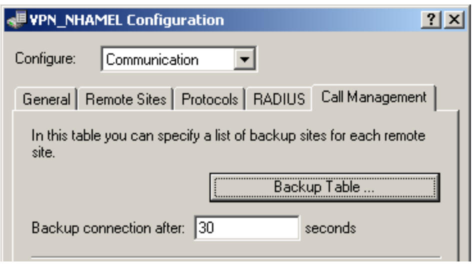
Triggering the backup connection

The backup is triggered when the monitoring mechanisms defined for the standard connection (LCP or ICMP polling) detect that contact to the remote site has been lost.

The backup connection will be established if:

- The backup delay time has expired and
- either
  - a data packet is to be transferred or
  - a hold time of 9999 seconds has been defined for the backup connection.

The backup delay time is set with LANconfig in the configuration area 'Communication' on the 'Call management' tab or alternatively with Telnet under `/Setup/WAN-Modul/Backup-delay-seconds`.



Configure: Communication

In this table you can specify a list of backup sites for each remote site.

Backup connection after: 30 seconds

Return to the standard connection

The router constantly tries to establish the standard connection while the backup connection is active. As soon as the standard connection has been established, the backup connection is terminated and the line monitoring with LCP or ICMP polling is resumed.

Only keep-alive connections return automatically!

The standard connection will only be automatically re-established after a backup event if the hold time for the connection is configured properly:

- A hold time of "0" means that the connection will not be actively terminated. If the connection is interrupted, it will not be automatically established again. Only when communication is required of the connection will it be established.
- A hold time of "9999" means that the connection is permanently kept open. If it is interrupted, then the connection will be actively opened up again. This behavior is known as **keep alive**.

Set the hold time to "9999" for connections to the Internet provider (in the corresponding peer list) and backed-up VPN connections (in the VPN connection list) to ensure that the connection is automatically re-established and resumes data transfer after interruption.

14.1.3 High-availability of gateways – redundant gateways with VPN load balancing

Another cause of failure apart from the connection to the provider or to another network may lie with the local gateway. Severe effects can result from the failure of a central VPN gateway that is used, for example, to connect the networks of multiple remote locations with the central network at headquarters.

To ensure that the headquarters remains in contact, multiple VPN endpoints (generally identically configured VPN gateways operated in parallel) can be installed. Should line polling (with dead-peer detection, ICMP line polling) indicate a failure, then a variety of strategies (e.g. the random selection of one of the available gateways) can be used to enable communication to a different VPN end point. At the central headquarters, the new router and the local default gateway are propagated by dynamic routing (RIP V2).

To avoid the situation where the additional VPN gateways remain unused, intelligent load balancing ensures that all of the devices share the load of incoming and outgoing connections also under normal operating conditions.

More information about redundant gateways and load balancing is available under 'VPN connections: High availability with VPN load balancing' → page 10-63.

14.1.4 High-availability of the Internet access – Multi-PPPoE

The third of the different basic sources of failures is the case where the gateways and connections are in order but the provider's own network is down. Such cases are handled by setting up multiple PPoE connections at the physical interface of a single device (Multi-PPPoE).

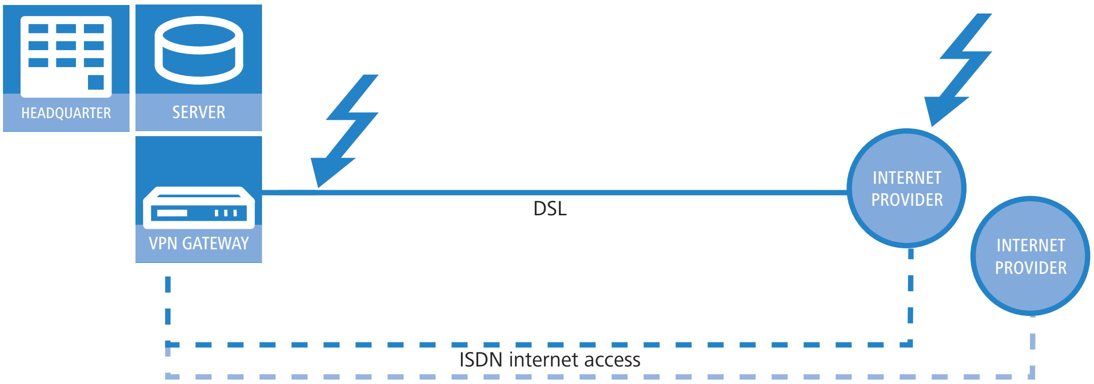
To define these backup solutions as alternative Internet accesses you can use, for example, the Setup Wizard to set up two Internet access accounts one after another. The standard Internet access for normal operations should be set up last. Consequently, the entries in the routing table will be associated with the appropriate remote site.

Additionally, an entry is made in the backup table that defines the alternative Internet access account as the backup to the remote site at the standard provider.

More information about the definition of multiple PPPoE connections is available under 'Multi-PPPoE' → page 7-22.

14.1.5 Example applications

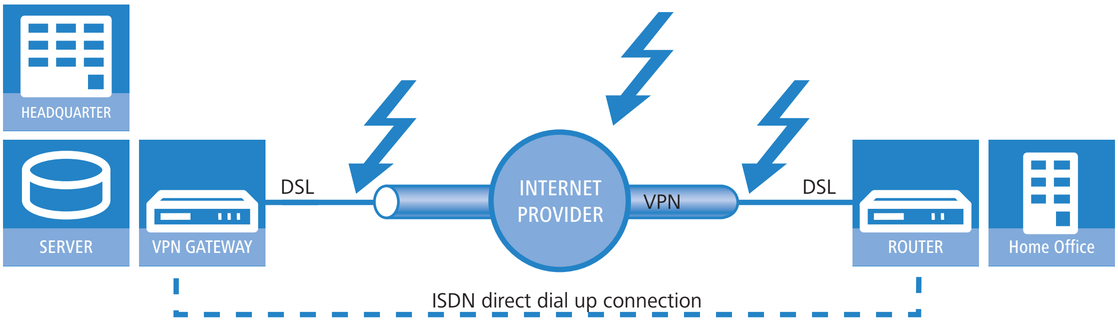
Backup DSL Internet access with ISDN internet access



In this simple backup scenario, Internet access is realized via a DSL connection. An ISDN connection is defined as a backup in case of failure of the DSL Internet access.

This backup solution can be quickly and easily set up with the help of the LANconfig Setup Wizard, for example. A further degree of security is available by defining another Internet provider in addition to the standard provider. This solution caters for the contingency where the provider's network fails and the problem is not caused by the DSL connection.

Backup dynamic VPN network coupling with an ISDN direct dial up connection



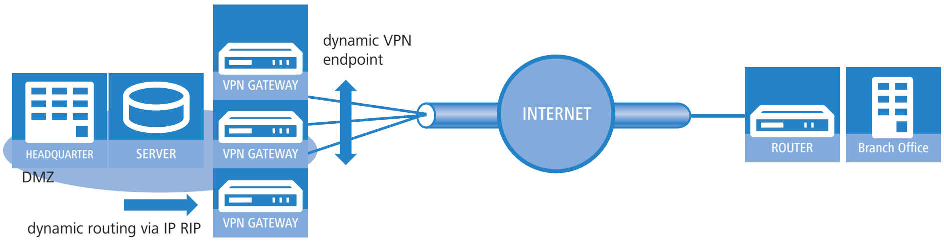
In the case that a branch office is connected to the headquarters via a VPN connection, the Internet-based VPN connection can be backed up by a direct ISDN dial-in connection. Should the Internet connection fail at either of the two routers, the data transmission is transferred to the ISDN link.

In this scenario we are assuming a fully configured VPN connection between the two networks.

- A LAN-LAN coupling via ISDN is additionally set up between the two networks. Do **not** use the Setup Wizard to set up this network coupling! The Wizard would change the entries in the routing table and would thus upset the function of the VPN network connection. Set up the ISDN network coupling in both routers manually—with the appropriate entries for the remote sites in the peer list, the PPP list and with the necessary telephone numbers and access identifiers.
- In the gateway at the headquarters, create an entry in the backup table that acts to backup the VPN remote site via a directly dialled ISDN remote site.
- Further, the router at the headquarters requires an entry for the monitoring of a remote device in the network at the branch office: Typically in the form of the LAN IP address at the remote VPN gateway. This entry ensures that the router at the headquarters can react immediately to a failure of the VPN connection.

Should there be a failure in the connection between the headquarters and branch office (on the way to the Internet provider or at the provider itself) then the ISDN connection takes over the data transfer independent of the Internet.

Redundant VPN gateways



In decentralized company structures that rely on VPN for networking the various locations, the availability of the central VPN gateway is of particular significance. The company-wide communications only remain reliable as long as these central dial-in nodes are working properly.

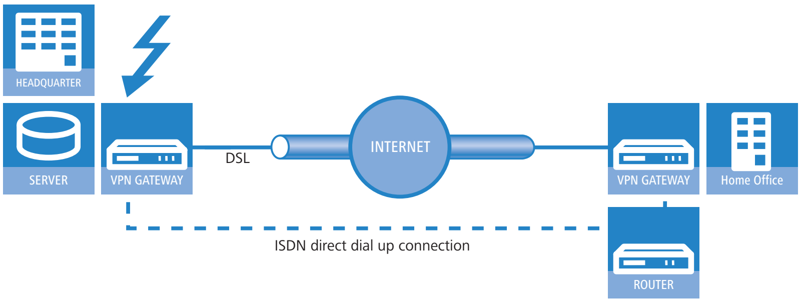
With the option of configuring several "remote gateway" addresses as "dynamic VPN endpoints" for a VPN connection, LANCOM VPN gateways offer a high level of availability by using redundant devices. This involves multiple gateways at the headquarters being set up with identical VPN configurations. On location at the satellite sites, all of these available gateways are entered as possible remote stations for the VPN connection. If one of the gateways is unavailable, the remote router automatically redirects the request to one of the other routers.

To ensure that the computers in the LAN at the headquarters know which VPN gateway it to be used to reach a particular satellite station, the outband router currently connected to the remote site is propagated via RIPv2 to the network at the headquarters.

A powerful mechanism for load balancing between the VPN gateways at the headquarters is attained with the configuration of the satellite stations to select the remote site for VPN connection on a random basis ("VPN load balancing").

Further information to redundant gateways and "VPN Load Balancing" can be found in 'VPN connections: High availability with VPN load balancing' → page 10-63.

Backup a VPN gateway with an ISDN gateway and RIP



Going a step further, the VPN gateways themselves can be backed up in case of failure. This case assumes the existence of a VPN connection between two gateways. In the event that one of the two VPN devices should fail, an ISDN connection is to take over the data transfer; in this case via a direct dial-in connection.

Regarding the configuration of this solution, we again assume a functional VPN coupling of the two networks. The following additional steps are required:

- A standard ISDN network coupling that routes the same subnets as the VPN connection is set up between the two ISDN routers. In the routing table, however, a distance is entered that is at least 1 higher than the corresponding route in the VPN gateway.
- The local RIP (RIP V2) has to be activated in all routers so that the VPN and ISDN routers can exchange information about the routes with the remote sites. The higher distance of the route via the ISDN gateway is, under normal circumstances, the poorer route.
- It is not necessary to define a backup connection in this case as a different device should take over the data transmission.

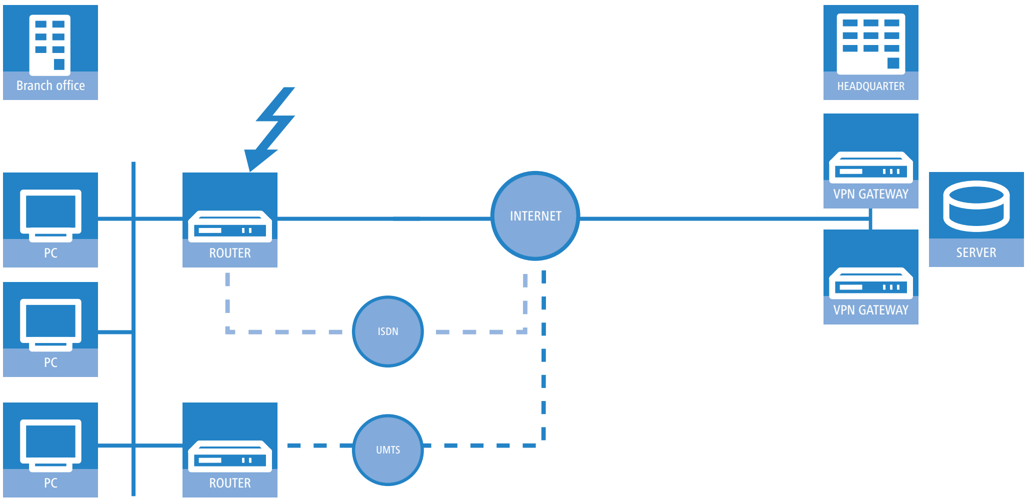
If there is a disturbance in the connection between the VPN devices, the value for the distance of the corresponding routes changes automatically: A route which is not available is marked with a distance of 16. Consequently, the route entered into the ISDN router automatically becomes the "better" solution and all data packets will be re-routed over the ISDN connection. As soon as the VPN connection is re-established, the distance changes to a value below that of the ISDN connection and the backup will be terminated as intended.

14.2 Backup Solutions and Load Balancing with VRRP

14.2.1 Introduction

For businesses in particular, the high availability of data connections presents an essential requirement of the network components. LANCOM Systems devices provide various mechanisms for securing data transfer as a backup solution:

- Various WAN interfaces (DSL, ISDN, UMTS) enable data transfer over a second physical medium if the primary WAN interface is disturbed or fails.
- In order to provide protection from failure of an Internet provider's network, different Internet access accounts can be configured with Multi-PPoE.
- Two or more VPN gateways in a network can share the VPN tunnels required, thus keeping data traffic alive even in cases of temporary failure of a VPN end point.
- VRRP can now also be used to implement a sophisticated backup system for protection against router hardware failure. Two or more routers are installed in a network, one of which can replace the other in case of device failure.
- In addition to normal VRRP, LANCOM devices can link the backup event triggering function to the availability of a data connection. With this additional feature, LANCOM devices with more than one WAN interface (e.g. DSL and ISDN interface) can be implemented flexibly in backup solutions. The backup event is triggered for example, when the default route is no longer available via the DSL interface. The device's ISDN interface can take its place further along in the backup chain should the the backup router also fail ('Backup chains' → page 14-11).



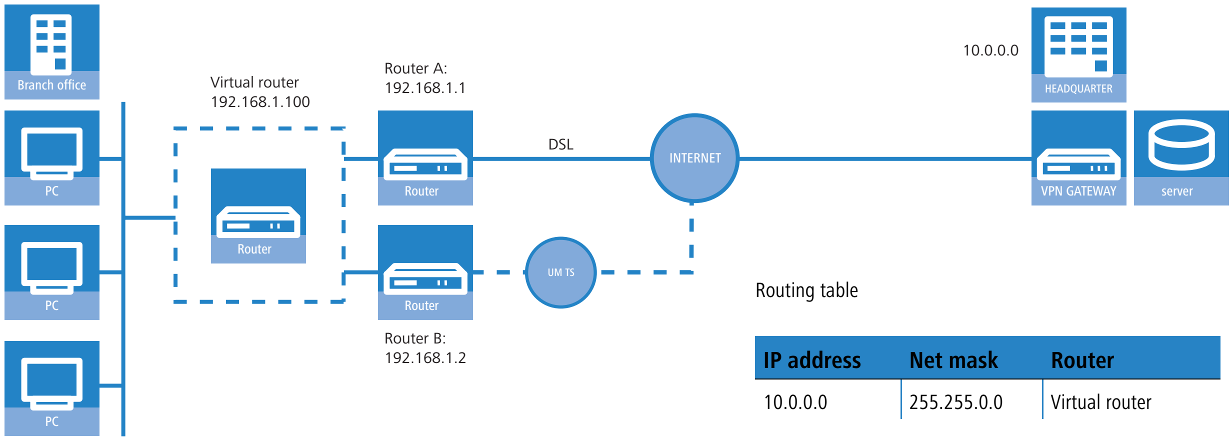
14.2.2 Virtual Router Redundancy Protocol

VRRP – Virtual Router Redundancy Protocol – enables multiple physical routers to appear as a single "virtual" router. Of the existing physical routers, one is always the "master". The master is the only router that establishes a data connection to the Internet, for example, and transfers data. The other routers only play a role when the master fails (e.g. due to a hardware defect or because its Internet connection is no longer available). Using the VRRP protocol, which is described in RFC 3768, they negotiate which device should assume the role of master. The new master completely takes over the tasks that were carried out by the previous master.

Virtual and physical routers

Dynamic routing protocols such as RIP adapt the entries in dynamic routing tables when, for example, a route is no longer available. When using VRRP, hosts in the LAN can use a static routing table even though the gateway IP address may change, for example, when a device fails due to a defect and another device takes over its functions. VRRP uses "virtual routers" in the routing tables so that the network users always find the right gateway nevertheless. A virtual router is broadcasted in the network with the IP address '192.168.1.100' in the same way as a "normal" router would be and takes over the function of a gateway to certain remote stations. The actual work of data transfer is carried out by the physical routers behind the virtual router.

- Under normal operating conditions, for example, router A with the IP address '192.168.1.1' establishes the connection to the Internet.
- If router A fails, then router B with the IP address '192.168.1.2' takes over the functions of router A. The network clients do not notice this change; for them, the "virtual" router '192.168.1.100' is still the gateway.



Routing table

IP address	Net mask	Router
10.0.0.0	255.255.0.0	Virtual router

From a more technical standpoint, a router in a network requires a unique MAC address in addition to an IP address. Therefore, when defining a virtual router, a virtual MAC address is defined simultaneously which the virtual router reacts to. The virtual MAC address is formed as '00-00-54-00-01-xx', whereby 'xx' stands for the unique router ID.

In order to determine which physical router reacts to the combination of virtual IP and MAC address, priorities are used for the physical routers. For this purpose, every physical router is assigned a priority. The router with the highest priority takes over the functions of the virtual router as master and thus reacts to the virtual IP and MAC addresses. If two physical routers have the same priority, then the router with the "higher" physical IP address is considered to be the master.

All physical routers report their availability on a regular basis so that, should the current master fail, the router with the next highest priority can take over the routing function at the end of this interval at the latest. If a device determines that it cannot complete the tasks required, it can actively log off before the end of the interval thereby triggering the transfer of the master role to the router with the next priority.

The major advantage of virtual routers is that they enable very flexible scenarios with backup and load balancing functions which remain virtually undetected by the LAN. Clients in the local network randomly select a DHCP server from those available and retrieve the required address information from this server.

Address assignment via DHCP with more than one DHCP server in the LAN

Several DHCP servers can be operated parallel to each other in a LAN without disrupting one another's functionality. Upon establishing a network connection, the DHCP clients request an IP address selecting one of the available DHCP servers. The DHCP server receiving the request checks to determine whether the address requested is available or already in use within the LAN before assigning the address. This check prevents address conflicts even when several DHCP servers are in use.

For the clients, it is irrelevant which physical router subsequently establishes the data connection. Similarly, the LAN clients do not notice when a router or WAN interface fails due to the fact that, in this case, another router steps in and is available under the same virtual addresses as before.

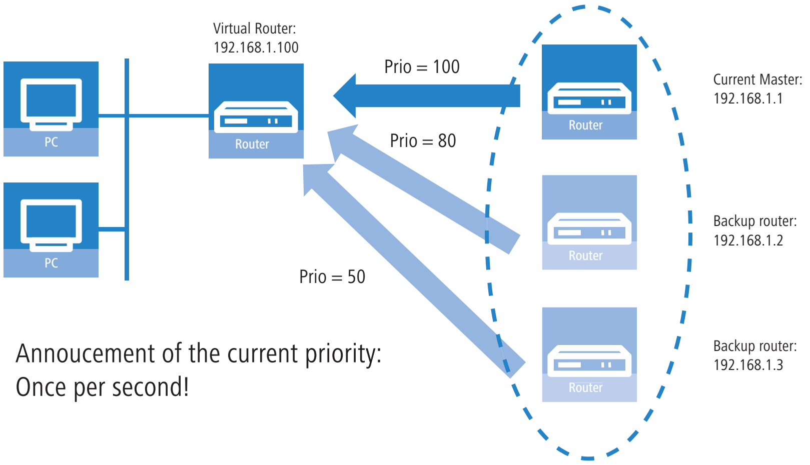
Device, connection or remote station backup

A device can disconnect itself from the VRRP group, an option which indicates that the possibilities offered by VRRP are not restricted only to the failure of a device.

VRRP only provides one backup mechanism which safeguards against device failure. In practice, however, the failure of a physical data transfer medium (e.g. DSL, ISDN or UMTS) or the unavailability of a remote station prevent the router from completing its tasks as planned. For this reason, the LANCOM-specific enhancements to VRRP also offer the ability to define the availability of a remote station as a trigger for the backup event—regardless of whether the data connection is denied due to device, connection or remote station problems.

For the definition of a virtual router, the IP address by which it can be accessed, its priority and its logical router ID are required as a minimum. The router ID serves to ensure that the regular messages from the physical routers can be assigned to the respective virtual routers.

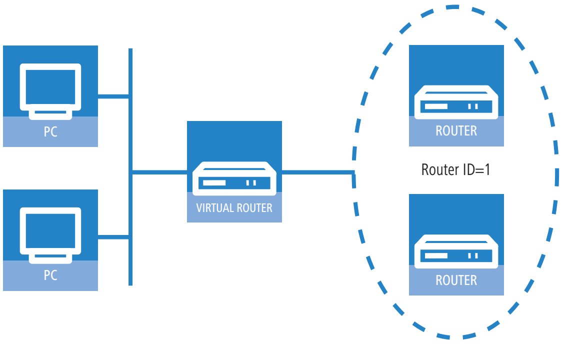
- The router ID can assume a value between 1 and 255. The router ID also reveals the router's virtual MAC address as 00:00:5E:00:01:router ID. The router ID 0 is not permitted.
- The IP address for the virtual router can be chosen freely, however, it must obviously be within the local network. If the virtual router's address is the same as the physical router's address, then the physical router is the "main master" of the system. The main master automatically has the highest priority, that is, when it signals that it is ready for operation, it immediately becomes the active master.
- The priority can assume a value between 1 and 254. The values 0 and 255 have special meanings: With the priority '0', the virtual router is not active, with '255', this virtual router is the main master.



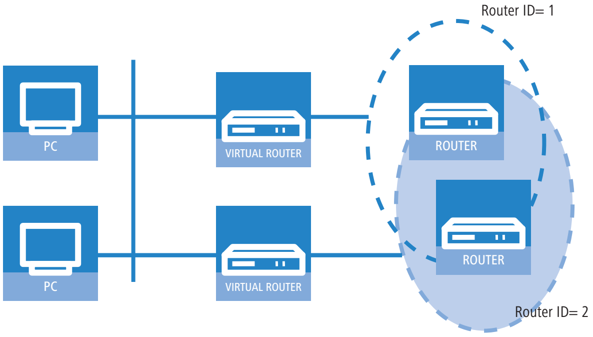
Router ID defines "standby groups"

The physical routers can be assigned to the virtual routers with the router ID that is determined when defining the virtual router. All devices in which virtual routers are set up with the same router ID form a "standby group" in which the devices can act as replacements for one another. There are three different examples of standby groups:

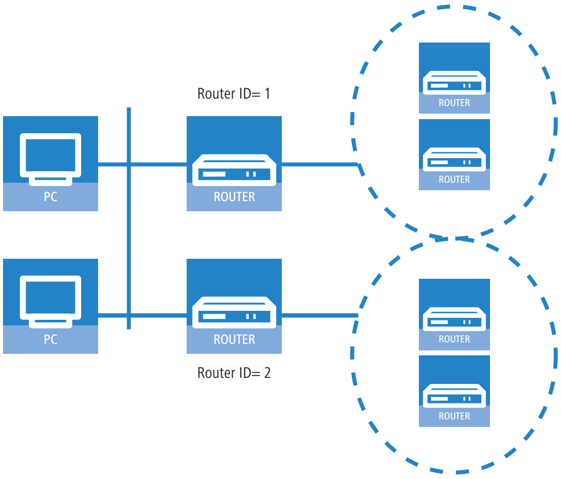
- In a simple backup scenario, two or more routers form **one** standby group. A virtual router with the same router ID and the same virtual IP address is configured in both physical routers.



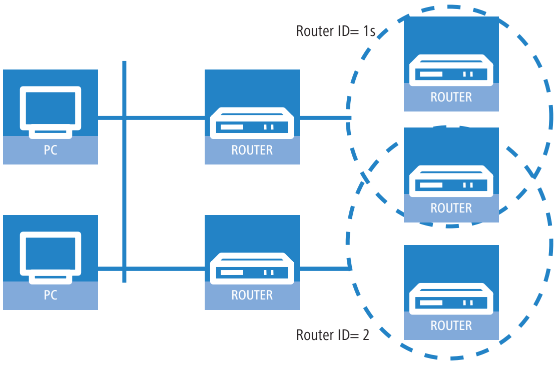
- In order to perform load balancing, the same number of virtual routers with differing IDs and IPs are defined as there are physical routers planned for the VRRP group. For example, two devices would each belong to **two** standby groups.



- It is also possible to create more complex combinations with many devices. For example, two devices can form their own standby group with router ID 1 and two other devices can form another group with the ID 2.



- Depending on the requirements, it is also possible to selectively assign certain devices to a single group while other devices remain members of all groups.



The Priority System

With the analysis of the priorities, VRRP controls the order in which the physical routers take over the function of the master in a VRRP group. VRRP only considers the failure of an entire device to be a trigger for the backup event.

Since numerous LANCOM devices have more than one WAN interface, the VRRP application in LCOS takes not only the failure of a device but also interruptions to the data connection or the unavailability of a remote station as triggers for the backup event. In order to enable the backup behavior of the LANCOM devices and the formation of backup chains, every virtual LANCOM router is assigned two priorities: a main and a backup priority.

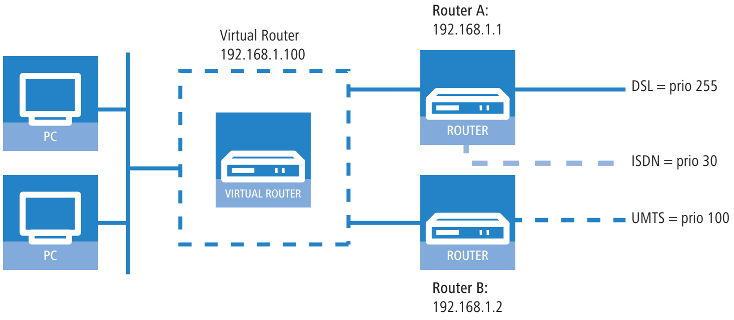
- The main priority is used (propagated into the network) as long as the device is in normal operating condition (i.e. the remote station for the standard connection is still available).
- The backup priority is propagated when the device is in backup mode (i.e. the backup delay has expired and the connection could not be reestablished).
- If '0' is set as the backup priority, the router will not send any signals until the end of the backup event, i.e. the device is not available to the VRRP router group when the remote station is not available.

Since VRRP only knows "priorities" and does not differentiate between main or backup priority, it simply analyzes the priority that is currently being propagated by the device. The device with the currently highest priority is considered to be master.

> Normally, priorities are configured so that the main priorities of the devices in a VRRP group are larger than the backup priorities used. However this is a general rule and not a requirement. The main priority of router A can be smaller than the backup priority of another router B. In this case, the backup connection of device B is used **before** the standard connection of router A in the backup chain ('Backup chains' → page 14-11).

The assignment of priorities to the various WAN interfaces can be determined from the configuration of the backup connections in the backup table (under LANconfig in the configuration area 'Communication' on the 'Call management' tab).

- The main priority refers to the interface on which the standard connection is configured.
- The backup priority refers to the interface on which the backup connection is configured.



VRRP list router A:

Main prio:	Backup prio:	Remote site
255	30	INTERNET DSL

Backup list router A:

Remote site	Backup list
INTERNET DSL	INTERNET ISDN

VRRP list router B:

Main prio:	Backup prio:	Remote site
100	0	INTERNET UMTS

A master that has been activated due to the priority status will now attempt to establish a connection if this has been configured as a keep alive connection. If the connection is set up as a normal connection with a hold time, then it will not be established until the next packet is transmitted. If this connection fails, thereby triggering the backup event, then the router will also log off and then propagate itself with its backup priority.

Backup chains

The use of two priorities enables the formation of flexible backup chains by which each physical router does not merely take a single place within the chain but takes a place for every physical WAN interface:

- The first physical router, the main router in the network, has a DSL and an ISDN interface for example, the second router (backup router) has a DSL and a UMTS interface.
- The first router receives the main priority '255'. Consequently, it will become the main router with the value '50' as its backup priority.
- The second router receives the main priority '150' and the value '100' as its backup priority.

Under normal operating conditions, data traffic is processed by the DSL interface on the first router. If the router or this interface fails, the second router attempts (due to the next highest main priority) to establish the connection via its own DSL interface. If this does not succeed, then both devices will propagate their backup priority. Since the second router has the higher backup priority, the connection is established using its UMTS interface. Only when this interface is also unable to establish a connection will the ISDN interface on the first router (with the lower backup priority) be used.

Only keep alive connections return automatically!

The standard connection will only be automatically reestablished after a backup event if the hold time for the connection is configured properly:

- A hold time of "0" means that the connection will not be actively terminated. If the connection is terminated or interrupted due to interference, it will not be automatically established again. The connection will only be reestablished when communication is required of it.
- A hold time of "9999" means that the connection is permanently held open. If it is interrupted, then the connection will be actively opened up again. This behavior is known as **keep alive**.

Set the hold time to "9999" for connections to the Internet provider (in the corresponding name list) and backed-up VPN connections (in the VPN connection list) to ensure that the connection is automatically reestablished and resumes data transfer after interruption.

Return to the VRRP group

After an adjustable amount of time (reconnect delay), a router that has logged off attempts to establish its main or backup connection again without propagating its priority first. If the main connection was successfully established, the backup event is terminated and the router returns to propagating its main priority. If only the backup connection was established, then the router falls back into the normal backup event and begins propagating its backup priority again.

As soon as a device can reestablish its main connection, the router begins propagating with its main priority again and becomes the master:

- Devices that are in backup mode with a lower main priority than the active master can also leave backup mode and propagate their main priority due to the fact that their backup connection is not required in this state.
- Devices that are in backup mode with a higher main priority than the active master can remain in backup mode as long as they are not able to establish their higher-prioritized main connection.
- Devices that have completely logged out of the VRRP group due to the unavailability of a VRRP remote site over the backup connection return to the normal backup mode.

Connection establishment

In order to allow coordinated connection establishment and prevent standby routers from attempting to establish connections, connections from a router are only established when this router:

- is the master **or**
- it is in backup mode and its main connection is configured with a keep alive **or**
- it has completely logged off and the timer for the renewed connection attempt (reconnect delay) expires

This simple rule allows the main connection to be configured as a keep alive connection even in standby routers. It also makes it possible only to use connections with hold time even in the main router.

Connections are always established when all virtual routers connected to the remote site have switched to standby mode. This either happens because another router propagates a higher priority or a LAN connection is lost.

14.2.3 Application scenarios

VRRP is normally employed for two different uses:

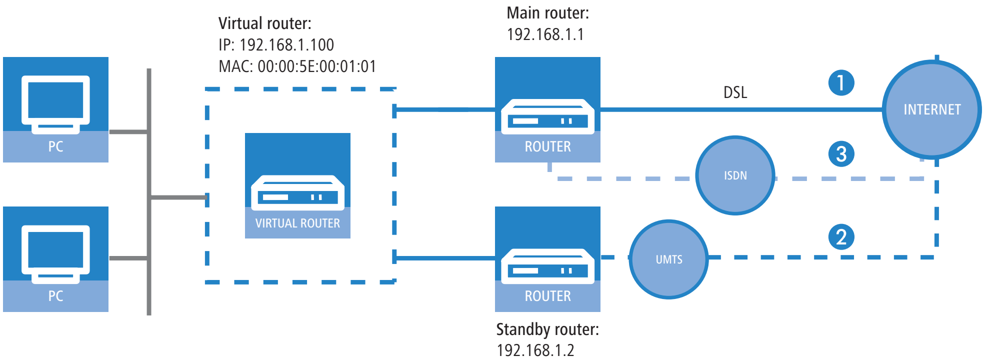
- In the simple backup case with two routers, one device under normal operation establishes the connection to the Internet. The second device is only operated in wait mode as a "standby device" and takes over the function of the main router should it fail.
- In the second case, two or more devices function parallel to each other as routers in the same network and distribute the incoming data connections using static load balancing. If one of these devices fails, the other router in the group can take over the failed device's functions.

Backup solution with VRRP

Possibly the most important application of VRRP is the provision of backup connections in which one or more routers serve as backup for the main router. These routers can use different physical media for the Internet connection, such as DSL in the main router and UMTS or ISDN in the backup routers. A normal backup chain thus resembles the following:

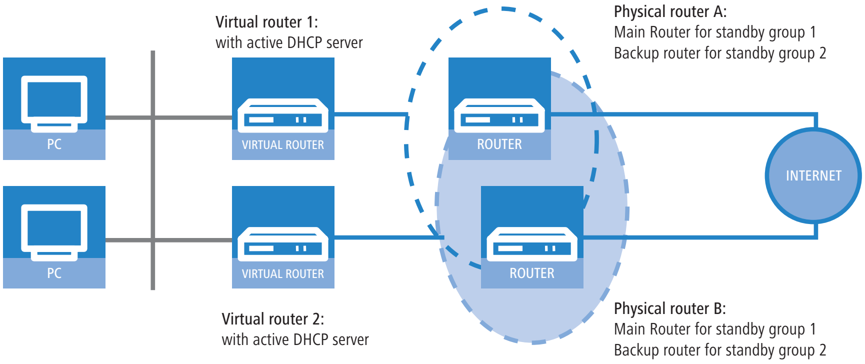
- If the DSL connection fails 1, the UMTS router takes over 2 the function.
- If the UMTS connection fails 2, the ISDN router takes over 3 the function.

Since almost all LANCOM devices with a DSL interface also have an ISDN interface, the main router can also take over ISDN backup functions at the end of the backup chain—as long as the hardware does not fail completely.



Load Balancing

With load balancing, several routers exist which can accomplish the same tasks. These routers are pronounced to be the default gateway and evenly distributed among the computers in the LAN using the DHCP server active in every router (see also ’Address assignment via DHCP with more than one DHCP server in the LAN’ → page 14-9). If one of the routers fails, then another can take over its functions providing both routers work with VRRP. On every router, as many virtual routers are defined as there are actual routers. The computers in the LAN are assigned one of the virtual routers as a gateway. Using the virtual router priorities, it is now defined in which order the other routers take over when a master fails. It is also possible to establish a backup chain using the main and backup priority here.



Example application: Secure Internet access via two DSL/ISDN combination routers

Two load-balancing default gateways that provide security for one another are to be the basis for operating the LAN at two DSL lines. On average, 50% of the LAN stations log in to router 1 and 50% to router 2. The failure of a router or the non-availability of a DSL connection is compensated for by the other router, which the takes over the full load.

Under normal operational circumstances, each router handles on average 50% of users in the LAN (prio 250 for the DSL connection). Should a router or DSL connection fail, then the load is distributed to the other router (prio 100 for the DSL connection of the backup router). If both DSL connections fail, then the traffic is directed over the ISDN connections (each with backup prio 50, ISDN connections not illustrated).

Notes for the configuration of the virtual router

Router A			Router B	
	DHCP= On (10.1.1.x)			DHCP= On (10.1.1.x)
Router ID = 1	Router IP = 10.1.1.1		Router ID=1	Router IP=10.1.1.1
	Prio = 250			Prio = 100
	Backup prio=50			Backup prio=50
	Remote station = DSL-INTERNET			Remote station = DSL-INTERNET
	Comment: Main router for group 1			Comment: Backup router for group 1
Router ID = 2	Router IP = 10.1.1.2		Router ID=2	Router IP=10.1.1.2
	Prio = 100			Prio = 250
	Backup prio=50			Backup prio=50
	Remote station = DSL-INTERNET			Remote station = DSL-INTERNET
	Comment: Backup router for group 2			Comment: Main router for group 2

14.2.4 Interaction with internal services

When using VRRP virtual routers with virtual IP and MAC addresses are used which, in turn, influences the internal services of LANCOM devices. They must behave differently depending on whether a virtual router or a physical router is addressed. Depending on the service or protocol used, the answers to address requests must be changed or completely denied.

ARP

The most important protocol when dealing with virtual routers is ARP (Address Resolution Protocol), which provides the ability to match logical addresses such as IP addresses to hardware addresses such as MAC addresses. The use of virtual and physical IP and MAC addresses means that the router's reaction to ARP requests is of great importance:

- An ARP request to the virtual router's address may only be answered when the LANCOM is the master. This request must be answered with the corresponding virtual MAC address. All other requests must be ignored.
- ARP requests that list a virtual router's address as the sender address must be ignored.
- When using proxy ARP, an ARP request must be checked in order to determine if a virtual router is associated with the remote station through which the requested address can be reached. If so, then the request may only be answered when the LANCOM is the master. This also applies to virtual remote stations (i.e. PPTP or VPN) when they use a remote station that is associated with a virtual router as a physical connection.
- ARP requests sent by the LANCOM itself are always sent with the real sender address, as long as this is not the address of a virtual router. In this event, the virtual MAC address must be entered in the ARP request.

ICMP

When using ICMP, echo requests and replies should be differentiated from error messages. For the error messages, ICMP redirect will require and additional inspection.

- An ICMP echo request directed to the virtual router's address may only be answered by the LANCOM when it is the master.
- ICMP redirects may also be sent from virtual routers but the address of the router to which the packet was sent must be entered as the sender address. This is to be determined from the packet's target MAC address.
- If the LANCOM is addressed via its physical MAC address and the target of the packet is linked to a virtual router, the address of which is connected to the receiving interface, then an ICMP redirect is returned and the sender receives the address of the virtual router.

- For all other error messages, it does not matter whether the virtual router's address or the real address is used as the sender address. To simplify matters, the real address is always used.

ⓘ With the implementation of VRRP in LANCOM, the previous option 'local routing' in the IP Router menu has been replaced with 'Send ICMP redirects'. If this option is enabled, ICMP redirects are sent, if the option is disabled, the packets are always forwarded.

DHCP

- Gateway address

  Although the computers in the LAN can use ICMP redirects to learn which router is the correct virtual router, it is still advisable to designate the correct router as gateway directly during the DHCP negotiation. This allows the assigning gateway address to be determined as follows:

  - If a gateway is explicitly defined for the interface in the DHCP module, then only this will be assigned.
  - If no explicit gateway is set, then the default route is looked up in the routing table. If the default route exists and is connected to a virtual router which is directly linked to the interface through which the DHCP request is received, then the virtual router's address is assigned as gateway.
  - If other remote sites are linked to virtual routers, then these will not be assigned via DHCP since there can only be one default gateway. A host can only learn the corresponding routers via ICMP redirects.
  - Otherwise, the address corresponding to the address pool or interface (intranet or DMZ) will be assigned.

  If more than one virtual router is connected by the default route, then the address of the router with the highest priority will be assigned. This allows for automatic load balancing ('Load Balancing' → page 14-13) through the selection of the DHCP server by the respective client. The DHCP server is to be activated on all routers involved in load balancing. All routers then define many virtual routers, each with different priorities. If the client randomly selects a DHCP server from those that answer, then it will also be randomly assigned a virtual router.

  Example with two routers

  LANCOM A defines the following virtual routers:

Router ID	Virt. address	Prio	B Prio	Peer
1	10.0.0.1	100	50	INTERNET
2	10.0.0.2	60	50	INTERNET

  and, correspondingly LANCOM B:

Router ID	Virt. address	Prio	B Prio	Peer
1	10.0.0.1	60	30	INTERNET
2	10.0.0.2	100	30	INTERNET

  Depending on whether it chooses LANCOM A or LANCOM B, a DHCP client will now be assigned 10.0.0.1 or 10.0.0.2 as gateway and is initially distributed on both LANCOM devices.

  Using this example, it becomes clear how load balancing can be combined with backup. If LANCOM A falls into backup mode, then LANCOM B will become the master for all clients. If LANCOM B fails, then LANCOM A will become the master for all clients and will attempt to establish its backup. If this fails, then it is LANCOM B's turn again (this signals the end of the backup chain).

- Further addresses

  If the DHCP server is to assign explicit addresses for certain services which the LANCOM provides, such as DNS and NBNS server, then either the configured addresses or the real addresses are assigned to the respective interfaces. Assigning a virtual router violates the RFC which prohibits a virtual router from offering other services (a device may only react to a virtual address when it is also the "owner" of this address, i.e. when the address is also the real interface address. At the same time, this means that DNS and NBNS must receive special treatment.

DNS server

Since the RFC prohibits a virtual router from offering additional services when the physical router is not the "owner" of the virtual IP address, the LANCOM DNS server requires special treatment. The LANCOM offers two options.

- The solution which conforms to the RFC works in the DNS forwarder. If an external IP address is entered as primary or secondary DNS server, then forwarding to the responsible virtual router functions automatically using the ICMP redirect treatment since the packet is simply forwarded to the virtual router.

However, if no address is entered and no connection has been made to the remote station to which the packet should be forwarded, then the DNS forwarder checks to see if a virtual router is connected to the remote station.

- □ If this is the case and the LANCOM is also the master for one of the virtual routers, then the connection is established and the packet is forwarded to the DNS server assigned to this connection.
- □ If the LANCOM is not the master for all connected routers, then the packet is forwarded to the master of the first connected router.

This procedure only works when all routers behave in accordance with the RFC and use port forwarding. If all of the routers involved are LANCOM devices, then this requirement is fulfilled.

- With the second option, a virtual router reacts to DNS requests itself.
  - □ In order to enable this behavior, the option 'Internal Services' must be enabled. The LANCOM accepts the requests to the internal services (here, for example, DNS) via the virtual addresses as if it had been addressed through one of the physical addresses.
  - □ In the default setting (Off) the LANCOM behaves in accordance with the RFC and drops the corresponding packets.
  - □ The default setting is 'On'.

  If a virtual router is connected to the default route when using the internal services, then this will be assigned by the LANCOM DHCP server as the DNS server. If more than one virtual router is connected by the default route, then the router with the highest priority will be assigned (as is the case with gateway addresses).

This option can only guarantee trouble-free operation if all of the routers involved are LANCOM devices.

NBNS/NetBIOS proxy

Since a NetBIOS proxy does not forward packets, the question of the virtual or physical addresses responded to is of no significance here. However, it is important that all routers and backup routers in the VRRP group can store the same host, group and server addresses learned from the remote site in their own database and propagate these upon connection establishment. This is the only method of ensuring that an NBNS request can be answered in every case.

Since the NetBIOS proxy propagates all host, group and server addresses learned from the remote site, it need only be ensured that this information is also recorded by the backup routers in their databases. Under normal circumstances, however, this is prevented by the route verification.

Since the transfer of addresses is usually prevented by the route verification, the addresses are only accepted in VRRP operation when **all** of the following requirements are fulfilled:

- There is a WAN route to the propagated address.
- The corresponding remote site is connected to a virtual router.
- The corresponding address is propagated by the master of this virtual router.
- The switch 'Internal Services' is activated.

Only when all of these requirements are fulfilled, will the respective address be accepted in the database. This ensures that the individual router databases remain consistent and all addresses are immediately recognized when a backup router becomes master.

The position of the 'Internal Services' switch influences the NetBIOS proxy.

- When it is enabled, the NetBIOS proxy accepts NBNS requests that are directed to virtual routers.
- If a virtual router is also connected to the default route, then this will be assigned by the LANCOM DHCP server as the NBNS server.
- If more than one virtual router is connected by the default route, then the router with the highest priority will be assigned (as is the case with gateway addresses).

RIP

The use of VRRP has a particularly strong influence on RIP, through which information on the accessible routes and the corresponding routers is propagated.

- On the one hand, routers must be made known in the network to remote stations which can be reached through a virtual router.
- On the other hand, the routes that are propagated by the virtual routers themselves must be ignored.
- Ultimately, the propagated information is dependent upon the interface which it is to be passed on to.

The announcement of routing information via RIP is governed by the following rules:

- Routes are propagated on all virtual and physical interfaces and every virtual router counts as its own virtual interface.
- If routes are currently being propagated on a physical interface (LAN/DMZ) and a route that must be propagated is connected to a virtual router, then two cases must be differentiated:
  - When the virtual router is active on the interface, i.e. its address is in the address range of the respective interface, then the route will not be propagated.
  - If the virtual router on the interface is not active, then the route will be propagated normally, i.e. the physical interface address will be propagated as the best route.
- If routes are propagated on a virtual router, then only the routes that are connected to this virtual router may be propagated.
- If routes are propagated on a WAN interface, then all routes are propagated.
- Upon receiving a RIP packet, the sender address of the RIP packet must be taken into consideration. The routes contained in the packet must be ignored when they are propagated by a virtual router known by the LANCOM device.
- If the LANCOM cannot establish a connection to the remote site because all channels are occupied, then RIP propagates the routes accessible through this remote site as "unavailable".
  - In addition, the VRRP module is notified in this case so that it can log off of the router connected to this remote site allowing a new master to be determined.
  - Similarly, VRRP receives notification when the connection is can be re-established in order to allow the virtual router to propagate with its main or backup priority again.

NTP

When the 'Internal Services' switch is enabled, then the LANCOM also accepts (S)NTP requests that are directed to virtual routers since the exact address of the time source is not relevant for an NTP client.

Other services

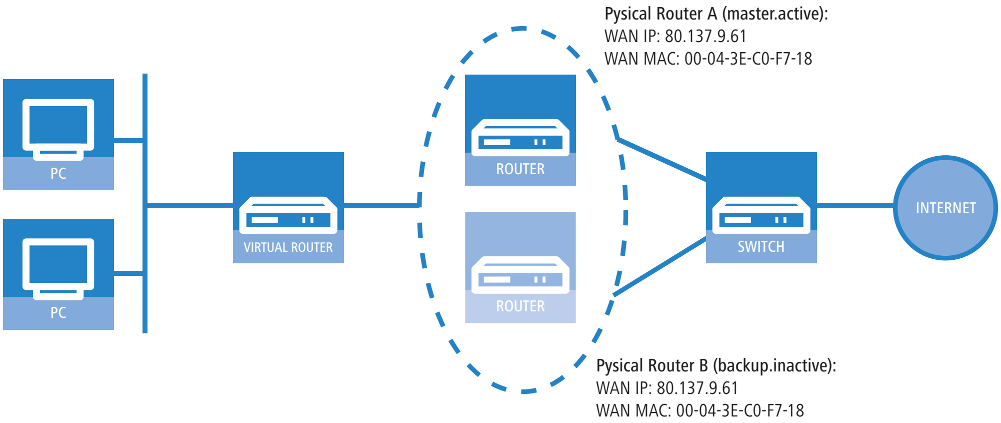
The LANCOM only processes other services when it is addressed via its physical address.

14.2.5 VRRP in the WAN

The description of VRRP is only in regard to the LAN portion of data networks and leaves the regulation of the WAN portion to dynamic routing protocols such as RIP. In order to enable WAN failover all the same, LANCOM VRRP provides two alternatives.

Same IP and MAC addresses

The first possibility entails assigning all of the routers in the VRRP group on the WAN side the same MAC and the same IP address. The routers are then connected to a commonly used DSL line, for example by a switch. In order to avoid address conflicts, only one router may actually react to these addresses on its WAN side, which is achieved through the use of VRRP.


Pysical Router A (master.active):
WAN IP: 80.137.9.61
WAN MAC: 00-04-3E-C0-F7-18
PC
PC
VIRTUAL ROUTER
ROUTER
ROUTER
SWITCH
INTERNET
Pysical Router B (backup.inactive):
WAN IP: 80.137.9.61
WAN MAC: 00-04-3E-C0-F7-18

- Due to the fact that the LANCOM terminates its WAN connection when the last virtual router switches to backup mode, this requirement is definitely fulfilled when a total of only one virtual router has been defined.
- In the backup scenario, the necessary requirement is also fulfilled because the main connection is guaranteed to have been terminated or else the backup router would not have become master.

Routing protocols

In the load balancing scenario, however, there are two different WAN connections online simultaneously, which is why the use of the same MAC and IP address is not possible here. In this case, a routing protocol such as RIP, OSPF or BGP must be used as a second option.

In order to accelerate the switch using RIP, which is rather slow, a LANCOM propagates to all networks that it is no longer available before the connection is established, thereby ensuring a quick change of routing priorities.

14.2.6 Configuration

In order to configure failover or load balancing with VRRP, the following parameters can be set:

- **Activation**: The switch 'VRRP activate' enables the VRRP module to be switched on or off (default = off).
- **VRRP list**: In the VRRP list, up to 16 virtual routers can be defined. This table has the following fields:
  - **Router ID**: Unique ID for the virtual router. Values between 1 and 255 are possible. The router ID is used to consolidate several physical routers into a single virtual router or a standby group (’Router ID defines "standby groups“’ → page 14-9).
  - **Router IP**: IP address for the virtual router.

All routers on which the virtual router is set up must assign this router the same IP address.

  - **Main priority**: The main priority of the virtual router with regard to routers with several interfaces refers to the main interface, i.e. with routers with DSL and ISDN support to the DSL interface. Values between 0 and 255 are permitted. The values 0 and 255 have special meanings:

    '0' turns the virtual router off.
  - '255' is only accepted when the virtual router address is identical to the address of the interface that is connected to the router. In other cases, the priority is automatically lowered.
  - **Backup priority**: The backup priority of the virtual router refers to the interface for which a backup connection is configured, i.e. with routers with DSL and ISDN support to the ISDN interface. Here again, values between 0 and 255 are permitted. The values 0 and 255 also have special meanings here:

    0 disables the virtual router in the backup event. Checks are conducted regularly in order to determine whether or not the standard connection can be reestablished. The inspection interval is defined in the reconnect delay.

    '255' is only accepted when the virtual router address is identical to the address of the interface that is connected to the router. In other cases, the priority is automatically lowered.

  When the backup connection cannot be established in backup mode, then the virtual router logs off completely and attempts to reestablish the standard or backup connection in intervals defined by the reconnect delay.

  - **Remote site**: Name of the remote station that controls the virtual router behavior. The remote site can also be assigned to other virtual routers.

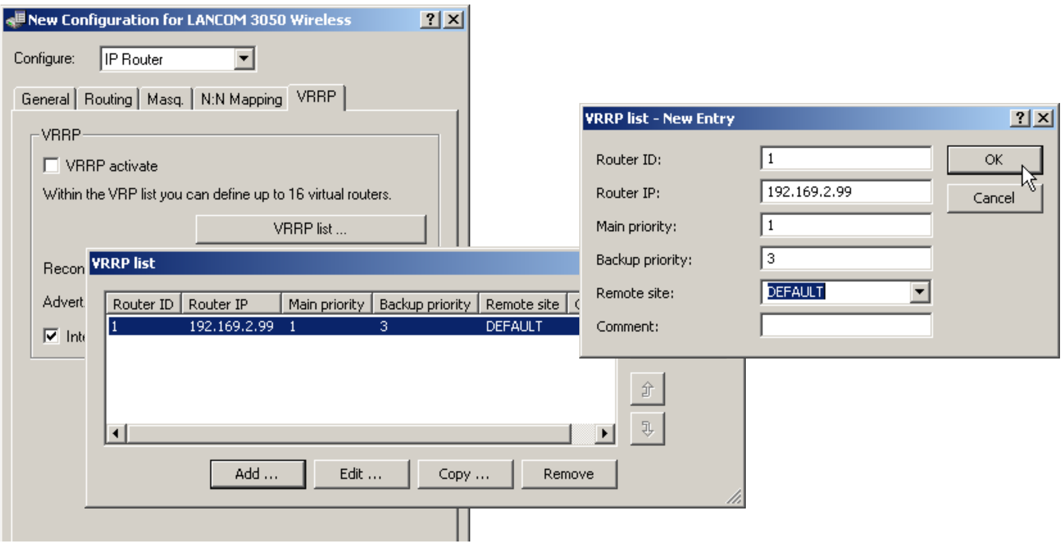
Entering the remote site is optional. Linking the backup requirement to a remote site allows the use of the LANCOM-specific enhancement to VRRP not only to secure against device failure (VRRP standard) but also against interface failure or disruption at a remote site.

  - **Comment**: 64 character-long commentary describing the virtual router.
- **Reconnect delay**: The reconnect delay time shows after how many minutes a virtual router that has logged off attempts to reestablish its standard connection. The router remains logged off during this connection attempt. It is only broadcasted with its main or backup priority after the connection has been established successfully. The default value is 30 minutes.
- **Advert. interval**: The advertising interval shows how many seconds until a virtual router is propagated again. The default value is 1 second.

With a propagation time of 1 second, the routers in the VRRP group can change quickly when a device or interface fails. An interruption of this type will usually remain undetected due to the fact that the TCP connection is not interrupted. Other routing protocols require up to 5 minutes or longer in order to conduct the transfer to a backup router.

- **Internal services**: The Internal services check box controls how the device should behave when it is addressed via a virtual router address.
  - In the 'On' position, the LANCOM reacts to certain services exactly as if it had been addressed via its actual address. Naturally, this only occurs when the device itself is the master of the virtual router. The behavior of the DHCP server changes simultaneously (’Interaction with internal services’ → page 14-14).

- □ The default setting 'Off' results in behavior in accordance with the RFC, meaning means that the corresponding packets are silently dropped.
- □ The default setting is 'On'.



New Configuration for LANCOM 3050 Wireless

Configure: IP Router

General | Routing | Masq. | N:N Mapping | VRRP

VRRP

☐ VRRP activate

Within the VRP list you can define up to 16 virtual routers.

VRRP list ...

VRRP list

Router ID	Router IP	Main priority	Backup priority	Remote site
1	192.169.2.99	1	3	DEFAULT

Add ... | Edit ... | Copy ... | Remove

VRRP list - New Entry

Router ID:	1
Router IP:	192.169.2.99
Main priority:	1
Backup priority:	3
Remote site:	DEFAULT
Comment:	

OK | Cancel

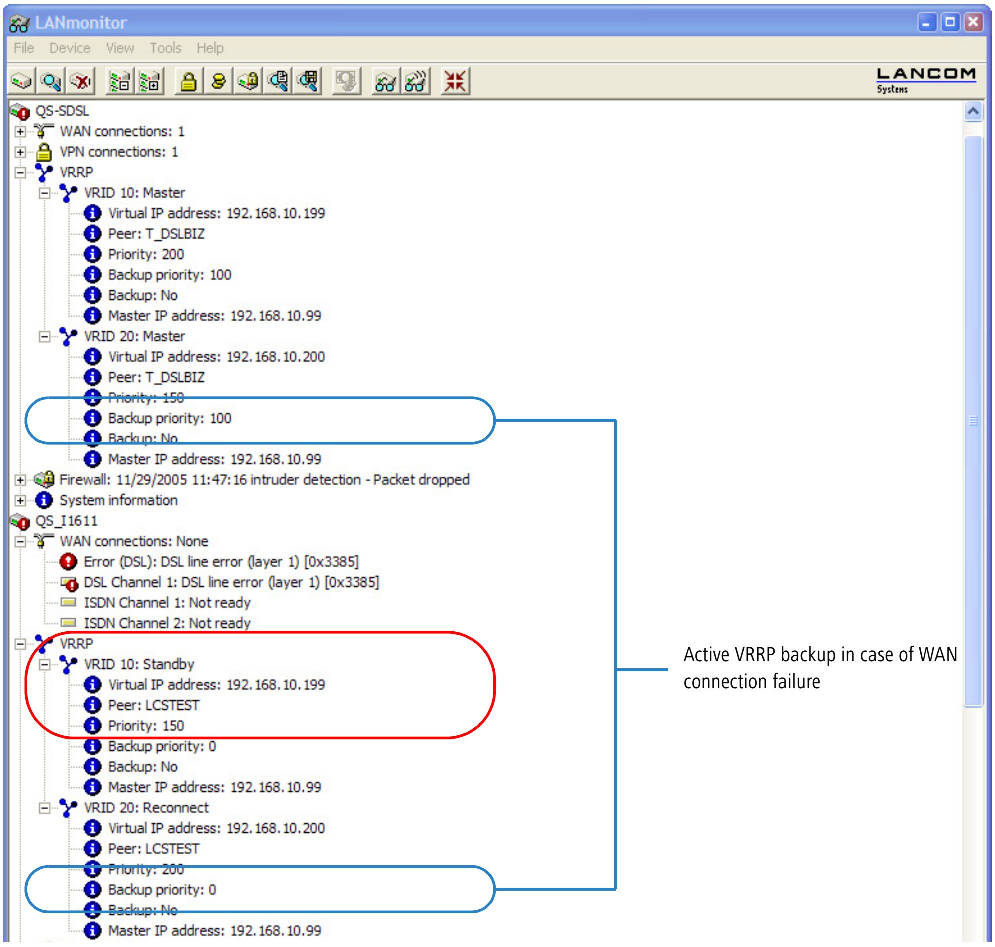
LANconfig: IP router ▶ VRRP

WEBconfig: LCOS menu tree ▶ Setup ▶ IP router ▶ VRRP

14.2.7 Status Information

Status request with LANmonitor

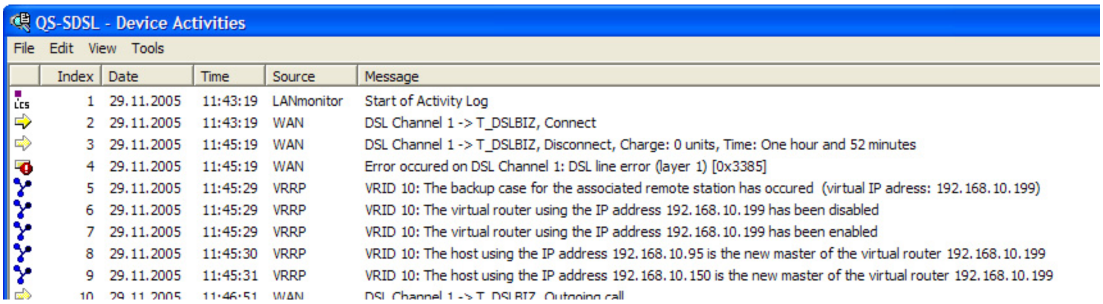
The current status of the devices in the VRRP group is showed in LANmonitor as long as the VRRP module is activated:



```
QS-SDSL
  WAN connections: 1
  VPN connections: 1
  VRRP
    VRID 10: Master
      Virtual IP address: 192.168.10.199
      Peer: T_DSLBIZ
      Priority: 200
      Backup priority: 100
      Backup: No
      Master IP address: 192.168.10.99
    VRID 20: Master
      Virtual IP address: 192.168.10.200
      Peer: T_DSLBIZ
      Priority: 150
      Backup priority: 100
      Backup: No
      Master IP address: 192.168.10.99
  Firewall: 11/29/2005 11:47:16 intruder detection - Packet dropped
  System information
QS_I1611
  WAN connections: None
    Error (DSL): DSL line error (layer 1) [0x3385]
    DSL Channel 1: DSL line error (layer 1) [0x3385]
    ISDN Channel 1: Not ready
    ISDN Channel 2: Not ready
  VRRP
    VRID 10: Standby
      Virtual IP address: 192.168.10.199
      Peer: LCSTEST
      Priority: 150
      Backup priority: 0
      Backup: No
      Master IP address: 192.168.10.99
    VRID 20: Reconnect
      Virtual IP address: 192.168.10.200
      Peer: LCSTEST
      Priority: 200
      Backup priority: 0
      Backup: No
      Master IP address: 192.168.10.99
```

Active VRRP backup in case of WAN connection failure

In the device activity log, VRRP events can be viewed in chronological order.



QS-SDSL - Device Activities

Index	Date	Time	Source	Message
1	29.11.2005	11:43:19	LANmonitor	Start of Activity Log
2	29.11.2005	11:43:19	WAN	DSL Channel 1 -> T_DSLBIZ, Connect
3	29.11.2005	11:45:19	WAN	DSL Channel 1 -> T_DSLBIZ, Disconnect, Charge: 0 units, Time: One hour and 52 minutes
4	29.11.2005	11:45:19	WAN	Error occured on DSL Channel 1: DSL line error (layer 1) [0x3385]
5	29.11.2005	11:45:29	VRRP	VRID 10: The backup case for the associated remote station has occured (virtual IP adress: 192.168.10.199)
6	29.11.2005	11:45:29	VRRP	VRID 10: The virtual router using the IP address 192.168.10.199 has been disabled
7	29.11.2005	11:45:29	VRRP	VRID 10: The virtual router using the IP address 192.168.10.199 has been enabled
8	29.11.2005	11:45:30	VRRP	VRID 10: The host using the IP address 192.168.10.95 is the new master of the virtual router 192.168.10.199
9	29.11.2005	11:45:31	VRRP	VRID 10: The host using the IP address 192.168.10.150 is the new master of the virtual router 192.168.10.199
10	29.11.2005	11:46:51	WAN	DSL Channel 1 -> T_DSLBIZ, Outgoing call

Status request with WEBconfig, Telnet or SSH

Status information on VRRP can be found in the IP router's status menu and offers the following entries:

- The values Rx and Tx count the VRRP packets received or sent, respectively.
- Error counts all fatal protocol errors that are logged.
- Drop counts all VRRP packets that are dropped, e.g. when a serious error occurred.

In the Virtual Router table, all active virtual routers are listed with their current status. This table has the following fields:

- **Router ID**: Unique ID for the virtual router.
- **Virt. address**: IP address for the virtual router.
- **Prio**: Main priority for the virtual router.
- **B-Prio**: Backup priority for the virtual router.
- **Remote site**: Name of the remote station that controls the virtual router behavior.
- **State**: State of the virtual router. The following states are possible:
  - Init: The router is currently being set up.
  - Listen: The router is currently learning which device is the master.
  - Standby: The router is the standby router.
  - Master: The router is the master.
  - Down: The router is deactivated.
  - Reconnect: The reconnect timer is running and the router is currently not propagating itself.
- **Backup**: Shows if the remote station (peer) is in backup or not. If the remote station is in backup, then the device will propagate its backup priority, otherwise it will propagate its main priority.
- **Master**: Shows which of the physical routers is currently the master.

The MAC list table displays the MAC addresses for the virtual routers that are currently masters. This table has the following fields:

- **Virt. address**: IP address for the virtual router.
- **MAC address**: MAC address for the virtual router.
- **Router ID**: Unique ID for the virtual router.

15 Office communications with LANCAPI

This section only applies to devices with ISDN interface.

LANCAPI from LANCOM Systems is a special version of the popular CAPI interface. CAPI (Common ISDN Application Programming Interface) establishes the connection between ISDN adapters and communications programs. For their part, these programs provide the computers with office communications functions such as a fax machine or answering machine.

15.1 What are the advantages of LANCAPI?

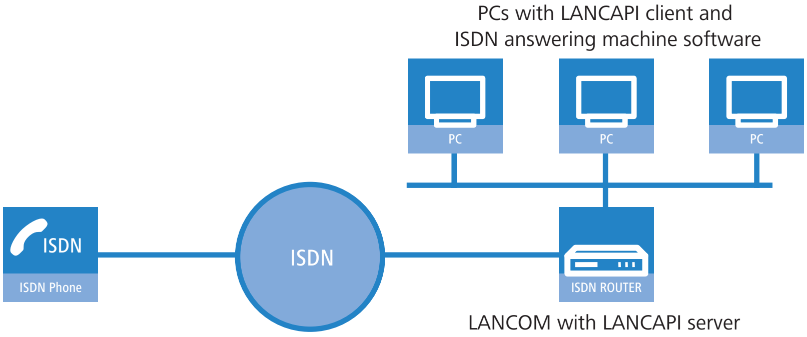
The main advantages of using LANCAPI are economic. LANCAPI provides all Windows workstations integrated in the LAN (local-area network) with unlimited access to office communications functions such as fax machines, answering machines, online banking and eurofile transfer. All functions are supplied via the network without the necessity of additional hardware at each individual workstation, thus eliminating the costs of equipping the workstations with ISDN adapters or modems. All you need do is install the office communications software on the individual workstations.

For example, faxes are sent by simulating a fax machine at the workstation. With LANCAPI, the PC forwards the fax via the network to the router which establishes the connection to the recipient.

Please note: All LANCAPI-based applications access the ISDN directly and do not run across the router of the device. The connect-charge monitoring and firewall functions are thus disabled! The LANCAPI is also independent from all routing or VPN functions.

15.2 The client and server principle

The LANCAPI is made up of two components, a server (in the LANCOM) and a client (on the PCs). The LANCAPI client must be installed on all computers in the LAN that will be using the LANCAPI functions.


PCs with LANCAPI client and
ISDN answering machine software
PC
PC
PC
ISDN
ISDN Phone
ISDN
ISDN ROUTER
LANCOM with LANCAPI server

15.2.1 Configuring the LANCAPI server

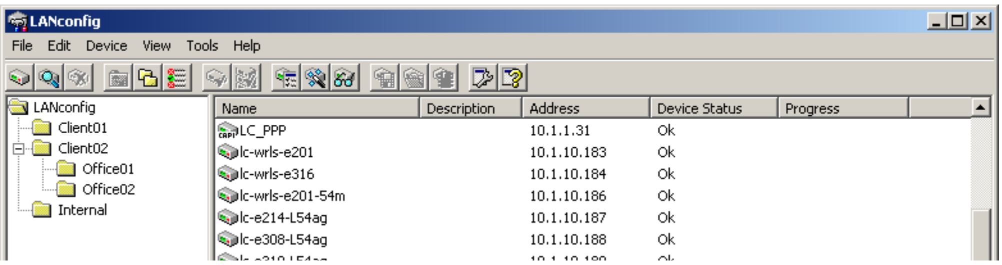
Two basic issues are important when configuring the LANCAPI server:

- What call numbers from the telephone network should LANCAPI respond to?
- Which of the computers in the local network should be able to access the telephone network via LANCAPI?

The configuration of the router takes place in the configuration tables of LANconfig or WEBconfig. In the following two sections you can find the instructions for both of these configuration programs.

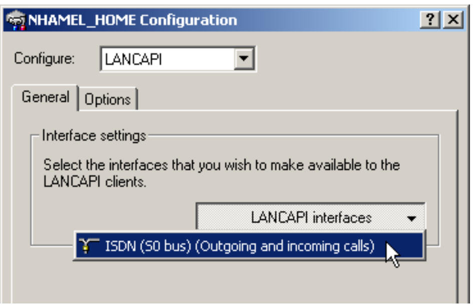
Configuration with LANconfig

① Open the configuration of the router by double-clicking on the device name in the list and enter your password if requested.



Name	Description	Address	Device Status	Progress
LC_PPP		10.1.1.31	Ok	
lc-wrls-e201		10.1.10.183	Ok	
lc-wrls-e316		10.1.10.184	Ok	
lc-wrls-e201-54m		10.1.10.186	Ok	
lc-e214-L54ag		10.1.10.187	Ok	
lc-e308-L54ag		10.1.10.188	Ok	

② In the configuration area 'LANCAPI' click on the tab 'General' and select at the **LANCAPI interfaces** the ISDN port you want to set.



NHAMEL_HOME Configuration

Configure: LANCAPI

General | Options

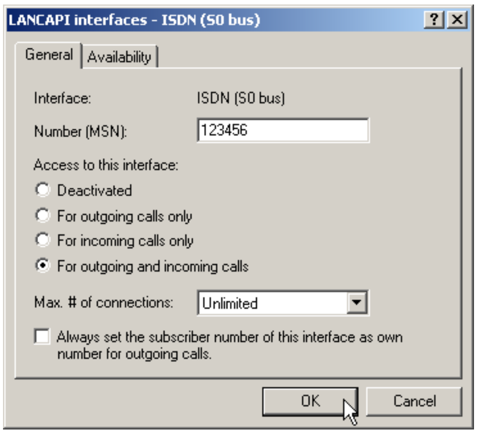
Interface settings

Select the interfaces that you wish to make available to the LANCAPI clients.

LANCAPI interfaces

ISDN (S0 bus) (Outgoing and incoming calls)

③ Activate the LANCAPI server for the outgoing and incoming calls, or allow only outgoing calls.



LANCAPI interfaces - ISDN (S0 bus)

General | Availability

Interface: ISDN (S0 bus)

Number (MSN): 123456

Access to this interface:

○ Deactivated

○ For outgoing calls only

○ For incoming calls only

● For outgoing and incoming calls

Max. # of connections: Unlimited

□ Always set the subscriber number of this interface as own number for outgoing calls.

OK | Cancel

If the LANCAPI server is supposed to respond to incoming calls, enter the call numbers to which the LANCAPI should respond in the 'Number (MSN)' field. You can enter several call numbers separated by semicolons. If you do not enter a call number here, all incoming calls are reported to LANCAPI.

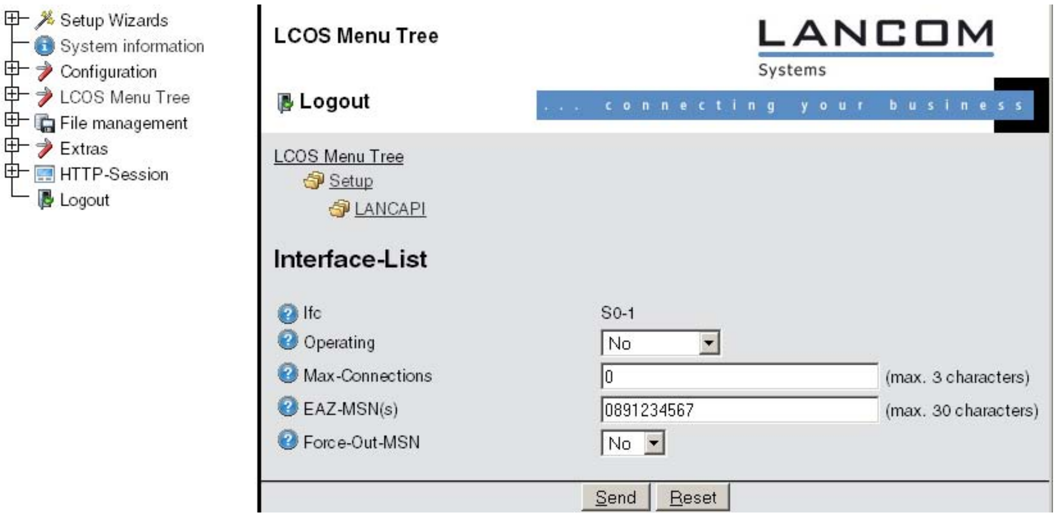
Configuration of WEBconfig

① Select in the main menu the **LCOS menu tree**.

② Select in the following menus **Setup** ▶ **LANCAPI-module** ▶ **Interface-list**.

③ Select in the **Interface-list** the (only) entry **S0-1**.

④ Activate the LANCAPI server for outgoing and incoming calls ('On'), or only allow outgoing calls ('Dail-only').



Interface-List

Ifc: S0-1

Operating: No

Max-Connections: 0 (max. 3 characters)

EAZ-MSN(s): 0891234567 (max. 30 characters)

Force-Out-MSN: No

Send | Reset

If the LANCAPI server is supposed to respond to incoming calls, enter the call numbers to which the LANCAPI should respond in the 'Number (MSN)' field. You can enter several call numbers separated by semicolons. If you do not enter a call number here, all incoming calls are reported to LANCAPI.

15.2.2 Installing the LANCAPI client

For the installation of the LANCAPI client on a system with Windows XP or Windows 2000 administrator rights are required.

① Place the LANCOM CD in your CD-ROM drive. If the setup program does not automatically start when you insert the CD, simply click 'autorun.exe' in the main directory of the LANCOM CD in the Windows Explorer.

② Select the Install LANCOM software entry.

③ Highlight the **LANCAPI** option. Click **Next** and follow the instructions for the installation routine.

If necessary, the system is restarted and LANCAPI is then ready to accept all jobs from the office communications software. After successful installation, an icon for LANCAPI will be available in the toolbar. A double-click on this icon opens a status window that permits current information on the LANCAPI to be displayed at any time.

The LANCAPI client starts automatically and shows the status in the windows task bar.

CAPI = active | **= Error** | **= inactive**

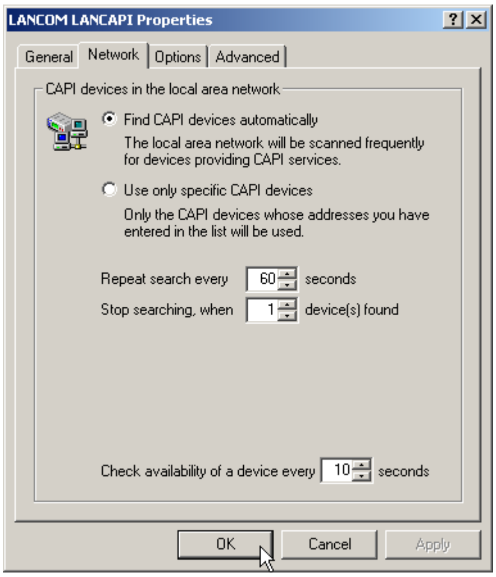
15.2.3 Configuration of the LANCAPI clients

The configuration of the LANCAPI clients is used to determine which LANCAPI servers will be used and how these will be checked. All parameters can remain at their default settings if you are using only one LANCOM in your LAN as an LANCAPI server.

① Start the LANCAPI client in the 'LANCOM' program group. Information regarding the drivers for the available service can be found on the 'General' tab.

② In the LANCAPI client, change to the **Network** tab. First, select whether the PC should find its own LANCAPI server, or specify the use of a particular server.

- For the former, determine the interval at which the client should search for a server. It will continue searching until it has found the number of servers specified in the next field. Once the required number of servers has been found, it will stop searching.
- In the event that the client should not automatically search for servers, list the IP addresses of the servers to be used by the client. This can be useful if you are operating several LANCOM in your LAN as LANCAPI servers and you would like to specify a server for a group of PCs, for example.
- It is also possible to set the interval at which the client checks whether the found or listed servers are still active.



LANCOM LANCAPI Properties

General | Network | Options | Advanced

CAPI devices in the local area network

● Find CAPI devices automatically

The local area network will be scanned frequently for devices providing CAPI services.

○ Use only specific CAPI devices

Only the CAPI devices whose addresses you have entered in the list will be used.

Repeat search every 60 seconds

Stop searching, when 1 device(s) found

Check availability of a device every 10 seconds

15.3 How to use the LANCAPI

Two options are available for the use of the LANCAPI:

- You may use software which interacts directly with a CAPI (in this case, the LANCAPI) port. This type of software searches for the CAPI during its installation and uses it automatically.

- Other programs such as LapLink can establish a variety of connection types, for example, using Windows Dial-Up Networking. You may select the installed communications device that you would like to use when creating a new dial-up connection. For the LANCAPI, select the entry 'ISDN WAN Line 1'.

15.4 The LANCOM Systems CAPI Faxmodem

The CAPI Faxmodem provides a Windows fax driver (Fax Class 1) as an interface between the LANCAPI and applications, permitting the use of standard fax programs with an LANCOM. The LANCOM CAPI Faxmodem emulates the modem functions, as well as the fax protocols in the software on the PC. For this purpose an adequate performance (500 MHz Pentium and more) is required.

Installation

The CAPI Faxmodem can be installed from the CD setup. Always install the CAPI Faxmodem together with the current version of LANCAPI. After restarting, the CAPI Faxmodem will be available for you, e.g. in Windows 98 under **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Modems**.

Faxing with the CAPI Faxmodem

Most major fax programs recognize the CAPI Faxmodem automatically during installation and identify it as a 'Class 1' fax modem. Fax transmissions can thus be realized at speeds of up to 14,400 bps. If your fax program offers you a choice (such as WinFax and Talkworks Pro), select the option 'CLASS 1 (Software Flow Control)' when setting up the modem.

Faxing under Windows XP and Windows 2000

Windows XP or Windows 2000 provide with the CAPI Faxmodem full functionality for faxing. An additional fax program is not required.

Thereto start in the Control Panel under “Add or Remove Programs”, “Add/Remove Windows Components” and select “Fax Services”.

After the installation the fax can be found under “Printers and Faxes”, and can be chosen in any Windows program instead of a printer.

The CAPI Faxmodemis only able to transmit fax messages, if the LANCAPI ist active.

15.5 LANCOM Faxmodem option

Additionally to the CAPI Faxmodem some LANCOM models (LANCOM 800, 4000, 4100) have a faxmodem option. With this solution the fax and modem services are implemented in the LANCOM itself, the PCs are released from the load of the modem emulation.

15.6 Provided B channel protocols

Following CAPI-Protocols are provided

Value		Remark
B1 protocol		
	0	64 Kbps with HDLC framing
	1	64 Kbps transparent with byte framing of the network
	2	V.110 asynchron with start-stop-byte framing
	4*	T.30-Modem for fax group 3
	7*	Modem with full negotiations (B2 has to be 7)
B2-Protocol		
	0	ISO 7776 (X.75 SLP)
	1	Transparent
	4*	T.30 for fax group 3
	7*	Modem with full negotiations (e.g. V.42 bis, MNP 5)
	9	V.120 asynchron
B3-Protocol		

Value		Remark
	0	Transparent
	1	T.90NL, compatible with T.70NL in accordance with T.90, Appendix II
	2	ISO 8208 (X.25 DTE-DTE)
	4*	T.30 for fax group 3
	5*	T.30 for fax group 3 extended
	7*	Modem

* = valid only for LANCOM faxmodem option

16 More services

An LANCOM offers a number of services for the PCs in the LAN. These are central functions that can be used by workstation computers. They are in particular:

- Automatic address administration with DHCP
- Name management of computers and networks with DNS
- Logging of network traffic with SYSLOG
- Recording of charges
- Office communications functions with LANCAPI
- Time server

16.1 Automatic IP address administration with DHCP

New in LCOS 7.60:

- BOOTP: Assignment of fixed IP addresses or boot images to specific workstations depending on the IP network (ARF)

16.1.1 Introduction

DHCP server

All devices in a local area network require a unique IP address in order for a TCP/IP network to function smoothly. They also require the addresses of DNS and NBNS servers and also of a standard gateway that can route data packets to addresses not located on the local network.

In a small network it is still possible to enter these addresses on all the computers in the network "by hand". However, in a large network with many workstations this soon becomes an unmanageable task. This is where the use of DHCP (dynamic host configuration protocol) comes in. A DHCP server in a TCP/IP-based LAN can use this protocol to assign the required addresses to the individual workstations dynamically.

LANCOM devices have an integrated DHCP server that can assume the task of assigning IP addresses. This process involves communicating the following parameters to the workstations:

- IP address
- Network mask
- Broadcast address
- Standard gateway
- DNS server
- NBNS server
- Lease (validity period) of the assigned parameters

The DHCP server either takes the IP addresses from a freely defined address pool or determines the addresses independently based on its own IP address. A completely unconfigured device in DHCP auto-mode can even specify IP addresses for itself and for network devices autonomously. Therefore in the most basic scenario you only need to connect a new out-of-the-box device to a network without a DHCP server and switch it on. The DHCP server will then manage all further address assignment in the LAN by itself in cooperation with LANconfig using a Wizard.

DHCP settings can be different for each network. It is possible to define several IP networks in the LANCOM devices in conjunction with advanced routing and forwarding (ARF). DHCP settings therefore apply to a particular IP network, with the exception of a few general settings.

DHCP relay

If another DHCP server is located in the LAN, the device can obtain the address information it requires from the other DHCP server if it is in DHCP client mode.

The LANCOM can also operate as a DHCP relay agent and as a DHCP relay server.

- As a DHCP relay agent the LANCOM forwards DHCP requests to another DHCP server.
- As a DHCP relay server the LANCOM processes DHCP requests forwarded from DHCP relay agents.

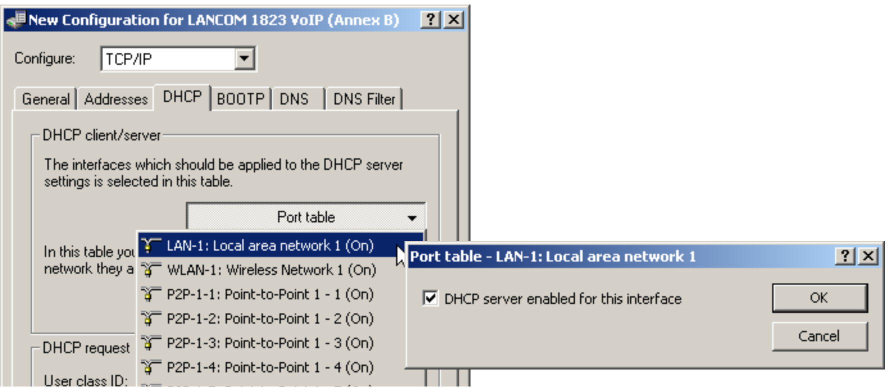
BOOTP

The bootstrap protocol (BOOTP) can be used to send a certain IP address and other parameters to a workstation when it boots up. Workstations without hard drives can use BOOTP to load a boot image, i.e. a complete operating system, from a boot server.

16.1.2 Configuring DHCP parametersLANconfig

Activating/deactivating a DHCP server for specific logical interfaces

The DHCP server can be activated or deactivated separately for each logical interface (e. g. LAN-1, WLAN-1, P2P-1-1 etc.). To do this, select the appropriate logical interface from the port list and switch the DHCP server on or off for this interface. You can find the parameters for activating the ports in LANconfig in the configuration area "TCP/IP" on the "DHCP" tab.



New Configuration for LANCOM 1823 VoIP (Annex B)

Configure: TCP/IP

DHCP client/server

The interfaces which should be applied to the DHCP server settings is selected in this table.

In this table you network they a

DHCP request

User class ID:

Port table - LAN-1: Local area network 1

☑ DHCP server enabled for this interface

General
Addresses
DHCP
BOOTP
DNS
DNS Filter
Port table
LAN-1: Local area network 1 (On)
WLAN-1: Wireless Network 1 (On)
P2P-1-1: Point-to-Point 1 - 1 (On)
P2P-1-2: Point-to-Point 1 - 2 (On)
P2P-1-3: Point-to-Point 1 - 3 (On)
P2P-1-4: Point-to-Point 1 - 4 (On)
OK
Cancel

Configuring DHCP networks

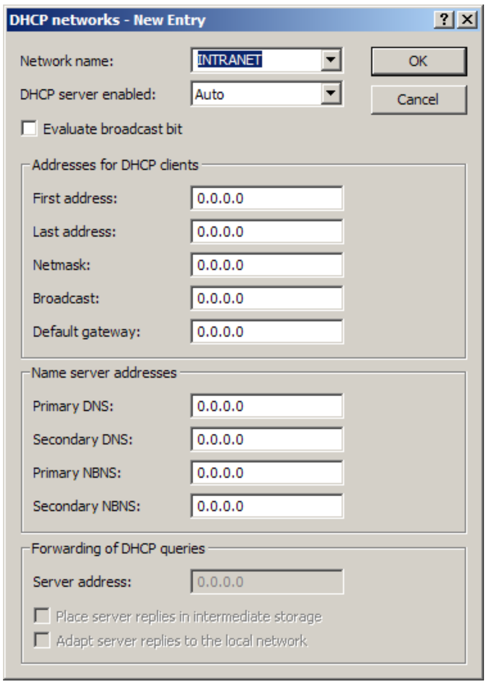
The appropriate DHCP settings can be specified separately for any IP network defined in the device. You can find the parameters for defining DHCP networks in LANconfig in the configuration area "TCP/IP" on the "DHCP" tab.

When configuring DHCP networks, the addresses are defined that can be assigned to the DHCP clients (address pool). When a client is activated in the network and requests an IP address via DHCP, the device with an activated DHCP server will offer to issue an address. This address is selected from the pool of valid IP addresses. A computer which received an IP address in the past requests this address again and, assuming the DHCP server has not assigned this number to another computer in the meantime, it will attempt to issue this address again.

The DHCP server also checks the LAN to confirm that the selected address is free. Once the address is confirmed as unique, it is assigned to the requesting computer.

The device factory settings include the IP networks 'Intranet' and 'DMZ', although there are no settings for IP addresses and netmasks. The device is in a special operating mode. It then uses the IP address '172.23.56.254' and the address pool '172.23.56.x' for assigning IP addresses to the network.

Multiple networks on one interface: With the configuration of IP and DHCP networks, multiple networks with different DHCP settings can be active at a logical interface. In this case, the DHCP settings for the first suitable network are applied. A prioritization of networks may be necessary here.



DHCP networks - New Entry

Network name: INTRANET

DHCP server enabled: Auto

☐ Evaluate broadcast bit

Addresses for DHCP clients

First address: 0.0.0.0

Last address: 0.0.0.0

Netmask: 0.0.0.0

Broadcast: 0.0.0.0

Default gateway: 0.0.0.0

Name server addresses

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

Primary NBNS: 0.0.0.0

Secondary NBNS: 0.0.0.0

Forwarding of DHCP queries

Server address: 0.0.0.0

☐ Place server replies in intermediate storage

☐ Adapt server replies to the local network

- **Selecting the IP network**

Select the IP network which the subsequent DHCP settings should apply to. You can find the parameters for defining DHCP networks in LANconfig in the configuration area "TCP/IP" on the "General" tab.

- **Enabling the DHCP server**

The DHCP server can be configured to run in the following modes:

- 'Yes': DHCP server is permanently switched on. When this value is entered the server configuration (validity of the address pool) is checked.
  - If the configuration is correct then the device starts operating as a DHCP server in the network.
  - Errors in the configuration (e.g. invalid pool limits) will cause the DHCP server to be disabled.

Only use this setting if you are certain that no other DHCP server is active in the LAN.

- 'No': DHCP server is permanently switched off.
- 'Auto': With this setting, the device regularly searches the local network for other DHCP servers. The LAN-Rx/Tx LED flashes briefly when this search is in progress.
  - If another DHCP server is discovered the device switches its own DHCP server off. If the LANCOM Router is not configured with an IP address, then it switches into DHCP client mode and queries the LAN DHCP server for an IP address. This prevents unconfigured devices introduced to the network from assigning addresses unintentionally.
  - If no other DHCP server is discovered the device switches its own DHCP server on. If another DHCP server is activated later, then the DHCP server in the LANCOM Router will be disabled.
- 'Client mode': The DHCP server is disabled, the device behaves as a DHCP client and obtains its address from another DHCP server in the LAN.

Only use this setting if you are certain that another DHCP server is in the LAN and actively assigning IP addresses.

- 'Queries forwarded': The DHCP server is active and receives requests from DHCP clients in the LAN. The device does not respond to requests itself, but forwards them to a central DHCP server in a different network segment.

The DHCP statistics show whether the DHCP server is enabled or not.

The default setting for this parameter is 'Auto'.

- **Assigning IP addresses**

The DHCP server must first know which IP addresses it can use to assign before it can actually assign them to workstations in the network There are three different methods for selecting possible addresses:

- An IP address can be taken from the defined address pool (First address: to Last address:). Any address can be entered provided it is valid for the IP network segment.
- If '0.0.0.0' is entered, the DHCP server determines the relevant first and last addresses itself using the settings for the IP network (network address and netmask).
- The device will be in a special operating mode if no IP network has yet been defined. It then uses the IP address '172.23.56.254' and the address pool '172.23.56.x' for assigning IP addresses to the network.

When a client is activated in the network and requests an IP address via DHCP, the device with an activated DHCP server will offer to assign an address. This address is selected from the pool of valid IP addresses. A computer which received an IP address in the past requests this address again and, assuming the DHCP server has not assigned this number to another computer in the meantime, it will attempt to issue this address again.

The DHCP server also checks the LAN to confirm that the selected address is free. Once the address is confirmed as unique, it is assigned to the requesting computer.

- **Assigning the netmask**

The netmask is assigned in a similar way to assigning addresses. If a netmask has been entered in the DHCP settings, it will be used when assignment is made. Otherwise the IP network's netmask will be used.

- **Assigning the broadcast address**

As a rule, broadcast packets in a local network have an address which results from the valid IP addresses and the netmask. In special cases (e.g. when using subnets for a selection of workstations) it may be necessary to use a different broadcast address. In this case the broadcast address to be used is entered in the DHCP settings.

We recommend that only experienced network specialists change the pre-setting for the broadcast address. Errors in the configuration here can lead to costly connections being established!

- **Assigning the standard gateway**

As standard, the LANCOM issues its own IP address as the gateway address to computers making requests. If necessary, the IP address of another gateway can be transmitted if a corresponding address is entered here.

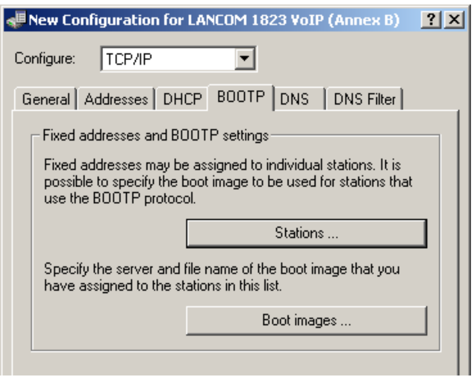
- **Assigning DNS and NBNS servers**

IP address of the DNS and NBNS name servers to which DNS and NBNS requests should be forwarded.

If no server is defined in the relevant fields, the router will forward its own IP network address as DNS or NBNS address if the DNS server has been enabled for the network in question. If the DNS server is not active for this network, then the IP address in the global TCP/IP settings is communicated as the DNS server.

Configuring the assignment of fixed IP addresses to specific clients

You can find the parameters for configuring BOOTP in LANconfig in the configuration area "TCP/IP" on the "BOOTP" tab.



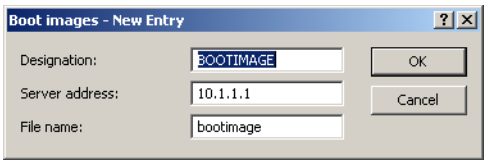
Configure: TCP/IP

Fixed addresses and BOOTP settings

Fixed addresses may be assigned to individual stations. It is possible to specify the boot image to be used for stations that use the BOOTP protocol.

Specify the server and file name of the boot image that you have assigned to the stations in this list.

Optionally: You can define a boot image in the list of boot images that you wish to assign to a client.

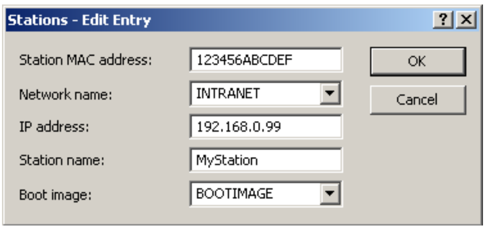


Designation: BOOTIMAGE

Server address: 10.1.1.1

File name: bootimage

Enter the MAC address of the client that you wish to assign a fixed IP address to in the list of stations. You may also select a boot image that is to be assigned to this client. If this address assignment is only to be used if the client is in a particular IP network, enter the appropriate IP network.



Stations - Edit Entry

Station MAC address: 123456ABCDEF

Network name: INTRANET

IP address: 192.168.0.99

Station name: MyStation

Boot image: BOOTIMAGE

16.1.3 Configuring DHCP parameters with telnet or WEBconfig

General DHCP settings

- **User class identifier**

  The DHCP client in the LANCOM can insert additional information in the DHCP request sent, which simplify request recognition within the network. The vendor class identifier (DHCP option 60) shows the device type, e.g. 'LANCOM L-54ag'. The vendor class ID is always transmitted. The user class ID (DHCP option 77) specifies a user-defined string. The user class ID is only transmitted when the user has configured a value.

- **Default lease minutes**

  When a client requests an address without asking for a specific lease, the address will be assigned the value set here as lease.

- **Max. lease minutes**

  When a client requests an IP address from a DHCP server, it can also ask for a lease for the address. This values governs the maximum length of lease that the client may request.

Alias list

The alias list defines the names for the boot images that are used to reference the images in the hosts table.

- **Image alias**

  Enter any name you wish for this boot image. This name is used when you assign a boot image to a particular client in the station list.

- **Image server**

  Enter the IP address of the server that provides the boot image.

- **Image file**

  Enter the name of the file on the server containing the boot image.

DHCP table

The DHCP table provides an overview of the IP addresses used in the IP networks. The DHCP table is purely a status table where no parameters can be configured.

- **IP address**

  IP address used by the client.

- **MAC address**

  The client's MAC address.

- **Timeout**

  Period of validity (lease) for the address assignment in minutes.

- **Client name**

  Name of the client, if it was possible to determine this.

- **Type**

  The 'Type' field indicates how the address was assigned. This field may contain the following values:

  - New: The client made the request for the first time. The DHCP checks that the address to be assigned to the client is unique.
  - Unknown: When the server checked if the address was unique, it was found that the address had already been assigned to another client. Unfortunately, the DHCP doe not have any possibility of obtaining further information about this client.
  - Stat: A client has informed the DHCP server that it has a fixed IP address. This address may not be used for any other clients in the network.
  - Dyn.: The DHCP server has assigned an address to the client.

- **LAN Ifc**

  Logical interface connecting the client to the device.
- **Ethernet port**

  Physical interface connecting the client to the device.
- **VLAN ID**

  The VLAN ID used by the client.
- **Network name**

  Name of the IP network where the client is located.

Hosts table

The bootstrap protocol (BOOTP) can be used to communicate a certain IP address and other parameters to a workstation when it boots up. For this, the workstation's MAC address is entered into the hosts table.

- **MAC address**

  Enter the MAC address of the workstation to which an IP address is to be assigned.

  Possible values:
- **Network name**

  Enter the name of a configured IP network here. Only if a requesting client is located in this IP network will it be assigned the relevant IP address defined for the MAC address.

> If the requesting client is located in an IP network for which there is no corresponding entry in the hosts table, the client will be assigned an IP address from the address pool of the appropriate IP network.

- **IP address**

  Enter the client IP address that is to be assigned to the client.
- **Client name**

  Enter the name that is to be used to identify the client. If the client does not communicate its name, the device will use the name entered here..
- **Image alias**

  If the client uses the BOOTP protocol, you can select a boot image that the client should use to load its operating system from.

> You must enter the server providing the boot image and the name of the file on the server in the boot image table.

Network list

DHCP settings for the IP networks are defined in this table.

- **Network name**

  The name of the network which the DHCP server settings apply to.
- **DHCP server enabled**

  DHCP server operating mode in this network. Depending on the operating mode, the DHCP server can enable or disable itself. You can see whether the DHCP server is enabled from the DHCP statistics.

  Possible values:

  - No: DHCP server is permanently switched off.
  - Automatic: With this setting, the device regularly searches the local network for other DHCP servers. The LAN-Rx/Tx LED flashes briefly when this search is in progress.

    If another DHCP server is discovered the device switches its own DHCP server off. If the LANCOM Router is not configured with an IP address, then it switches into DHCP client mode and queries the LAN DHCP server for an IP address. This prevents unconfigured devices introduced to the network from assigning addresses unintentionally.

    If no other DHCP server is discovered the device switches its own DHCP server on. If another DHCP server is activated later, then the DHCP server in the LANCOM Router will be disabled.

- 'Yes': DHCP server is permanently switched on. When this value is entered the server configuration (validity of the address pool) is checked.

  If the configuration is correct then the device starts operating as a DHCP server in the network.

  Errors in the configuration (e.g. invalid pool limits) will cause the DHCP server to be deactivated.
- 'Client mode': The DHCP server is disabled, the device behaves as a DHCP client and obtains its address from another DHCP server in the LAN.
- 'Relay requests': The DHCP server is active and receives requests from DHCP clients in the LAN. The device does not respond to requests, but forwards them to a central DHCP server elsewhere in the network (DHCP relay agent mode).

Default:

- Automatic

ⓘ Only use the setting "Yes" if you are certain that no other DHCP server is active in the LAN.

ⓘ Only use the "client mode" setting if you are certain that another DHCP server is in the LAN and actively assigning IP addresses.

- **Broadcast bit check**

  This setting decides whether the broadcast bit from clients is to be checked. If the bit is not checked then all DHCP messages are sent as broadcasts.
- **Start address**

  The first IP address in the pool available to the clients. If no address is entered here the DHCP takes the first available IP address from the network (as determined by network address and netmask).
- **End address**

  The last IP address in the pool available to the clients. If no address is entered here the DHCP takes the last available IP address from the network (as determined by network address and netmask).
- **Network mask**

  Corresponding netmask for the address pool available to the clients. If no address is entered here the DHCP server uses the netmask from the corresponding network.
- **Broadcast**

  As a rule, broadcast packets in a local network have an address which results from the valid IP addresses and the netmask. In special cases (e.g. when using subnets for a selection of workstations) it may be necessary to use a different broadcast address. In this case the broadcast address is entered into the DHCP module.

ⓘ We recommend that only experienced network specialists change the pre-setting for the broadcast address. Errors in the configuration here can lead to costly connections being established!

- **Standard gateway**

  As standard, the LANCOM issues its own IP address as the gateway address to computers making requests. If necessary, the IP address of another gateway can be transmitted if a corresponding address is entered here.
- **DNS default**

  IP address of the DNS name server for the forwarding of DNS requests.
- **DNS backup**

  IP address of the backup DNS name server for the forwarding of DNS requests, in the event that the first name server fails.
- **NBNS default**

  IP address of the NetBIOS name server for the forwarding of NetBIOS requests.
- **NBNS backup**

  IP address of the backup NBNS name server for the forwarding of NBNS requests, in the event that the first name server fails.
- **Server address**

  This is where the IP address for the superordinate DHCP server is entered when the mode 'Relay requests' is selected.

- **Caching of server responses**

  This option allows the responses from the superordinate DHCP server to be stored in the LANCOM Router. Subsequent requests can then be answered by the LANCOM Router itself. This option is useful if the superordinate DHCP server can only be reached via a connection which incurs costs.

- **Adapting server responses to the local network**

  This option allows the responses from the superordinate DHCP server to be adapted to the local network. When activated, the LANCOM adapts the responses from the superordinate DHCP server by replacing the following entries with its own address (or locally configured addresses):

  - Gateway
  - Network mask
  - Broadcast address
  - DNS server
  - NBNS server
  - Server ID

  This option is worthwhile if the superordinate DHCP server does not permit the separate configuration for DHCP clients in another network.

Port table

The port table is where the DHCP server is enabled for the appropriate logical interface of the device.

- Path: Setup/DHCP/Ports

- **Port**

  Select the logical interface for which the DHCP server should be enabled or disabled.

- **Enable DHCP**

  Enables or disables the DHCP server for the selected logical interface.

Additional options

DHCP options can be used to send additional configuration parameters to the clients. The vendor class ID (DHCP option 60) shows e. g. the type of device. This table allows additional options for DHCP operations to be defined.

- **Option number**

  Number of the option that should be sent to the DHCP client. The option number describes the transmitted information. For example "17" (root path) is the path to a boot image that a PC without its own hard disk uses to obtains its operating system via BOOTP. You can find a complete list of all DHCP options in RFC 2132 – "DHCP Options and BOOTP Vendor Extensions" of the Internet Engineering Task Force (IETF).

- **Network name**

  Name of the IP network where this DHCP option is to be used.

- **Option value**

  This field defines the contents of the DHCP option. For the option "17", for example, the path is entered for a boot image that a PC without its own hard disk uses to obtains its operating system via BOOTP.

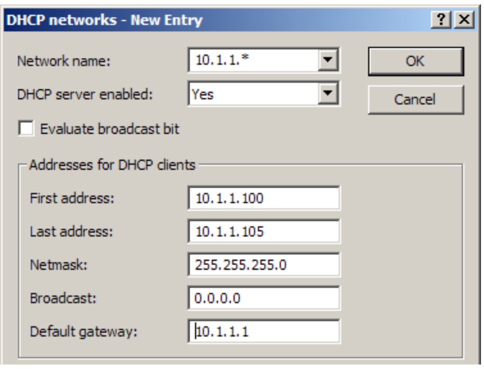
The maximum possible length value depends on the selected option number. RFC 2132 lists the maximum length allowed for each option.

16.1.4 DHCP relay server

A LANCOM is not limited to forwarding DHCP requests to superordinate DHCP servers; it can also function as a central DHCP server (DHCP relay server).

In order for a LANCOM to be provided as a DHCP relay server to other networks, the relay agent IP address (GI address) is entered as the network name in the table of IP networks.

If the same network is being used by several relay agents (e.g. multiple access points are forwarding requests to a central DHCP server) then the GI address can also be abbreviated with a "*". If for example clients in the remote network '10.1.1.0/255.255.255.0' are to be assigned with addresses and several relay agents are available in this network, all of which use the LANCOM as superordinate DHCP server, then the assignment of IP addresses and standard gateway to the clients can take place as follows:



DHCP networks - New Entry

Network name:	10.1.1.*
DHCP server enabled:	Yes

□ Evaluate broadcast bit

Addresses for DHCP clients

First address:	10.1.1.100
Last address:	10.1.1.105
Netmask:	255.255.255.0
Broadcast:	0.0.0.0
Default gateway:	10.1.1.1

To operate as DHCP relay server, it is imperative that the address pool and the netmask are given.

DNS resolution of names learned via DHCP

The DNS server considers the interface tags when resolving names learned via DHCP, i.e. the only names to be resolved are those which were learned from a network with the same interface tag as the requesting computer. If the request arrives from an untagged network, then all names are resolved, including those that were learned via tagged networks. Similarly, all names that were learned from untagged networks are visible for tagged networks.

Names learned from relay agents are handled as though they were learned from an untagged network, i.e. these names are visible to all networks.

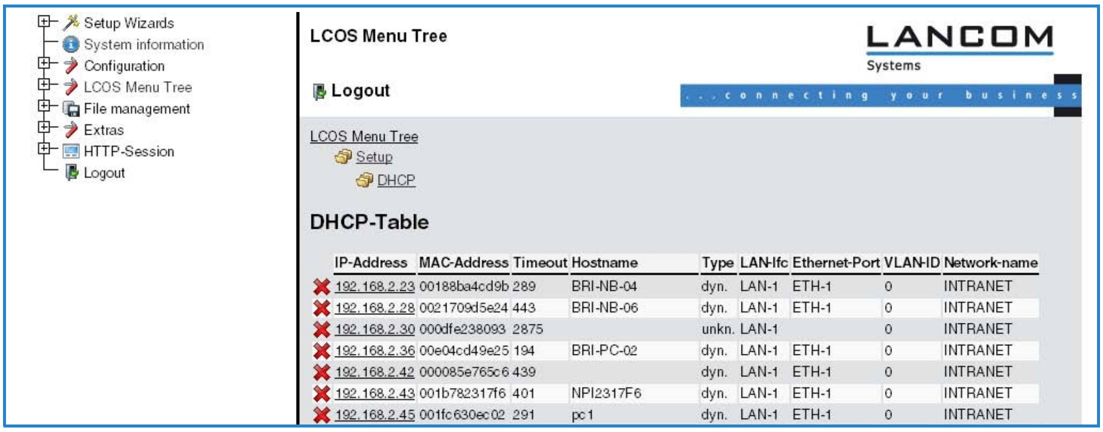
16.1.5 Configuring clients

It is standard in a Windows network environment for nearly all settings to be configured in such a way that required parameters can be requested via DHCP. You can check your Windows settings by clicking on **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Network**. Select the entry for **TCP/IP** on your network adapter and open **Properties**. You can now see on the various tabs whether there are special entries for e.g. the IP address or the standard gateway. If you wish to have all the values assigned by the DHCP server, just delete the corresponding entries.

If a client is to use a different parameter from the one assigned (e.g. for a standard gateway), this parameter must be configured at the workstation itself. The client will then ignore the corresponding parameter(s) in those assigned by the DHCP server.. Under Windows this can be effected for example via the properties of the network environment. Click on **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Network**. Select the entry for 'TCP/IP' on your network adapter and open **Properties**. You can now enter the desired values on the various tabs.

16.1.6 Checking IP addresses in the LAN

You can view a summary of the LAN IP addresses in the DHCP table (WEBconfig: Setup/DHCP/DHCP Table). It shows the assigned and used IP address, the MAC address, the lease, the client's name (if available) as well as the type of address assignment.



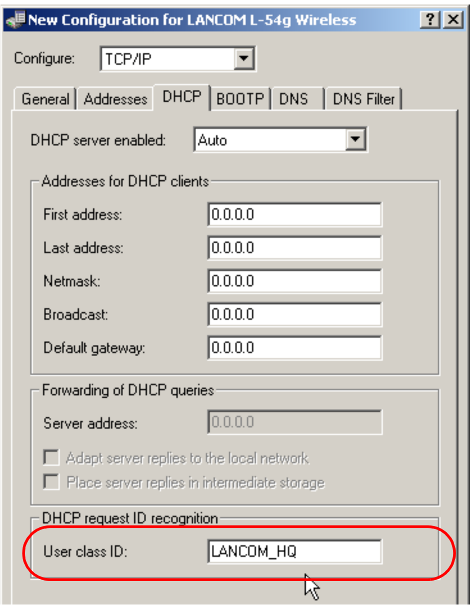
DHCP-Table

IP-Address	MAC-Address	Timeout	Hostname	Type	LAN-Ifc	Ethernet-Port	VLAN-ID	Network-name
192.168.2.23	00188ba4cd9b	289	BRI-NB-04	dyn.	LAN-1	ETH-1	0	INTRANET
192.168.2.28	0021709d5e24	443	BRI-NB-06	dyn.	LAN-1	ETH-1	0	INTRANET
192.168.2.30	000dfe238093	2875		unkn.	LAN-1		0	INTRANET
192.168.2.36	00e04cd49e25	194	BRI-PC-02	dyn.	LAN-1	ETH-1	0	INTRANET
192.168.2.42	000085e765c6	439		dyn.	LAN-1	ETH-1	0	INTRANET
192.168.2.43	001b782317f6	401	NPI2317F6	dyn.	LAN-1	ETH-1	0	INTRANET
192.168.2.45	001fc630ec02	291	pc1	dyn.	LAN-1	ETH-1	0	INTRANET

16.2 Vendor Class and User Class Identifier

The DHCP client in LANCOM can insert additional information in the DHCP request sent, which simplify request recognition within the network.

- The vendor class identifier (DHCP option 60) shows the device type, e.g. 'LANCOM L-54'. The vendor class ID is always transmitted.
- The user class identifier (DHCP option 77) displays a user-defined string, which can be entered under `Setup/DHCP` or in LANconfig in the configuration area under 'TCP/IP' on the 'DHCP' tab in the 'User Class ID' field (default: empty). The user class ID is only transmitted when the user has configured a value.


New Configuration for LANCOM L-54g Wireless

Configure: TCP/IP

DHCP server enabled: Auto

Addresses for DHCP clients

First address: 0.0.0.0
Last address: 0.0.0.0
Netmask: 0.0.0.0
Broadcast: 0.0.0.0
Default gateway: 0.0.0.0

Forwarding of DHCP queries

Server address: 0.0.0.0

□ Adapt server replies to the local network
□ Place server replies in intermediate storage

DHCP request ID recognition

User class ID: LANCOM_HQ

16.3 DNS

The domain name service (DNS) is responsible in TCP/IP networks for associating computer names and/or network (domains) and IP addresses. This service is required for Internet communications, to return the correct IP address for a request such as 'www.lancom.de' for example. However, it's also useful to be able to clearly associate IP addresses to computer names within a local network or in a LAN interconnection.

16.3.1 What does a DNS server do?

The names used in DNS server requests are made up of several parts: one part consists of the actual name of the host or service to be addressed; another part specifies the domain. Specifying the domain is optional within a local network. These names could thus be 'www.domain.com' or 'ftp.domain.com', for example.

If there is no DNS server in the local network, all locally unknown names will be searched for using the default route. By using a DNS server, it's possible to immediately go to the correct remote station for all of the names with known IP addresses. In principle, the DNS server can be a separate computer in the network. However, the following reasons speak for locating the DNS server directly in the LANCOM:

- LANCOM can automatically distribute IP addresses for the computers in the local network when in DHCP server mode. In other words, the DHCP server already knows the names and IP addresses of all of the computers in its own network that were assigned IP addresses via DHCP. With the dynamic address assignments of a DHCP server, an external DNS server might have difficulties in keeping the associations between the names and IP addresses current.
- When routing Microsoft Networks via NetBIOS, the LANCOM also knows the computer names and IP addresses in the other connected NetBIOS networks. In addition, computers with fixed IP addresses can also enter themselves in the NetBIOS table and thus be known by their names and addresses.
- The DNS server in the LANCOM can also be used as an extremely convenient filter mechanism. Requests for domains can be prohibited throughout the LAN, for subnetworks, or even for individual computers—simply by specifying the domain name.

How does the DNS server react to the request?

When processing requests for specific names, the DNS server takes advantage of all of the information available to it:

- First, the DNS server checks whether access to the name is not prohibited by the filter list. If that is the case, an error message is returned to the requesting computer stating that access to the address has been denied.
- Next, it searches in its own static DNS table for suitable entries.
- If the address cannot be found in the DNS table, it searches the dynamic DHCP table. The use of DHCP information can be disabled if required.

- If no information on the name can be located in the previous tables, the DNS server then searches the lists of the NetBIOS module. The use of the NetBIOS information can also be disabled if necessary.
- Finally, the DNS server checks whether the request to another DNS server is to be forwarded to another DNS server via a WAN interface (special DNS forwarding via the DNS destination table).

If the requested name cannot be found in any of the information sources available to it, the DNS server sends the request to another server—that of the Internet provider, for example—using the general DNS forwarding mechanism, or returns an error message to the requesting computer.

16.3.2 DNS forwarding

If it cannot serve the request from its own DNS tables, the DNS server forwards the request to other DNS servers. This process is called DNS forwarding.

Here a distinction is made between

- special DNS forwarding
  Requests for certain name areas are forwarded to certain DNS servers.
- general DNS forwarding
  All other names not specified in detail are forwarded to the "higher-level" DNS server.

Special DNS forwarding

With "special DNS forwarding" name areas can be defined for the resolution of which specified DNS server are addressed.

A typical application for special DNS forwarding results for a home workstation: The user wants to be able to connect to the company intranet and directly to the Internet at the same time. The requests sent into the intranet must be routed to the company DNS server, and all other requests to the DNS server of the provider.

General DNS forwarding

All DNS requests that cannot be resolved in another way are forwarded to a DNS server. This DNS server is determined according to the following rules:

- Initially the router checks whether a DNS server has been entered in its own settings. If it is successful there, it obtains the desired information from this server. Up to two higher-level DNS servers can be specified.

LANconfig: TCP/IP ▶ Addresses ▶ Primary DNS / Secondary DNS

WEBconfig: LCOS menu tree ▶ Setup ▶ TCP-IP ▶ DNS-default ▶ DNS-backup

- If no DNS server is entered in the router, it will attempt to reach a DNS server over a PPP connection (e.g. from the Internet provider) to get the IP address assigned to the name from there. This can only succeed if the address of a DNS server is sent to the router during PPP negotiation.
- The default route is established and the DNS server searched for there if no connection exists.

This procedure does not require you to have any knowledge of the DNS server address. Entering the Intranet address of your router as the DNS server for the workstation computers is sufficient to enable you obtain the name assignment. This procedure also automatically updates the address of the DNS server. Your local network always receives the most current information even if, for example, the provider sending the address changes the name of his DNS server or you change to another provider.

16.3.3 Setting up the DNS server

The settings for the DNS server are contained in the following menu or list:

LANconfig:TCP/IP ▶ DNS

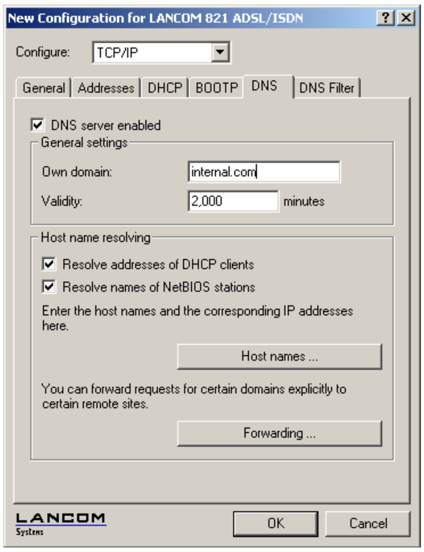
WEBconfig: LCOS menu tree ▶ Setup ▶ DNS

Proceed as follows to set the DNS server:

① Switch the DNS server 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.

③ Specify whether information from the DHCP server and the NetBIOS module should be used.



Configure: TCP/IP

☑ DNS server enabled

General settings

Own domain: internal.com

Validity: 2,000 minutes

Host name resolving

☑ Resolve addresses of DHCP clients

☑ Resolve names of NetBIOS stations

Enter the host names and the corresponding IP addresses here.

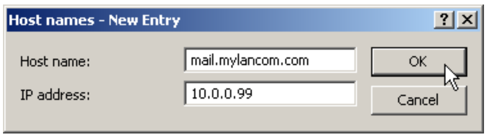
You can forward requests for certain domains explicitly to certain remote sites.

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.

For example, if would like to access the mail server at your headquarters (name: mail.yourdomain.com, IP: 10.0.0.99) via the router from a branch office, enter:



Host name: mail.mylancom.com

IP address: 10.0.0.99

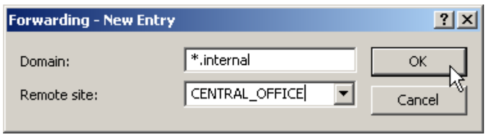
Stating the domain is optional but recommended.

When you now start your mail program, it will probably automatically look for the server 'mail.yourdomain.com'. The DNS server thereupon returns the IP address '10.0.0.99'. The mail program will then look for that IP address. With the proper entries in the IP routing table and peer list, a connection is automatically established to the network in the headquarters, and finally to the mail server.

⑤ To resolve entire name areas of another DNS server, add a forwarding entry consisting of a name area and remote station:

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:



Domain: *.internal

Remote site: CENTRAL_OFFICE

The DNS server may either be specified by the remote site name (for automatic setting via PPP), or by an explicit IP address of the according name server.

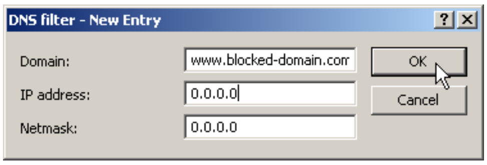
16.3.4 URL blocking

① Finally, one can restrict access to certain names or domains with the filter list.

To block the domain (in this case the web server) 'www.offlimits.com' for all computers in the LAN, the following commands and entries are required:

LANconfig: TCP/IP ▶ DNS Filter ▶ DNS filter... ▶ Add

WEBconfig: … ▶ Filter-list ▶ Add

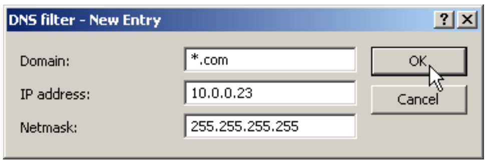

DNS filter - New Entry

Domain: www.blocked-domain.com
IP address: 0.0.0.0
Netmask: 0.0.0.0

The index '001' in the console command can be selected as desired and is used only for clarity.

When entering the domains, the wildcards '?' (represents exactly one character) and '*' (for any number of characters) are permitted.

To only block the access of a certain computer (e.g. with IP 10.0.0.123) to COM domains, enter the following values:


DNS filter - New Entry

Domain: *.com
IP address: 10.0.0.23
Netmask: 255.255.255.255

In the console mode the command is:

```
set 002 *.com 10.0.0.123 255.255.255.255
```

The hit list in the DNS statistics contains the 64 most frequently requested names and provides a good basis for setting up the filter list.

If your LAN uses subnetting, you can also apply filters to individual departments by carefully selecting the IP addresses and subnet masks. The IP address '0.0.0.0' stands for all computers in the network, and the subnet mask '0.0.0.0' for all networks.

16.3.5 Dynamic DNS

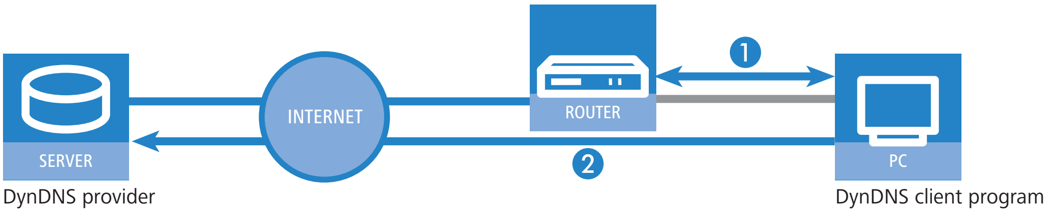
Systems with dynamic IP addresses become accessible over the WAN - for example over the Internet - via so-called Dynamic DNS service providers, e.g. www.dynDNS.org.

Thereby a LANCOM becomes available under a certain DNS-resolvable name (FQDN -’fully qualified Domain Name’, for example "http://MyLANCOM.dynDNS.org").

The advantage is obvious: If you want to accomplish e.g. remote maintenance for a remote site without ISDN available (e.g. over WEBconfig/HTTPS), or to connect with the LANCOM VPN Client to a branch office with dynamic IP address, then you just need to know the appropriate Dynamic DNS name.

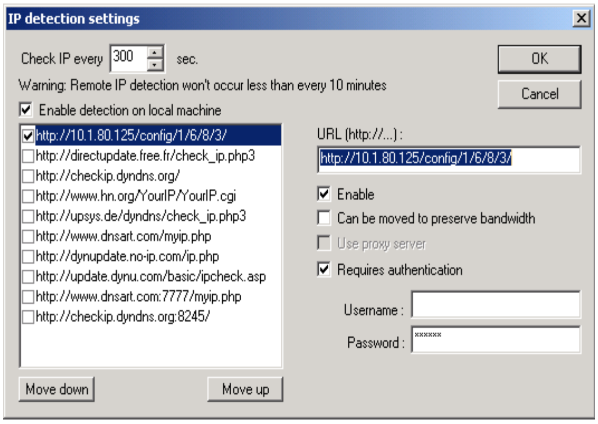
How to deposit the current IP address at the Dynamic DNS server?

All Dynamic DNS provider support a set of client programs, which can determine the current assigned WAN IP address of a LANCOM via different methods ①, and transfer this address - in case of a change - to their respective Dynamic DNS server ②.



The current WAN IP address of a LANCOM can be picked under the following address:

```
http://<address of LANCOM>/config/1/6/8/3/
```



IP detection settings

Check IP every 300 sec.

Warning: Remote IP detection won't occur less than every 10 minutes

☑ Enable detection on local machine

- ☑ http://10.1.80.125/config/1/6/8/3/
- □ http://directupdate.free.fr/check_ip.php3
- □ http://checkip.dyndns.org/
- □ http://www.hn.org/YourIP/YourIP.cgi
- □ http://upsys.de/dyndns/check_ip.php3
- □ http://www.dnsart.com/myip.php
- □ http://dynupdate.no-ip.com/ip.php
- □ http://update.dynu.com/basic/ipcheck.asp
- □ http://www.dnsart.com:7777/myip.php
- □ http://checkip.dyndns.org:8245/

URL (http://...) : http://10.1.80.125/config/1/6/8/3/

☑ Enable

□ Can be moved to preserve bandwidth

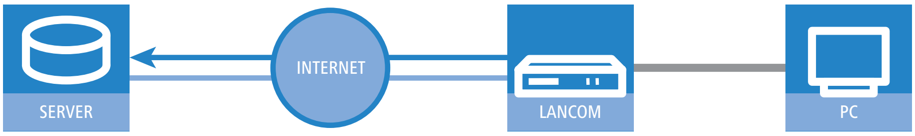
□ Use proxy server

☑ Requires authentication

Username :

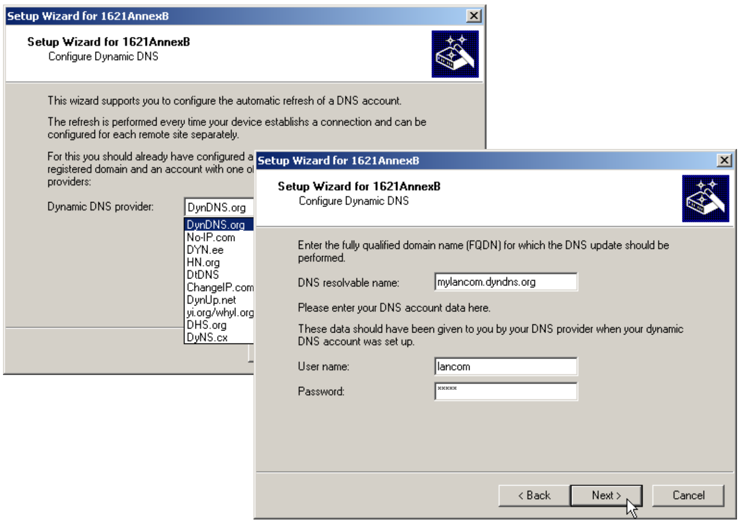
Password : ******

Alternatively the LANCOM can directly transmit the present WAN IP to the DynDNS provider.



DynDNS provider

The required settings can be changed comfortably with the Setup Wizard:



Setup Wizard for 1621AnnexB

Setup Wizard for 1621AnnexB
Configure Dynamic DNS

This wizard supports you to configure the automatic refresh of a DNS account.

The refresh is performed every time your device establishs a connection and can be configured for each remote site separately.

For this you should already have configured a registered domain and an account with one o providers:

Dynamic DNS provider: DynDNS.org

- DynDNS.org
- No-IP.com
- DYN.ee
- HN.org
- DtDNS
- ChangeIP.com
- DynUp.net
- yi.org/whyl.org
- DHS.org
- DyNS.cx

Setup Wizard for 1621AnnexB

Setup Wizard for 1621AnnexB
Configure Dynamic DNS

Enter the fully qualified domain name (FQDN) for which the DNS update should be performed.

DNS resolvable name: mylancom.dyndns.org

Please enter your DNS account data here.

These data should have been given to you by your DNS provider when your dynamic DNS account was set up.

User name: lancom

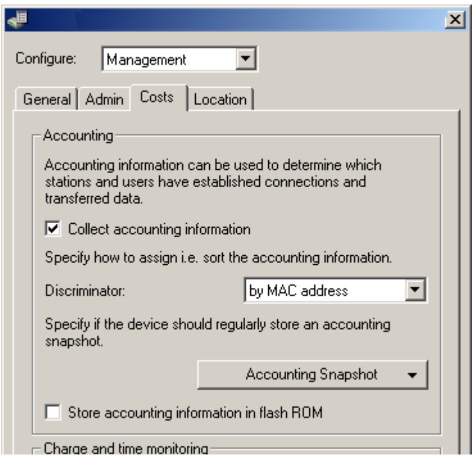
Password: *****

16.4 Accounting

Information on connections between clients in the local network and various remote stations is saved in the accounting table with entries for the connection time and the transferred data volume. Using accounting snapshots, accounting data can be regularly saved at specific times for later evaluation.

Configuring accounting

When configuring accounting, the general parameters must be defined:



Configure: Management

General | Admin | Costs | Location

Accounting

Accounting information can be used to determine which stations and users have established connections and transferred data.

☑ Collect accounting information

Specify how to assign i.e. sort the accounting information.

Discriminator: by MAC address

Specify if the device should regularly store an accounting snapshot.

Accounting Snapshot

☐ Store accounting information in flash ROM

Charge and time monitoring

LANconfig: Management ▶ Costs

WEBconfig: LCOS menu tree ▶ Setup ▶ Accounting

- **Collect accounting information**
  - Turn accounting on or off.
- **Store accounting information in flash ROM**
  - Turn accounting data in flash memory on or off. Accounting data saved to flash will not be lost in the event of a power outage.
- **Discriminator**

  Selection of the feature according to which the accounting data are to be gathered:
  - MAC address: The data are collected according to the client's MAC address.
  - IP address: The data are collected according to the client's IP address.

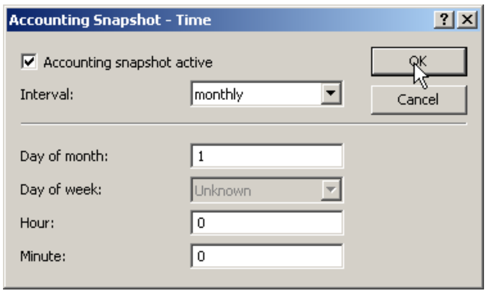
When varying IP addresses are in use, e.g. when using a DHCP server, the option 'IP address' can lead to inaccurate accounting data. In this case, it may not be possible to accurately assign the data to users. Conversely, with this setting, data can be separated from clients that are behind another router and therefore appear with the same MAC address as the router in the accounting list.

- **Sort according to**

  Select here whether the data should be sorted in the accounting table according to connection times or data volume.

Snapshot configuration

When configuring the snapshot, the interval is set in which the accounting data are temporarily saved into a snapshot:



Accounting Snapshot - Time

☑ Accounting snapshot active

Interval: monthly

Day of month: 1

Day of week: Unknown

Hour: 0

Minute: 0

LANconfig: Management ▶ Costs ▶ Accounting Snapshot

WEBconfig: LCOS menu tree ▶ Setup ▶ Accounting ▶ Time snapshot

The snapshot function can only be used when the device is set with the correct system time.

- **Accounting snapshot active**
  - Turn intermediate storage of accounting data on or off.
- **Interval**
  - Daily, weekly or monthly
- **Day of month**

  The day of the month on which caching will take place: Only relevant if the interval is 'monthly'.

- **Day of week**
  The weekday on which caching will take place. Only relevant if the interval is 'weekly'.
- **Hour**
  The hour on which caching will take place:
  - □ '0' to '23'
- **Minute**
  The minute in which caching will take place:
  - □ '0' to '59'

16.5 Call charge management

The capability of the router to automatically establish connections to all desired remote sites and to close them again when no longer required provides users with extremely convenient access, e.g. to the Internet. However, quite substantial costs may be incurred by data transfer over paid lines if the router is not configured properly (e.g. in the filter configuration) or by excessive use of the communications opportunities (e.g. extended surfing in the Internet).

To reduce these costs, the software provides various options:

- The available online minutes can be restricted to a specific period.
- For ISDN connections, a limit on time or charges can be set for a particular period.

16.5.1 Connection limits for DSL and cable modem

Even though a DSL or cable modem connection behaves like a leased line, which is always online, depending on the provider connection charges can be accounted by the time.

In this section all connections over a ethernet WAN port of the LANCOM, e. g. cable modem connection, will be referred as DSL connection.

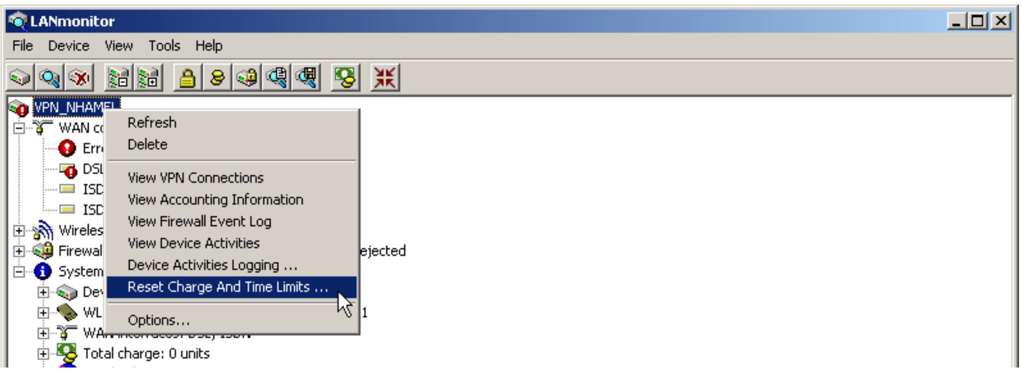
To limit the costs, the maximal connection duration can be controlled with time, by arranging a time limit for DSL connections for a period of time. By default the DSL connections can only be used for a maximum of 600 minutes in six days.

If the limit is reached, all DSL connections are automatically terminated. As soon as the current period has passed the time count is reset and the connection enabled. The administrator can of course reset the time count and enable the connection beforehand.

If the connection has a charge limit and a short hold of '0' or '9999' seconds, the charge control is switched off and the connection is kept even if the limit is exceeded.

If in an exceptional case you would like to extend the online budget, e.g. to download a large file from the internet, you do not necessarily have to change the time limit. In this case you can manually reset the limit.

Click with the right mouse button on the error in LANmonitor and select in the menu the entry 'Reset Charge And Time Limit'



If you cannot see the system information in LANmonitor, activate the view with **View** ▶ **Show Details** ▶ **System Information**.

In WEBconfig and in the console the commands to activate the additional time limit are as follows:

WEBconfig: LCOS menu tree ▶ Setup ▶ Charges ▶ Activate-additional-budget

The additional time limit is activated for the current period, in the following period normal time limit is set.

16.5.2 Charge-based ISDN connection limits

If charge information is sent to an ISDN connection, the resulting connection charges can be limited quite easily. For example, in its default state, a maximum of 830 charge units may be used in six days. The router will not permit the establishment of any further connections once this limit has been reached.

ⓘ The best way to use the router's call charge monitoring function is if you have "call charge information enabled **during** the connection" to the ISDN network (i.e. AOCD). If necessary, subscribe to this facility from your telecommunications carrier. Charge monitoring with the "Charge information **after** connection" feature is also possible in principle, but in this case continuous connections may not be detected!

If you have enabled least-cost routing on the router modules, connections may be established to providers who do not transmit any charge information!

16.5.3 Time dependent ISDN connection limit

However, this mechanism of ISDN connection monitoring will not work if the ISDN connection does not provide charge information. That may be the case, for example, if the provision of charge information was not requested for the connection, or if the telecommunications provider generally does not supply this information.

To reduce the costs of ISDN connections even if no call charge information is available, maximum connection lengths based on time can be regulated. This requires setting up a time budget for a specified period. In the router's default state, for example, connections may only be established for a maximum of 210 minutes within six days.

When the limit of a budget is reached, all open connections that were initiated by the router itself will be shut down automatically.The budgets will not be reset to permit the establishment of connections until the current period has elapsed. Needless to say, the administrator can reset the budgets at any time if required!

The charge and time monitoring of the router functions can be disabled by entering a budget of 0 units or 0 minutes.

! Only the router functions are protected by the charge and time monitoring functions! Connections via LANCAPI are not affected.

16.5.4 Settings in the charge module

LANconfig: Management ▶ Costs

WEBconfig: LCOS menu tree ▶ Setup ▶ Charges

In the charges module, the online time can be monitored and used to control call establishment.

- Day(s)/Period

  The duration of the monitoring period in days can be specified here.

- Budget units, Online minutes budget

  The maximum number of ISDN units or online minutes in a monitoring period

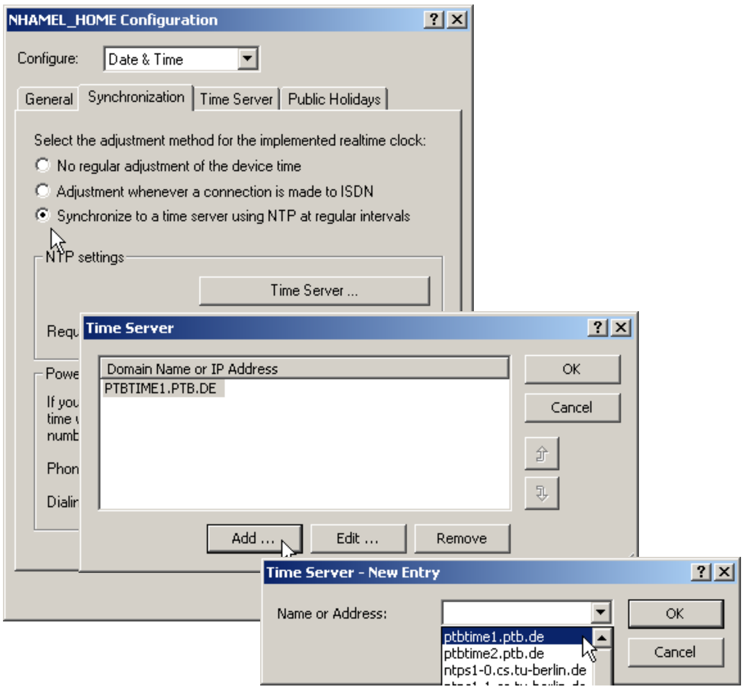
ⓘ The current charge and connect-time information is retained when rebooting (e.g. when installing new firmware) is not lost until the unit is switched off. All the time references here are in minutes.

16.6 Time server for the local net

LANCOM routers can apply exact information of time either over ISDN or over public time servers on the internet (NTP-Server with 'Open Access' policy). The LANCOM can then provide the detected time for all stations in the local network.

16.6.1 Configuration of the time server under LANconfig

To provide the current time in the local network your LANCOM has to regularly apply the time from a time server. For this so called real time clock click in the configuration area 'Date & time' on the tab 'Synchronization'. Under 'NTP settings' open the list of time servers by clicking on the button **Time Server ...**. With the button **Add...** you can extend the list.



NHAMEL_HOME Configuration

Configure: Date & Time

Select the adjustment method for the implemented realtime clock:

○ No regular adjustment of the device time

○ Adjustment whenever a connection is made to ISDN

● Synchronize to a time server using NTP at regular intervals

NTP settings

Time Server

Domain Name or IP Address

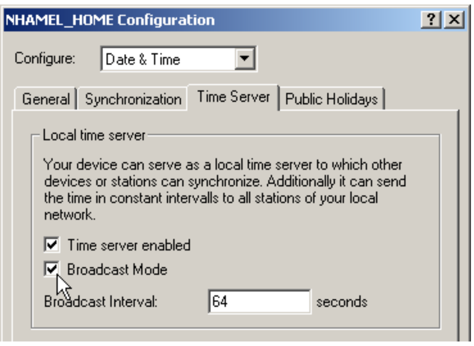
PTBTIME1.PTB.DE

Time Server - New Entry

Name or Address:

ptbtime1.ptb.de
ptbtime2.ptb.de
ntps1-0.cs.tu-berlin.de

With these settings only the LANCOM applies the time from public time servers. To provide the real time for the remaining device enable the local time server under the tab 'Time Server'. Furthermore activate the broadcast mode and enter the broadcast interval.



NHAMEL_HOME Configuration

Configure: Date & Time

Local time server

Your device can serve as a local time server to which other devices or stations can synchronize. Additionally it can send the time in constant intervalls to all stations of your local network.

☑ Time server enabled

☑ Broadcast Mode

Broadcast Interval: 64 seconds

16.6.2 Configuration of the time server with WEBconfig or Telnet

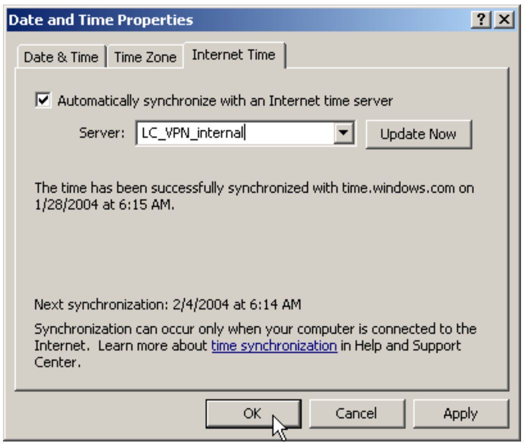
When configuring with WEBconfig or Telnet you can find the required parameters in the following areas:

WEBconfig: LCOS menu tree ▶ Setup ▶ NTP

16.6.3 Configuring the NTP clients

The NTP clients must be configured so that they use the time information from the LANCOM. Not all operating systems provide an integrated NTP client: Windows XP does so, for other Windows operating systems a separate NTP client is required, Linux distributions have to be installed with NTP.

The settings of date and time in a XP system can be opened with a double click on the time at the bottom left, where you can select the server for synchronization.


Date and Time Properties

☑ Automatically synchronize with an Internet time server

Server: LC_VPN_internal

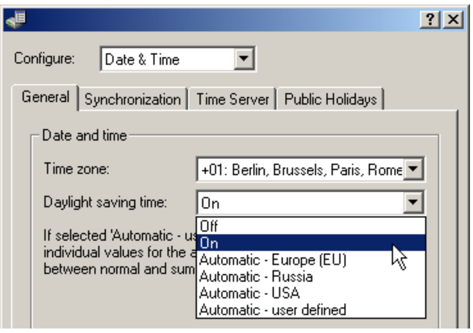
The time has been successfully synchronized with time.windows.com on 1/28/2004 at 6:15 AM.

Next synchronization: 2/4/2004 at 6:14 AM

Synchronization can occur only when your computer is connected to the Internet. Learn more about time synchronization in Help and Support Center.

■ Configuring daylight-saving time change according to UTC

LANCOM devices work internally with the coordinated world time (UTC). For protocol displays and time-related settings (e.g. cron jobs), the local time is taken as calculated from the defined time zone. To take local daylight-saving time into account, settings can be configured according to requirements.


Configure: Date & Time

Date and time

Time zone: +01: Berlin, Brussels, Paris, Rome

Daylight saving time: On

If selected 'Automatic - us individual values for the c between normal and sum

LANconfig: Date & time ▶ General

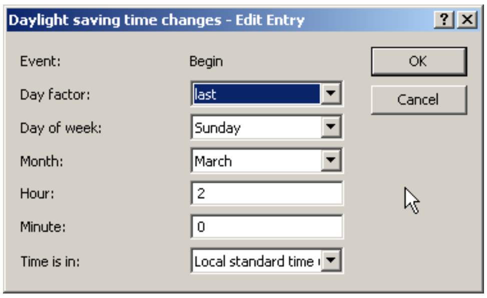
WEBconfig: LCOS menu tree ▶ Setup ▶ Time ▶ Daylight-saving time

■ Daylight-saving time

- □ Off: The system time will not be adjusted to daylight-saving time.
- □ On: As long as this option is enabled, one hour is added statically to the current system time (comprised of UTC and time zone).
- □ Automatic (EU, USA, Russia): In this setting, the daylight-saving time change is performed automatically in conformance with the time zone of the device's location.
- □ Automatic (user-defined): If the device is located in an area that is not listed here, then the daylight-saving time change options can be manually defined by the user.

User-defined daylight-saving time change

User-defined values can be set for the beginning and the end of the automatic daylight-saving time change.


Daylight saving time changes - Edit Entry

Event: Begin

Day factor: last

Day of week: Sunday

Month: March

Hour: 2

Minute: 0

Time is in: Local standard time

LANconfig:Date & time ▶ General ▶ Daylight-saving time

WEBconfig: LCOS menu tree ▶ Setup ▶ Time ▶ DST clock changes

■ Index

- □ First, second, third, fourth, last, second to last, third to last, fourth to last: The time change will take place on this recurring day of the month.

- **Day of week**
  - Monday to Sunday: The day on which the change will take place.
- **Month**
  - January to December: The month on which the change will take place.
- **Hour**
  - 0 to 23: The hour in which the change will take place.
- **Minute**
  - 0 to 59: The minute in which the change will take place.
- **Time type**
  - Local standard time or UTC: Defines the time zone the data refers to.

! In the last hour of daylight-saving time or the first hour that follows in standard time, it is possible for time entries to be ambiguous. If the time is acquired via ISDN or set manually during this time, then it is always assumed that the time entry is in daylight-saving time.

16.7 Scheduled Events

16.7.1 Regular Execution of Commands

This feature is intended to allow the device to execute predefined commands in a telnet-like environment, at times defined by the user. The functionality is equivalent to the UNIX cron service. Subject of execution can be any LANCOM command line command. Therefore, the full feature set of all LANCOM devices can be controlled by this facility.

Application examples:

- scheduled connection

  Many leased lines disconnect automatically after 24 hours of continuous operation. This enforced disconnection can have some unwanted side-effects for example if it happens to an unsuitable time during the day, because e.g. the VPN tunnel is disconnected and the IP address of the LANCOM is changed. To control the disconnecting time a manual disconnection can be set e.g. at midnight, so it can not happen at an unsuitable time.

  As a second example devices with a distributed network with only dynamic IP addresses can build up a connection at a certain time to a VPN gateway, so that data can be transferred safely. This way a protected access is even possible without an ISDN connection.

- time-dependant firewall or QoS rules

  The firewall and QoS rules are at first temporally constant. But it can be useful to make variable settings for different daytimes or weekdays. At e. g. off-hours or weekends different priorities for guaranteed bandwidths can be set than at business hours.

- regular firmware or configuration updates

  Time-controlled rules do not only provide the settings of particular values, it is even possible to switch to a whole different configuration. This possibility allows you to pool a whole string of settings and change them all at once with one command. Therefore changing the configuration of the device with completely different values at the weekend and switching back on monday mornings can be done with just one command.

  Additionally the regular update of the newest firmware from one single source is adjustable.

- Email messages

  With the time-controlled rules you have the option that the LANCOM informs the administrator by email not only about specific firewall events, but even to set times. The email can e.g. inform about building up an internet connection successfully after an enforced disconnection or after booting the device because of a restart.

- time-dependant interfaces

  The time dependant use of interfaces for a set duration is also provided by the time-controlled rules. Therewith e.g. a WLAN interface can permit the wireless access to the network only at certain times.

- Deleting certain tables

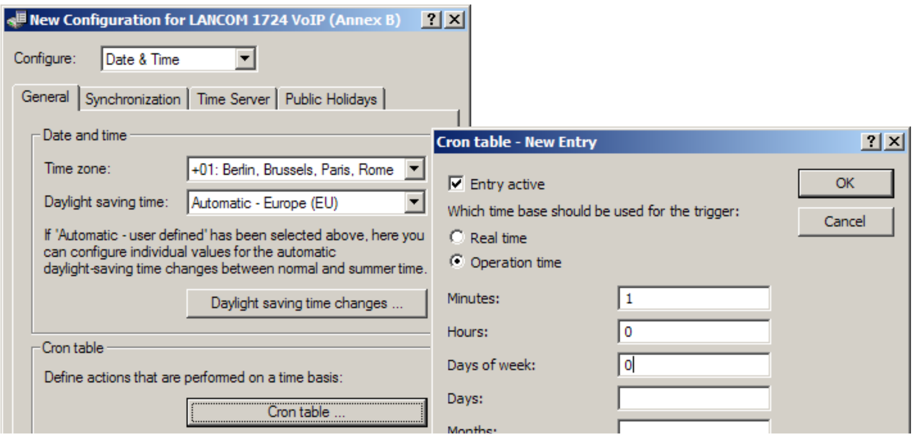
  It can be useful to delete the content of some tables in LCOS regularly. If your internet access for example has a monthly limited transfer volume, you can delete your accounting table monthly to have a survey of the present transferred data volume.

16.7.2 CRON jobs with time delay

CRON jobs are used to carry out recurring tasks on a LANCOM automatically at certain times. If the installation features a large number of active devices, all of which are subjected to the same CRON job at the same time (e.g. updating a configuration by script), unpleasant side effects can result if, for example, all devices try to establish a VPN connection at once. To avoid these effects, the CRON jobs can be set with a random delay time between 0 and 59 minutes.

16.7.3 Configuring the CRON job

The following parameters are available in the LANCOM for configuring CRON jobs:



New Configuration for LANCOM 1724 VoIP (Annex B)

Configure: Date & Time

General | Synchronization | Time Server | Public Holidays

Date and time

Time zone: +01: Berlin, Brussels, Paris, Rome

Daylight saving time: Automatic - Europe (EU)

If 'Automatic - user defined' has been selected above, here you can configure individual values for the automatic daylight-saving time changes between normal and summer time.

Daylight saving time changes ...

Cron table

Define actions that are performed on a time basis:

Cron table ...

Cron table - New Entry

☑ Entry active

Which time base should be used for the trigger:

○ Real time

● Operation time

Minutes: 1

Hours: 0

Days of week: 0

Days:

Months:

OK

Cancel

LANconfig: Date & time ▶ General ▶ CRON table

WEBconfig: LCOS menu tree ▶ Setup ▶ Config ▶ CRON table

- **Entry active**

  Activates or deactivates the entry.

  - Default: Active

- **Time base**

  The 'Time base' field determines whether time control is based on real time or on the device's operating time.

  - Real time: These rules evaluate all time/date information.
  - Operation time: These rules only evaluate the minutes and hours since the last time the device was started.
  - Default: Real time

- **Minutes**
- **Hours**
- **Week days**
- **Month days**
- **Months**

  The values 'minutes' to 'months' define the times when a command is to be executed. With no value entered, it is not included in the controlling.
  For each parameter, a comma-separated list of values can be entered, or alternatively a range of minimum and maximum values.

  The syntax of the 'Week day' field corresponds with the usual CRON interpretation:

  - 0: Sunday
  - 1: Monday
  - 2: Tuesday
  - 3: Wednesday
  - 4: Thursday
  - 5: Friday
  - 6: Saturday

- **Command**

  The command to be executed or a comma-separated list of commands. **Any** LANCOM command-line function can be executed.

- **Owner**

  An administrator defined in the device can be designated as owner of the CRON job. If an owner is defined, then the CRON job commands will be executed with the rights of the owner.

  - Default: root

- **Variation**

  This parameter specifies the maximum delay in minutes for the start of the CRON job after the set start time. The actual delay time is determined randomly and lies between 0 and the time entered here.

  - Default: 0
  - Values: 0 to 65535 seconds.
  - Particular values: With the variation set to zero the CRON job will be executed at the set time.

Real-time based rules can only be executed if the device has a time from a relevant source, e.g. via NTP.

Examples:

time base	min.	hours	w.-days	m.-days	months	command
real time	0	4	0-6	1-31	1-12	do /oth/man/disconnect internet
real time	59	3	0-6	1-31	1-12	mailto:admin@mylancom.de?subject=disconnection?body=Manual disconnection of the internet connection
real time	0	0		1		do /setup/accounting/delete
real time	0	18	1,2,3,4,5			do /oth/man/connect HEADQUARTER

- The first entry cuts the connection to the internet provider every morning at 4 am (forced disconnection).
- The second entry sends an information mail every morning at 3:59 am (directly before the forced disconnection) to the admin.
- The third entry deletes on the first of every month the accounting table.
- The fourth entry builds up a connection to the headquarter every week day at 6 pm.

Time based rules are performed with an exactness of one minute.
Please keep in mind, that the language of the used commands should be the same as the language of the console, otherwise the commands of the time automatic can not be considered. The default language is english, but can be changed.

16.8 PPPoE Servers

16.8.1 Introduction

In accordance with the widespread availability of DSL, PPPoE clients have now been widely integrated into all operating systems. These can be used to "log on to the network" as well as to manage access rights to services such as the Internet, e-mail or remote stations.

PPPoE can only be used on a network segment.

As it is what is known as a "Layer 2" technology, PPPoE can only be used within a network segment, i.e. it cannot be used across IP subnets. The PPPoE connection cannot be established across network segment limits, such as via a router.

After a user logs on to the LAN (e.g. username: 'Purchasing', password: 'secret') using a specified PPPoE logon, further rights can be regulated via the firewall. This enters the PPPoE user name as a 'remote station' in the firewall. With a deny all rule, and a PPPoE rule in the following format, user Anyone can be permitted to use the Internet with Web and FTP:

- Source: Anyone
- Target: All stations
- Services: WWW, FTP

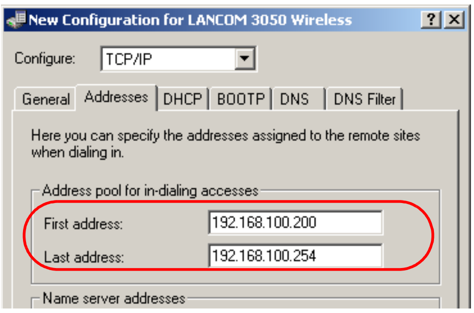
16.8.2 Example application

All employees in the 'Purchasing' department must first authenticate themselves to the LANCOM using PPoE (IP routing, PAP check) in order to access the Internet.

Constraint: The LANCOM can be accessed directly by the users in the LAN as a router, firewall and gateway, i.e. there are no other routers in between them.

The computers in Purchasing are assigned with an IP address from a certain address range (e.g. 192.168.100.200 to 192.168.100.254) from the list of addresses for dial-in connections (LANconfig ▶ TCP/IP ▶ Addresses).

The LANCOM itself is in a different IP address range!



New Configuration for LANCOM 3050 Wireless

Configure: TCP/IP

Here you can specify the addresses assigned to the remote sites when dialing in.

Address pool for in-dialing accesses

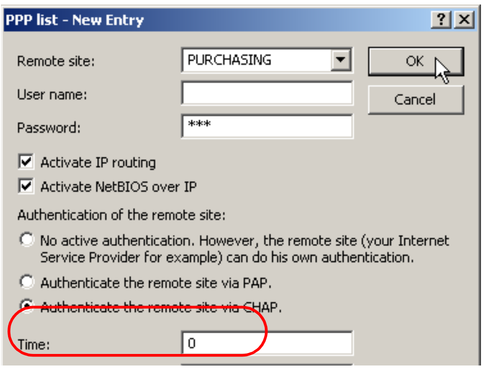
First address: 192.168.100.200

Last address: 192.168.100.254

Name server addresses

To prevent users from bypassing the authentication, a DENY ALL rule is defined in the firewall to stop local connections from being established.

The user 'Purchasing' is then entered into the PPP list (LANconfig ▶ Communication ▶ Protocols) without a user name but with a password which is to be used by all staff members in the department, and authentication (encrypted) is set up as CHAP. Both IP routing and NetBIOS (Windows Networking) are to be activated for this PPP user:



PPP list - New Entry

Remote site: PURCHASING

User name:

Password: ***

☑ Activate IP routing

☑ Activate NetBIOS over IP

Authentication of the remote site:

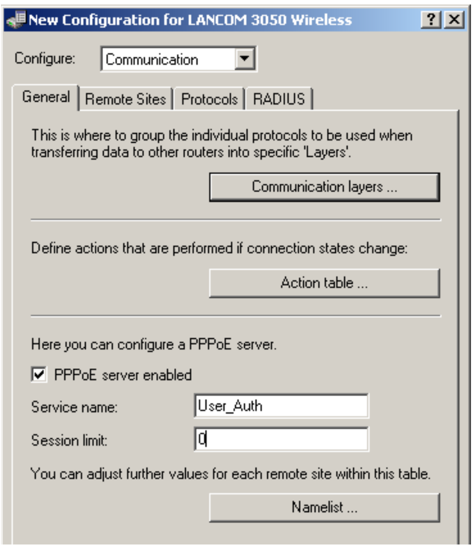
○ No active authentication. However, the remote site (your Internet Service Provider for example) can do his own authentication.

○ Authenticate the remote site via PAP.

● Authenticate the remote site via CHAP.

Time: 0

Along with the activation of the PPPoE server (LANconfig ▶ Communication ▶ General), further limitations (e.g. permissible MAC addresses) can also be defined in the PPPoE server. The example uses the existing entry 'DEFAULT' with the MAC address '00.00.00.00.00.00', thereby permitting all MAC addresses.



New Configuration for LANCOM 3050 Wireless

Configure: Communication

This is where to group the individual protocols to be used when transferring data to other routers into specific 'Layers'.

Define actions that are performed if connection states change:

Here you can configure a PPPoE server.

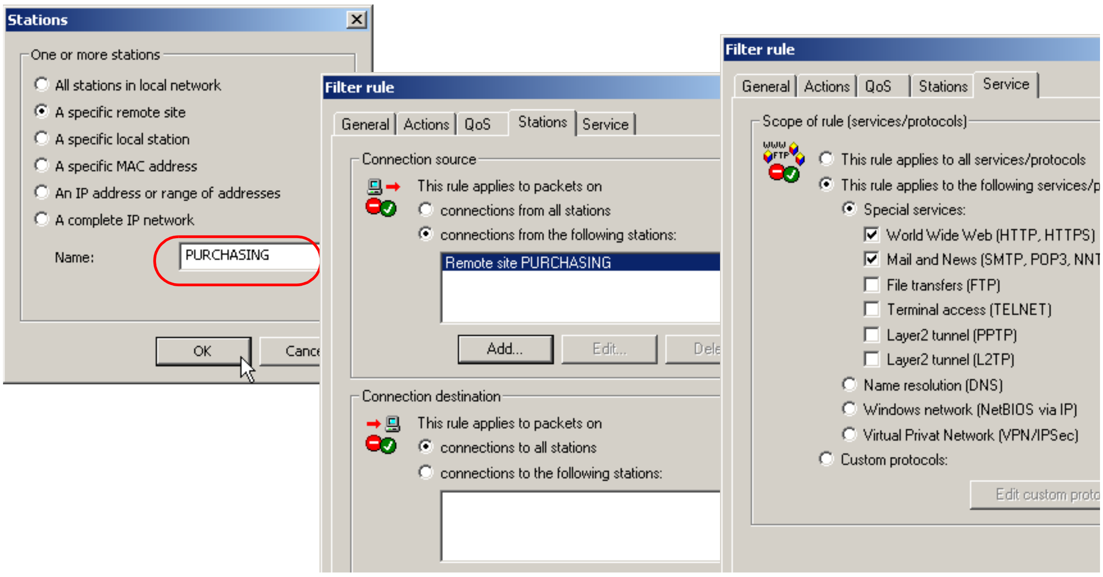
☑ PPPoE server enabled

Service name: User_Auth

Session limit: 0

You can adjust further values for each remote site within this table.

The firewall (LANconfig ▶ Firewall/QoS ▶ Rules) can be used to control which services are available to the employees in Purchasing (e.g. release of HTTP and EMAIL only).



Stations

One or more stations

○ All stations in local network
● A specific remote site
○ A specific local station
○ A specific MAC address
○ An IP address or range of addresses
○ A complete IP network

Name: PURCHASING

OK | Cance

Filter rule

General | Actions | QoS | Stations | Service

Connection source

This rule applies to packets on
○ connections from all stations
● connections from the following stations:

Remote site PURCHASING

Add... | Edit... | Dele

Connection destination

This rule applies to packets on
● connections to all stations
○ connections to the following stations:

Filter rule

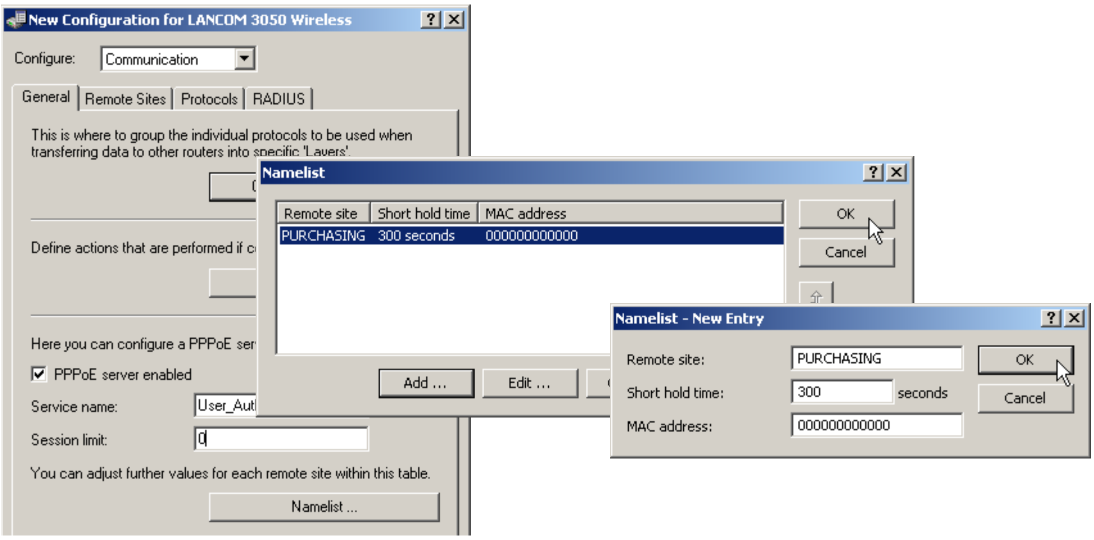
General | Actions | QoS | Stations | Service

Scope of rule (services/protocols)

○ This rule applies to all services/protocols
● This rule applies to the following services/p
● Special services:
☑ World Wide Web (HTTP, HTTPS)
☑ Mail and News (SMTP, POP3, NNT
☐ File transfers (FTP)
☐ Terminal access (TELNET)
☐ Layer2 tunnel (PPTP)
☐ Layer2 tunnel (L2TP)
○ Name resolution (DNS)
○ Windows network (NetBIOS via IP)
○ Virtual Privat Network (VPN/IPSec)
○ Custom protocols:

Edit custom proto

16.8.3 Configuration



New Configuration for LANCOM 3050 Wireless

Configure: Communication

General | Remote Sites | Protocols | RADIUS

This is where to group the individual protocols to be used when transferring data to other routers into specific 'Layers'.

Define actions that are performed if c

Here you can configure a PPPoE ser

☑ PPPoE server enabled

Service name: User_Aut

Session limit: 0

You can adjust further values for each remote site within this table.

Namelist ...

Namelist

Remote site	Short hold time	MAC address
PURCHASING	300 seconds	000000000000

OK | Cancel | Add ... | Edit ...

Namelist - New Entry

Remote site: PURCHASING

Short hold time: 300 seconds

MAC address: 000000000000

OK | Cancel

LANconfig: Communication ▶ General

WEBconfig: LCOS menu tree ▶ Setup ▶ PPPoE server

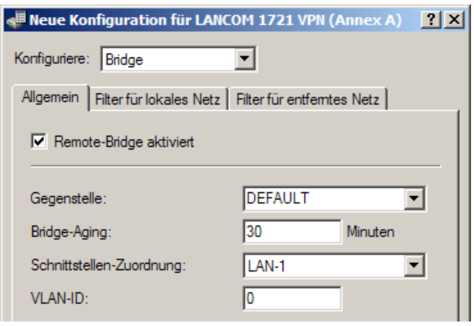
- **Operating**: The 'Operating' button switches the server on or off. The default value is 'Off'.
- **Service**: The name of the service offered is entered under 'Service'. This enables a PPPoE client to select a certain PPPoE server that is entered for the client.
- **Session limit**: The 'Session limit' specifies how often a client can be logged on simultaneously with the same MAC address. Once the limit has been reached, the server no longer responds to the client queries that are received. Default value is '1', maximum value '99'. A Session limit of '0' stands for an unlimited number of sessions.
- **Name list**: Different parameters (such as shorthold time and MAC address) can be assigned to users in the name list:

A MAC address of '000000000000' means that the user may log on with any MAC address. If a MAC address is entered, then the PPP negotiation is terminated if the user logs on from a different MAC address. The user's shorthold time is set after the logon. If no entry exists, then the time belonging to user 'DEFAULT' is used.

In addition to this table, an entry has to be made in the PPP table in which the password, the rights (IP, IPX,NetBIOS) and other PPP parameters (LCP polling) are entered. The user can therefore also be authenticated using a RADIUS server.

16.9 Remote bridge

The remote bridge links two remotely networks, as they would be linked physical. The two networks are completely independently from the used network protocols.



Neue Konfiguration für LANCOM 1721 VPN (Annex A)

Konfiguriere: Bridge

Allgemein | Filter für lokales Netz | Filter für entferntes Netz

☑ Remote-Bridge aktiviert

Gegenstelle: DEFAULT

Bridge-Aging: 30 Minuten

Schnittstellen-Zuordnung: LAN-1

VLAN-ID: 0

LANconfig: Bridge ▶ General

WEBconfig: LCOS menu tree ▶ Setup ▶ Bridge

- **Remote station**

  Name of the remote station, which is linked with the remote bridg.

- **Bridge-Aging**

  Duration after a once learned MAC address will be deleted.

- **Interface allocation**

  Logical interface, which the remote bridge is assigned to.

For the interface allocation are no WLANs possible, because the WAN bridge exists only in devices without WLAN. Therefore the interface allocation “any” is not possible.

- **VLAN-ID**

  ID of the VLAN, on which the remote bridge is active.

16.10 RADIUS

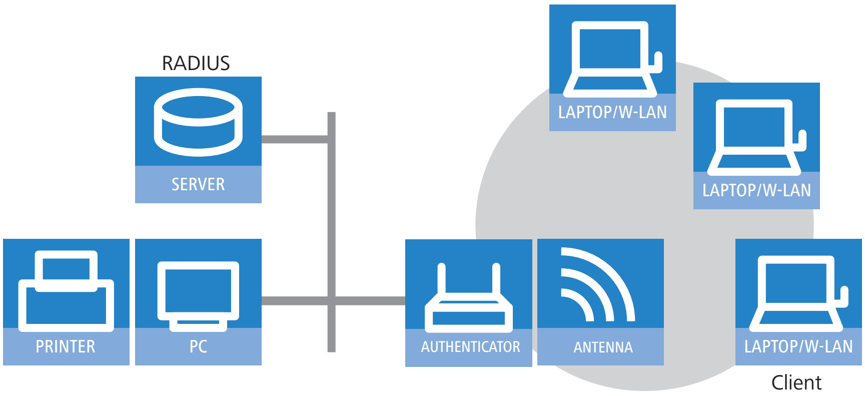
RADIUS stands for "Remote Authentication Dial-In User Service“ and is referred to as a "triple-A" protocol. The three "A"s stand for

- Authentication
- Authorization
- Accounting (billing)

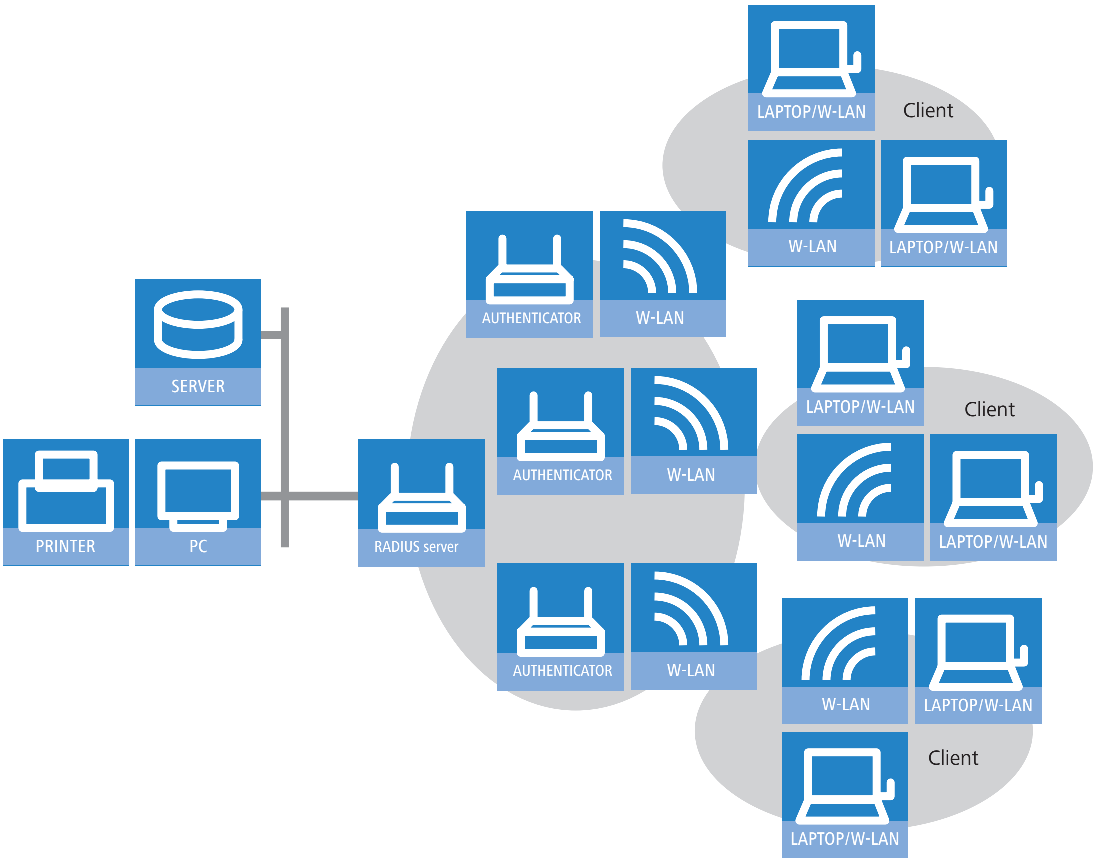
This protocol allow you to grant users access to a network, to assign them certain rights and to track their actions. Where necessary, the RADIUS server can also be used in the billing of user services such as WLAN hot spots. For every action performed by the user, the RADIUS server can run an authorization procedure releasing or blocking access to network resources on a per user basis.

3 different devices are required for RADIUS to work.

- Client: This is a device (PC, notebook etc.) from which the user wishes to dial in to the network.
- Authenticator: A network component positioned between network and client and which forwards on the authorization. This task can be performed by an LANCOM Access Point for example. The authenticator is referred to as the Network Access Server (NAS).



- Authentication server: RADIUS server on which user data is configured. This is usually located within the same network for which it issues access authorizations. It is accessible to the client via the authenticator. Some scenarios may also allow the use of a LANCOM access point for this task.



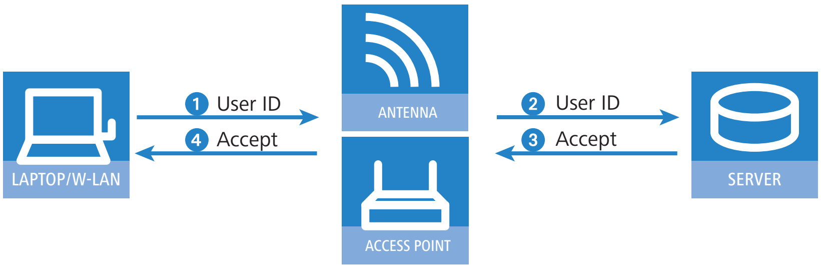
The authenticator has no initial information on the clients wanting to register. This is all stored in a database on the RADIUS server. The registration information the RADIUS server needs for the authentication process is stored in the database there and can vary from network to network. The authenticator has just the one task, that of transferring the information between the client and the RADIUS server.

Access to a RADIUS server can be configured in several ways:

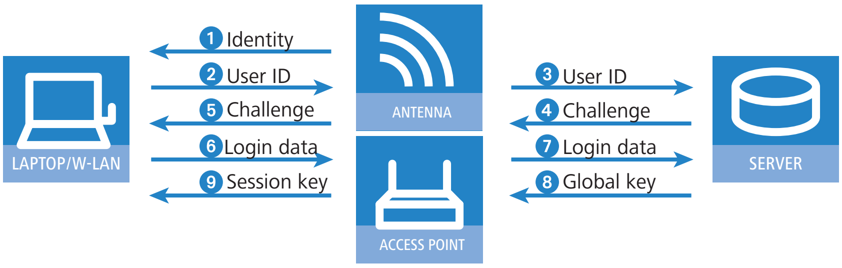
- Using PPP when dialing into a network (see 'Dial-in using PPP and RADIUS' → page 16-28)
- Via WLAN (see 'Dial-in using WLAN and RADIUS' → page 16-29)
- Via a public spot for users who register using a browser (see 'Dial-in using a public spot and RADIUS' → page 16-30
- Via the 802.1x protocol (see 'Dial-in using 802.1x and RADIUS' → page 16-31)

16.10.1 How RADIUS works

The authentication process of a client using the authenticator on a RADIUS server can vary in complexity and is implementation dependent. In a simplified application, the client sends its registration data to the RADIUS server via the authenticator and receives back either an "Accept" or a "Reject".



In more complicated applications, the RADIUS server can request additional registration data using what is known as a "Challenge". The handshake sequence looks something like this:

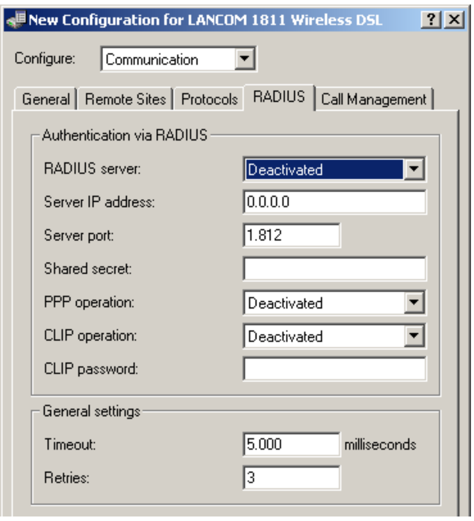


16.10.2 Configuration of RADIUS as authenticator or NAS

The RADIUS protocol is supported by LANCOM devices in a range of different applications. For each of these cases there is a specific set of parameters which may be configured independently of other applications. There are also general parameters which need to be configured for each of these applications. Not all devices support all applications.

General settings

General settings apply to all RADIUS applications. Default values have been selected such that they need not usually be changed.


New Configuration for LANCOM 1811 Wireless DSL

Configure: Communication

Authentication via RADIUS

RADIUS server: Deactivated

Server IP address: 0.0.0.0

Server port: 1.812

Shared secret:

PPP operation: Deactivated

CLIP operation: Deactivated

CLIP password:

General settings

Timeout: 5.000 milliseconds

Retries: 3

LANconfig: Communication ▶ RADIUS

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS module

- **Timeout [default: 5.000]**

  This value specifies how many milliseconds should elapse before retrying RADIUS authentication.

With PPP authentication using RADIUS, please note that the device dialing accepts the RADIUS timeout configured here.

- **Retries [default: 3]**

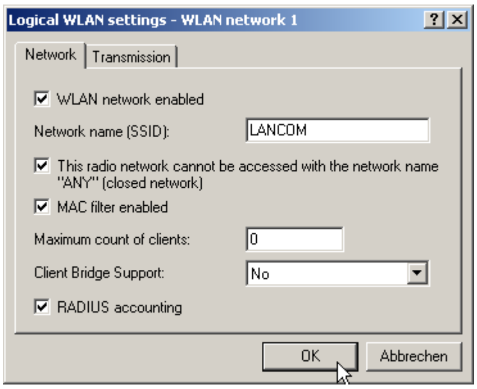
  This value specifies how many authentication attempts are made in total before a Reject is issued.

RADIUS accounting

Accounting for a logical WLAN network can be enabled from a RADIUS server by enabling the "RADIUS Accounting" option in the logical WLAN settings for the network.

LANconfig: Interfaces ▶ Wireless LAN ▶ Logical WLAN settings

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS module



☑ WLAN network enabled

Network name (SSID): LANCOM

☑ This radio network cannot be accessed with the network name "ANY" (closed network)

☑ MAC filter enabled

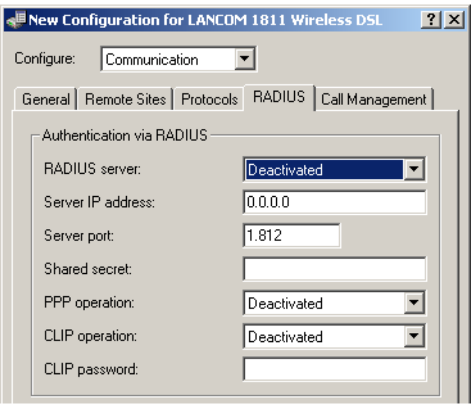
Maximum count of clients: 0

Client Bridge Support: No

☑ RADIUS accounting

Dial-in using PPP and RADIUS

When dialing-in using the PPP protocol (Point-to-Point protocol), RADIUS can be used to check client access authorizations. A client can dial-in to the network from anywhere. The resulting data transmission between client and authenticator is encrypted.


New Configuration for LANCOM 1811 Wireless DSL
General
Remote Sites
Protocols
RADIUS
Call Management
Authentication via RADIUS

Configure: Communication

RADIUS server: Deactivated

Server IP address: 0.0.0.0

Server port: 1.812

Shared secret:

PPP operation: Deactivated

CLIP operation: Deactivated

CLIP password:

LANconfig: Communication ▶ RADIUS

WEBconfig: LCOS menu tree ▶ Setup ▶ WAN ▶ RADIUS

- **Radius server [default: disabled]**

  When authenticating using RADIUS, the user administration and authentication tasks are passed on to a RADIUS server.

  - Disabled: The functionality of RADIUS is disabled and no requests are forwarded to the RADIUS server.
  - Enabled: The functionality of RADIUS is enabled and requests may be forwarded to the configured RADIUS server. Depending on the setting, other sources may be used for the authentication process (e.g. PPP list).
  - Exclusive: RADIUS functionality is enabled and the authentication process is run exclusively by RADIUS.

  The appropriate RADIUS server must be configured to use the functionality of RADIUS. All user data, such as user name and password, is entered on the RADIUS server.

- **Server IP address**

  Specify here the IP address of your RADIUS server from which users are managed centrally.

- **Server port [default: 1.812]**

  Specify here the port used for communication to your RADIUS server.

- **Key (shared secret)**

  Specify here the key to be used for coding data. The key must also be configured on the RADIUS server.

- **PPP mode [default: disabled]**

  A RADIUS server may be used for the authentication process when dialing-in using PPP.

  - Disabled: PPP clients are not authenticated using RADIUS. They are checked **exclusively** using the PPP list.
  - Enabled: RADIUS authentication for PPP clients is enabled. User data supplied by clients is **first** checked using the PPP list. If no matching entry is found in the PPP list, the client is checked by the RADIUS server. Authentication is successful if the PPP list check**or** RADIUS server check returns as positive.

- □ Exclusive: RADIUS authentication for PPP clients is enabled. User data supplied by clients is checked **exclusively** by the RADIUS server. In this mode, it is just the advanced settings of the PPP list for the user which are interpreted (e.g. check for PAP/CHAP – or the allowed protocols IP, IPX and/or NetBIOS).

- **CLIP mode [default: disabled]**

  A RADIUS server may be used for control of a return call when dialing-in using PPP.

  - □ Disabled: The return call function is not controlled by RADIUS. **Only** those entries in the name list are used.
  - □ Enabled: The RADIUS function for the return call is enabled. Telephone numbers reported by clients are **first** checked using the name list. If no matching entry is found in the name list, the telephone number is checked by the RADIUS server. If the name list check **or** RADIUS server check returns as positive, a return call can be established.

> If the telephone number communicated is in the name list, but no return call is active there, RADIUS ceases checking.

  - □ Exclusive: The RADIUS function for the return call is enabled. User data reported by clients is checked **exclusively** by the RADIUS server.

  In order to use the return call control from RADIUS, a user must be set up on the RADIUS server for each telephone number to be authenticated. The user name corresponds to the telephone number and the user password is the CLIP password specified here.

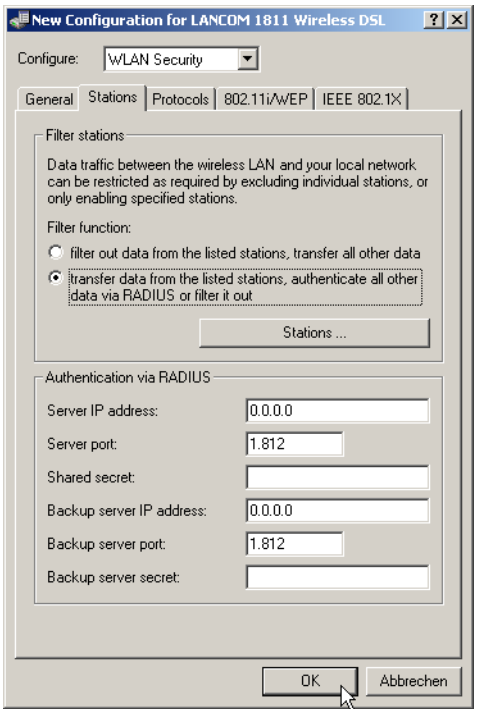
- **CLIP password**

  Password for return call control.

> The generic values for retry and timeout must also be configured (see 'Configuration of RADIUS as authenticator or NAS' → page 16-27). They are under PPP on the same page as PPP parameters.

Dial-in using WLAN and RADIUS

When using a RADIUS server for the authentication of WLAN clients, the RADIUS server uses the MAC address to check client authorizations.



New Configuration for LANCOM 1811 Wireless DSL

Configure: WLAN Security

General | Stations | Protocols | 802.11i/WEP | IEEE 802.1X

Filter stations

Data traffic between the wireless LAN and your local network can be restricted as required by excluding individual stations, or only enabling specified stations.

Filter function:

○ filter out data from the listed stations, transfer all other data

● transfer data from the listed stations, authenticate all other data via RADIUS or filter it out

Stations ...

Authentication via RADIUS

Server IP address: 0.0.0.0

Server port: 1.812

Shared secret:

Backup server IP address: 0.0.0.0

Backup server port: 1.812

Backup server secret:

OK | Abbrechen

LANconfig: WLAN Security ▶ Stations

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN ▶ RADIUS access check

> To use the RADIUS functionality for WLAN clients, the option "Transfer data from the listed stations, authenticate all others via RADIUS or filter them out" must be selected for the "Filter stations" parameter.

- **Server IP address**

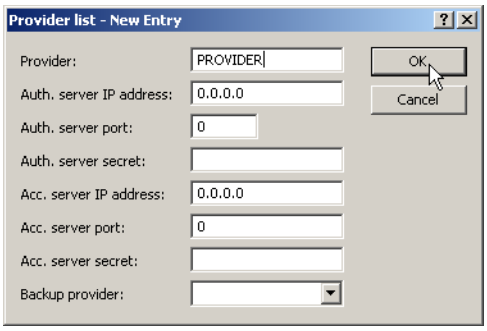
  Specify here the IP address of your RADIUS server from which users are managed centrally.

- **Server port [default: 1.812]**
  Specify here the port used for communication to your RADIUS server.
- **Key (shared secret)**
  Specify here the key to be used for coding data. The key must also be configured on the RADIUS server.
- **Backup server IP address [default: 1.812]**
  Specify here the IP address of your backup RADIUS server from which users are managed centrally.
- **Backup server port**
  Specify here the port used for communication to your backup RADIUS server.
- **Backup key**
  Specify here the key to be used for coding data. The key must also be configured on the backup RADIUS server.

The generic values for retry and timeout must also be configured (see 'Configuration of RADIUS as authenticator or NAS' → page 16-27).

Dial-in using a public spot and RADIUS

When configuring a public spot (enable using software option for the LANCOM access points), user registration data can be forwarded to one or more RADIUS servers. These are configured in the provider list. The registration data individual RADIUS servers require from the clients is not important to the LANCOM access point since this data is passed on transparently to the RADIUS server.


Provider list - New Entry

Provider: PROVIDER
Auth. server IP address: 0.0.0.0
Auth. server port: 0
Auth. server secret:
Acc. server IP address: 0.0.0.0
Acc. server port: 0
Acc. server secret:
Backup provider:

LANconfig: Public Spot ▶ Public Spot Users▶ Provider list

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN ▶ RADIUS accounting

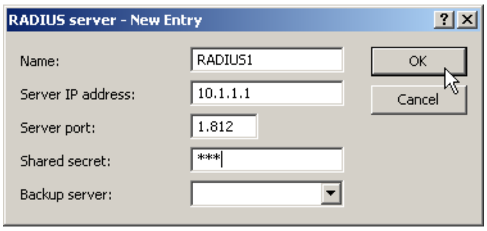
- **Provider**
  Name of the provider for whom the RADIUS server is defined.
- **Auth. server IP address**
  The IP address of the RADIUS server for this provider.
- **Auth. server port**
  The port over which the LANCOM access point can communicate with the RADIUS server for this provider.
- **Auth. server secret**
  Key (shared secret) for access to the RADIUS server of the provider. The key must also be configured on the appropriate RADIUS server.
- **Acc. Server IP address**
  IP address of the Accounting server for accesses to the public spot.
- **Acc. server port**
  The port over which the LANCOM access point can communicate with the accounting server.
- **Acc server secret**
  Key (shared secret) for access to the Accounting server. The key must also be configured on the Accounting server.
- **Backup provider**
  The name of a different provider can be selected as the backup from the current table. Using these types of entries, backup chains linking several RADIUS servers can be easily configured.

The generic values for retry and timeout must also be configured (see 'Configuration of RADIUS as authenticator or NAS' → page 16-27).

Dial-in using 802.1x and RADIUS

WLAN clients can use the 802.1x protocol for network registration. The LANCOM access point can use this protocol to forward the registration to the RADIUS server. The MAC address is used for user identification.

Please refer to 'IEEE 802.1x/EAP' → page 11-41 for further information on the 802.1 x protocol.



RADIUS server - New Entry

Name: RADIUS1

Server IP address: 10.1.1.1

Server port: 1.812

Shared secret: ***

Backup server:

LANconfig: WLAN Security ▶ IEEE 802.1X ▶ RADIUS server

WEBconfig: LCOS menu tree ▶ Setup ▶ IEEE802.1x ▶ Radius server

- **Name**

  In this table, each RADIUS server needs a unique name. The name 'DEFAULT' is reserved for all WLAN networks that use an authentication process in line with IEEE 802.1x and that have not specified their own RADIUS server.

  By using the name defined in the 'Key 1/passphrase' field, each WLAN network using authentication in line with IEEE 802.1x can be assigned its own RADIUS server.

- **Server IP address**

  Specify here the IP address of your RADIUS server from which users are managed centrally.

- **Server port**

  Specify here the port used for communication to your RADIUS server.

- **Key (shared secret)**

  Specify here the key to be used for coding data. The key must also be configured on the RADIUS server.

- **Backup server**

  Name of the backup server from the list of RADIUS servers configured so far.

The generic values for retry and timeout must also be configured (see 'Configuration of RADIUS as authenticator or NAS' → page 16-27).

WLAN clients must be entered as follows on the RADIUS server:

The user name is the MAC address in the format AABBCC-DDEEFF. The password for all users is identical to the key (shared secret) for the RADIUS server.

16.10.3 Configuring RADIUS as server

In addition to its function as RADIUS authenticator or NAS, an LANCOM access point can also operate as a RADIUS server. When in this mode, information in the device on users authorized to register is made available to other access points in Authenticator mode.

RADIUS server parameters

When configuring the RADIUS server, a definition is needed of which authenticator can access the RADIUS server, the password required for this access, and the open port that is to be used to communicate with the RADIUS server. The authentication port applies globally for all authenticators.

LANconfig: WLAN security ▶ RADIUS

WEBconfig: LCOS menu tree ▶ Setup ▶ Radius ▶ Server

- **Authentication port [default: 0]**

  Specify here the port used by the authenticators to communicate with the RADIUS server in the LANCOM access point. Port '1812' is normally used.

  Port '0' disables the RADIUS server.

In addition to the port, 16 authenticators that are allowed to communicate with the RADIUS server may be entered here. Entries are made in the corresponding table and with the following parameters:

- **IP address**

  IP address of the authenticator which may communicate with the RADIUS server in the LANCOM access point.
- **Secret**

  Password required by the authenticator for access to the RADIUS server in the LANCOM access point.

In addition to the configuration of the RADIUS server, the client information source must also be defined 'WLAN access list as a basis for RADIUS information' → page 16-32.

WLAN access list as a basis for RADIUS information

512 WLAN clients, all able to register with the LANCOM access point, may be entered in the access list. When operating in RADIUS server mode, this list can also be used to check on RADIUS clients wanting to register at other access points. In an installation having several access points, client access authorizations can be maintained centrally.

LANconfig: WLAN security ▶ RADIUS

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN ▶ RADIUS access check

- **Provide server database [default: yes]**

  This parameter specifies whether the WLAN access list is to be used as an information source for the RADIUS server in the LANCOM access point.

  The WLAN access list contains the user name in the form of the MAC address and the password ('WPA passphrase'). In addition to this access data, the access list provides information such as bandwidth restriction and association to a specific VLAN.
- **Recheck cycle [default: 0]**

  Once a WLAN client is logged on after authentication by RADIUS, it remains active until it logs off itself or is logged off by the RADIUS server. By specifying a recheck cycle [minutes], the RADIUS server can regularly check whether the WLAN clients logged in are still in the access list. If a WLAN client is removed from the access list, it remains logged in to the WLAN up to the point when the recheck cycle runs again.

A recheck cycle of '0' disables regular checking. WLAN clients remain logged in until they log themselves out.

16.11 Extensions to the RADIUS server

16.11.1 New authentication method

Up to version 6.30 the LCOS RADIUS server supported PAP as an authentication method only, i.e. the RADIUS client (henceforth referred to as the NAS, Network Access Server) passed on the user name and password and the server responded with an access accept or access reject. This is just one of a range of authentication methods which can be processed by RADIUS. With LCOS version the RADIUS server in the LANCOM supports additional methods of authentication:

- PAP: The NAS passes the user name and password. The RADIUS server searches its data sets for an entry matching the user name, compares the password, and responds with a RADIUS accept or RADIUS reject.
- CHAP: The NAS passes the user name, the CHAP challenge and characteristics of the password (but not the password itself). The RADIUS server searches its data sets for an entry matching the user name; it uses the associated password and the CHAP challenge from the NAS to compute the CHAP response. If this computed response and the answer sent by the client via the NAS correspond, then the RADIUS server sends a RADIUS accept; otherwise it sends a RADIUS reject.
- MS-CHAP: The NAS passes the user name, the MS-CHAP challenge and the MS-CHAP password characteristics. The method continues in the same way as CHAP, although the responses are computed with the MS-CHAP algorithm (RFC 2433).
- MS-CHAPv2: The NAS passes the user name, the MS-CHAP challenge and the MS-CHAPv2 response. The method continues in the same way as CHAP and MS-CHAP, although the responses are computed with the MS-CHAPv2 algorithm (RFC 2759). Furthermore the RADIUS server transmits an MS-CHAPv2 confirmation once the authentication was successful. This confirmation contains the server's response to the client's challenge, so enabling a mutual authentication.
- EAP: The NAS passes the user name and an EAP message. Unlike the methods outlined above, EAP is not stateless, i.e. in addition to sending an access accept or access reject, the RADIUS server issues its own challenge before authentication is completed. EAP itself is a modular authentication protocol that accommodates various methods of authentication.

16.11.2 EAP authentication

EAP is not a specific authentication mechanism, it is more like a framework for various authentication methods. The LCOS RADIUS server supports a range of EAP methods:

- EAP/MD5, defined in RFC 2284. EAP/MD5 is a simple challenge/response protocol. It does not cater for mutual authentication nor does it offer a dynamic key such as those required for 802.1x authentication in wireless networks (WLANs). Thus it is only used for the authentication of non-wireless clients or as a tunneled method as a part of TTLS.
- EAP/MSCHAPv2, defined in draft-kamath-pppext-eap-mschapv2-01.txt. As opposed to EAD/MD5, EAP/MSCHAPv2 does supports mutual authentication but does not support dynamic keys, making it just as prone to dictionary attacks as EAP/MD5. This method is usually used within PEAP tunnels.
- EAP/TLS, defined in RFC2716. The use of EAP/TLS requires the use of a root certificate, a device certificate and a private key in the device. EAP/TLS provides outstanding security and the dynamic keys necessary for wireless connections; its implementation is complex, however, because each individual client requires a certificate and a private key.

Please note that the TLS implementation in LCOS does not support certificate chains or certificate revocation lists (CRLs).

- EAP/TTLS, defined in draft-ietf-pppext-eap-ttls-05.txt. TTLS is based on TLS; it does not make use of client certificates and it utilizes the existing TLS tunnel to authenticate the client. The LCOS RADIUS server supports the following TTLS methods:
  - PAP
  - CHAP
  - MSCHAP
  - MSCHAPv2
  - EAP, preferably EAP/MD5
- EAP/PEAPv0, defined in draft-kamath-pppext-peapv0-00.txt. Similar to TTLS, PEAP is based on TLS and works with an EAP negotiation inside the TLS tunnel.

Please note that although PEAP enables the use of any authentication method, the LCOS RADIUS server only supports MSCHAPv2 for tunneling.

At this time, authentication methods cannot be suppressed. The EAP supplicant and the RADIUS server negotiate the EAP method with the standard EAP mechanism. Clients requesting a non-EAP method will be rejected by the RADIUS server.

16.11.3 RADIUS forwarding

In the case of multi-layer EAP protocols such as TTLS or PEAP, the actual "internal" authentication can be carried out by a separate RADIUS server. Thus an existing RADIUS server can continue to be operated to provide user tables, even though it is not EAP(/TLS) capable itself. In this situation the TLS/TTLS/PEAP tunnel is managed from the LCOS RADIUS server.

The configuration of multi-layer protocols of this type is an element of a general method for the forwarding of RADIUS requests, whereby a LCOS RADIUS server can also be used as a RADIUS proxy. The concept of "realms" is the basis for request forwarding and the proxy function. A realm is a character string which defines the validity of a range of user accounts. Once defined, the realm is a suffix to the user name separated by an @ character as follows:

```
user@realm
```

The realm can be seen as a pointer to the RADIUS server where the user account is managed. The realm is removed from the string prior to the search of the RADIUS server's user table. Realms allow entire networks which are mutually trustworthy to work with common RADIUS servers located in partner networks, and to authenticate users who move between these networks. The LCOS RADIUS server stores any connected RADIUS servers along with their associated realms in a forwarding table. The realm is searched for in this table in connection with the communicated user name. If no entry is found, the request is answered with an access reject. An empty realm is treated as a local request, i.e. the LCOS RADIUS server searches its own user tables and generates its response accordingly.

To support the processing of realms the LCOS RADIUS server uses two special realms:

- Default realm: This realm is used where a realm is communicated for which no specific forwarding server has been defined. Importantly, a corresponding entry for the default realm itself must be present in the forwarding table.
- Empty realm: This realm is used when **no** realm is communicated, but the user name only.

In the default state the forwarding table has no entries, i.e. the default and empty realms are empty. This means that all requests are treated as local requests and any realms which are communicated are ignored. To operate the LCOS RADIUS server purely as a forwarding server or RADIUS proxy, the default and empty realms must be set to a value that corresponds with a server defined in the forwarding table.

Please note that the forwarding of RADIUS requests does not alter the user name. No realm is added, changed or removed. The next server may not be the last one in the forwarding chain, and the realm information may be required by that server to ensure that forwarding is carried out correctly. Only the active RADIUS server which processes the request resolves the realm from the user name, and only then is a search made of the table containing the user accounts. Accordingly the LCOS RADIUS server resolves the realm from the user name for processing requests locally.

The processing of tunneled EAP requests using TTLS and PEAP makes use of a special EAP tunnel server, which is also in the form of a realm. Here you select a realm that will not conflict with other realms. If no EAP tunnel server is defined then the LCOS RADIUS server forwards the request to itself, meaning that both the internal and the external EAP authentications are handled by the LCOS RADIUS server itself.

16.11.4 RADIUS server parameters

For the configuration of the RADIUS server, the clients which are permitted to access the RADIUS server are defined (including password), as is the UDP port which the clients can use to communicate with the RADIUS server. The authentication port applies globally for all clients.

WEBconfig: LCOS menu tree ▶ Setup ▶ Radius ▶ Server

Global settings for the RADIUS server

- **Authentication port [default: 0]**

  Specify here the port used by the authenticators to communicate with the RADIUS server in the LANCOM access point. Port '1812' is normally used.

  - Port '0' disables the RADIUS server.
- **Default realm**

  This realm is used if the user name is supplied with an **unknown** realm that is not in the list of forwarding servers.
- **Empty realm**

  This realm is used when the user name supplied does **not contain** a realm.

RADIUS clients

The client table can contain up to 16 clients that can communicate with the RADIUS server.

- **IP address**

  Enter the IP address of the client that may communicate with the RADIUS server in the LANCOM access point.
- **Secret**

  Password required by the client for access to the RADIUS server in the LANCOM access point.

! In addition to the configuration of the RADIUS server, the user information source must also be defined .

RADIUS user

Up to 64 users can be entered into the user table, and these can be authenticated by the RADIUS server without reference to other databases. This user table is used for local requests to the RADIUS server, i.e. for requests with user name but no realm.

- **User name**

  User name.
- **Password**

  User password.
- **Limit auth. methods**

  This option allows you to place limitations on the authentication methods permitted for the user.

  - Values: PAP, CHAP, MSCHAP, MSCHAPv2, EAP, All
  - Default: All

Forwarding server

The table of forwarding servers contains up to 16 realms with the associated forwarding destinations.

- **Realm**

  Character string identifying the forwarding destination.

- **IP address**
  IP address of the RADIUS server to which the request is to be forwarded.
- **Port**
  Open port for communications with the forwarding server.
- **Secret**
  Password required for accessing the forwarding server.
- **Backup**
  Alternative forwarding server in case the first forwarding server is not available.

EAP options for the RADIUS server

- **EAP tunnel server**
  This realm refers to the entry in the table of the forwarding server that is to be used for tunneled TTLS or PEAP requests.
- **TLS check username**
  TLS authenticates the client via certificate only. If this option is activated, the RADIUS server additionally checks if the username in the certificate is contained in the RADIUS user table.

16.12 RADSEC

RADIUS has become established as the standard for server-based authentication, authorization and billing. RADIUS is now being used for applications outside of its original design purpose, for example in combination with EAP/802.1x, and a number of deficits have become apparent:

- RADIUS operates via UDP and thus offers no native procedure for packet-loss detection. Although this is no problem in a LAN environment, it is becoming increasingly important over WAN connections or on the Internet.
- RADIUS is equipped only with simple procedures for authentication by means of a "shared secret" and a low level of confidentiality.

RADSEC is an alternative protocol that transmits RADIUS packets through a TLS-encrypted tunnel. TLS is based on TCP, thus providing a proven mechanism for monitoring packet loss. Furthermore, TLS is highly secure and it features a method of mutual authentication by means of X.509 certificates.

16.12.1 Configuring RADSEC for the client

LANCOM as a RADIUS client

To function as a RADIUS client, a LANCOM is set up to use RADIUS via UDP or RADSEC via TCP with TLS. Additionally the port to be used has to be set. 1812 for authentication with RADIUS, 1813 for billing with RADIUS and 2083 for RADSEC.

These settings are made at all locations where a LANCOM is configured as a RADIUS client.

WEBconfig: **Setup** ▶ **WAN** ▶ **RADIUS**

WEBconfig: **Setup** ▶ **WLAN** ▶ **RADIUS-access-check**

WEBconfig: **Setup** ▶ **WLAN** ▶ **RADIUS-accounting**

WEBconfig: **Setup** ▶ **Public-spot-module** ▶ **Provider-table**

WEBconfig: **Setup** ▶ **IEEE802.1x** ▶ **RADIUS-server**

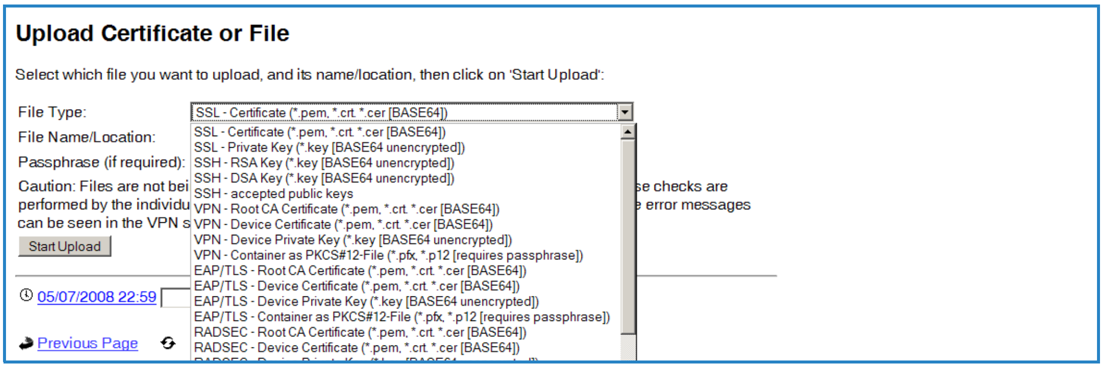
LANCOM as a RADIUS server

If a LANCOM operates as a RADIUS server, the RADSEC port for receiving logins can be set up. In addition to that, the protocol to be used (RADIUS, RADSEC or all) can be set for each of the RADIUS clients in the client list. This allows, for example, RADIUS to be used for LAN-based clients and the more robust RADSEC via TCP to be used for registrations arriving over the Internet.

16.12.2 Certificates for RADSEC

Separate X.509 certificates are required for TLS encryption of the RADSEC connection. The individual certificates (root certificate, devices certificate and private key) can be uploaded to the device individually or as a PKCS#12 container.

WEBconfig: **Upload certificate or file**



Upload Certificate or File

Select which file you want to upload, and its name/location, then click on 'Start Upload':

File Type: SSL - Certificate (*.pem, *.crt *.cer [BASE64])

File Name/Location:

Passphrase (if required):

Caution: Files are not bei … se checks are performed by the individu … e error messages can be seen in the VPN s

Start Upload
05/07/2008 22:59
Previous Page
SSL - Certificate (*.pem, *.crt *.cer [BASE64])
SSL - Private Key (*.key [BASE64 unencrypted])
SSH - RSA Key (*.key [BASE64 unencrypted])
SSH - DSA Key (*.key [BASE64 unencrypted])
SSH - accepted public keys
VPN - Root CA Certificate (*.pem, *.crt *.cer [BASE64])
VPN - Device Certificate (*.pem, *.crt *.cer [BASE64])
VPN - Device Private Key (*.key [BASE64 unencrypted])
VPN - Container as PKCS#12-File (*.pfx, *.p12 [requires passphrase])
EAP/TLS - Root CA Certificate (*.pem, *.crt *.cer [BASE64])
EAP/TLS - Device Certificate (*.pem, *.crt *.cer [BASE64])
EAP/TLS - Device Private Key (*.key [BASE64 unencrypted])
EAP/TLS - Container as PKCS#12-File (*.pfx, *.p12 [requires passphrase])
RADSEC - Root CA Certificate (*.pem, *.crt *.cer [BASE64])
RADSEC - Device Certificate (*.pem, *.crt *.cer [BASE64])

16.13 Operating printers at the USB connector of the LANCOM

With the USB port of various LANCOM models, printers can be connected up and made available to the entire network. The LANCOM provides a print server to manage the printing jobs from the network. Supported protocols are RawIP and LPR/LPD.

Parallel print jobs arriving from different stations are saved on the respective computer. The print server in the LANCOM processes the waiting jobs one after the other.

16.13.1 Configuring the printer server in the LANCOM

When configuring the USB port for the connection of a printer, the first thing is to define the ports which will receive the print jobs as transported by the various protocols.

Printer table

The printer table contains the settings for the connected printer.

WEBconfig: Expert-Configuration ▶ Setup ▶ Printer ▶ Printer

Normally there will be no need to adjust the printer settings. With the default settings, the print server works with RawIP and LPR/LPD and reacts to the standard ports as suggested by Windows when the printer connection is being configured. If printer operation does not work with these settings, the printing parameters can be adjusted.

- **Printer [Default: *]**

  Printer name.

- **RawIP-Port [Default: 9100]**

  This port can be used to accept print jobs over RawIP.

RawIP is used by Windows as standard and is recommended for operating printers at a USB port.

- **LDP-Port [Default: 515]**

  This port can be used to accept print jobs over LDP.

The protocol and port options entered here must agree with the settings for the printer connection in the corresponding computer's operating system.

- **Active [Default: No]**
  - Yes: The print server is active.
  - No: The print server is not active.
- **Bidirectional [Default: No]**
  - Yes: The LANCOM transmits the printer's status information at regular intervals to the connected computers.
  - No: The LANCOM does not transmit and status information.

Access list:

Up to 16 networks that have access to the configured printer can be entered into the access list.

LANconfig: Printer ▶ General ▶ Access list

WEBconfig: Expert-Configuration ▶ Setup ▶ Printer ▶ Access-List

- **IP address**
  IP address of the network with clients requiring access to the printer.
- **Net mask**
  Netmask of the permitted networks.

ⓘ If the access list is empty, any computer with any IP address can use the printer at the LANCOM's USB port.

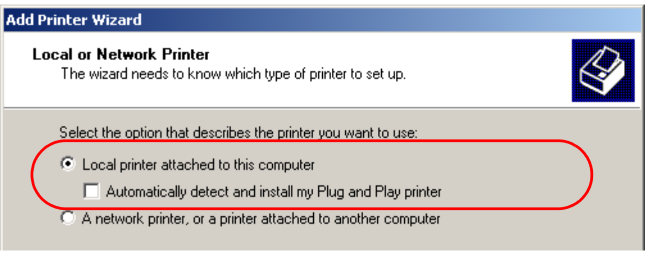
! For reasons of security, access from the WAN to the printer at the USB port of the LANCOM is not permitted.

16.13.2 Printer configuration at the computer

To use the printer at the USB port over the network, the printer drivers on the computers have to be connected with a corresponding printer connection. The following is a description of the setup under Windows XP; the configuration under Windows 2000 is similar. Controlling printers via TCP/IP ports with older version of Windows is rather unsatisfactory.

① In the Control Panel, open the dialog for the configuration of a new printer and start the Wizard to add a new printer.

② Select the option for a local printer and deactivate Plug&Play.



Add Printer Wizard

Local or Network Printer
The wizard needs to know which type of printer to set up.

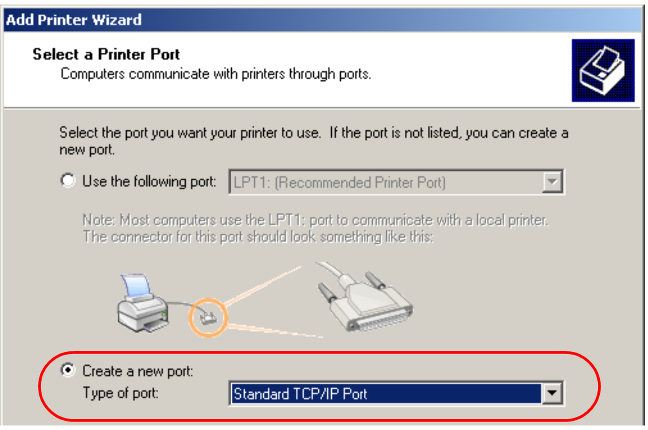
Select the option that describes the printer you want to use:

● Local printer attached to this computer

□ Automatically detect and install my Plug and Play printer

○ A network printer, or a printer attached to another computer

③ Select the option to add a new printer port.



Add Printer Wizard

Select a Printer Port
Computers communicate with printers through ports.

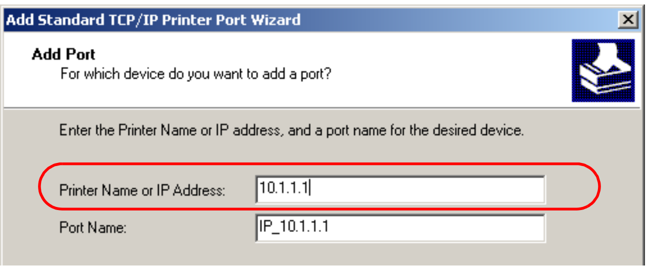
Select the port you want your printer to use. If the port is not listed, you can create a new port.

○ Use the following port: LPT1: (Recommended Printer Port)

Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:

● Create a new port:
Type of port: Standard TCP/IP Port

④ Enter the IP address of the LANCOM as the IP address of the printer port. The name for the printer port will automatically be filled out with 'IP_<IP address of the LANCOM>'.



Add Standard TCP/IP Printer Port Wizard

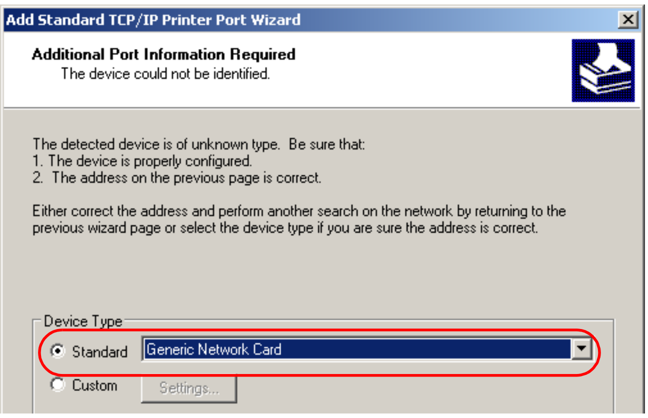
Add Port
For which device do you want to add a port?

Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 10.1.1.1

Port Name: IP_10.1.1.1

⑤ As the device type, select the option 'Standard' for a 'Generic Network Card'. If you wish to keep the standard settings (recommended), press on **Next** to proceed to the next dialog.



Add Standard TCP/IP Printer Port Wizard

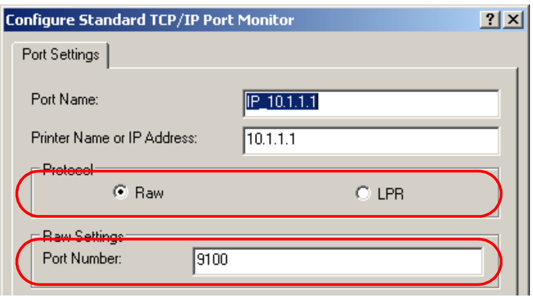
Additional Port Information Required
The device could not be identified.

The detected device is of unknown type. Be sure that:
1. The device is properly configured.
2. The address on the previous page is correct.

Either correct the address and perform another search on the network by returning to the previous wizard page or select the device type if you are sure the address is correct.

Device Type
● Standard: Generic Network Card
○ Custom

⑥ Alternatively, you can select 'Custom' and press on the **Settings** button to open an additional dialog. In this dialog, you can select the protocol to be used for transmitting the print jobs to the printer at the USB port of the LANCOM ('Raw' for RawIP or 'LPR').. The port to be used can be entered here too (for RawIP only). For LPR, port '515' is always used as standard.



Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: IP_10.1.1.1

Printer Name or IP Address: 10.1.1.1

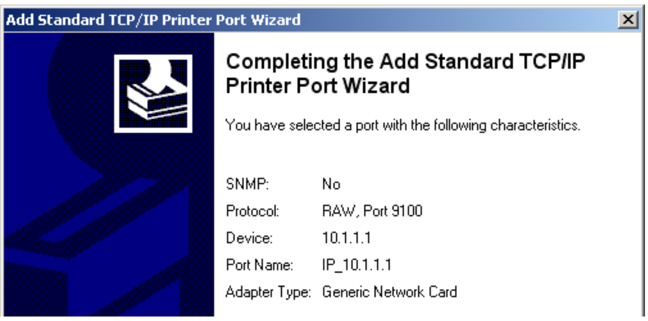
Protocol
● Raw ○ LPR

Raw Settings
Port Number: 9100

The protocol and port options entered here must agree with the settings for the printer in the LANCOM configuration.

The dialog for selecting the protocol and port can also be accesses via the Control Panel by opening the Printer Properties and accessing the 'Ports' tab.

⑦ Once the settings have been made, the printer port is set up. The Wizard now goes on with the selection of the printer driver.



Add Standard TCP/IP Printer Port Wizard

Completing the Add Standard TCP/IP Printer Port Wizard

You have selected a port with the following characteristics.

SNMP: No
Protocol: RAW, Port 9100
Device: 10.1.1.1
Port Name: IP_10.1.1.1
Adapter Type: Generic Network Card

Further information about the installation of a printer driver is available in the documentation for the printer.

LANCOM reference manual appendix

Version: LCOS 7.6 with addendum 7.7 (see appendix)
(last update August 2009)

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

Subject to change without notice. No liability for technical errors or omissions.

Products from LANCOM Systems include software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

Products from LANCOM Systems include cryptographic software written by Eric Young (eay@cryptsoft.com).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

Products from LANCOM Systems contain open source software components which are available as source text and which are subject to special licenses and the copyright of their authors. In particular the firmware components are subject to the terms of the GNU General Public License, version 2 (GPL). The license agreement with the text of the GPL is available on the LANCOM CD in the relevant product's directory. On request, you can obtain the source texts and licensing details electronically from the LANCOM Systems GmbH FTP server.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen
Deutschland

www.lancom.de

Würselen, August 2009

110650/0809

Contents

17 Appendix

17.1 Error messages in LANmonitor

It is possible to read out VPN error messages over the LANmonitor.

17.1.1 General error messages

Connection attempt cancelled	
Connection establishment failed (D-channel layer 1)	Bus activation failed
Connection establishment failed (D-channel layer 2)	no UA on SABME
Connection establishment failed (Layer 1)	a/b ports
Connection establishment failed (Layer 2)	a/b ports
ISDN line error (Layer 1)	Cable not connected
Connection aborted (layer 2)	X.75 / V.110
Local error	Required resource not available -> ISDN problem; boot telecommunications system
PP login at remote site - PAP rejected	Remote device can only handle PAP, but CHAP is required
PPP login from remote site - timeout (PPP-PAP RX)	Remote did not send PAP request
PPP login at remote site - timeout (PPP-PAP TX)	Remote did not respond to PAP request
PPP login from remote site - CHAP rejected	a CHAP reject was received after a CHAP challenge
PPP login from remote site - timeout (PPP-CHAP RX)	Remote did not send CHAP response
PPP login at remote site - timeout (PPP-CHAP TX)	Remote did not respond to CHAP response
Time limit exceeded	exactly like fee limit... .
Connection establishment failed (Layer 1)	no HDLC flags found
Connection establishment failed (Layer 2)	X.75 / V.110 not working
DSL line error (Layer 1)	Cable not connected

17.1.2 VPN error messages

For correct evaluation of error messages for VPN connections, at least LCOS version 3.22 must be installed on both LANCOM devices.

A VPN connection is always either an outgoing or an incoming connection. To make searching for the error faster and more efficient, the error messages are different for the initiator and the responder. The initiator is the remote device which initiates the connection. The responder is the device which receives the connection. After the error message is read out, look in the appropriate menu item on the corresponding remote.

Example:

For the error message 'IKE or IPSec establishment timeout (Initiator)', no direct error can be determined. The responder, however, has determined an error like 'No proposal matched (Responder, IPSec)', which it send to an SNMP client (LANmonitor) using an SNMP trap. Using this error message, the corresponding parameter in the configuration can be checked and changed if necessary. Thus is it always necessary to verify the error messages on both sides.

Message	Initiator	Responder	
License exceeded - no more VPN tunnels available (Responder, IKE)	x	x	The maximum number of possible VPN channels has been reached.
No route to remote gateway	x	x	The router to the remote gateway could not be found. Please check the public IP address or the DynDNS name of the remote device.
Dynamic VPN - no PPP table entry matched	x		In dynamic VPN, the outgoing call could not be authenticated with the PPP data sent. Please check the PPP username and PPP password on both sides under "Configure --> Communication --> Protocols --> PPP list --> Remote site".
Dynamic VPN - no PPP table entry matched		x	The incoming call cannot be authenticated with the PPP data received. Please check the PPP username and PPP password on both sides under "Configure --> Communication --> Protocols --> PPP list --> Remote site".

Message	Initiator	Responder	
IKE or IPSec establishment timeout	x	x	A time limit was reached. The router on the remote side is no longer responding. Please check the VPN error message in the LANmonitor on the remote device.
Line polling to remote gateway failed			The LCP polling failed. Please check on the remote device whether ping blocking is enabled in the firewall menu under "Configure --> Firewall --> General --> Ping blocking"
No entry in polling table and keep alive in configured			The holding time of the VPN tunnel under "Configure --> VPN --> Connection list --> Names" is set to Short hold (9999 sec.). However, the required ICMP polling is missing. Please add them under "Configure --> Communication --> Remote Sites --> Polling Table". As remote site, enter the VPN remote device, for the IP address enter an IP address from the LAN at the remote site.
Dynamic VPN - predefined charge limit exceeded	x		The fee limit under "Configure --> Costs --> Fees - Limit (ISDN)" was reached. Please reboot the device.
Dynamic VPN - preset time limit exceeded	x		The time limit under "Configure --> Costs --> Time limit (ISDN)" was reached. Please reboot the device.
Dynamic VPN - no ISDN call number for negotiator channel	x		The ISDN call number for the remote device for dynamic VPN is missing. Please enter the call number under "Configure --> Communication --> Remote sites --> Name list (ISDN) --> Name".
Dynamic VPN - Multiple connections on ISDN interface for negotiator channel not allowed			While establishing multiple ISDN connections, a limit was reached. Please check under "Configure --> Management --> Interfaces --> Interface Settings --> ISDN --> Max. outgoing calls".
Predefined charging limit exceeded	x		The fee limit under "Configure --> Management --> Costs --> Charge limit (ISDN)" was reached. Indicated by a synchronized blinking of the Power LED.
Predefined time limit exceeded	x		The time limit under "Configure --> Management --> Costs --> Time Limit (ISDN)" was reached. Indicated by a synchronized blinking of the Power LED.
No IP address for PPTP server	x		The IP address of the PPTP selected has not been entered. Enter the IP address under "Configure --> Communication --> Protocols --> PPTP list". Also see .
Exchange type mismatch (Main or Aggressive mode)		x (IKE)	The exchange type does not match that of the remote device. Please check the value under "Configure --> VPN --> Connection list --> Edit VPN remote site entry --> IKE Exchange"
No proposal matched	x (IKE)		The IKE proposals do not match. -- > Check VPN rules
No proposal matched		x (IKE)	The IKE proposals do not match. -- > Check VPN rules
IKE group mismatch		x (IKE)	Please check the IKE groups on both sides under "Configure --> VPN --> Connection parameters --> VPN remote site identification --> IKE Group"
Life type unsupported (other than Kbytes or seconds?)		x (IKE)	The value for the lifetime is not supported. Please use a life type in "sec = seconds" or "kb = kilobytes". Check this entry under "Configure --> VPN --> Parameters --> Lifetime"
Lifetime mismatched		x (IKE)	The lifetime specified does not match that of the remote device. Check this entry under "Configure --> VPN --> Parameters --> Lifetime"
ID type value unsupported (other than IP network, domain, or email)		x (IKE)	False entry of identity. Please correct your entry under "Configure --> VPN --> IKE --> IKE key"
ID type mismatch (e.g. IP network, domain, or email)		x (IKE)	The two sites are using different identities. Compare the identification at both sites under "Configure --> VPN --> IKE --> IKE key"
No rule matched ID - unknown connection or wrong ID (e.g. remote gateway definition)		x (IKE)	The incoming VPN connection could not be assigned to a remote device.
IKE key mismatch	x (IKE)		Please compare the preshared keys under "Configure --> VPN --> IKE --> IKE key"
IKE key mismatch		x (IKE)	Please compare the preshared keys under "Configure --> VPN --> IKE --> IKE key"
Out of memory	x (IKE)		The number of VPN connections has overloaded the device's memory. To maintain the stability of the device, no further VPN connections should be established.
Out of memory		x (IKE)	The number of VPN connections has overloaded the device's memory. To maintain the stability of the device, no further VPN connections should be established.

Message	Initiator	Responder	
No rule matched IDs - unknown connection or wrong ID (e.g. IP network definition)		x (IKE)	The incoming VPN connection could not be assigned to a remote device. Please check the following parameters: ID type does not match (see this document), incorrect network definition, VPN rules do not match (see VPN RULES).
No proposal matched	x (IPsec)	x (IPsec)	The devices cannot agree on a matching proposal. Please check the settings under "Configure --> VPN --> IKE --> IKE Proposals" and under "Configure --> VPN --> IPSec parameters --> IPSec proposal lists".
IPSec PFS group mismatch			Please check the PFS (Perfect Forward Sequence) under "Configure --> VPN --> Connection parameters --> VPN remote identification --> PFS Group"

17.2 SNMP Traps

MIB2 Traps	Explanation
coldstart	Device was restarted by switching power off and on.
warmstart	LCOS was restarted, for instance by a software reboot
authentication failed (= console login failed)	Login failed during access to the configuration

Enterprise specific Traps	Explanation
Firmware upload started	Firmware upload was started
Configuration upload started	The reading of the firmware or configuration was started
Upload succeeded	The reading of the firmware or configuration was successful
Upload failed (timeout)	The reading of the firmware or configuration failed: maximum time was exceeded
Upload failed (incomplete)	The reading of the firmware or configuration failed: incomplete configuration
Upload failed (bad device)	The reading of the firmware or configuration failed: wrong device
Configuration download started	Output of the configuration was started
Download succeeded	Output of the configuration was successful
Console login	Login to configuration successful
Console logout	Logout from configuration was successful
Firewall trap	Information about a firewall event
Connection status	WAN connection status
VPN Connection status	Status of VPN connection
WAN-Ethernet UP/DOWN	WAN interface available or not available

WLAN traps	Operating mode	Explanation
WLAN Scan started	Access point or client	The WLAN station has started a scan for free radio channels
Started WLAN BSS ID	Access point	The WLAN station has created a new radio cell
Joined WLAN BSS ID	Client	The WLAN station has found a radio cell
Authenticated WLAN station	Access point	The authentication of a client WLAN station was successful
Deauthenticated WLAN station	Access point	The client WLAN station has signed off
Associated WLAN station	Access point	Client WLAN station connected
Reassociated WLAN station	Access point	Client WLAN station has reconnected, was previously signed in to another access point
RADIUS access check for WLAN station succeeded	Access point	Checking of RADIUS access to the WLAN station was successful
RADIUS access check for WLAN station failed	Access point	Checking of RADIUS access to the WLAN station was unsuccessful
Disassociated WLAN station due to station request	Access point	WLAN station was signed off due to a request from the station
Rejected association from WLAN station	Access point	The sign on of the WLAN station was rejected
WLAN card hung, resetting	Access point or client	WLAN card stopped, reset

17.3 Radio channels

17.3.1 Radio channels in the 2,4 GHz frequency band

In the frequency range from 2400 to 2483 MHz are up to 13 channels available. The following overview shows which channels are supported by the different regions (EU/WORLD). The last column shows which channels can be used without overlapping.

Frequency range	2400–2500 MHz		no overlapping with
Channel No.	EU (ETSI)	WORLD (ETSI + FCC)	
1	2412	2412	6, 11
2	2417	2417	7
3	2422	2422	8
4	2427	2427	9
5	2432	2432	10
6	2437	2437	1, 11
7	2442	2442	2
8	2447	2447	3
9	2452	2452	4
10	2457	2457	5
11	**2462**	**2462**	1, 6
12	2467	–	–
13	2472	–	–

Bold values indicate the default setting of the *LANCOM DSL/I-10 Office* radio adapters when utilized in a base station.

17.3.2 Radio channels in the 5 GHz frequency band

In the frequency range from 5,13 to 5,805 GHz up to 19 non-overlapping channels are available in Europe, defined as the sub-bands as follows:

- Band 1: 5150 - 5350 MHz (channels 36, 40, 44, 48, 52, 56, 60 and 64)
- Band 2: 5470 - 5725 MHz (channels 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 and 140)
- Band 3: 5725 - 5875 MHz (channels 147, 151, 155, 167)

Please note that frequency ranges an radio channels in band 3 are reserved for operation in UK only!

The following overview shows which channels are allowed in different regions.

	Channel No.	Frequency	ETSI (EU)	FCC (US)
Band 1	36	5,180 GHz	yes	yes
	40	5,200 GHz	yes	yes
	44	5,220 GHz	yes	yes
	48	5,240 GHz	yes	yes
	52	5,260 GHz	yes	yes
	56	5,280 GHz	yes	yes
	60	5,300 GHz	yes	yes
	64	5,320 GHz	yes	yes

	Channel No.	Frequency	ETSI (EU)	FCC (US)
Band 2	100	5,500 GHz	yes	no
	104	5,520 GHz	yes	no
	108	5,540 GHz	yes	no
	112	5,560 GHz	yes	no
	116	5,580 GHz	yes	no
	120	5,600 GHz	yes	no
	124	5,620 GHz	yes	no
	128	5,640 GHz	yes	no
	132	5,660 GHz	yes	no
	136	5,680 GHz	yes	no
	140	5,700 GHz	yes	no
Band 3 (UK only)	147	5,735 GHz	no	yes
	151	5,755 GHz	no	yes
	155	5,775 GHz	no	yes
	167	5,835 GHz	no	yes

17.3.3 Radio channels and frequency ranges for Indoor and Outdoor operating

In several countries specific regulations are valid concerning the use of frequency ranges and radio channels for indoor and outdoor operating. The following table gives information on the permitted application:

Country	Band (GHz)	Sub band	Frequency	Channels	Turbo channels	Emitted power (dBm)	Indoor/ Outdoor
Germany, Austria, Switzerland, Netherlands, Belgium, Luxembourg, Italy, Malta, France	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	200/23	I
		2	5,470-5,725	100-140	106-130	1000/30	I+O
UK	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	200/23	I
		2	5,470-5,725	100-140	106-130	1000/30	I+O
		3	5,725-5,585	147, 151, 155, 167	–	2000/33,1	(only fixed WLAN outdoor installations!)
Czechia	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	200/23	I

Further details to the restrictions for the use of wlan adapters within the EU can be found in the internet:

Country	Organization	Link
Belgium	Institut Belge des Postes et Telecommunications (BIPT)	www.bipt.be
Denmark	National Telecom Agency	www.tst.dk
Germany	Regulierungsbehörde für Telekommunikation und Post	www.regtp.de
Finland	Finnish Communications Regulatory Authority (FICORA)	www.ficora.fi
France	Autorité de Régulation des Télécommunications (ART)	www.art-telecom.fr
Greece	National Telecommunications Commission (EET)	www.eett.gr
Great Britain	Office of Telecommunications (Oftel)	www.oftel.gov.uk
	Postal Services Commission (Postcomm)	www.postcomm.gov.uk/
	Radiocommunications Agency	www.open.gov.uk/radiocom
Ireland	Commission for Communications Regulation (ComReg)	www.comreg.ie
Iceland	Post and Telecom Administration (PTA)	www.pta.is
Italy	L'Autorità per le garanzie nelle communicazioni (AGC)	www.agcom.it

Country	Organization	Link
Latvia	Telecommunication State Inspection	www.vei.lv
Liechtenstein	Amt für Kommunikation (AK)	www.ak.li
Lithuania	Radio Administration	www.rrt.lt/
Luxembourg	Institut Luxembourgeois des Télécommunications (ILT)	www.etat.lu/ILT
Netherlands	Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA)	www.opta.nl
	Agentschap Telecom	www.agentschap-telecom.nl
	Ministerie Economische Zaken	www.ez.nl
Norway	Norwegian Post and Telecommunications Authority (NPT)	www.npt.no
Austria	Rundfunk und Telekom Regulierungs-GmbH	www.rtr.at
	Bundesministerium für Verkehr, Innovation und Technologie	www.bmvit.gv.at
Poland	Urzad Regulacji Telekomunikacji (URT)	www.urt.gov.pl
Portugal	Autoridad Nacional De Comunicaçòes (ICP-Anacom)	www.anacom.pt
Sweden	National Post and Telecom Agency	www.pts.se
Switzerland	Bundesamt für Kommunikation	www.bakom.ch
Slowenia	Agencija za telekomunikacije, radiodifuzijo in pošto	www.atrp.si
Spain	Comision del Mercado de las Telecomunicaciones (CMT)	www.cmt.es
Czechia	Czech Telecommunication Office	www.ctu.cz
Hungary	Communication Authority (HIF)	www.hif.hu

ⓘ Please inform yourself about the current radio regulations of the country you want to operate a Wireless LAN device.

17.4 RFCs supported

RFC	Title
1058	Routing Information Protocol
1331	The Point-to-Point Protocol (PPP) for the Transmission of Multi-protocol Datagrams over Point-to-Point Links
1334	PPP Authentication Protocols
1389	RIP Version 2 MIB Extensions
1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
1542	Clarifications and Extensions for the Bootstrap Protocol
1552	The PPP Internetworking Packet Exchange Control Protocol (IPXCP)
1577	Classical IP and ARP over ATM
1631	The IP Network Address Translator (NAT)
1877	PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
1974	PPP Stack LZS Compression Protocol
2284	Extensible Authentication Protocol
2104	HMAC: Keyed-Hashing for Message Authentication
2131	Dynamic Host Configuration Protocol
2132	DHCP Options and BOOTP Vendor Extensions
2225	Classical IP and ARP over ATM
2364	PPP Over AAL5
2401	Security Architecture for the Internet Protocol
2402	IP Authentication Header
2403	The Use of HMAC-MD5-96 within ESP and AH
2404	The Use of HMAC-SHA-1-96 within ESP and AH
2405	The ESP DES-CBC Cipher Algorithm With Explicit IV
2406	IP Encapsulating Security Payload (ESP)
2407	The Internet IP Security Domain of Interpretation for ISAKMP
2408	Internet Security Association and Key Management Protocol (ISAKMP)
2409	The Internet Key Exchange (IKE)
2410	The NULL Encryption Algorithm and Its Use With IPsec
2412	The OAKLEY Key Determination Protocol
2451	The ESP CBC-Mode Cipher Algorithms
2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5
3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

17.5 Glossary

802.11	Wireless LAN specification of the IEEE; data rate up to 2 Mbps; in 2.4 GHz ISM band; FHSS and DSSS; infrared spectrum communications also planned
802.11a	Extension to 802.11; data rate up to 54 Mbit/s; in 5 GHz band; OFDM
802.11b	Extension to 802.11; data rate up to 11 Mbit/s; in 2.4 GHz band; high market penetration; DSSS/CCK
802.11g	Extension to 802.11; data rate up to 54 Mbit/s; in 2.4 GHz band; OFDM and DSSS
802.11h	802.11a customization, data rate up to 54 Mbit/s; in 5 GHz band; in area of transmission power and frequency management; for use in Europe; OFDM
802.11i	Future 802.11 extension with additional security features
802.1x	Specification of a port-based authentication mechanism from the IEEE
AES	Advanced Encryption Standard

Access point	Base station in a wireless LAN; independent LAN-WLAN bridge; connects stations of a LAN (local network) with a WLAN (wireless network) in a point-to-multipoint mode; connects two networks over a wireless network in point-to-point mode
Access router	Active network component for connection of a local network to the Internet or a company network
ADSL	Asymmetrical Digital Subscriber Line - transmission process for high-speed data transmission over normal telephone lines. With ADSL, transmissions (downstream) of up to 6 Mbps can be implemented over normal telephone lines; for bidirectional transmission there is a second frequency band with transmission speeds of up to 640 kbps (upstream) - hence the name "asymmetric".
Bandwidth	Data rate with which a user can surf the Internet; the higher the bandwidth, the faster the connection
Broadband	Service which provides high bandwidth; e.g.: DSL or WLAN
Bridge	Transport protocol-independent, transparent network component; transmits all packets which are identified as "not local" and only understands the difference between "local" and "remote". Works on Layer 2 of the OSI model
Broadcast	Broadcasts are packets to all stations of a local network; bridges transmit broadcasts; routers do not transmit broadcasts
BSS	Basic Service Set
CAPI	Common ISDN Application Programming Interface - CAPI is a standard for control of ISDN adapters
CCK	Code Complementary Keying; type of modulation used by DSSS
Client	Any computer equipped with a wireless LAN adapter (wireless LAN card), which uses services provided by other participants in the wireless network
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance; access procedure to the radio channel used under 802.11
CRC	Cyclic Redundancy Check; process for detecting bit errors
Data throughput	Speed at which you can surf on the Internet; depends on the bandwidth and the number of users
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service - computers communicate with computers in remote networks using IP addresses; DNS servers translate names into IP addresses; without DNS servers, you would have to remember all IP addresses and couldn't work with names (e.g. www.lancom.de)
Domain	area of network closed to outside; => Intranet
Download / Downstream	Download / downstream denotes the direction of dataflow in a WAN. Downstream is the direction from the head end or Internet to the participant connected to the network.
DS	Distribution System
DSL	Digital Subscriber Line - DSL procedures include all procedures for digital-broadband use of telephone lines, such as ADSL, HDSL, SDSL, VDSL and so on, which are also called xDSL.
DSSS	Direct Sequence Spread Spectrum; code multiplex -- band spreading process
Dynamic DNS	IPsec-VPN implementation which allows the transparent connection of local networks into a VPN solution, even when their routers work with dynamic addresses (dial-up)
EAP	Extensible Authentication Protocol
EAP-MD5	EAP variant which uses password for one-sided authentication
EAP-TLS	EAP Transport Layer Security; EAP variant which uses certificates for mutual authentication
EAP-TTLS	EAP Tunneled Transport Layer Security; EAP variant which uses certificates for mutual authentication
EIRP	Effective Isotropic Radiated Power
ESS	Extended Service Set
ESSID	Extended Service Set Identity; “network name" of the wireless LAN
Ethernet	Strand or star-formed physical transport medium; all stations can send simultaneously; collisions are detected and corrected through the network protocol
FHSS	Frequency Hopping Spread Spectrum; frequency skipping band spread procedure
Firewall	Protective mechanism for an Intranet against attacks from outside
Frequency	Number of oscillations per second (given in Hertz; 1 Hz = 1 oscillation per second; GHz = Gigahertz = 1 billion Hertz or oscillations per second)
FTP	File Transfer Protocol enables data transfer between different systems and simple file manipulation; FTP is based on the TCP transmission protocol
Frequency band	Contiguous frequency range which has the same transmission properties
Radio frequency	Every radio application uses globally regulated radio frequencies
Gateway	Network component which provides access to other network components on a layer of the => OSI model. Packets which do not go to a local partner are sent to the gateway. The gateway takes care of communication with remote networks.
Hub	Network component; distributor; collector; also used to translate from one connection type to another

HotSpot	Locally limited wireless network with a base station with Internet access; public wireless Internet access
IAPP roaming	Roaming between the cells of a wireless network using IAPP (Inter Access Point Protocol)
IBSS	Independent Basic Service Set
IDS	Intrusion Detection System -- earliest possible detection of attacks on the network
IEEE	Institute of Electrical and Electronics Engineers, New York - www.ieee.org
IP	Internet Protocol
IP masquerading	Combination of PAT (Port Address Translation) and NAT (Network Address Translation) from LANCOM Systems process used for connection of an intranet (multiple workstations) to the Internet over a single IP address; simultaneously, the internal computers are protected from attacks from outside
IPSec	Internet Protocol Security
IP Quality of Service	These functions give precedence to enterprise-critical applications, particular services, or user groups
ISDN	Integrated Services Digital Network -- fast connection; two independent channels; higher transmission rates than analog (up to 128 Kbit/s); uses the old analog lines; comfort features (call forwarding, callback on busy, etc.); supports both analog and digital services
ISM frequency band	Industrial-Scientific-Medical, license-free frequency bands which can be used for industrial, scientific, and medical purposes.
ISP	Internet Service Provider -- service provider with a connection to the Internet (backbone) who provides connection points for end customers
LCOS	LANCOM Operating System - uniform operating system for LANCOM products
LAN	Local Area Network - local network limited to one site
LANcapi	Virtual CAPI which is provided over the network; with LANcapi, which is implemented in all LANCOM routers with ISDN interfaces, a PC connected to the LAN can use ISDN telematic services
LANconfig	Software for configuration of LANCOM devices under Windows
LANtools	Diverse, user-friendly set of tools for the management and monitoring of LANCOM products and systems
MAC	Media Access Control; radio access protocol on ISO Layer 2 data link; it defines packet format, packet addressing, and error detection
MAC address	Serial number of a network component which is assigned by the manufacturer
Mbit	Megabit: standard unit for the specification of data quantities in the context of bandwidths
MIC	Message Integrity Check, cryptographic integrity protection mechanism
NetBIOS	Network Basic Input/Output System. Non-routable network protocol for local networks developed by IBM and later taken over by Microsoft.
NTBA	Network Termination Basic Adaptor . The NTBA (network termination adapter) is responsible in an ISDN base connection for the translation of the connection created by the telephone company to the S0 bus.
OFDM	Orthogonal Frequency Divison Multiplex
PEAP	Protected EAP, EAP variant for mutual authentication
PKI	Public Key Infrastructure
PPP	Point to Point Protocol: network protocol for connections between two computers. PPP is based on TCP/IP.
PPTP	Point to Point Tunneling Protocol: Network protocol for the construction of virtual private networks over the Internet.
Point-to-Multipoint (WLAN)	Multiple WLAN stations log into a base station and constitute a common network with the wired stations
Point-to-Point (WLAN)	Two base stations connect two wired networks over WLAN; point-to-point operation enables coupling of networks even across streets without cables
QoS	Quality of Service (see also IP Quality of Service)
RADIUS	Remote Authentication Dial-In User Service; authentication and monitoring protocol on the application level for authentication, integrity protection, and accounting for network access
RC4	Streaming cipher process by Ron Rivest, "Ron's Code"
RFC	Request for Comments
Router	Intelligent network components; comparable with a post office, which can determine from the logical destination address of a packet which next network component should transmit the packet; knows the overall topology of the network
SDSL	Single Line Digital Subscriber Line - downstream and upstream with 2.048 Mbit/s (two-strand wire)
Server	Computer which provides services over the network (e.g. files, news, email, WWW pages)
SINA	Secure Inter-Network Architecture
SMTP	Simple Mail Transfer Protocol - SMTP protocol is the Internet standard for distribution of electronic mail; the protocol is based on the TCP protocol

SNMPv3	Simple Network Management Protocol Version 3
SSID	Service Set Identity; “network name" of the wireless LAN
SSL	Secure Socket Layer
Splitter	The splitter is comparable with an audio frequency filter; in an ADSL connection, the splitter separates the ISDN signals from the DSL signals; the ISDN signals go to the NTBA and the DSL signals go to the DSL modem
Switch	A central distributor in a star-shaped network; each station has the entire bandwidth available; if a station fails, the rest of the network is not affected; is used for collision prevention; increases the overall throughput of the network; switches are cascadable
TAE	Telephone connection unit used in Germany. Plug for the connection of analog devices like a telephone or modem into the telephone network.
TCP/IP	Transmission Control Protocol/Internet Protocol; family of protocols (ARP, ICMP, IP, UDP, TCP, HTTP, FTP, TFTP) used mainly in the Internet, although it is making headway in intranets as well
TKIP	Temporal Key Integrity
TLS	Transport Layer Security
TPC	Transmission Power Control
Upload/Upstream	Upload / upstream denotes the direction of dataflow in a WAN; upstream is the direction from the node connected to the network to the head end/Internet
Chaining	Concatenation of bit sequences
VPN	Virtual Private Network - a VPN is a network consisting of virtual connections over which non-public or company internal data can be transmitted securely, even if public network infrastructures are used
WAN	Wide Area Network - network connection over long distances (e.g. over ISDN with a LANCOM router)
WECA	Wireless Ethernet Compatibility Alliance; alliance of manufacturers of wireless LAN components based on IEEE 802.11; renamed the WiFi Alliance
WEBconfig	Web-based configuration interface for LANCOM devices.
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity; marketing concept generated by the WECA
WiFi-Alliance	Alliance of manufacturers of wireless LAN components based on IEEE 802.11; formerly the WECA
WLAN	Wireless Local Area Network - local radio network
WPA	WiFi Protected Access; name for security mechanisms beyond IEEE 802.11; generated by the WiFi Alliance
WISP	Wireless Internet Service Provider
xDSL	xDSL stands for the family of Digital Subscriber Line technologies
XOR	Logical operation "exclusive OR"

17.6 Overview of functions by model and LCOS* version

	800 1000 1100	I-10 HW-Rv. A	I-10 HW-Rv. C	DSL/I-10+	800+	821	821+	1511	1521
Interfaces									
ADSL modem						✔	✔		✔
ADSL 2+							5.20		ADSL 2
VLAN							7.00	✔	✔
DMZ port				5.20	5.20	1)	5.20	5.20	5.20
Switch ports				3	4	4	4	4	4
Ethernet port mapping				5.00			✔	5.00	5.00
DSLoL						3.10			
Security									
Stateful Inspection, DoS, IDS	2.80	2.80	2.80	✔	✔	2.80	✔	✔	✔
IP QoS, Traffic Shaping	3.30	3.30	3.30	✔	✔	3.30	✔	3.30	✔
SSH configuration access				✔	✔	4.00	✔	4.00	4.00
ISDN-based anti-theft device				5.00	5.00	5.00	✔	5.00	5.00
Management									
Rights management for admins				✔	✔	4.00	✔	4.00	4.00
Multiple loopback addresses				✔	✔	4.00	✔	4.00	4.00
Modem operation at serial interface				4.10	4.10	4.10	✔	4.10	4.10
Scripting				5.00	5.00	5.00	✔	5.00	5.00
CRON	3.10	3.10	3.10	✔	✔	3.10	✔	✔	✔
Port monitor				5.00	5.00		✔	5.00	5.00
Other functions									
Advanced routing and forwarding (ARF networks)				2 7.00	2 7.00		8 7.00	2 7.00	2 7.00
DHCP auto client mode	3.42	3.42	3.42	✔	✔	3.42	✔	3.42	3.42
N:N mapping				4.10	4.10	4.10	✔	✔	4.10
Dynamic DNS	3.10	3.10	3.10	✔	✔	3.10	✔	✔	✔
Free port mapping				✔	✔	4.00	✔	4.00	4.00
Multi-PPPoE				✔		4.00	✔	4.00	4.00
Load balancing (4 channels)				2 5.00		2 5.00	2	2 5.00	2 5.00
Policy-based routing				5.00	5.00	5.00	✔	5.00	5.00
VRRP				5.20	5.20	5.20	5.20	5.20	5.20
PPPoE servers				5.20	5.20	5.20	5.20	5.20	5.20
WAN RIP				5.20	5.20	5.20	5.20	5.20	5.20
Spanning Tree Protocol								5.20	5.20
Layer 2 QoS tagging							6.10	6.10	6.10
VPN functions									
VPN channels									

	800	I-10	I-10	DSL/I-	800+	821	821+	1511	1521
	1000	HW-Rv.	HW-Rv.	10+					
	1100	A	C						
VPN hardware acceleration									
AES, 3-DES, DES, Blowfish, CAST									
Digital certificates (X.509) incl. PKCS #12									
Certificate revocation list - CRL									
Certificate enrollment via SCEP									
Simplified RAS with certificates									
AES 256 / IPCOMP									
Redundant VPN gateways									
NAT Traversal (NAT-T)									
IKE config mode									
WLAN functions									
WLAN-802.11b								✔	✔
WLAN-802.11g								✔	✔
WLAN-802.11a (incl. turbo mode)									
LEPS								4.00	4.00
Multi-SSID, IP-redirect								3.42	3.42
Super A/G								3.42	3.42
Standard WEP encryption								4.00	4.00
802.11i with HW-AES								3.50	3.50
802.11i for P2P in WLAN								4.00	4.00
WLANmonitor								5.00	5.00
Group configuration								5.00	5.00
Fully transparent client bridge mode								5.00	5.00
Bandwidth limitations in the WLAN								5.20	5.20
QoS for WLAN (IEEE 802.11e, WMM/WME)								6.10	6.10
RADIUS server								6.10	6.10
VoIP functions (detailed information about your device's VoIP functions can be found in the user manual)									
SIP users				4/-7)			4/-7)		
ISDN users				40			40		
SIP lines				16			16		
Lines to SIP PBXs				4			4		
External ISDN busses for VoIP				1			1		
Internal ISDN busses for VoIP									
Analog exchange line connections									
Connectors for analog terminal equipment									
Software options									
ISDN leased line option	Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10
Public spot option								✔	✔
Fax modem option	✔	✔							
VPN-25 Option									
VPN-500 Option									
VPN-1000 Option									

□ *Overview of functions by model and LCOS* version*

	800 1000 1100	I-10 HW-Rv. A	I-10 HW-Rv. C	DSL/I- 10+	800+	821	821+	1511	1521
VoIP basic option				✔			✔		
VoIP advanced option									
VoIP-32 Option									

* The numbers in the table indicate the LCOS version in which the function was implemented

[1] Port separation (private mode)

[2] Only if the VPN options have been activated for the device

[3] Not with 11-Mbit WLAN cards

[4] Optional VPN-500 and VPN-1000 available

[5] Compatible with ADSL and ADSL2

[6] 3050; only with external MC-54 card

[7] depending on VoIP option (Basic/Advanced)

[8] With VoIP Advanced and VoIP-32 Option

[9] With VoIP-32 Option

[10] Requires VoIP Advanced Option

	1611	1611+	1620	1621	1711	1721	1722	1723	1724
Interfaces									
ADSL modem			✔	✔		✔	✔	✔	✔
ADSL 2+			✔			✔	✔	✔	✔
VLAN		7.00	7.00		7.00	7.00	7.00	✔	✔
DMZ port		5.20	✔	1)	5.20	5.20	✔	✔	✔
Switch ports		3	4	4	4	4	4	2	2
Ethernet port mapping		✔	✔		5.00	✔	✔	✔	✔
DSLoL				3.10					
Security									
Stateful Inspection, DoS, IDS	2.80	✔	✔	2.80	✔	✔	✔	✔	✔
IP QoS, Traffic Shaping	3.30	✔	✔	3.30	✔	✔	✔	✔	✔
SSH configuration access	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔
ISDN-based anti-theft device	5.00	✔		5.00	5.00	✔	✔	✔	✔
Management									
Rights management for admins	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔
Multiple loopback addresses	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔
Modem operation at serial interface	4.10	4.10	✔	4.10	4.10	✔	✔	✔	✔
Scripting	5.00	✔	✔	5.00	5.00	✔	✔	✔	✔
CRON	3.10	✔	✔	3.10	✔	✔	✔	✔	✔
Port monitor		✔	✔		5.00	✔	✔	✔	✔
Other functions									
Advanced routing and forwarding (ARF networks)		2 7.00	2 7.00		8 7.00	8 7.00	8 7.00	8 7.00	8 7.00
DHCP auto client mode	3.42	3.42	✔	3.42	3.42	✔	✔	✔	✔
N:N mapping	3.30	✔	✔	3.30	✔	✔	✔	✔	✔
Dynamic DNS	3.10	✔	✔	3.10	✔	✔	✔	✔	✔
Free port mapping	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔
Multi-PPPoE	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔
Load balancing		2	2	2 5.00	4 Kanäle 5.00	4 Kanäle	4 Kanäle	2 Kanäle	2 Kanäle
Policy-based routing	5.00	✔	✔	5.00	5.00	✔	✔	✔	✔
VRRP	5.20	5.20	✔	5.20	5.20	✔	✔	✔	✔
PPPoE servers	5.20	5.20	✔	5.20	5.20	✔	✔	✔	✔
WAN RIP	5.20	5.20	✔	5.20	5.20	✔	✔	✔	✔
Spanning Tree Protocol									
Layer 2 QoS tagging		6.10	6.10		6.10	6.10	6.10	✔	✔
VPN functions									
VPN channels	5	5	5	5	5	5	5	5	5

	1611	1611+	1620	1621	1711	1721	1722	1723	1724
VPN hardware acceleration					wth VPN-25-Option	wth VPN-25-Option	wth VPN-25-Option	wth VPN-25-Option	wth VPN-25-Option
AES, 3-DES, DES, Blowfish, CAST	3.32	✔	✔	3.32	✔	✔	✔	✔	✔
Digital certificates (X.509) incl. PKCS #12	5.00	✔	✔	5.00	5.00	✔	✔	✔	✔
Certificate revocation list - CRL					6.10	6.10	6.10	✔	✔
Certificate enrollment via SCEP					7.00	7.00	7.00	7.00	7.00
Simplified RAS with certificates					6.20	6.20	6.20	6.20	6.20
AES 256 / IPCOMP	5.00	✔	✔	5.00	5.00	✔	✔	✔	✔
Redundant VPN gateways	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔
NAT Traversal (NAT-T)	5.20	5.20	✔	5.20	5.20	✔	✔	✔	✔
IKE config mode	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔
WLAN functions									
WLAN-802.11b									
WLAN-802.11g									
WLAN-802.11a (incl. turbo mode)									
LEPS									
Multi-SSID, IP-redirect									
Super A/G									
Standard WEP encryption									
802.11i with HW-AES									
802.11i for P2P in WLAN									
WLANmonitor									
Group configuration									
Fully transparent client bridge mode									
Bandwidth limitations in the WLAN									
QoS for WLAN (IEEE 802.11e, WMM/WME)									
RADIUS server									
VoIP functions (detailed information about your device's VoIP functions can be found in the user manual)									
SIP users		4/-[7]			4/8[7]/32[8]	4/8[7]/32[8]	8/32[9]	8/32[9]	8/32[9]
ISDN users		40			40	40	40	40	40
SIP lines		16			16	16	16	16	16
Lines to SIP PBXs		4			4	4	4	4	4
External ISDN busses for VoIP		1			1	1	0-2	0-1	0-4
Internal ISDN busses for VoIP							0-2	0-2	0-4
Analog exchange line connections								0-1	
Connectors for analog terminal equipment								2	
Software options									
ISDN leased line option	Integr. as of 6.10	Integr. as of 6.10		Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10	Integr. as of 6.10	Integr.	Integr.
Public spot option									
Fax modem option									
VPN-25 Option	✔	✔	✔	✔	✔	✔	✔	✔	✔
VPN-500 Option									
VPN-1000 Option									

	1611	1611+	1620	1621	1711	1721	1722	1723	1724
VoIP basic option		✔			✔	✔			
VoIP advanced option					✔	✔			
VoIP-32 Option					✔[10]	✔[10]	✔	✔	✔

* The numbers in the table indicate the LCOS version in which the function was implemented

[1] Port separation (private mode)

[2] Only if the VPN options have been activated for the device

[3] Not with 11-Mbit WLAN cards

[4] Optional VPN-500 and VPN-1000 available

[5] Compatible with ADSL and ADSL2

[6] 3050; only with external MC-54 card

[7] depending on VoIP option (Basic/Advanced)

[8] With VoIP Advanced and VoIP-32 Option

[9] With VoIP-32 Option

[10] Requires VoIP Advanced Option

	1811	1821	1821+	1823	3050 3550	4000 4100	6000 6001 6021	7011	7111	8011
Interfaces										
ADSL modem		✔	✔	✔						
ADSL 2+		ab Hardware Release E	✔	✔						
VLAN	3.30	✔	✔	✔	3.30			7.00	7.00	7.00
DMZ port	5.20	5.20	✔	✔				✔	5.20	5.20
Switch ports	4	4	4	2					4	4
Ethernet port mapping	5.00	5.00	✔	✔					5.00	5.00
DSLoL										
UMTS Support					Integr. as of 6.20					
Security										
Stateful Inspection, DoS, IDS	✔	✔	✔	✔	2.80	2.80	2.80	2.80	✔	✔
IP QoS, Traffic Shaping	✔	✔	✔	✔	3.30	3.30	3.30	3.30	✔	✔
SSH configuration access	4.00	4.00	✔	✔	4.00	4.00	4.00	4.00	✔	4.00
ISDN-based anti-theft device	5.00	5.00	✔	✔		5.00	5.00	5.00	5.00	5.00
Management										
Rights management for admins	4.00	4.00	✔	✔	4.00	4.00	4.00	4.00	✔	4.00
Multiple loopback addresses	4.00	4.00	✔	✔	4.00	4.00	4.00	4.00	✔	4.00
Modem operation at serial interface	4.10	4.10	✔	✔					4.10	4.10
Scripting	5.00	5.00	✔	✔	5.00	5.00	5.00	5.00	5.00	5.00
CRON	✔	✔	✔	✔	3.10	3.10	3.10	3.10	✔	3.10
Port monitor	5.00	5.00	✔	✔					5.00	5.00
Other functions										
Advanced routing and forwarding (ARF networks)	8 7.00	8 7.00	8	8 7.00	8 7.00			2 7.00	64 7.00	64 7.00
DHCP auto client mode	3.42	3.42	✔	✔	3.42	3.42	3.42	3.42	✔	3.42
N:N mapping	3.30	✔	✔	✔	3.30	3.30	3.30	3.30	✔	✔
Dynamic DNS	✔	✔	✔	✔	3.10	3.10	3.10	3.10	✔	✔
Free port mapping	4.00	4.00	✔	✔	4.00	4.00	4.00	4.00	✔	4.00
Multi-PPPoE	4.00	4.00	✔	✔	4.00			4.00	✔	4.00
Load balancing	4 channels 5.00	4 channels 5.00	4 channels	2 channels					4 channels 5.00	4 channels 5.00
Policy-based routing	5.00	5.00	✔	✔	5.00	5.00	5.00	5.00	5.00	5.00
VRRP	5.20	5.20	✔	✔	5.20	5.20	5.20	5.20	5.20	5.20
PPPoE servers	5.20	5.20	✔	✔	5.20	5.20	5.20	5.20	5.20	5.20
WAN RIP	5.20	5.20	✔	✔	5.20	5.20	5.20	5.20	5.20	5.20

	1811	1821	1821+	1823	3050 3550	4000 4100	6000 6001 6021	7011	7111	8011
Spanning Tree Protocol	5.20	5.20	✔	✔	5.20					
Layer 2 QoS tagging	6.10	6.10	✔	✔	6.10	6.10	6.10	6.10	6.10	6.10
VPN functions										
VPN channels	5	5	5	5			100	200	100	200
VPN hardware acceleration	with VPN-25-Option	with VPN-25-Option	with VPN-25-Option	with VPN-25-Option					✔	✔
AES, 3-DES, DES, Blowfish, CAST	3.32	✔	✔	✔	✔	✔	✔	✔	✔	✔
Digital certificates (X.509) incl. PKCS #12	5.00	5.00	✔	✔	5.00			5.00	5.00	5.00
Certificate revocation list - CRL	7.00	7.00	✔	✔	6.10				6.10	6.10
Certificate enrollment via SCEP	7.00	7.00	✔	7.00	7.00				7.00	7.00
Simplified RAS with certificates	7.00	7.00	✔	✔	6.20				6.20	6.20
AES 256 / IPCOMP	5.00	5.00	✔	✔	5.00	5.00	5.00	5.00	5.00	5.00
Redundant VPN gateways	4.00	4.00	✔	✔	4.00 [2]	4.00	4.00	4.00	✔	4.00
NAT Traversal (NAT-T)	5.20	5.20	✔	✔	5.20	5.20	5.20	5.20	5.20	5.20
IKE config mode	4.00	4.00	✔	✔	4.00	4.00	4.00	4.00	✔	4.00
WLAN functions										
WLAN-802.11b	✔	✔	✔	✔	✔					
WLAN-802.11g	✔	✔	✔	✔	✔ [6]					
WLAN-802.11a (incl. turbo mode)	✔	✔	✔	✔	✔ [6]					
LEPS	4.00	4.00	✔	✔	4.00					
Multi-SSID, IP-redirect	3.42	3.42	✔	✔	3.42 [3]					
Super A/G	3.42	3.42	✔	✔	3.42[3]					
Standard WEP encryption	4.00	4.00	✔	✔	4.00					
802.11i with HW-AES	3.50	3.50	✔	✔	- / 3.50					
802.11i for P2P in WLAN	4.00	4.00	✔	✔	4.00 [3]					
WLANmonitor	5.00	5.00	✔	✔	5.00					
Group configuration	5.00	5.00	✔	✔	5.00					
Fully transparent client bridge mode	5.00	5.00	✔	✔	5.00 [3]					
Bandwidth limitations in the WLAN	5.20	5.20	✔	✔	5.20					
QoS for WLAN (IEEE 802.11e, WMM/WME)	6.10	6.10	✔	✔	6.10 [3]					
RADIUS server	6.10	6.10	✔	✔	6.10					
VoIP functions (detailed information about your device's VoIP functions can be found in the user manual)										
SIP users	4/8[7]/ 32[8]		8/32[9]	32					4/8[7]/ 32[8]	4/8[7]/ 32[8]
ISDN users	40		40	40					40	40
SIP lines	16		16	16					16	16
Lines to SIP PBXs	4		4	4					4	4

□ *Overview of functions by model and LCOS* version*

	1811	1821	1821+	1823	3050 3550	4000 4100	6000 6001 6021	7011	7111	8011
External ISDN busses for VoIP	1		1	0-1					1	1
Internal ISDN busses for VoIP				0-2					0	0
Analog exchange line connections				0-1						
Connectors for analog terminal equipment				2						
Software options										
ISDN leased line option	Integr. as of 6.10	Integr. as of 6.10	Integr.	Integr.		Integr.	Integr.	Integr.	Integr.	Integr.
Public spot option	✓	✓	✓	✓	✓					
Fax modem option										
VPN-25 Option	✓	✓	✓	✓	✓	✓				
VPN-500 Option										✓
VPN-1000 Option										✓
VoIP basic option	✓		✓						✓	✓
VoIP advanced option	✓		✓						✓	✓
VoIP-32 Option	✓[10]		✓[10]	✓					✓[10]	✓[10]

* The numbers in the table indicate the LCOS version in which the function was implemented

[1] Port separation (private mode)

[2] Only if the VPN options have been activated for the device

[3] Not with 11-Mbit WLAN cards

[4] Optional VPN-500 and VPN-1000 available

[5] Compatible with ADSL and ADSL2

[6] 3050; only with external MC-54 card

[7] depending on VoIP option (Basic/Advanced)

[8] With VoIP Advanced and VoIP-32 Option

[9] With VoIP-32 Option

[10] Requires VoIP Advanced Option

	L-2	IL-2	L-11	IL-11	L-54g	L-54ag IAP	L-54 dual	OAP	XAP
Interfaces									
ADSL modem									
ADSL 2+									
VLAN			✔	✔	✔	✔	✔	✔	✔
DMZ port									
Switch ports							2		
Ethernet port mapping								5.00	
DSLoL	3.10	3.10	3.10	3.10	3.10	3.10	✔		✔
Security									
Stateful Inspection, DoS, IDS	2.80	2.80	2.80	2.80	2.80	2.80	✔	✔	✔
IP QoS, Traffic Shaping	3.30	3.30	3.30	3.30	3.30	3.30	✔	✔	✔
SSH configuration access					4.00	4.00	✔	✔	✔
ISDN-based anti-theft device									
Management									
Rights management for admins					4.00	4.00	✔	✔	✔
Multiple loopback addresses					4.00	4.00	✔	✔	✔
Modem operation at serial interface					4.10	4.10	✔		
Scripting					5.00	5.00	✔	5.00	5.00
CRON	3.10	3.10	3.10	3.10	3.10	3.10	✔	✔	✔
Port monitor								5.00	
Other functions									
Advanced routing and forwarding (ARF networks)					8 7.00	8 7.00	8 7.00	8 7.00	8 7.00
DHCP auto client mode					3.42	3.42	✔	✔	✔
N:N mapping					4.10	4.10	✔	✔	✔
Dynamic DNS	3.10	3.10	3.10	3.10	3.10	3.10	✔	✔	✔
Free port mapping					4.00	4.00	✔	✔	✔
Multi-PPPoE					4.00	4.00	✔	✔	✔
Load balancing									
Policy-based routing					5.00	5.00	✔	5.00	5.00
VRRP					5.20	5.20	✔	5.20	5.20
PPPoE servers					5.20	5.20	✔	5.20	5.20
WAN RIP					5.20	5.20	✔	5.20	5.20
Spanning Tree Protocol					5.20	5.20	✔	5.20	5.20
Layer 2 QoS tagging					6.10	6.10	✔	6.10	6.10
VPN functions									
VPN channels									
VPN hardware acceleration								with VPN-25-Option	
AES, 3-DES, DES, Blowfish, CAST									

	L-2	IL-2	L-11	IL-11	L-54g	L-54ag IAP	L-54 dual	OAP	XAP
Digital certificates (X.509) incl. PKCS #12								5.00	
Certificate revocation list - CRL									
Certificate enrollment via SCEP								7.00	
Simplified RAS with certificates									
AES 256 / IPCOMP								5.00	
Redundant VPN gateways								✔	
NAT Traversal (NAT-T)								5.20	
IKE config mode								✔	
WLAN functions									
WLAN-802.11b	✔	✔	✔	✔	✔	✔	✔	✔	✔
WLAN-802.11g					✔	✔	✔	✔	✔
WLAN-802.11a (incl. turbo mode)						✔	✔	✔	✔
LEPS					4.00	4.00	✔	✔	✔
Multi-SSID, IP-redirect					3.42	3.42	✔	✔	✔
Super A/G					3.42	3.42	✔	✔	✔
Standard WEP encryption					4.00	4.00	✔	✔	✔
802.11i with HW-AES					3.50	3.50	✔	✔	✔
802.11i for P2P in WLAN					4.00	4.00	✔	✔	✔
WLANmonitor					5.00	5.00	✔	5.00	✔
Group configuration					5.00	5.00	✔	5.00	✔
Fully transparent client bridge mode					5.00	5.00	✔	5.00	✔
Bandwidth limitations in the WLAN					5.20	5.20	✔	5.20	✔
QoS for WLAN (IEEE 802.11e, WMM/WME)					6.10	6.10	✔	6.10	✔
RADIUS server					6.10	6.10	✔	6.10	✔
VoIP functions (detailed information about your device's VoIP functions can be found in the user manual)									
SIP users									
ISDN users									
SIP lines									
Lines to SIP PBXs									
External ISDN busses for VoIP									
Internal ISDN busses for VoIP									
Analog exchange line connections									
Connectors for analog terminal equipment									
Software options									
ISDN leased line option		int. as of 6.10		int. as of 6.10					
Public spot option	✔	✔	✔	✔	✔	✔	✔	✔	✔
Fax modem option									
VPN-25 Option								✔	
VPN-500 Option									
VPN-1000 Option									

	L-2	**IL-2**	**L-11**	**IL-11**	**L-54g**	**L-54ag IAP**	**L-54 dual**	**OAP**	**XAP**
VoIP basic option									
VoIP advanced option									
VoIP-32 Option									

* The numbers in the table indicate the LCOS version in which the function was implemented

[1] Port separation (private mode)

[2] Only if the VPN options have been activated for the device

[3] Not with 11-Mbit WLAN cards

[4] Optional VPN-500 and VPN-1000 available

[5] Compatible with ADSL and ADSL2

[6] 3050; only with external MC-54 card

[7] depending on VoIP option (Basic/Advanced)

[8] With VoIP Advanced and VoIP-32 Option

[9] With VoIP-32 Option

[10] Requires VoIP Advanced Option

Index

A Addendum to LCOS-Version 7.7

A.1 Overview

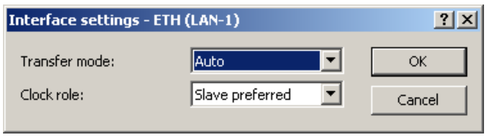
A.2 Extending the temperature range for L-305/310

Some applications require higher operating temperatures than the standard specified temperature range for the access points LANCOM L-305agn and LANCOM L-310agn. The operating temperature range for these two products can be extended to 45° C by limiting the speed of the Gigabit Ethernet interface to 100 Mbps.

As of LCOS version 7.70, the interface speed is automatically reduced to 100 Mbps if the standard maximum operating temperature of 35° C is exceeded. Often, these temperature increases are not long lasting (e.g. during a warm summer's day), so a temporary reduction of transfer rates has little effect on the device's operation.

The settings for the Ethernet port transfer speeds are to be found under the following paths:

LANconfig: Interfaces ▶ LAN ▶ Interface settings



Interface settings - ETH (LAN-1)

Transfer mode: Auto

Clock role: Slave preferred

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces

- **Transfer mode**

  Select the transfer mode for the connection to your local network.

  Possible values:

  □ Automatic, 10 Mbps half-duplex, 10 Mbps full-duplex, 100 Mbps half-duplex, 100 Mbps full-duplex, 100 Mbps automatic, 1000 Mbps full-duplex. The values available for selection here can vary between models.

  Special values:

  □ The setting "Automatic" enables the transfer mode to adapt automatically to the available connection. The maximum available transfer rate common to the two interfaces is taken.

  □ The setting "100 Mbps automatic" corresponds to the setting "Automatic", although the maximum speed that can be negotiated is 100 Mbps. If in doubt, this setting is to be preferred to setting a fixed 100 Mbps, as this avoids potential duplex conflicts.

  Default:

  □ Automatic

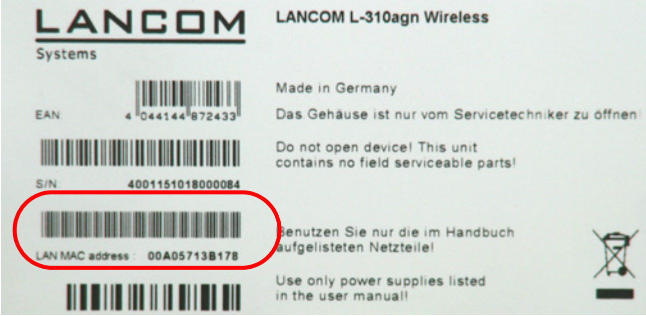
By manually selecting "100 Mbps full-duplex" some models with Gigabit interfaces and temperature sensors can operate within an extended temperature range. With these models, setting transfer mode to "Automatic" limits the speed to 100 Mbps for the time that the temperature inside the device exceeds a device-specific maximum. If the temperature sinks below the threshold, then the higher transfer rate is activated automatically. Interruptions from the re-negotiation of transfer rates is unnoticeable in the WLAN networks. Further information on permissible operating temperatures is to be found in the technical specifications for the device.

A.3 Standard encryption with WPA2

The factory settings (or those after resetting the device) are different in LANCOM access points than in LANCOM wireless routers.

- Unconfigured access points with standard factory settings cannot be commissioned by means of the WLAN interface. The WLAN modules are switched off and the devices search the LAN for a LANCOM WLAN controller which will supply a configuration profile.
- Unconfigured wireless routers with standard factory settings cannot be commissioned by means of the WLAN interface. Furthermore, encryption with WPA-PSK as described here is used as standard.

The preshared key (PSK) for the standard WPA encryption consists of the first letter “L” followed by the LAN MAC address of the access point in ASCII characters. The LAN MAC addresses of the LANCOM devices always begin with the character string “00A057”. You will find the LAN MAC address on a sticker on the base of the device. **Only** use the number labeled as “LAN MAC address” that starts with “00A057”. The other numbers that may be found are **not** the LAN MAC address.



LANCOM Systems

LANCOM L-310agn Wireless

EAN 4 044144 872433

Made in Germany

Das Gehäuse ist nur vom Servicetechniker zu öffnen!

Do not open device! This unit
contains no field serviceable parts!

S/N 4001151018000084

LAN MAC address : 00A05713B178

Benutzen Sie nur die im Handbuch
aufgelisteten Netzteile!

Use only power supplies listed
in the user manual!

A device with the LAN MAC address “00A05713B178” thus has a preshared key of “L00A05713B178”. This key is entered into the ‘WPA or private WEP settings’ of the device for each logical WLAN network as ‘Key 1/Passphrase’.

To use a WLAN adapter to establish a connection to a LANCOM wireless router that has factory settings, the WPA encryption must be activated for the WLAN adapter and the standard 13-character preshared key.

After registering for the first time, change the WPA preshared key to ensure that you have a secure connection.

A.4 APSD – Automatic Power Save Delivery

A.4.1 Introduction

Automatic Power Save Delivery (APSD) is an extension to the IEEE 802.11e standard. APSD is available in two versions:

- Unscheduled APSD (U-APSD)
- Scheduled APSD (S-APSD)

These two methods differ in the way that they use the transmission channels, among others. LANCOM access points and wireless routers support U-APSD, which forms the basis for the WiFi-certified WMM Power Save (WMMPS).

U-APSD allows WLAN devices to save considerable amounts of energy. This function has come into demand due to the increasing use of WLAN-capable telephones (Voice over WLAN – VoWLAN). Activating U-APSD for a wireless LAN enables WLAN devices making calls to switch into "doze mode" while they wait for the next data packet. Transmission of VoIP data takes place in a fixed time pattern—WLAN devices synchronize their phases of activity with this cycle, so that they are ready in good time to receive the next packet. This significantly reduces power consumption and the batteries provide a considerably longer call time.

The precise behavior of the power-saving mode is negotiated between the access point and WLAN client under consideration of the actual application at hand. This makes APSD much more flexible than former power saving methods, referred to in this context as "legacy power save".

A.4.2 Configuration

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ Network

- **APSD**

  Activates APSD power saving for this logical WLAN network.

  Possible values:

  □ On, off

  Default:

  □ Off

Please note that in order for the APSD function to work in a logical WLAN, QoS must be activated on the device. APSD uses mechanisms in QoS to optimize power consumption for the application.

A.4.3 Statistics

WEBconfig: LCOS menu tree ▶ Status ▶ WLAN ▶ Networks

- **APSD**

  Indicates whether APSD is activated or deactivated for the respective WLAN (SSID). APSD is only indicated as active if it is activated in the settings for the logical WLAN and also if the general QoS module is activated.

- **WEBconfig: LCOS menu tree ▶ Status ▶ WLAN ▶ Station table**

  Displays the access categories for which associated WLAN clients are using APSD:

  □ Voice (highest priority)

  □ Video

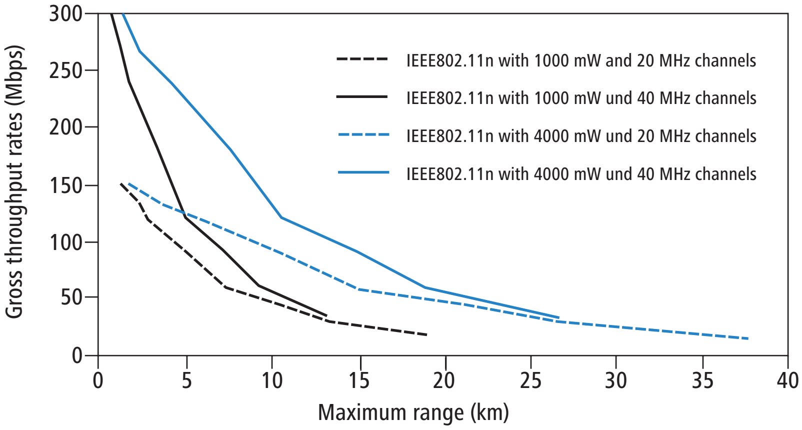
  □ Best effort (including data traffic from legacy power-save clients)

  □ Background (lowest priority).

A.5 BFWA – higher transmission power for longer ranges

BFWA stands for Broadband Fixed Wireless Access. A typical application would be to support a network node that provides Internet to subscribers connected to it. In Germany, the frequencies were provided as part of a general frequency allocation by the German Federal Network Agency. BFWA transmits at a frequency of 5.8 GHz. The maximum permitted transmission power for the operation of BFWA wireless bridges is 4000 mW EIRP (Equivalent Isotropic Radiated Power).

These high transmission powers are the advantage from BFWA. Without BFWA, the maximum permissible transmission power for outdoor WLAN directional radio systems in the 5-GHz band is limited to 1000 mW. This increases the legal transmission power to allow the same directional radio systems to function over significantly longer distances.



LANCOM access points based on 802.11n and all of the current LANCOM 54 Mbps access points support BFWA as of LCOS version 7.70. For older access points, support depends on the chipset (AR-5414 chipset). LANCOM Support can inform you whether these models are able to support BFWA.

For further information see the tech-paper "Broadband Fixed Wireless Access (BFWA)", available for download from www.lancom.eu.

A.6 Restarting RADIUS accounting

The accounting function in the LANCOM can be used to check the budgets of associated wireless LAN clients, among other things. Wireless Internet Service Providers (WISPs) use this option as a part of their accounting procedure. Accounting periods generally switch at the end of the month. A suitable action will cause the accounting session to be restarted at this time. Existing WLAN connections remain intact. A cron job can be used to automate a restart.

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN ▶ RADIUS accounting

- **Restart accounting**

  Terminates all current accounting sessions and opens new accounting sessions on the RADIUS server.

A.7 Voucher for Public Spot with time budget

A.7.1 Introduction

With the Voucher Printing Wizard, setting up time-limited access to a wireless LAN Public Spot takes just a few mouse-clicks. All that is required is to set the access-account time budget; the user name and password are generated automatically and entered into the configuration of the LANCOM device. As a result, a personalized voucher is printed out that contains the information required for a user to register with a wireless LAN Public Spot for a limited period of time.

Users may not want to access the Public Spot WLAN at the moment when the voucher is printed out. For this situation, vouchers can be printed out in advance. The access is set up so that the time budget only starts running when the user logs in for the first time. A maximum period of validity is also defined, after which the access account is automatically deleted, even if the access time budget has not been used up.

Public Spot access with a time limit can only be set up if the LANCOM is set with the correct time.

In LCOS versions prior to 7.70, Public Spot access accounts were entered into the user list for the Public Spot module with the Wizard. As of LCOS version 7.70, the Wizard stores the Public Spot access accounts in the user database of the internal RADIUS server. To be able to use Public Spot access accounts, the RADIUS server has to be configured in the LANCOM. Please observe the notices about this under 'Configuring the RADIUS server to operate a Public Spot' → Page 5.

A.7.2 Setting up Public-Spot users and printing vouchers

To set up a Public-Spot access account, the employee opens a browser and enters the IP address of the wireless router or access point (for example by means of a link on the desktop) and logs in with the appropriate user name and password. If this administrator access account is configured appropriately, the user will only be able add new Public Spot users after starting the Wizard.

① After starting the Wizard, set the time budget for the access.

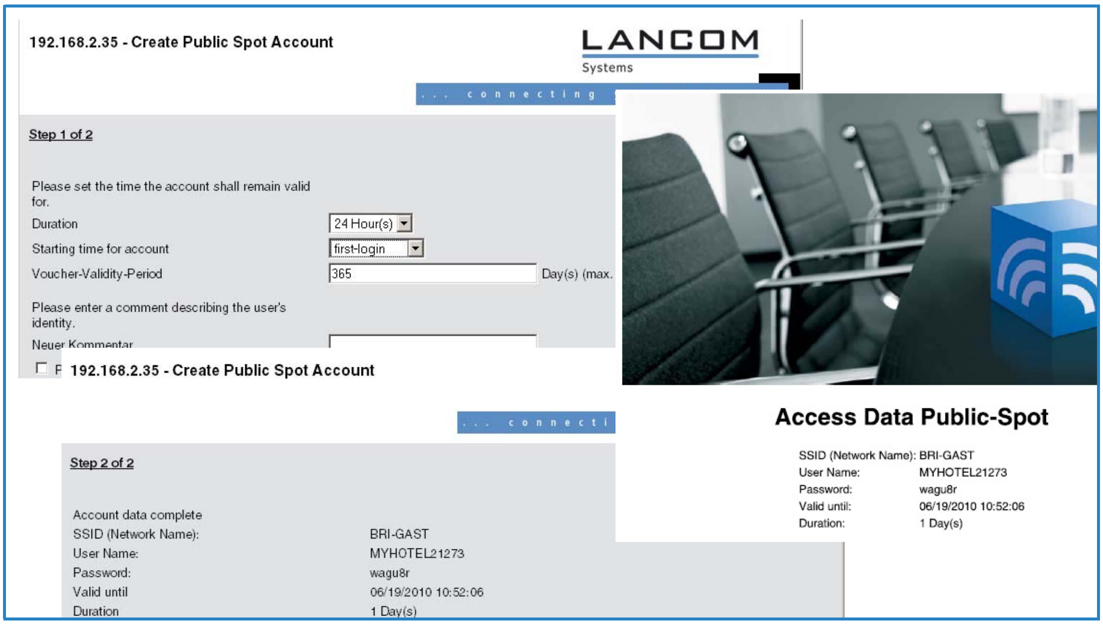
② Select whether the access should be activated immediately or after the first login.

③ If the time budget is only to be consumed after logging in, specify the number of days after which the access account is to expire (validity period).

④ The commentary field gives you the option of entering text to identify the user (e.g. name or room number of the guest). As an alternative to the predefined commentary field, you can use up to five customer-specific commentary fields.

⑤ You then click on **Save and print out user data** to save the access data to the device+ and print it out.

You will find notices on the rights and obligations that apply to operators of Public Spot accesses in the LANCOM White Paper on the subject under www.lancom.eu.



192.168.2.35 - Create Public Spot Account

Step 1 of 2

Please set the time the account shall remain valid for.

Duration: 24 Hour(s)

Starting time for account: first-login

Voucher-Validity-Period: 365 Day(s) (max.

Please enter a comment describing the user's identity.

Neuer Kommentar

192.168.2.35 - Create Public Spot Account

Step 2 of 2

Account data complete

SSID (Network Name): BRI-GAST

User Name: MYHOTEL21273

Password: wagu8r

Valid until: 06/19/2010 10:52:06

Duration: 1 Day(s)

Access Data Public-Spot

SSID (Network Name): BRI-GAST

User Name: MYHOTEL21273

Password: wagu8r

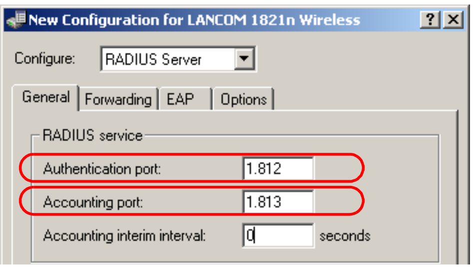
Valid until: 06/19/2010 10:52:06

Duration: 1 Day(s)

A.7.3 Configuring the RADIUS server to operate a Public Spot

In LCOS versions prior to 7.70, Public Spot access accounts were defined by entering users into into the Public Spot module's user list by using the Wizard. As of LCOS version 7.70, the Wizard no longer stores the Public Spot access accounts in this list, but in the user database of the internal RADIUS server instead. In order to use Public Spot access accounts, the RADIUS server **must** be configured and the Public Spot module must be set to use the RADIUS server.

① In order to use the user database in the internal RADIUS server, the RADIUS server in the LANCOM must be activated first. Activate the RADIUS server by entering authentication and accounting ports. Use the authentication port 1,812 and the accounting port 1,813.



New Configuration for LANCOM 1821n Wireless

Configure: RADIUS Server

RADIUS service

Authentication port: 1.812

Accounting port: 1.813

Accounting interim interval: 0 seconds

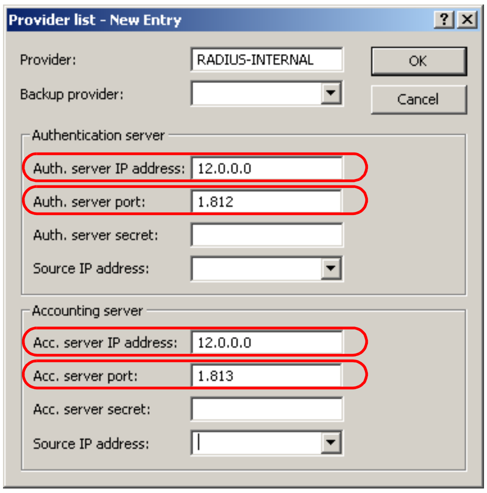
LANconfig: RADIUS ▶ General

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS ▶ Server ▶ Authentication port and Accounting port

② In order for the Public Spot access accounts to be authenticated by the LANCOM's internal RADIUS server, the Public Spot must know the address of the RADIUS server. To ensure that this is the case, create a new entry to define the internal RADIUS server as a "Provider". Enter the IP address for the LANCOM with the activated RADIUS server as the authentication and accounting server.

If the Public Spot and the RADIUS server are provided by the same LANCOM, enter the device's internal loopback address (127.0.0.1) here.

③ Use the authentication and accounting port settings from the RADIUS server (1,812 and 1,813).



Provider list - New Entry

Provider: RADIUS-INTERNAL

Backup provider:

Authentication server

Auth. server IP address: 12.0.0.0

Auth. server port: 1.812

Auth. server secret:

Source IP address:

Accounting server

Acc. server IP address: 12.0.0.0

Acc. server port: 1.813

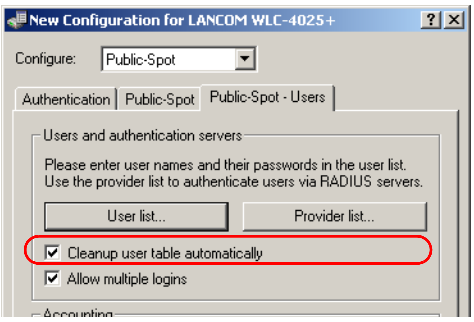
Acc. server secret:

Source IP address:

LANconfig: Public Spot ▶ Public Spot users ▶ Provider list

WEBconfig: LCOS menu tree ▶ Setup ▶ Public Spot module ▶ Port table

④ In the Public Spot module, activate the "Cleanup user table automatically" option to ensure that unwanted entries are automatically deleted.



New Configuration for LANCOM WLC-4025+

Configure: Public-Spot

Users and authentication servers

Please enter user names and their passwords in the user list.
Use the provider list to authenticate users via RADIUS servers.

☑ Cleanup user table automatically

☑ Allow multiple logins

Accounting

LANconfig: Public Spot ▶ Public Spot users

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS ▶ Server

After updating to LCOS 7.70, user accounts created in the Public Spot module's user list with previous versions of LCOS remain valid.

A.7.4 Internal and external RADIUS servers combined

Some companies use an external RADIUS server to authenticate internal WLAN users by IEEE 802.1x. For applications with a WLAN controller and multiple access points, the access points initially address the WLAN controller as their RADIUS server. The WLAN controller then forwards the RADIUS requests to the external RADIUS server.

The settings described below are only necessary if you are operating an external RADIUS server in addition to the Public Spot in the LANCOM.

A Public Spot providing guest-access accounts requires the following settings:

- Authentication requests from internal employees are to be forwarded to an external RADIUS server.
- The authentication requests for Public Spot access accounts are to be handled by the internal RADIUS server.

Realm tagging for RADIUS forwarding

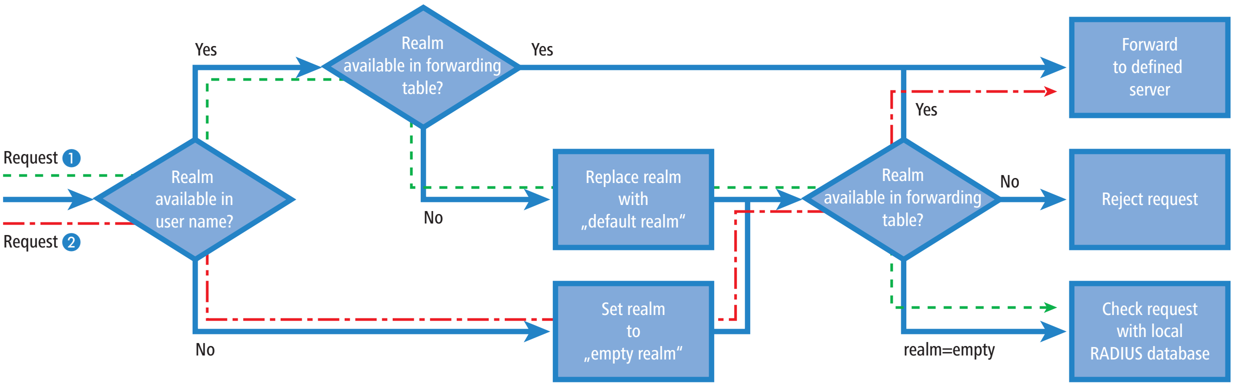
Authentication requests from the two user groups are to be handled separately. The WLAN controller uses what are known as "realms" to differentiate between these two groups. Realms are used for addressing domains, in which user accounts are valid. Realms can be sent with the authentication requests to the WLAN controller's RADIUS server. Alternatively, the RADIUS server can modify the realms in accordance with the following rules for RADIUS forwarding:

- The value defined as the "Default realm" replaces an existing realm of an incoming request, if no forwarding is is defined for this realm.
- The value defined under "empty realm" is used **only if** the incoming user name **does not yet have** a realm.

An entry in the forwarding table causes all authentication requests with a certain realm to be forwarded to a RADIUS server. If no corresponding entry can be found in the forwarding table, the request will be rejected.

If an empty realm is detected, then the authentication request is **always** checked against the LANCOM's internal RADIUS database.

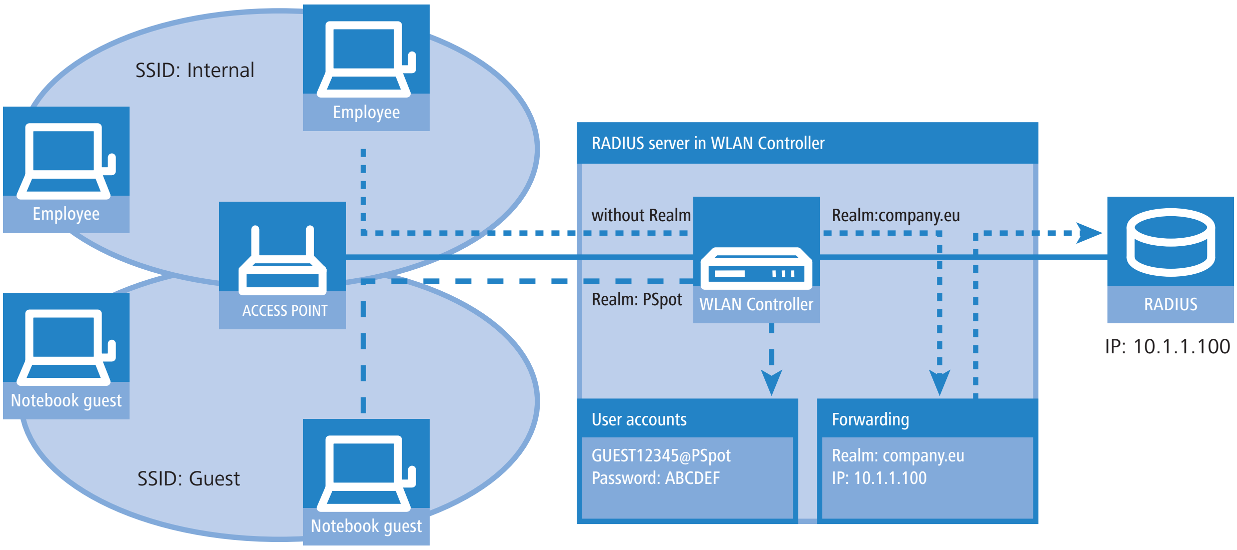
The following flow chart shows the working principle of the RADIUS server when processing realms:


Request 1
Request 2
Realm available in user name?
Yes
No
Realm available in forwarding table?
Yes
No
Replace realm with „default realm"
Set realm to „empty realm"
Realm available in forwarding table?
Yes
No
realm=empty
Forward to defined server
Reject request
Check request with local RADIUS database

Using different realm tags allows different RADIUS servers to be targeted with requests. The decision making process can be tracked in the flow chart.

1. Because the user names for guest access accounts are generated automatically, they can use the realm "PSpot". Because the forwarding table does not contain this entry, all authentication requests with this realm are forwarded to the internal RADIUS server.

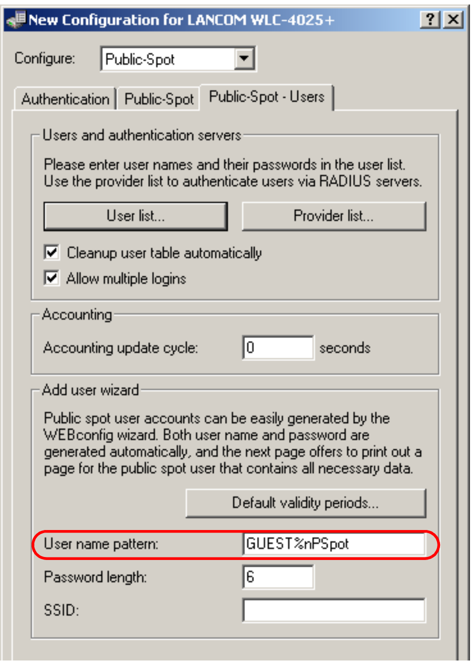
2. To limit the amount of work required for the configuration, internal users are listed without a realm. The RADIUS server in the LANCOM can automatically replace an empty realm with another realm in order to identify internal users. In this example, the empty realm is replaced by the domain of the company "company.eu". The information specified in the forwarding table allows all authentication requests with this realm to be forwarded to the external RADIUS server.



Configuring RADIUS forwarding

The following configuration steps allow you to specify the different manners in which internal users and guests are processed.

① In the Public Spot, adapt the pattern of user names such that a unique realm can be used. For example, the pattern 'GUEST%n@PSpot" generates user names that appear like "GUEST12345@PSpot".



Configure: Public-Spot

Users and authentication servers

Please enter user names and their passwords in the user list. Use the provider list to authenticate users via RADIUS servers.

☑ Cleanup user table automatically

☑ Allow multiple logins

Accounting

Accounting update cycle: 0 seconds

Add user wizard

Public spot user accounts can be easily generated by the WEBconfig wizard. Both user name and password are generated automatically, and the next page offers to print out a page for the public spot user that contains all necessary data.

User name pattern: GUEST%nPSpot

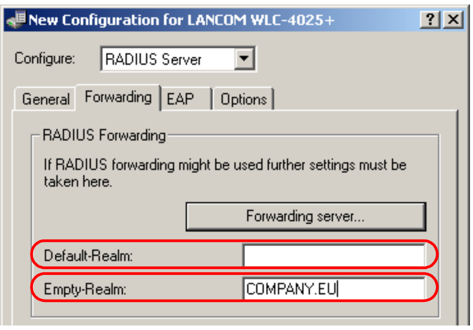
Password length: 6

SSID:

LANconfig: Public Spot ▶ Public Spot users

WEBconfig: LCOS menu tree ▶ Setup ▶ Public Spot module

② In the WLAN controller's RADIUS server, define an "empty realm" (e.g. "COMPANY.EU"). This realm is used for all user names which request authentication from the WLAN controller and which do not already have a realm. In this application, the internal users have no realm defined. In order to prevent the WLAN controllers RADIUS server from inserting a realm, the "Default realm" field must be left empty.



Configure: RADIUS Server

RADIUS Forwarding

If RADIUS forwarding might be used further settings must be taken here.

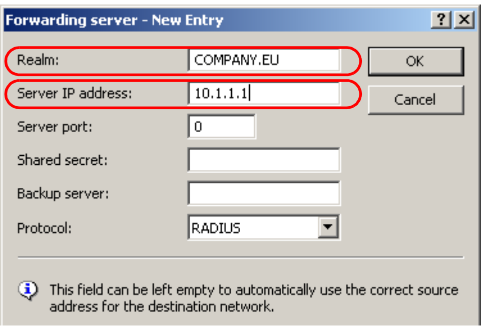
Default-Realm:

Empty-Realm: COMPANY.EU

LANconfig: RADIUS server ▶ Forwarding

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS ▶ Server

③ In order for authentication requests from internal users to be forwarded to the external RADIUS server, suitable entries must be entered into the forwarding settings. The realm "COMPANY.EU" causes all incoming RADIUS requests to be forwarded to the specified IP address.



Realm: COMPANY.EU

Server IP address: 10.1.1.1

Server port: 0

Shared secret:

Backup server:

Protocol: RADIUS

This field can be left empty to automatically use the correct source address for the destination network.

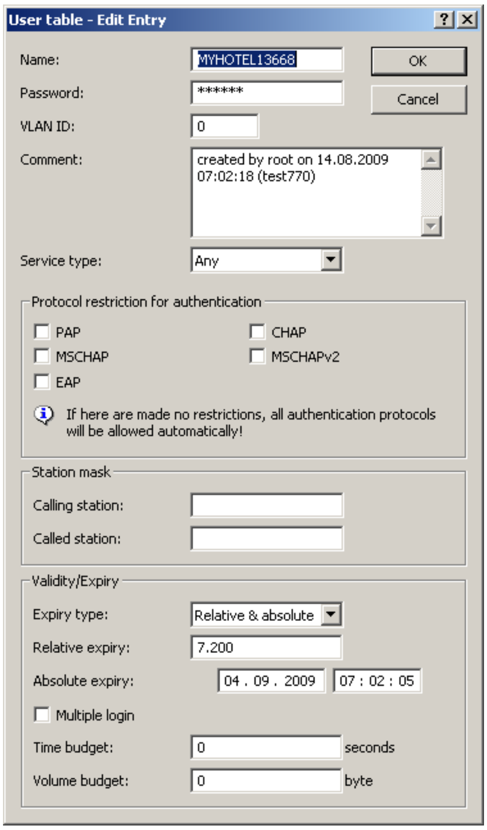
LANconfig: RADIUS server ▶ Forwarding ▶ Forwarding server

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS ▶ Servers ▶ Forward servers

④ Authentication requests from Public Spot users have the realm "@PSpot" and are received by the WLAN Controller. With no forwarding defined for this realm, the usernames are automatically checked with the internal RADIUS database. Because the Public Spot access accounts created with the Wizard are stored in this database, these requests can be authenticated as required.

A.8 Extensions to the RADIUS server

To set up Public Spot users with time and volume budgets, additional parameters have to be entered into the RADIUS server user table.



Name: MYHOTEL13668

Password: ******

VLAN ID: 0

Comment: created by root on 14.08.2009 07:02:18 (test770)

Service type: Any

Protocol restriction for authentication

□ PAP □ CHAP

□ MSCHAP □ MSCHAPv2

□ EAP

If here are made no restrictions, all authentication protocols will be allowed automatically!

Station mask

Calling station:

Called station:

Validity/Expiry

Expiry type: Relative & absolute

Relative expiry: 7.200

Absolute expiry: 04 . 09 . 2009 07 : 02 : 05

□ Multiple login

Time budget: 0 seconds

Volume budget: 0 byte

LANconfig: RADIUS ▶ General ▶ User accounts

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS ▶ Server ▶ Users

- **Multiple logins**

  Allows a single user account to login multiple times simultaneously.

  Possible values:

  □ Yes, No

  Default:

  □ Yes

! The multiple-login option must be deactivated if the RADIUS server is to monitor a time budget. The time budget can only be monitored if the user is running just one session at a time.

- **Expiry type**

  This option defines how the validity period is limited for a user account.

  Possible values:

  □ Absolute: The validity of the user account terminates at a set time.

  □ Relative: The validity of the user account terminates a certain period of time after the first user login.

  Default:

  □ Blank: The user account never expires, unless a predefined time or volume budget expires.

ⓘ The two options can be combined. In this case the user account expires when one of the two limiting values has been reached.

The device must have a valid time in order for the device to work with user-account time budgets.

- **Abs. expiry**

  If "absolute" has been selected as the expiry type, the user account becomes invalid at the time defined by this value.

  Possible values:

  - □ Valid time information (date and time). Max. 20 characters from `0123456789/:.Pp`

  Default:

  - □ Blank

  Special values:

  - □ 0 switches off the monitoring of the absolute expiry time.

- **Rel. expiry**

  If "relative" has been selected as the expiry type, the user account becomes invalid after this time period has expired since the user logged in for the first time.

  Possible values:

  - □ Time span in seconds. Max. 10 characters from `0123456789`

  Default:

  - □ 0

  Special values:

  - □ 0 switches off the monitoring of the relative expiry time.

- **Time budget**

  The maximum duration of access time for this user account. The user can use this duration of access time until a relative or absolute expiry time (if set) is reached.

  Possible values:

  - □ Time span in seconds. Max. 10 characters from `0123456789`

  Default:

  - □ 0

  Special values:

  - □ 0 switches off the monitoring of the time budget.

- **Volume budget**

  The maximum data volume for this user account. The user can use this data volume until a relative or absolute expiry time (if set) is reached.

  Possible values:

  - □ Time span in seconds. Max. 10 characters from `0123456789`

  Default:

  - □ 0

  Special values:

  - □ 0 switches off the monitoring of data volume.

- **Comment**

  Comment on this entry.

- **Service type**

  The service type is a special attribute of the RADIUS protocol. The NAS (Network Access Server) sends this with the authentication request. The response to this request is only positive if the requested service type agrees with the user account service type.

  Possible values:

  - □ Framed: For checking WLAN MAC addresses via RADIUS or IEEE 802.1x.
  - □ Login: For Public-Spot logins.
  - □ Auth. only: For RADIUS authentication of dialup peers via PPP.
  - □ Any

  Default:

  - □ Any

The number of entries permissible with the service type "any" or "login" is 64 or 256, depending on the model. This means that the table is not completely filled with entries for Public Spot access accounts (using the service type "Any") and it enables the parallel use of logins via 802.1x.

A.9 IGMP snooping

A.9.1 Introduction

All LANCOM devices with wireless LAN interfaces feature a "LAN bridge", a software entity for transferring data between the Ethernet ports and the WLAN interface(s). In many ways the LAN bridge works like a switch. The core task of a switch, as opposed to a hub, is to forward packets precisely to the port which the relevant user is connected to. Based on the incoming data packets, the switch automatically creates a table listing the senders' MAC addresses and their ports.

If the table contains the destination address for an incoming packet, the switch forwards the packet to the corresponding port. If the destination address is not in the table, the switch forwards the packet to all ports. This means that a switch can only deliver a packet precisely if the destination address appeared earlier in a packet arriving at a certain port from the sender's address. However, broadcast or multicast packets can never be entered as a sender address into a packet, and so these packets end up being "flooded" to all ports.

This may be the correct action for broadcasts which are supposed to reach all available receivers, but this may not be the case for multicasts. Multicasts are generally aimed at a certain group of receivers within a network, but not all of them:

- For example, video streams are frequently transmitted as multicasts, but not all of the network stations are intended to receive that stream.
- Various applications in the medical field rely on multicasts to send data to certain terminal devices, but this data should not be available to all stations.

A LAN bridge in the LANCOM will have ports to which no multicast recipients are connected. This "unnecessary" transmission of multicasts to ports without any receivers is not an error, but it can compromise overall performance.

- Many stations are unable to reject the unwanted multicasts in their hardware. Instead, the packets are forwarded to higher protocol layers, which leads to an increase in CPU load.
- WLANs are particularly susceptible to bandwidth restrictions due to multicasts if none of the associated WLAN clients want to receive the multicast.

The TCP/IP protocol suite defines a protocol called IGMP that allows network stations to register their desire to receive certain IP multicasts to their router. Stations carry out a multicast registration with their router to subscribe to certain multicast groups which deliver the relevant packets. IGMP makes use of Join messages and Leave messages to register and de-register respectively.

Information about which multicast groups a station can or should join are available from other protocols than IGMP.

As a layer-3 protocol, IGMP only performs multicast guiding/routing for whole IP subnets. However, network devices such as bridges, switches or WLAN access points only forward the packets on layer 2, meaning that IGMP itself does not help in any way to further guide multicast traffic through this substructure. For this reason, the bridges use the multicast registrations between stations and routers to receive additional information for targeting the distribution of multicasts. IP multicasts only need to be forwarded to an interface where a router is located that is capable of multicast routing and therefore of forwarding multicasts to other IP subnets. This method is called IGMP snooping. The bridges, which normally use the MAC on layer 2 for packet forwarding, thus additionally use the layer 3 information in the IP multicast packets.

For more detailed description of the functions of IGMP snooping in LCOS, we have to differentiate between two important terms:

- A port is "member" of a multicast group if at least one station connected to it wishes to receive the packets for a certain multicast address. Multicast registration can be dynamic via IGMP snooping or configured manually.
- A port is a "router port" if it is connected to a router that is capable of multicast routing and therefore of forwarding multicasts to other IP subnets.
- A multicast group is "unregistered" if none of the interfaces attached to the bridge is a member of this multicast group.

A.9.2 IGMP snooping operation

Whenever a packet is received, the bridge initially determines whether it is a unicast, broadcast, or multicast packet. For broadcast and unicast packets, the bridge operates in the usual way, i.e. it floods to all ports or sends to a specific port based on the MAC table entry for the receiver.

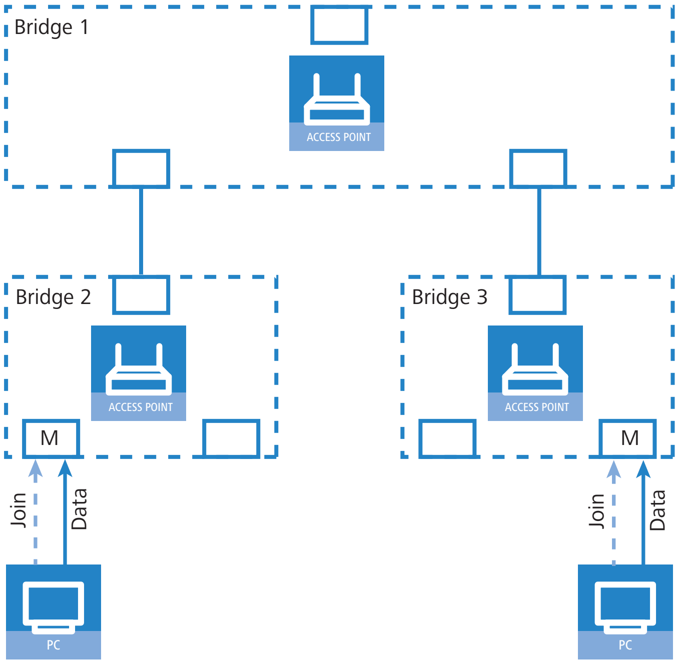
Two types of IP multicast packet are differentiated (whereby packets which are truncated or contain an invalid checksum are discarded entirely):

- IGMP messages are handled in different ways depending on their content:
  - A Join message results in the incoming port becoming member of the respective multicast group. This message is forwarded to router ports only.
  - Similarly, a Leave message results in the incoming port being removed from the multicast group’s member list. This message is also forwarded to router ports only.
  - An incoming IGMP query results in the port being marked as a router port. These messages are flooded to all interfaces.
  - All other messages are flooded to all interfaces—no ports experience a change of state.
- If an IP multicast packet does not contain an IGMP message, the IP destination address is examined. Packets for the destination address "224.0.0.x" are flooded to all ports because this is a "reserved" range. For all other packets the destination address is looked up in the IGMP membership table:
  - If the address is found, the packet is forwarded according to the membership stored in the table.
  - If the address is not found, the packet may either be discarded, flooded to all ports, or forwarded exclusively to all router ports (depending on the configuration).

  In either case, packets are forwarded to all router ports.

A.9.3 IGMP snooping through multiple bridges

As described, IGMP snooping only forwards incoming Join or Leave messages via router ports. In a structure with multiple bridges, initially none of the ports are router ports or members of a multicast group. If a station connected to the bridge registers with a multicast group, the port automatically becomes a member of this group. However, none of the ports are router ports at this phase, so the Join messages are not forwarded anywhere. Other bridges thus receive no information about the port's membership with the multicast group.



Consequently, bridges must have router ports in order for membership information to be propagated. Since the ports of a bridge only become router ports in the case of IGMP queries, one of the multicast-capable routers in the network must take over the task of distributing the necessary IGMP queries throughout the network. This router is referred to as the IGMP querier. If the network does not contain a multicast router, the LANCOM access points are capable of simulating a querier. To avoid parallel queries arriving from various queriers, a querier will deactivate itself if it discovers another querier with a lower IP number. The distribution of IGMP information by the querier can be explained with the following example:

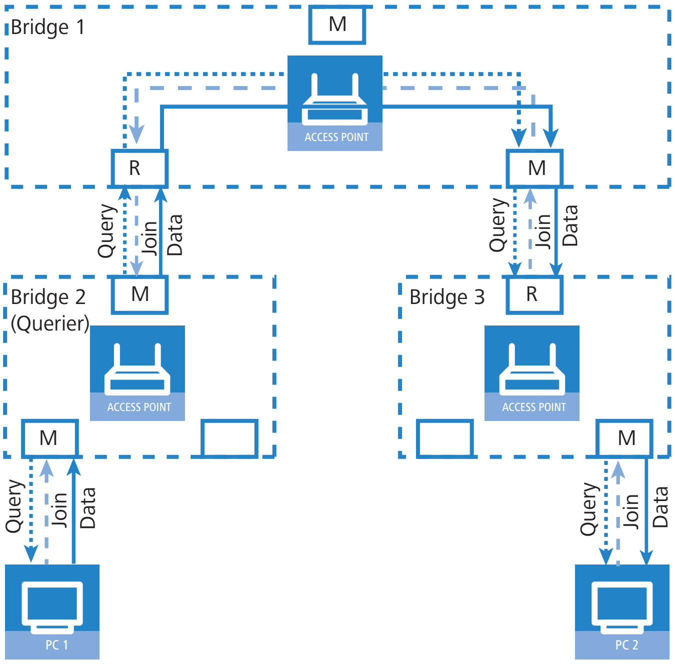
① The querier (Bridge 2 in this example) regularly sends out IGMP queries on all ports of bridge 2 (dotted lines). The next bridge (Bridge 1) receives the query on a port which is then marked as a router port (R). PC 1 responds to this query with a Join message for all multicast groups (light dashed lines) that it wishes to join. The port connecting PC 1 to Bridge 2 then becomes a member of the multicasting group(s).

② In addition to this, Bridge 1 sends the queries on all other ports to the bridges and stations lower down in the structure. In Bridge 3 the port receiving the query becomes a router port (R).

③ The station (PC 2) connected to bridge 3 responds to this query with a Join message for all registered multicast groups. The port connecting PC 2 to Bridge 3 then becomes a member of the multicasting group(s).

④ Bridge 3 forwards this Join message to Bridge 1 over the router port. The receiving port on Bridge 1 thus also takes on membership of the multicast groups that PC 2 has registered for.

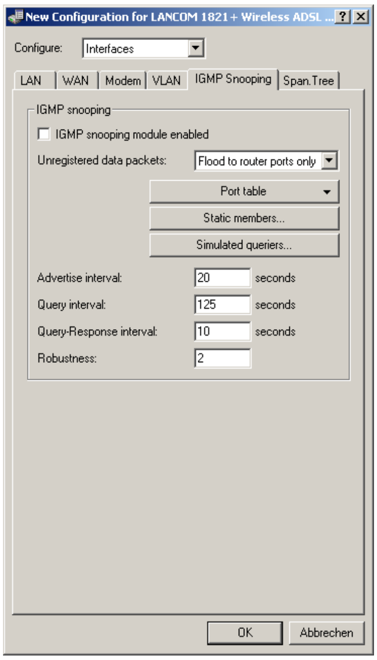
⑤ In the final step, Bridge 1 forwards the Join message from PC 2 via the router port to Bridge 2, where the receiving port also takes on membership of PC 2's multicast groups.



If PC 1 now transmits a multicast for which PC 2 has registered, all of the bridges (2, 1 and then 3) forward the packets to PC 2 via the member port.

A.9.4 Configuration

General settings



New Configuration for LANCOM 1821+ Wireless ADSL ...

Configure: Interfaces

IGMP snooping

□ IGMP snooping module enabled

Unregistered data packets: Flood to router ports only

Advertise interval: 20 seconds

Query interval: 125 seconds

Query-Response interval: 10 seconds

Robustness: 2

LANconfig: Interfaces ▶ IGMP snooping

WEBconfig: LCOS menu tree ▶ Setup ▶ LAN bridge ▶ IGMP snooping

- **Operating**

  Activates or deactivates IGMP snooping in the device and all of the defined querier instances. Without IGMP snooping the bridge functions like a simple switch and forwards all multicasts to all ports.

  Possible values:

  - Yes, No

  Default:

  - No

If this function is deactivated, all IP multicast packets are sent on all ports. If the device operating state changes, the IGMP snooping function is completely reset, i.e. all dynamically learned values are lost (membership, router-port states).

- **Query interval**

  Interval in seconds in which a multicast-capable router (or a simulated querier) sends IGMP queries to the multicast address 224.0.0.1, so prompting the stations to transmit return messages about multicast group memberships. These regular queries influence the time in which memberships age, expire, and are then deleted.

  - After the startup phase, the querier sends IGMP queries in this interval.
  - A querier returns to the querier status after a time equal to "Robustness*Query-Interval+(Query-Response-Interval/2)".
  - A port loses its router-port status after a time equal to "Robustness*Query-Interval+(Query-Response-Interval/2)".

  Possible values:

  - 10-figure number greater than 0.

  Default:

  - 125

The query interval must be greater than the query response interval.

- **Query response interval**

  Interval in seconds influencing the timing between IGMP queries and router-port aging and/or memberships.

Interval in seconds in which a multicast-capable router (or a simulated querier) expects to receive responses to its IGMP queries. These regular queries influence the time in which memberships age, expire, and are then deleted.

Possible values:

- □ 10-figure number greater than 0.

Default:

- □ 10

The query response interval must be less than the query interval.

- **Robustness**

  This value defined the robustness of the IGMP protocol. This option tolerates packet losses of IGMP queries with respect to Join messages.

  Possible values:

  - □ 10-figure number greater than 0.

  Default:

  - □ 2

- **Advertise interval**

  The interval in seconds in which devices send packets advertising themselves as multicast routers. This information makes it quicker for other IGMP-snooping devices to find which of their ports are to operate as router ports. When activating its ports, a switch (for example) can query for multicast routers, and the router can respond to this query with an advertisement of this type. Under some circumstances this method can be much quicker than the alternative IGMP queries.

  Possible values:

  - □ 4 to 180 seconds.

  Default:

  - □ 20

- **Unregistered data packet handling**

  This setting defines the handling of multicast data packets with a destination address outside the 224.0.0.x range and for which neither static memberships were defined nor were dynamic memberships learned.

  Possible values:

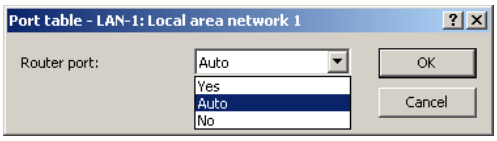
  - □ Router ports only: Sends these packets to all router ports.
  - □ Flood: Sends these packets to all ports.
  - □ Discard: Drops these packets.

  Default:

  - □ Router ports only

Port settings

This table defines the port-related settings for IGMP snooping.



Router port: Auto

LANconfig: Interfaces ▶ IGMP snooping ▶ Port table

WEBconfig: LCOS menu tree ▶ Setup ▶ LAN bridge ▶ IGMP snooping ▶ Port settings

- **Port**

  The port for which the settings apply.

  Possible values:

  - □ Selects a port from the list of those available in the device.

  Default:

  - □ N/A

- **Router port**

  This option defines the port's behavior.

  Possible values:

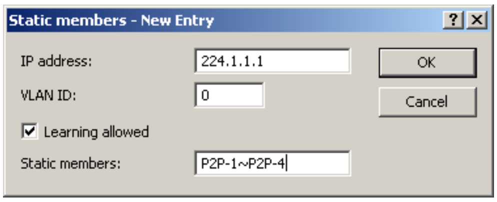
  - Yes: This port will always work as a router port, irrespective of IGMP queries or router messages received at this port.
  - No: This port will never work as a router port, irrespective of IGMP queries or router messages received at this port.
  - Auto: This port will work as a router port if IGMP queries or router messages are received. The port loses this status if no packets are received for the duration of "Robustness*Query-Interval+(Query-Response-Interval/2)".

  Default:

  - Auto

Static members

This table enables members to be defined manually, for example if they cannot or should not be learned automatically.



Static members - New Entry

IP address: 224.1.1.1

VLAN ID: 0

☑ Learning allowed

Static members: P2P-1~P2P-4

LANconfig: Interfaces ▶ IGMP snooping ▶ Static members

WEBconfig: LCOS menu tree ▶ Setup ▶ LAN bridge ▶ IGMP snooping ▶ Static members

- **Address**

  The IP address of the manually defined multicast group.

  Possible values:

  - Valid IP multicast address.

  Default:

  - Blank

- **VLAN ID**

  The VLAN ID which is to support this static member. Each IP multicast address can have multiple entries with different VLAN IDs.

  Possible values:

  - 0 to 4096.

  Default:

  - 0

  Special values:

  - If "0" is selected as VLAN, the IGMP queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

- **Allow learning**

  This option activates the automatic learning of memberships in this multicast group. If automatic learning is deactivated, packets can only be sent via the ports which have been manually defined for the multicast group.

  Possible values:

  - Yes, No.

  Default:

  - Yes

- **Static members**

  These ports will always be the destination for packets with the corresponding IP multicast address, irrespective of any Join messages received.

  Possible values:

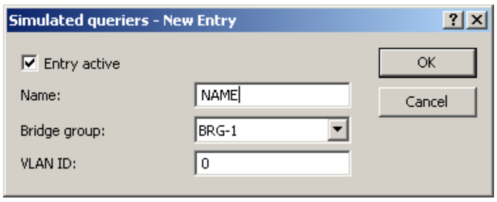
- □ Comma-separated list of the desired ports, max. 215 alphanumerical characters.

Default:

- □ Blank

Simulated queriers

This table contains all of the simulated queriers defined in the device. These units are employed if IGMP functions are required but there is no multicast router in the network. The querier can be limited to certain bridge groups or VLANs by defining multiple independent queriers to support the corresponding VLAN IDs.



Simulated queriers - New Entry

☑ Entry active

Name: NAME

Bridge group: BRG-1

VLAN ID: 0

LANconfig: Interfaces ▶ IGMP snooping ▶ Simulated queriers

WEBconfig: LCOS menu tree ▶ Setup ▶ LAN bridge ▶ IGMP snooping ▶ Simulated queriers

- **Name**

  Name of the querier instance

  Possible values:

  - □ 8 alphanumerical characters.

  Default:

  - □ Blank

- **Operating**

  Activates or deactivates the querier instance

  Possible values:

  - □ Yes, No.

  Default:

  - □ No

- **Bridge group**

  Limits the querier instance to a certain bridge group.

  Possible values:

  - □ Select from the list of available bridge groups.

  Default:

  - □ none

  Special values:

  - □ If bridge group is set to "none", the IGMP queries will the sent via all bridge groups.

- **VLAN ID**

  Limits the querier instance to a certain VLAN.

  Possible values:

  - □ 0 to 4096.

  Default:

  - □ 0

  Special values:

  - □ If "0" is selected as VLAN, the IGMP queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

A.9.5 IGMP status

General statistics

Status messages for IGMP snooping are to be found under the following paths:

WEBconfig: LCOS menu tree ▶ Status ▶ LAN bridge statistics ▶ IGMP snooping

- **Operating**

  Indicates whether IGMP snooping is activated or deactivated.
- **IPv4 packets**

  Shows the number of IPv4 multicast packets received at all ports, whether they were IGMP packets or not.
- **Data packets**

  Shows the number of intact IPv4 multicast packets received at all ports and which were not IGMP packets.
- **Control packets**

  Shows the number of intact IGMP packets received at all ports.
- **Bad packets**

  Shows the number of damaged data or IGMP packets received at all ports. Possible causes for damage to packets may be IP checksum errors or truncated packets.

For performance reasons, IP checksums are evaluated for IGMP packets only and not for the data portion of multicast packets. This is why packets with a faulty checksum in the TCP/UDP or IP header are not detected. These packets are counted as data packets.

- **Deleted values**

  This action deletes all statistical entries.

Port status

This table shows all port-related statistics.

WEBconfig: LCOS menu tree ▶ Status ▶ LAN bridge ▶ IGMP snooping ▶ Port status

- **Router port**

  Shows whether the port is currently in use as a router port or not, irrespective of whether this status was configured statically or learned dynamically.
- **IPv4 packets**

  Shows the number of IPv4 multicast packets received at this port, whether they were IGMP packets or not.
- **Data packets**

  Shows the number of intact IPv4 multicast packets received at this port and which were not IGMP packets.
- **Control packets**

  Shows the number of intact IGMP packets received at this port.
- **Bad packets**

  Shows the number of damaged data or IGMP packets received at this port. Possible causes for damage to packets may be IP checksum errors or truncated packets.

For performance reasons, IP checksums are evaluated for IGMP packets only and not for the data portion of multicast packets. This is why packets with a faulty checksum in the TCP/UDP or IP header are not detected. These packets are counted as data packets.

Groups

This table displays all the the multicast group memberships known to the device, irrespective of whether they were configured statically or learned dynamically. If both static and dynamic memberships exist for a multicast group, these are shown in separate entries.

WEBconfig: LCOS menu tree ▶ Status ▶ LAN bridge ▶ IGMP snooping ▶ Groups

- **Address**

  Shows the group's IP multicast address.
- **VLAN ID**

  Shows the VLAN ID that this entry applies to.
- **Allow learning**

  Shows whether new memberships for this group can be learned dynamically or not.
- **Static members**

  Shows the list of statically defined members for this group.
- **Dynamic members**

  Shows the list of dynamically learned members for this group.

Simulated queriers

This table shows the status of all defined and active IGMP querier instances.

- **Name**

  Shows the name of the multicast group.
- **Bridge group**

  Shows the bridge group that this entry applies to.
- **VLAN ID**

  Shows the VLAN that this entry applies to.
- **Status**

  Shows the current status of the entry.
  - □ Initial: The querier instance has just started and is sending IGMP queries in short intervals (four-times faster than the query interval defined).
  - □ Querier: The querier instance considers itself to be the active querier and is sending IGMP queries in the defined query interval.
  - □ Non-Querier: Another querier instance with a lower IP address has been detected, and the instance listed here is not sending any IGMP queries.

A.10 TACACS+

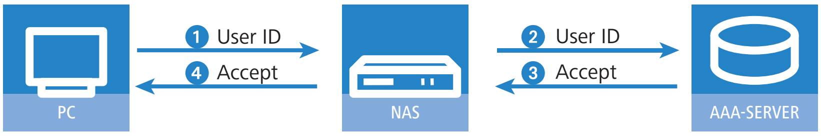
A.10.1 Introduction

Tacacs+ (Terminal Access Controller Access-Control System) is a protocol for authentication, authorization and accounting (AAA). It thus provides access to the network for certain authorized users only, it regulates the rights of those users, and it is a logging mechanism to keep track of user actions. TACACS+ is an alternative to other AAA protocols such as RADIUS.

TACACS+ must be used in order to meet with PCI compliance (Payment Card Industry).

Modern networks with their numerous types of service and network components present a massive challenge in terms of controlling access rights for the user. In large installations in particular, the overhead would be enormous to keep user data consistent on all devices or for all services. For this reason, user data should be managed on a central server.

As a simple example, a user wishes to register at a router and sends the corresponding login details (user ID) to it. In this case the router functions as a Network Access Server (NAS): It does not check the user data itself; rather, the data is forwarded to the central AAA server, which responds by checking the data and answering with an accept or a reject.



The advanced TACACS+ functions include, among others, the option of requesting user to change their passwords after logging in for the first time, or if the password has expired. The corresponding messages are sent from the NAS to the user.

Please note that LANconfig cannot process all of the messages in the extended login dialog. Should LANconfig reject a login attempt at a LANCOM even if the correct data is entered, please use an alternative method of configuration (such as WEBconfig or telnet).

TACACS+ is an alternative AAA server to the widespread RADIUS servers. The following table shows some of the major differences between RADIUS and TACACS+:

TACACS+	RADIUS
Connection-orientated data transfer via TCP	Connectionless data transfer via UDP
Fully encrypted data transfer	Password only encrypted, other content remains unencrypted
Complete separation of authentication, authorization and accounting possible	Authentication and authorization combined

- TCP-based communication with TACACS+ is more reliable than RADIUS. Communications between the NAS and AAA server are confirmed, so the NAS is always informed if the AAA server is unavailable.
- TACACS+ encrypts not only the password like RADIUS but the entire payload data (except for the TACACS+ header). This assures the confidentiality of information such as user names or the permitted services. TACACS+ encryption works with a one-time pad based on MD5 hashes.
- The separation of the three AAA functions enables TACACS+ to operate with multiple servers. Whereas RADIUS always combines authentication and authorization, TACACS+ allows these to be separated. In this way, for example, TACACS+ servers can be employed for authentication only, in that only the users are managed but not the permissible commands.

Please note: Even though TACACS+ is used to centrally manage user accounts on an AAA server, you should ensure that you set a secure password for root access to the LANCOM. If no root password is set, access to the device configuration can be blocked for security reasons if no connection is available to the TACACS+ server. In this case, the device may have to be reset to its factory settings in order to regain access to the configuration.

A.10.2 Configuring the TACACS+ parameters

The parameters for configuring TACACS+ are to be found under the following paths:

WEBconfig: LCOS menu tree ▶ Setup ▶ TACACS+

- **Accounting**

  Activates accounting via TACACS+ server. If TACACS+ accounting is activated, all accounting data is transmitted via TACACS+ protocol to the configured TACACS+ server.

  Possible values:

  □ Activated, deactivated

  Default

  □ Deactivated

TACACS+ accounting will only activate if the defined TACACS+ server is available.

- **Authentication**

  Activates authentication via TACACS+ server. If TACACS+ authentication is activated, all authentication data is transmitted via TACACS+ protocol to the configured TACACS+ server.

  Possible values:

  □ Activated, deactivated

  Default

  □ Deactivated

TACACS+ authentication will only activate if the defined TACACS+ server is available. Fallback to local users is only possible if a root password has been set for the LANCOM. The fallback to local users must be deactivated for devices without a root password. Otherwise a failure of the network connection (TACACS+ server unavailable) would make the LANCOM accessible without a password.

- **Authorization**

  Activates authorization via TACACS+ server. If TACACS+ authorization is activated, all authorization data is transmitted via TACACS+ protocol to the configured TACACS+ server.

  Possible values:

  □ Activated, deactivated

  Default

  □ Deactivated

TACACS+ authorization will only activate if the defined TACACS+ server is available.
If TACACS+ authorization is activated, the TACACS+ server will be queried for authorization each time a user enters a command. Data traffic during configuration will increase correspondingly. Also, the user rights must be defined in the TACACS+ server.

- **Fallback to local users**

  Should the defined TACACS+ server be unavailable, it is possible to fallback to local user accounts on the LANCOM. This allows for access to the device even if the TACACS+ connection should fail, e.g. when deactivating the usage of TACACS+ or for correcting the configuration.

  Possible values:

  □ Allowed, prohibited

  Default

  □ Allowed

The fallback to local user accounts presents a security risk if no root password is set for the LANCOM. For this reason, TACACS+ authentication with fallback to local user accounts can only be activated if a root password has been set. If no root password is set, access to the device configuration can be blocked for security reasons if no connection is available to the TACACS+ server. In this case, the device may have to be reset to its factory settings in order to regain access to the configuration.

- **Shared secret**

  The password for encrypting the communications between NAS and TACACS+ servers.

  Possible values:

  □ 31 alphanumerical characters

  Default

  □ Blank

! The password must be entered identically into the LANCOM and the TACACS+ server. We recommend that you do not operate TACACS+ without encryption.

- **SNMP-GET requests accounting**

  Numerous network management tools use SNMP for requesting information from network devices. LANmonitor also uses SNMP to access the LANCOM devices to display information about current connections, etc., or to execute actions such as disconnecting a connection. SNMP can be used to configure devices. For this reason TACACS+ requires authentication for SNMP access requests. Since LANmonitor regularly queries these values, a large number of unnecessary TACACS+ connections would be established. If authentication, authorization and accounting by TACACS+ are activated, then each request would initiate three sessions with the TACACS+ server.

  This parameter allows the regulation of the behavior of LANCOM devices with regard to SNMP access in order to reduce the number of TACACS+ sessions required for accounting. Authentication via the TACACS+ server remains necessary if authentication for TACACS+ is activated generally.

! Entering a read-only community under LCOS menu tree ▶ Setup ▶ SNMP enables authentication by TACACS+ to be deactivated for LANmonitor. The read-only community defined here is then entered into LANmonitor as a user name.

  Possible values:

  □ only_for_SETUP_tree: With this setting, accounting via TACACS+ server is only required for SNMP access via the setup branch of LCOS.

  □ All: With this setting, accounting by TACACS+ server will be carried out for every SNMP access. In case of regular request for status information, for example, the load on the TACACS+ server will increase significantly.

  □ None: With this setting, accounting by TACACS+ server will not be carried out for SNMP accesses.

  Default:

  □ only_for_SETUP_tree

- **SNMP-GET requests authorization**

  This parameter allows the regulation of the behavior of LANCOM devices with regard to SNMP access in order to reduce the number of TACACS+ sessions required for authorization. Authentication via the TACACS+ server remains necessary if authentication for TACACS+ is activated generally.

  Possible values:

  □ only_for_SETUP_tree: With this setting, authorization via TACACS+ server is only required for SNMP access via the setup branch of LCOS.

- All: With this setting, authorization by TACACS+ server will be carried out for every SNMP access. In case of regular request for status information, for example, the load on the TACACS+ server will increase significantly.
- None: With this setting, authorization by TACACS+ server will not be carried out for SNMP accesses.

Default:

- only_for_SETUP_tree

- **Encryption**

  Activates or deactivates the encryption of communications between NAS and TACACS+ servers.

  Possible values:

  - Activated, deactivated

  Default

  - Activated

! We recommend that you do not operate TACACS+ without encryption. If encryption is activated here, the password for encryption entered here must match with the password on the TACACS+ server.

A.10.3 Configuring the TACACS+ server

Two servers can be defined to work with TACACS+ functions. One server acts as a backup in case the other one fails. When logging in via telnet or WEBconfig, the user can select the server to be used.

The parameters for configuring the TACACS+ server are to be found under the following paths:

WEBconfig: LCOS menu tree ▶ Setup ▶ TACACS+ ▶ Server

- **Server address**

  Address of the TACACS+ server to which requests for authentication, authorization and accounting are to be forwarded.

  Possible values:

  - Valid DNS resolvable name or valid IP address.

  Default

  - Blank

- **Loopback address**

  Optionally you can configure a loopback address here.

  Possible values:

  - Name of the IP networks whose addresses are to be used
  - "INT" for the address of the first intranet.
  - "DMZ" for the address of the first DMZ.
  - LB0 to LBF for the 16 loopback addresses
  - Any valid IP address

  Default

  - Blank

- **Compatibility mode**

  TACACS+ servers are available as open-source or commercial versions, each of which works with different messages. The compatibility mode enables the processing of messages from free TACACS+ servers.

  Possible values:

  - Activated, deactivated

  Default

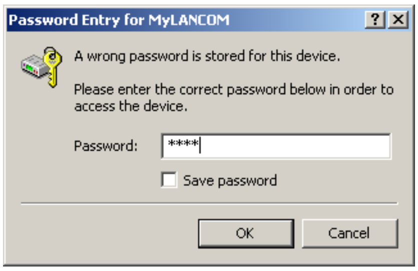
  - Deactivated

A.10.4 Login to the TACACS+ server

Once TACACS+ has been activated for authentication and/or authorization, all logins to the device are redirected to the TACACS+ server. The remaining login procedure differs according to the access method.

TACACS+ login via LANconfig

Using LANconfig to login to a device with activated TACACS+ authentication is only possible with the user named "root". Correspondingly, the user "root" must be configured on the TACACS+ server. To login via LANconfig, enter the password as configured for the user "root" on the TACACS+ server.



Password Entry for MyLANCOM

A wrong password is stored for this device.

Please enter the correct password below in order to access the device.

Password: ****

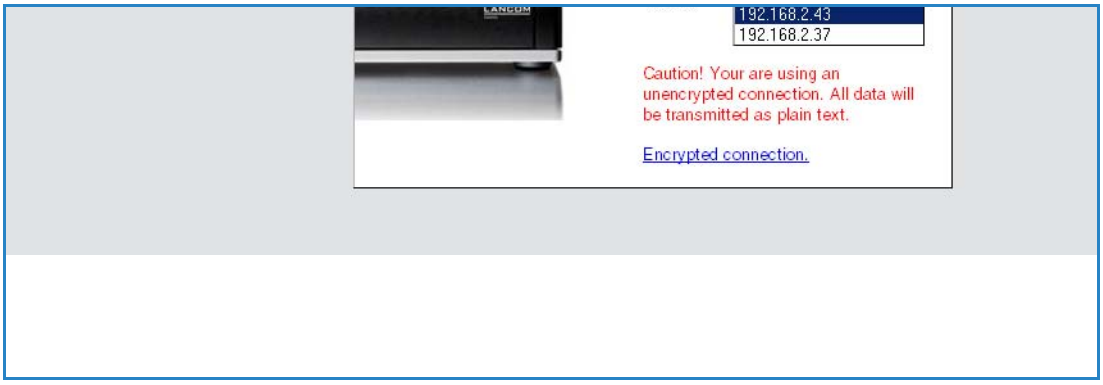
□ Save password

Once authenticated by TACACS+, "root" is the only user automatically assigned with full supervisor rights, and thus able to edit the configuration without having to change privilege level. When authorization is in use, the TACACS+ server decides whether this is allowed or not.

If authorization is activated for the device as well as authentication, the TACACS+ server must permit the commands "readconfig" and "writeconfig" for the user "root" in order for the user to read the configuration from the device and to upload any changes ('Assigning rights under TACACS+' → Page 24).

TACACS+ login via WEBconfig

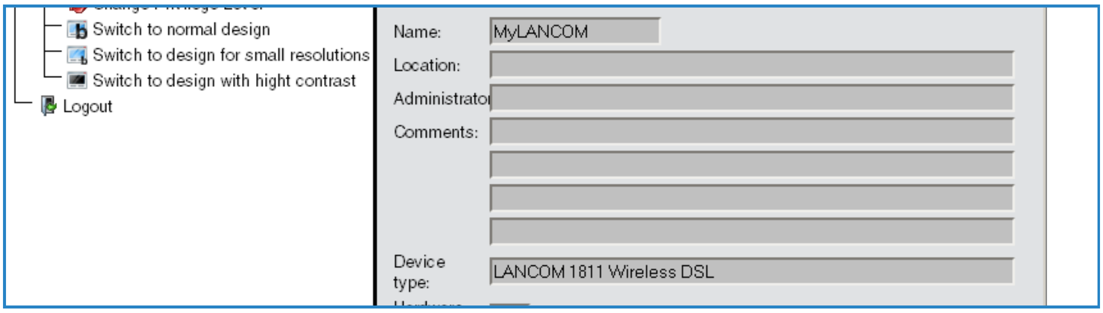
Using WEBconfig to login to a device with activated TACACS+ authentication is possible for any user configured on the TACACS+ server. When logging in with WEBconfig, enter the user name configured on the TACACS+ server and select the server which is to carry out authentication.



192.168.2.43
192.168.2.37

Caution! Your are using an unencrypted connection. All data will be transmitted as plain text.

The corresponding password is requested in the following dialog. After logging in, the user initially sees a reduced WEBconfig user interface. If authorization is not being used, all WEBconfig users (except for the user "root") initially have read rights only.



Switch to normal design
Switch to design for small resolutions
Switch to design with hight contrast
Logout

Name: MyLANCOM

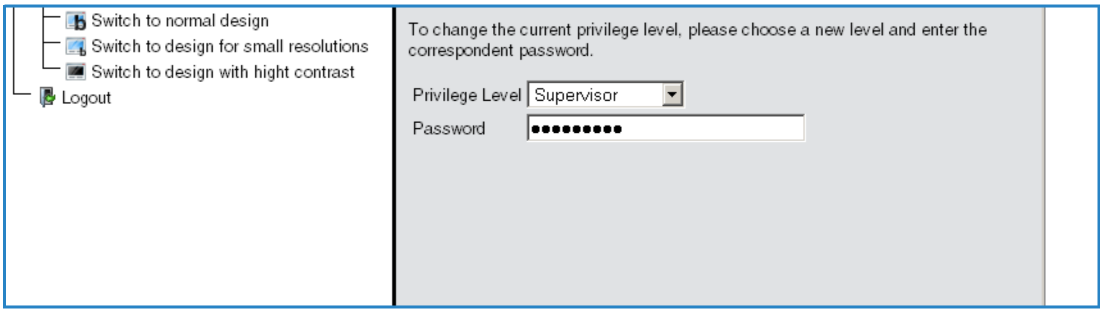
Location:

Administrator

Comments:

Device type: LANCOM 1811 Wireless DSL

To gain further rights, click on the link **Change privilege level** on the left of the screen.



Switch to normal design
Switch to design for small resolutions
Switch to design with hight contrast
Logout

To change the current privilege level, please choose a new level and enter the correspondent password.

Privilege Level: Supervisor

Password: ●●●●●●●●●●

In this dialog you select the required user rights and enter the corresponding password.

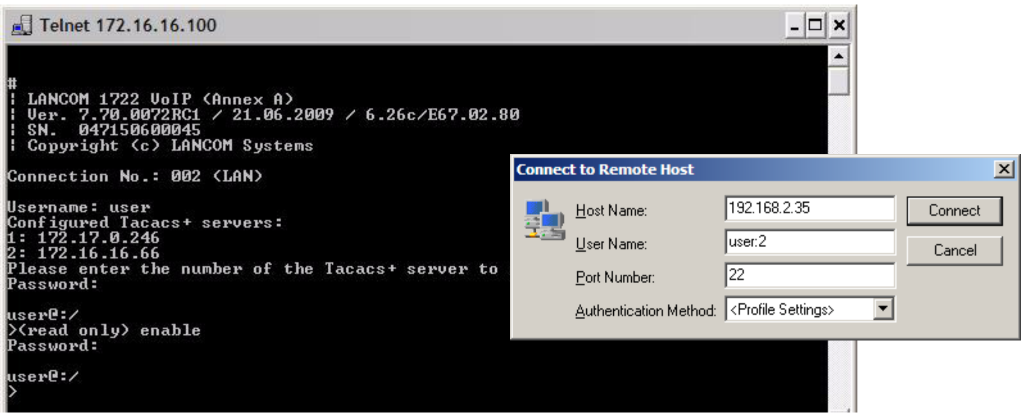
The passwords for individual user rights are configured as "enable" passwords in the TACACS+ server.

If authorization is activated for the device as well as authentication, the TACACS+ server must permit the required commands for each user in order for the user to read and edit the device configuration ('Assigning rights under TACACS+' → Page 24).

TACACS+ login with telnet or SSH

Using tenet or SSH to login to a device with activated TACACS+ authentication is possible for any user configured on the TACACS+ server.

When logging in with telnet, enter the user name configured on the TACACS+ server and select the server which is to carry out authentication. When logging in with SSH, enter the user name followed by a colon and then the server name, i.e. "user:1" or "user:2".



```
#
| LANCOM 1722 VoIP (Annex A)
| Ver. 7.70.0072RC1 / 21.06.2009 / 6.26c/E67.02.80
| SN.  047150600045
| Copyright (c) LANCOM Systems

Connection No.: 002 (LAN)

Username: user
Configured Tacacs+ servers:
1: 172.17.0.246
2: 172.16.16.66
Please enter the number of the Tacacs+ server to
Password:

user@:/
>(read only) enable
Password:

user@:/
>
```

Host Name: 192.168.2.35

User Name: user:2

Port Number: 22

Authentication Method: <Profile Settings>

After login, all users initially have read-rights only (except for the user "root").

To gain further rights, enter the command `enable` and enter the password. Rights will be assigned according to configuration for that password. The parameters for the enable command are the numbers 1-15. 1 is the lowest level, 15 the highest. If no parameter is entered, 15 is taken automatically.

The passwords for individual user rights are configured as "enable" passwords in the TACACS+ server.

If authorization is activated for the device as well as authentication, the TACACS+ server must permit the required commands for each user in order for the user to read and edit the device configuration ('Assigning rights under TACACS+' → Page 24).

A.10.5 Assigning rights under TACACS+

TACACS+ uses privilege levels to separate users into different groups. For the local authorization of users via the "enable" command under telnet/SSH or via privilege levels under WEBconfig, the various administrator rights of LCOS are mapped to the TACACS+ privilege levels:

TACACS+ level	LCOS administrator rights
0	No rights
1	Read only
3	Read-write
5	Read-only limited admin

TACACS+ level	LCOS administrator rights
7	Read-write limited admin
9	Read-only admin
11	Read-write admin
15	Supervisor (root)

A.10.6 Authorizing functions

If authorization is activated for the device as well as authentication, the TACACS+ server must permit the corresponding functions for the user. Enter the required values into the user configuration on the TACACS+ server.

LANconfig

Command	Arguments	Remark
readconfig	none	Read out the entire configuration
writeconfig	none	Write the entire configuration

WEBconfig

Command	Arguments	Remark
delRow	SNMP-ID of the table	Delete row
addRow	SNMP-ID of the table	Add row
editRow	SNMP-ID of the table	Edit row
modifyItem	SNMP-ID of the menu item	Edit a menu item
viewTable	SNMP-ID of the table	View table
viewRow	SNMP-ID of the row	View row
setValue	SNMP-ID of the menu item	Set value of a menu item
listmenu	SNMP-ID of the menu	List sub menu
action	SNMP-ID of the action	Execute an action
reboot	none	Restart device
$URL	none	Display a certain URL

! When working with WEBconfig, all URLs sent to the TACACS+ server during configuration must be enabled. For example, the URL "config2" under WEBconfig provides access to the configuration branch of the LCOS menu tree. Additionally, the individual parameters which the user may edit must also be enabled. You can view the URLs sent by WEBconfig to the TACACS+ server with the trace "trace+ tacacs".

Telnet/SSH

Command	Arguments	Remark
dir	SNMP-ID of the directory	View directory content
list	SNMP-ID of the directory	View directory content
ls	SNMP-ID of the directory	View directory content
llong	SNMP-ID of the directory	View directory content
del	SNMP-ID of the table	Delete row
delete	SNMP-ID of the table	Delete row
rm	SNMP-ID of the table	Delete row
cd	SNMP-ID of the target directory	Change directory
add	SNMP-ID of the table	Add row
tab	SNMP-ID of the table	Changes the order of the columns for adding values
do	SNMP-ID of the action	Execute action
show	Parameter name	View information
trace	Parameter name	Execute trace
time	Parameter name	Time
feature	Parameter name	Add function
repeat	Parameter name	Repeat the command
readmib	none	Read-out SNMP-MIB
readconfig	none	Read out the entire configuration
readstatus	none	Read-out status menu
writefiash	none	Update firmware
activateimage	Parameter name	Activate another firmware image
ping	Parameter name	Start ping
wakeup	Parameter name	Sends wakeup packet
linktest	Parameter name	WLAN link test
writeconfig	none	Write the entire configuration
ll2mdetect	none	Start LL2M detection
ll2mexec	Parameter name	Execute LL2M command
scp	Parameter name	Secure copy
rcp	Parameter name	Secure copy
readscript	Parameter name	Read-out script
beginscript	none	Start script
endscript	none	Stop script
flash	Parameter name	Activate/deactivate flash mode

For telnet access, all of the parameters that the user may edit must be enabled. You can view the values sent by telnet to the TACACS+ server with the trace "trace+ tacacs".

SNMP

Command	Arguments	Remark
get	SNMP-ID of the menu item	Read-out value
set	SNMP-ID of the menu item	Set value

A.11 Sending attachments with the mailto command

E-mails with information on device status can be sent automatically if certain events occur. To do this, just include the mailto command into entries in the action table or cron table.

Attachments can be sent with the e-mails. This allows the results of console commands executed on the device before sending the mail to be sent as an attachment. In this way, the content of tables or menus (e.g. detailed status messages) can be sent by e-mail.

- **Action (action table) or command (cron table) (max. 250 characters)**

  Here you describe the action that is be executed at a certain time or when a change in the status of the WAN connection occurs. Only one action can be triggered per entry.

  Possible values for the actions (max. 250 characters):

  □ mailto: – This prefix causes an e-mail to be sent.

  Optional variables for the actions:

  □ attach=`console command`

  Any console command can be entered which outputs useful information. The console command is enclosed in "backquotes" also known as backticks. This character is produced with the aid of the "accent grave" key.

  The output of the console command is written to a text file for attachment to the mail. This text file is headed by the command and a time/date stamp, followed by the output.

  Default:

  □ Blank

  Examples:

  The following action enables you to sent the ADSL status by e-mail:
  mailto:admin@mycompany.com?subject=ADSL_status?attach=`dir /status/adsl`.

  An action can be used to send mutliple console commands:
  mailto:admin@mycompany.com?subject=Status_reports?attach=`dir /status/adsl`?attach=`dir /status/config`
  The attached files are named 'cmd1.txt', 'cmd2.txt', etc.

A.12 Firmware upload for the UMTS module in the LANCOM 1751 UMTS

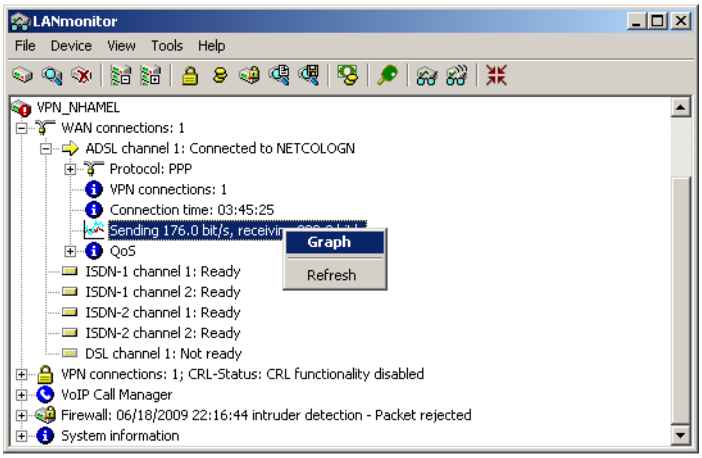
The firmware of the UMTS module in the LANCOM 1751 UMTS can be updated easily as of LCOS version 7.70. Firmware for the UMTS module is available in UPX format and can be uploaded to the LANCOM 1751 UMTS in the same manner as the LANCOM firmware.

A.13 Performance monitoring with LANmonitor

LANmonitor logs various parameters in the devices and displays these graphically:

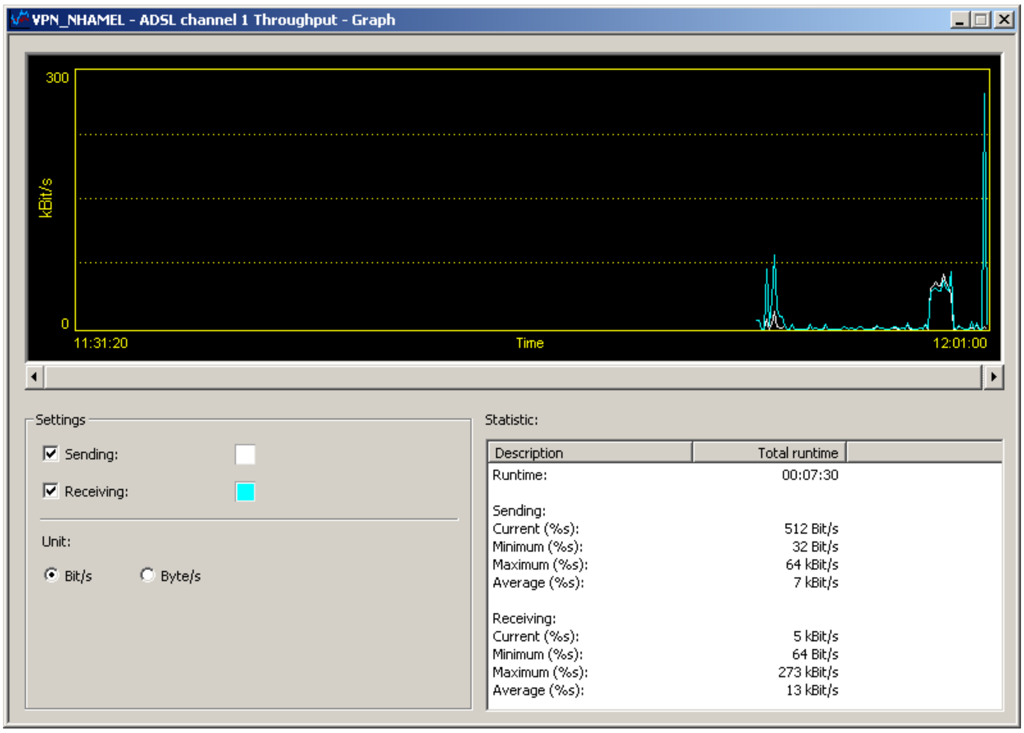
- Transmit and receive rates for WAN connections
- Transmit and receive rates for point-to-point connections
- Signal reception strength for point-to-point connections
- Link signal strength for point-to-point connections
- Throughput for point-to-point connections
- CPU load
- Free memory
- Temperature (not available on all models)

LANmonitor displays the current values directly in the corresponding groups.



VPN_NHAMEL
WAN connections: 1
ADSL channel 1: Connected to NETCOLOGN
Protocol: PPP
VPN connections: 1
Connection time: 03:45:25
Sending 176.0 bit/s, receivi
QoS
ISDN-1 channel 1: Ready
ISDN-1 channel 2: Ready
ISDN-2 channel 1: Ready
ISDN-2 channel 2: Ready
DSL channel 1: Not ready
VPN connections: 1; CRL-Status: CRL functionality disabled
VoIP Call Manager
Firewall: 06/18/2009 22:16:44 intruder detection - Packet rejected
System information

A click on the **Graph** item in the context menu opens a new window which displays these parameters over time.



Settings

☑ Sending: □

☑ Receiving: 🟦

Unit:

● Bit/s ○ Byte/s

Statistic:

Description	Total runtime
Runtime:	00:07:30
Sending:	
Current (%s):	512 Bit/s
Minimum (%s):	32 Bit/s
Maximum (%s):	64 kBit/s
Average (%s):	7 kBit/s
Receiving:	
Current (%s):	5 kBit/s
Minimum (%s):	64 Bit/s
Maximum (%s):	273 kBit/s
Average (%s):	13 kBit/s

You can use the left-hand mouse key to mark any period in the graph, and these statistical values will be displayed separately.

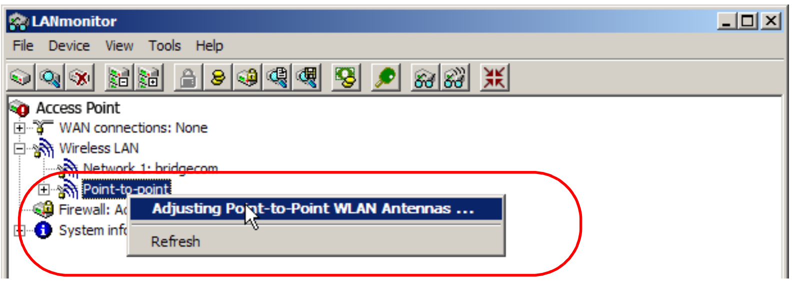
This dialog displays the values collected over the last 24 hours.

Please note that the values on display are deleted when the dialog is closed. For monitoring over a longer period, leave the window open.

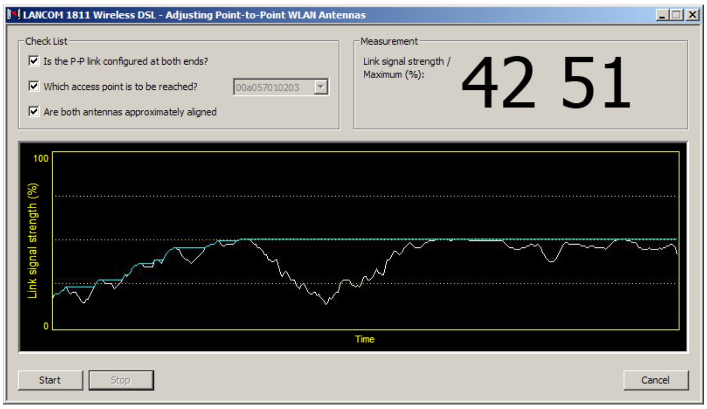
A.14 Setting up point-to-point connections with LANmonitor

To find the best possible alignment for point-to-point connection antennas, the current signal quality over a P2P connection can be displayed on the device's LEDs or in LANmonitor. LANmonitor provides not only an optical display of link strength, but an acoustic signal as well.

In LANmonitor the connection quality display is opened with the context menu. Right-clicking with the mouse on 'Point-to-point' activates the option 'Adjusting Point-to-Point WLAN Antennas...'



Once signal monitoring has commenced, the P2P dialog displays the absolute values for the current signal strength and the maximum value since starting the measurement. The development of the signal strength over time and the maximum value are displayed in a diagram, too.



LANCOM 1811 Wireless DSL - Adjusting Point-to-Point WLAN Antennas

Check List

☑ Is the P-P link configured at both ends?

☑ Which access point is to be reached? 00a057010203

☑ Are both antennas approximately aligned

Measurement

Link signal strength / Maximum (%): 42 51

Initially only one of the two antennas should be adjusted until a maximum value is achieved. This first antenna is then fixed and the second antenna is then adjusted to attain the best signal quality.

An acoustic signal can be activated to help align the antennas precisely. With this option, the PC can emit a tone which varies according to signal strength. Maximum signal strength over the link is signaled by a constant tone. If the signal strength drops below the maximum, tones are emitted at intervals indicating the difference from the former maximum. The shorter the interval, the closer the current link signal strength is to the maximum.

A Addendum to LCOS-Version 7.7

A.1 Overview

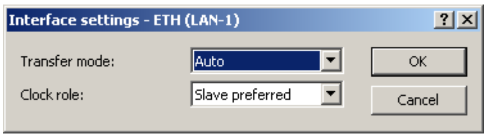
A.2 Extending the temperature range for L-305/310

Some applications require higher operating temperatures than the standard specified temperature range for the access points LANCOM L-305agn and LANCOM L-310agn. The operating temperature range for these two products can be extended to 45° C by limiting the speed of the Gigabit Ethernet interface to 100 Mbps.

As of LCOS version 7.70, the interface speed is automatically reduced to 100 Mbps if the standard maximum operating temperature of 35° C is exceeded. Often, these temperature increases are not long lasting (e.g. during a warm summer's day), so a temporary reduction of transfer rates has little effect on the device's operation.

The settings for the Ethernet port transfer speeds are to be found under the following paths:

LANconfig: Interfaces ▶ LAN ▶ Interface settings



Interface settings - ETH (LAN-1)

Transfer mode: Auto

Clock role: Slave preferred

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces

- **Transfer mode**

  Select the transfer mode for the connection to your local network.

  Possible values:

  □ Automatic, 10 Mbps half-duplex, 10 Mbps full-duplex, 100 Mbps half-duplex, 100 Mbps full-duplex, 100 Mbps automatic, 1000 Mbps full-duplex. The values available for selection here can vary between models.

  Special values:

  □ The setting "Automatic" enables the transfer mode to adapt automatically to the available connection. The maximum available transfer rate common to the two interfaces is taken.

  □ The setting "100 Mbps automatic" corresponds to the setting "Automatic", although the maximum speed that can be negotiated is 100 Mbps. If in doubt, this setting is to be preferred to setting a fixed 100 Mbps, as this avoids potential duplex conflicts.

  Default:

  □ Automatic

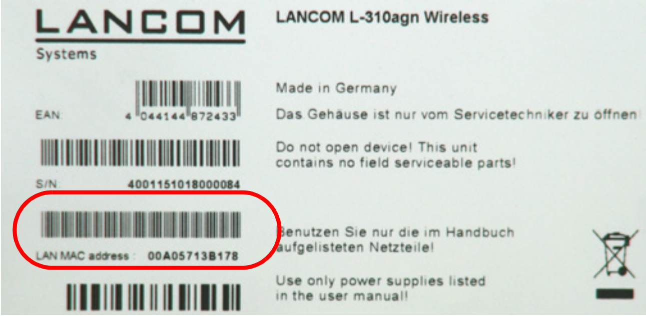
By manually selecting "100 Mbps full-duplex" some models with Gigabit interfaces and temperature sensors can operate within an extended temperature range. With these models, setting transfer mode to "Automatic" limits the speed to 100 Mbps for the time that the temperature inside the device exceeds a device-specific maximum. If the temperature sinks below the threshold, then the higher transfer rate is activated automatically. Interruptions from the re-negotiation of transfer rates is unnoticeable in the WLAN networks. Further information on permissible operating temperatures is to be found in the technical specifications for the device.

A.3 Standard encryption with WPA2

The factory settings (or those after resetting the device) are different in LANCOM access points than in LANCOM wireless routers.

- Unconfigured access points with standard factory settings cannot be commissioned by means of the WLAN interface. The WLAN modules are switched off and the devices search the LAN for a LANCOM WLAN controller which will supply a configuration profile.
- Unconfigured wireless routers with standard factory settings cannot be commissioned by means of the WLAN interface. Furthermore, encryption with WPA-PSK as described here is used as standard.

The preshared key (PSK) for the standard WPA encryption consists of the first letter "L" followed by the LAN MAC address of the access point in ASCII characters. The LAN MAC addresses of the LANCOM devices always begin with the character string "00A057". You will find the LAN MAC address on a sticker on the base of the device. **Only** use the number labeled as "LAN MAC address" that starts with "00A057". The other numbers that may be found are **not** the LAN MAC address.



LANCOM Systems

LANCOM L-310agn Wireless

EAN: 4 044144 872433

S/N: 4001151018000084

LAN MAC address: 00A05713B178

Made in Germany

Das Gehäuse ist nur vom Servicetechniker zu öffnen!

Do not open device! This unit contains no field serviceable parts!

Benutzen Sie nur die im Handbuch aufgelisteten Netzteile!

Use only power supplies listed in the user manual!

A device with the LAN MAC address "00A05713B178" thus has a preshared key of "L00A05713B178". This key is entered into the 'WPA or private WEP settings' of the device for each logical WLAN network as 'Key 1/Passphrase'.

To use a WLAN adapter to establish a connection to a LANCOM wireless router that has factory settings, the WPA encryption must be activated for the WLAN adapter and the standard 13-character preshared key.

After registering for the first time, change the WPA preshared key to ensure that you have a secure connection.

A.4 APSD – Automatic Power Save Delivery

A.4.1 Introduction

Automatic Power Save Delivery (APSD) is an extension to the IEEE 802.11e standard. APSD is available in two versions:

- Unscheduled APSD (U-APSD)
- Scheduled APSD (S-APSD)

These two methods differ in the way that they use the transmission channels, among others. LANCOM access points and wireless routers support U-APSD, which forms the basis for the WiFi-certified WMM Power Save (WMMPS).

U-APSD allows WLAN devices to save considerable amounts of energy. This function has come into demand due to the increasing use of WLAN-capable telephones (Voice over WLAN – VoWLAN). Activating U-APSD for a wireless LAN enables WLAN devices making calls to switch into "doze mode" while they wait for the next data packet. Transmission of VoIP data takes place in a fixed time pattern—WLAN devices synchronize their phases of activity with this cycle, so that they are ready in good time to receive the next packet. This significantly reduces power consumption and the batteries provide a considerably longer call time.

The precise behavior of the power-saving mode is negotiated between the access point and WLAN client under consideration of the actual application at hand. This makes APSD much more flexible than former power saving methods, referred to in this context as "legacy power save".

A.4.2 Configuration

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ Network

- **APSD**

  Activates APSD power saving for this logical WLAN network.

  Possible values:

  □ On, off

  Default:

  □ Off

Please note that in order for the APSD function to work in a logical WLAN, QoS must be activated on the device. APSD uses mechanisms in QoS to optimize power consumption for the application.

A.4.3 Statistics

WEBconfig: LCOS menu tree ▶ Status ▶ WLAN ▶ Networks

- **APSD**

  Indicates whether APSD is activated or deactivated for the respective WLAN (SSID). APSD is only indicated as active if it is activated in the settings for the logical WLAN and also if the general QoS module is activated.

- **WEBconfig: LCOS menu tree ▶ Status ▶ WLAN ▶ Station table**

  Displays the access categories for which associated WLAN clients are using APSD:

  □ Voice (highest priority)

  □ Video

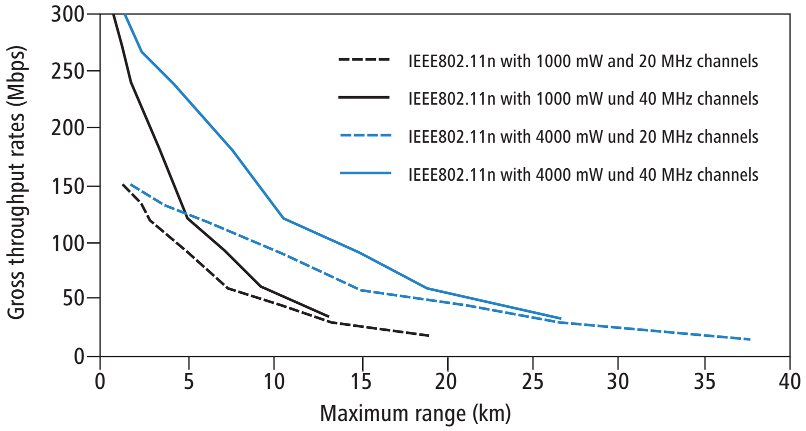
  □ Best effort (including data traffic from legacy power-save clients)

  □ Background (lowest priority).

A.5 BFWA – higher transmission power for longer ranges

BFWA stands for Broadband Fixed Wireless Access. A typical application would be to support a network node that provides Internet to subscribers connected to it. In Germany, the frequencies were provided as part of a general frequency allocation by the German Federal Network Agency. BFWA transmits at a frequency of 5.8 GHz. The maximum permitted transmission power for the operation of BFWA wireless bridges is 4000 mW EIRP (Equivalent Isotropic Radiated Power).

These high transmission powers are the advantage from BFWA. Without BFWA, the maximum permissible transmission power for outdoor WLAN directional radio systems in the 5-GHz band is limited to 1000 mW. This increases the legal transmission power to allow the same directional radio systems to function over significantly longer distances.



LANCOM access points based on 802.11n and all of the current LANCOM 54 Mbps access points support BFWA as of LCOS version 7.70. For older access points, support depends on the chipset (AR-5414 chipset). LANCOM Support can inform you whether these models are able to support BFWA.

For further information see the tech-paper "Broadband Fixed Wireless Access (BFWA)", available for download from www.lancom.eu.

A.6 Restarting RADIUS accounting

The accounting function in the LANCOM can be used to check the budgets of associated wireless LAN clients, among other things. Wireless Internet Service Providers (WISPs) use this option as a part of their accounting procedure. Accounting periods generally switch at the end of the month. A suitable action will cause the accounting session to be restarted at this time. Existing WLAN connections remain intact. A cron job can be used to automate a restart.

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN ▶ RADIUS accounting

- **Restart accounting**

  Terminates all current accounting sessions and opens new accounting sessions on the RADIUS server.

A.7 Voucher for Public Spot with time budget

A.7.1 Introduction

With the Voucher Printing Wizard, setting up time-limited access to a wireless LAN Public Spot takes just a few mouse-clicks. All that is required is to set the access-account time budget; the user name and password are generated automatically and entered into the configuration of the LANCOM device. As a result, a personalized voucher is printed out that contains the information required for a user to register with a wireless LAN Public Spot for a limited period of time.

Users may not want to access the Public Spot WLAN at the moment when the voucher is printed out. For this situation, vouchers can be printed out in advance. The access is set up so that the time budget only starts running when the user logs in for the first time. A maximum period of validity is also defined, after which the access account is automatically deleted, even if the access time budget has not been used up.

Public Spot access with a time limit can only be set up if the LANCOM is set with the correct time.

In LCOS versions prior to 7.70, Public Spot access accounts were entered into the user list for the Public Spot module with the Wizard. As of LCOS version 7.70, the Wizard stores the Public Spot access accounts in the user database of the internal RADIUS server. To be able to use Public Spot access accounts, the RADIUS server has to be configured in the LANCOM. Please observe the notices about this under 'Configuring the RADIUS server to operate a Public Spot' → Page 5.

A.7.2 Setting up Public- Spot users and printing vouchers

To set up a Public-Spot access account, the employee opens a browser and enters the IP address of the wireless router or access point (for example by means of a link on the desktop) and logs in with the appropriate user name and password. If this administrator access account is configured appropriately, the user will only be able add new Public Spot users after starting the Wizard.

① After starting the Wizard, set the time budget for the access.

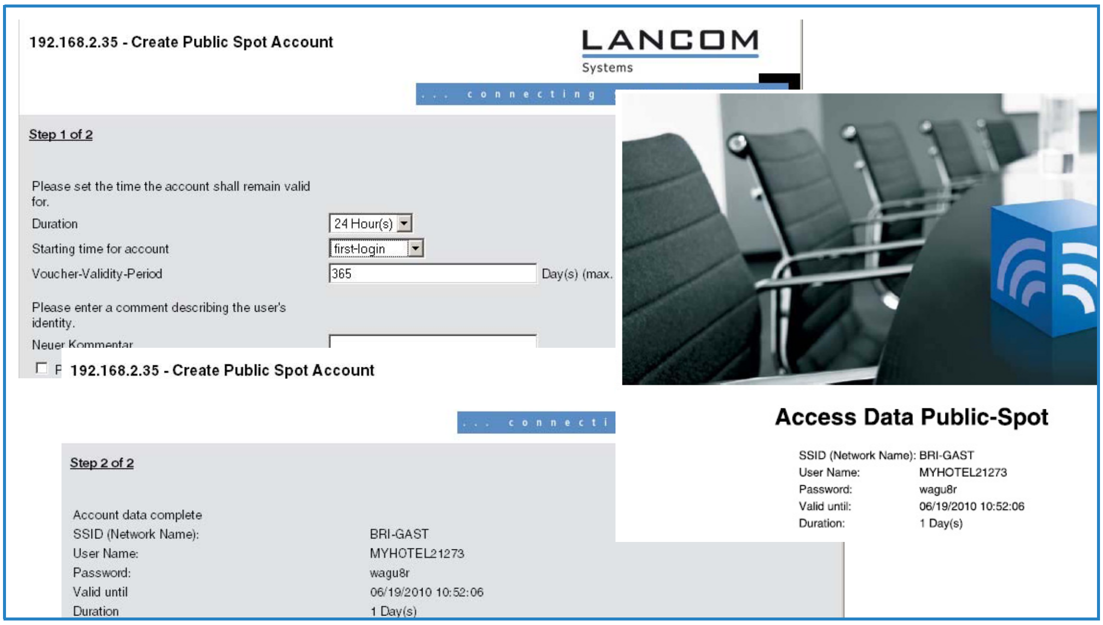
② Select whether the access should be activated immediately or after the first login.

③ If the time budget is only to be consumed after logging in, specify the number of days after which the access account is to expire (validity period).

④ The commentary field gives you the option of entering text to identify the user (e.g. name or room number of the guest). As an alternative to the predefined commentary field, you can use up to five customer-specific commentary fields.

⑤ You then click on **Save and print out user data** to save the access data to the device+ and print it out.

You will find notices on the rights and obligations that apply to operators of Public Spot accesses in the LANCOM White Paper on the subject under www.lancom.eu.



192.168.2.35 - Create Public Spot Account

Step 1 of 2

Please set the time the account shall remain valid for.

Duration: 24 Hour(s)

Starting time for account: first-login

Voucher-Validity-Period: 365 Day(s) (max.

Please enter a comment describing the user's identity.

Neuer Kommentar

☐ F

192.168.2.35 - Create Public Spot Account

Step 2 of 2

Account data complete

SSID (Network Name): BRI-GAST

User Name: MYHOTEL21273

Password: wagu8r

Valid until: 06/19/2010 10:52:06

Duration: 1 Day(s)

Access Data Public-Spot

SSID (Network Name): BRI-GAST

User Name: MYHOTEL21273

Password: wagu8r

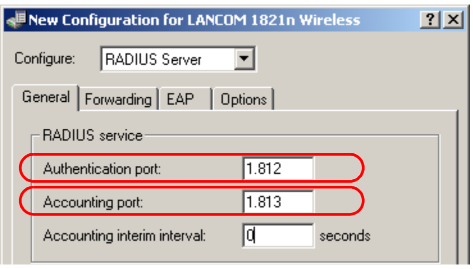
Valid until: 06/19/2010 10:52:06

Duration: 1 Day(s)

A.7.3 Configuring the RADIUS server to operate a Public Spot

In LCOS versions prior to 7.70, Public Spot access accounts were defined by entering users into into the Public Spot module's user list by using the Wizard. As of LCOS version 7.70, the Wizard no longer stores the Public Spot access accounts in this list, but in the user database of the internal RADIUS server instead. In order to use Public Spot access accounts, the RADIUS server **must** be configured and the Public Spot module must be set to use the RADIUS server.

① In order to use the user database in the internal RADIUS server, the RADIUS server in the LANCOM must be activated first. Activate the RADIUS server by entering authentication and accounting ports. Use the authentication port 1,812 and the accounting port 1,813.



New Configuration for LANCOM 1821n Wireless

Configure: RADIUS Server

RADIUS service

Authentication port: 1.812

Accounting port: 1.813

Accounting interim interval: 0 seconds

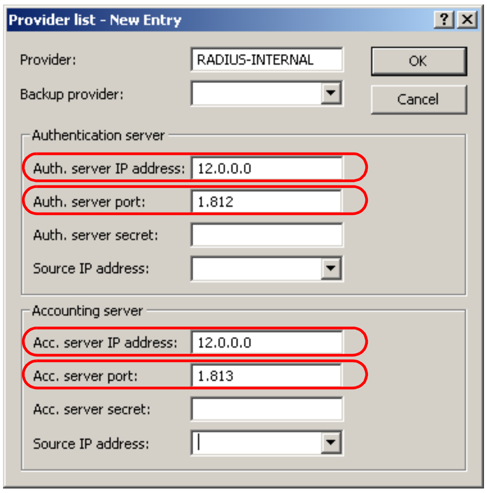
LANconfig: RADIUS ▶ General

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS ▶ Server ▶ Authentication port and Accounting port

② In order for the Public Spot access accounts to be authenticated by the LANCOM's internal RADIUS server, the Public Spot must know the address of the RADIUS server. To ensure that this is the case, create a new entry to define the internal RADIUS server as a "Provider". Enter the IP address for the LANCOM with the activated RADIUS server as the authentication and accounting server.

! If the Public Spot and the RADIUS server are provided by the same LANCOM, enter the device's internal loopback address (127.0.0.1) here.

③ Use the authentication and accounting port settings from the RADIUS server (1,812 and 1,813).



Provider list - New Entry

Provider: RADIUS-INTERNAL

Backup provider:

Authentication server

Auth. server IP address: 12.0.0.0

Auth. server port: 1.812

Auth. server secret:

Source IP address:

Accounting server

Acc. server IP address: 12.0.0.0

Acc. server port: 1.813

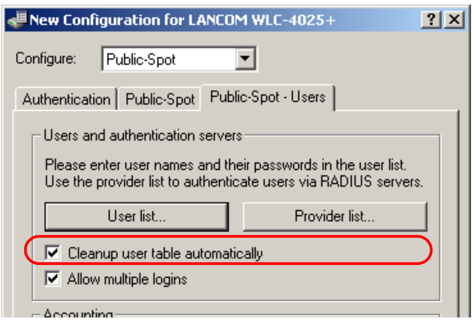
Acc. server secret:

Source IP address:

LANconfig: Public Spot ▶ Public Spot users ▶ Provider list

WEBconfig: LCOS menu tree ▶ Setup ▶ Public Spot module ▶ Port table

④ In the Public Spot module, activate the "Cleanup user table automatically" option to ensure that unwanted entries are automatically deleted.



New Configuration for LANCOM WLC-4025+

Configure: Public-Spot

Users and authentication servers

Please enter user names and their passwords in the user list.
Use the provider list to authenticate users via RADIUS servers.

☑ Cleanup user table automatically

☑ Allow multiple logins

Accounting

LANconfig: Public Spot ▶ Public Spot users

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS ▶ Server

After updating to LCOS 7.70, user accounts created in the Public Spot module's user list with previous versions of LCOS remain valid.

A.7.4 Internal and external RADIUS servers combined

Some companies use an external RADIUS server to authenticate internal WLAN users by IEEE 802.1x. For applications with a WLAN controller and multiple access points, the access points initially address the WLAN controller as their RADIUS server. The WLAN controller then forwards the RADIUS requests to the external RADIUS server.

The settings described below are only necessary if you are operating an external RADIUS server in addition to the Public Spot in the LANCOM.

A Public Spot providing guest-access accounts requires the following settings:

- Authentication requests from internal employees are to be forwarded to an external RADIUS server.
- The authentication requests for Public Spot access accounts are to be handled by the internal RADIUS server.

Realm tagging for RADIUS forwarding

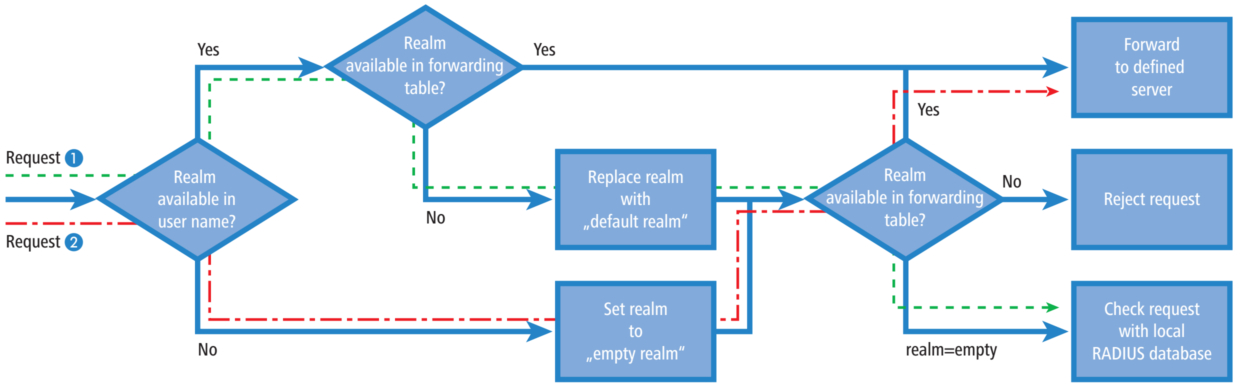
Authentication requests from the two user groups are to be handled separately. The WLAN controller uses what are known as "realms" to differentiate between these two groups. Realms are used for addressing domains, in which user accounts are valid. Realms can be sent with the authentication requests to the WLAN controller's RADIUS server. Alternatively, the RADIUS server can modify the realms in accordance with the following rules for RADIUS forwarding:

- The value defined as the "Default realm" replaces an existing realm of an incoming request, if no forwarding is is defined for this realm.
- The value defined under "empty realm" is used **only if** the incoming user name **does not yet have** a realm.

An entry in the forwarding table causes all authentication requests with a certain realm to be forwarded to a RADIUS server. If no corresponding entry can be found in the forwarding table, the request will be rejected.

! If an empty realm is detected, then the authentication request is **always** checked against the LANCOM's internal RADIUS database.

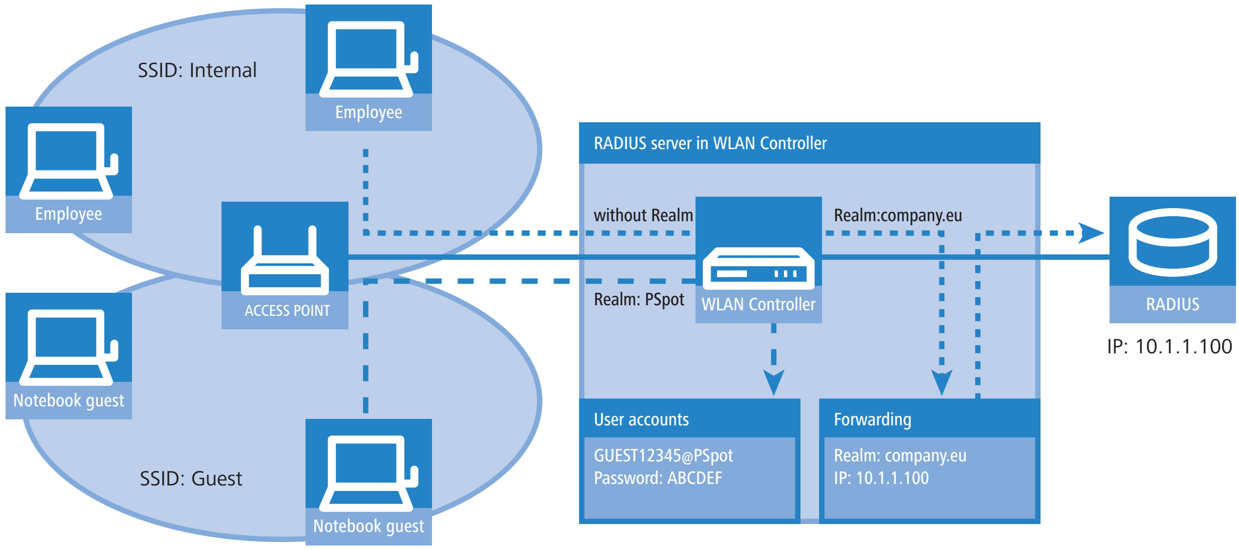
The following flow chart shows the working principle of the RADIUS server when processing realms:


Request 1
Request 2
Realm available in user name?
Yes
No
Realm available in forwarding table?
Yes
No
Replace realm with „default realm“
Set realm to „empty realm“
Realm available in forwarding table?
Yes
No
realm=empty
Forward to defined server
Reject request
Check request with local RADIUS database

Using different realm tags allows different RADIUS servers to be targeted with requests. The decision making process can be tracked in the flow chart.

1. Because the user names for guest access accounts are generated automatically, they can use the realm "PSpot". Because the forwarding table does not contain this entry, all authentication requests with this realm are forwarded to the internal RADIUS server.

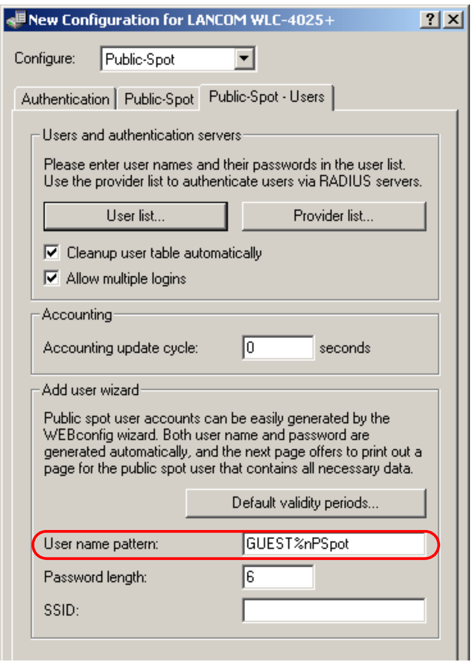
2. To limit the amount of work required for the configuration, internal users are listed without a realm. The RADIUS server in the LANCOM can automatically replace an empty realm with another realm in order to identify internal users. In this example, the empty realm is replaced by the domain of the company "company.eu". The information specified in the forwarding table allows all authentication requests with this realm to be forwarded to the external RADIUS server.



Configuring RADIUS forwarding

The following configuration steps allow you to specify the different manners in which internal users and guests are processed.

① In the Public Spot, adapt the pattern of user names such that a unique realm can be used. For example, the pattern 'GUEST%n@PSpot" generates user names that appear like "GUEST12345@PSpot".



New Configuration for LANCOM WLC-4025+

Configure: Public-Spot

Authentication | Public-Spot | Public-Spot - Users

Users and authentication servers

Please enter user names and their passwords in the user list. Use the provider list to authenticate users via RADIUS servers.

User list... | Provider list...

☑ Cleanup user table automatically

☑ Allow multiple logins

Accounting

Accounting update cycle: 0 seconds

Add user wizard

Public spot user accounts can be easily generated by the WEBconfig wizard. Both user name and password are generated automatically, and the next page offers to print out a page for the public spot user that contains all necessary data.

Default validity periods...

User name pattern: GUEST%nPSpot

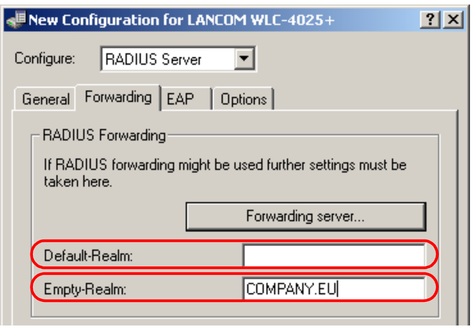
Password length: 6

SSID:

LANconfig: Public Spot ▶ Public Spot users

WEBconfig: LCOS menu tree ▶ Setup ▶ Public Spot module

② In the WLAN controller's RADIUS server, define an "empty realm" (e.g. "COMPANY.EU"). This realm is used for all user names which request authentication from the WLAN controller and which do not already have a realm. In this application, the internal users have no realm defined. In order to prevent the WLAN controllers RADIUS server from inserting a realm, the "Default realm" field must be left empty.



New Configuration for LANCOM WLC-4025+

Configure: RADIUS Server

General | Forwarding | EAP | Options

RADIUS Forwarding

If RADIUS forwarding might be used further settings must be taken here.

Forwarding server...

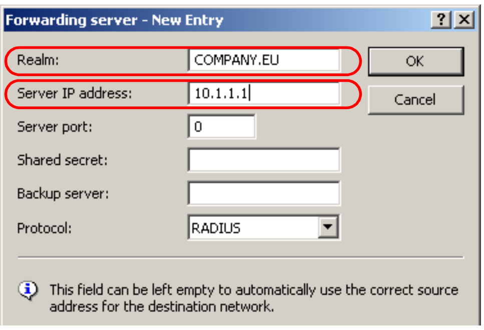
Default-Realm:

Empty-Realm: COMPANY.EU

LANconfig: RADIUS server ▶ Forwarding

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS ▶ Server

③ In order for authentication requests from internal users to be forwarded to the external RADIUS server, suitable entries must be entered into the forwarding settings. The realm "COMPANY.EU" causes all incoming RADIUS requests to be forwarded to the specified IP address.



Forwarding server - New Entry

Realm: COMPANY.EU

Server IP address: 10.1.1.1

Server port: 0

Shared secret:

Backup server:

Protocol: RADIUS

OK | Cancel

This field can be left empty to automatically use the correct source address for the destination network.

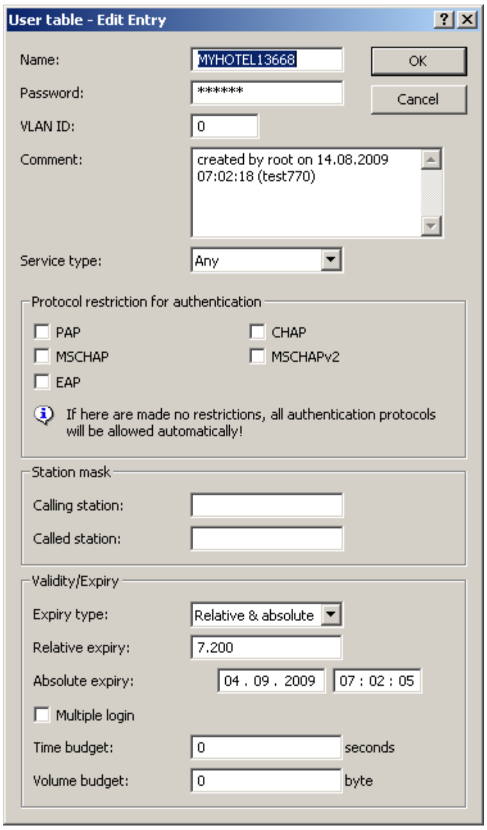
LANconfig: RADIUS server ▶ Forwarding ▶ Forwarding server

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS ▶ Servers ▶ Forward servers

④ Authentication requests from Public Spot users have the realm "@PSpot" and are received by the WLAN Controller. With no forwarding defined for this realm, the usernames are automatically checked with the internal RADIUS database. Because the Public Spot access accounts created with the Wizard are stored in this database, these requests can be authenticated as required.

A.8 Extensions to the RADIUS server

To set up Public Spot users with time and volume budgets, additional parameters have to be entered into the RADIUS server user table.



User table - Edit Entry

Name: MYHOTEL13668

Password: ******

VLAN ID: 0

Comment: created by root on 14.08.2009 07:02:18 (test770)

Service type: Any

Protocol restriction for authentication

☐ PAP ☐ CHAP
☐ MSCHAP ☐ MSCHAPv2
☐ EAP

If here are made no restrictions, all authentication protocols will be allowed automatically!

Station mask

Calling station:

Called station:

Validity/Expiry

Expiry type: Relative & absolute

Relative expiry: 7.200

Absolute expiry: 04 . 09 . 2009 07 : 02 : 05

☐ Multiple login

Time budget: 0 seconds

Volume budget: 0 byte

LANconfig: RADIUS ▶ General ▶ User accounts

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS ▶ Server ▶ Users

- **Multiple logins**

  Allows a single user account to login multiple times simultaneously.

  Possible values:

  □ Yes, No

  Default:

  □ Yes

The multiple-login option must be deactivated if the RADIUS server is to monitor a time budget. The time budget can only be monitored if the user is running just one session at a time.

- **Expiry type**

  This option defines how the validity period is limited for a user account.

  Possible values:

  □ Absolute: The validity of the user account terminates at a set time.

  □ Relative: The validity of the user account terminates a certain period of time after the first user login.

  Default:

  □ Blank: The user account never expires, unless a predefined time or volume budget expires.

The two options can be combined. In this case the user account expires when one of the two limiting values has been reached.

! The device must have a valid time in order for the device to work with user-account time budgets.

- **Abs. expiry**

  If "absolute" has been selected as the expiry type, the user account becomes invalid at the time defined by this value.

  Possible values:

  □ Valid time information (date and time). Max. 20 characters from `0123456789/:.Pp`

  Default:

  □ Blank

  Special values:

  □ 0 switches off the monitoring of the absolute expiry time.

- **Rel. expiry**

  If "relative" has been selected as the expiry type, the user account becomes invalid after this time period has expired since the user logged in for the first time.

  Possible values:

  □ Time span in seconds. Max. 10 characters from `0123456789`

  Default:

  □ 0

  Special values:

  □ 0 switches off the monitoring of the relative expiry time.

- **Time budget**

  The maximum duration of access time for this user account. The user can use this duration of access time until a relative or absolute expiry time (if set) is reached.

  Possible values:

  □ Time span in seconds. Max. 10 characters from `0123456789`

  Default:

  □ 0

  Special values:

  □ 0 switches off the monitoring of the time budget.

- **Volume budget**

  The maximum data volume for this user account. The user can use this data volume until a relative or absolute expiry time (if set) is reached.

  Possible values:

  □ Time span in seconds. Max. 10 characters from `0123456789`

  Default:

  □ 0

  Special values:

  □ 0 switches off the monitoring of data volume.

- **Comment**

  Comment on this entry.

- **Service type**

  The service type is a special attribute of the RADIUS protocol. The NAS (Network Access Server) sends this with the authentication request. The response to this request is only positive if the requested service type agrees with the user account service type.

  Possible values:

  □ Framed: For checking WLAN MAC addresses via RADIUS or IEEE 802.1x.

  □ Login: For Public-Spot logins.

  □ Auth. only: For RADIUS authentication of dialup peers via PPP.

  □ Any

  Default:

  □ Any

The number of entries permissible with the service type "any" or "login" is 64 or 256, depending on the model. This means that the table is not completely filled with entries for Public Spot access accounts (using the service type "Any") and it enables the parallel use of logins via 802.1x.

A.9 IGMP snooping

A.9.1 Introduction

All LANCOM devices with wireless LAN interfaces feature a "LAN bridge", a software entity for transferring data between the Ethernet ports and the WLAN interface(s). In many ways the LAN bridge works like a switch. The core task of a switch, as opposed to a hub, is to forward packets precisely to the port which the relevant user is connected to. Based on the incoming data packets, the switch automatically creates a table listing the senders' MAC addresses and their ports.

If the table contains the destination address for an incoming packet, the switch forwards the packet to the corresponding port. If the destination address is not in the table, the switch forwards the packet to all ports. This means that a switch can only deliver a packet precisely if the destination address appeared earlier in a packet arriving at a certain port from the sender's address. However, broadcast or multicast packets can never be entered as a sender address into a packet, and so these packets end up being "flooded" to all ports.

This may be the correct action for broadcasts which are supposed to reach all available receivers, but this may not be the case for multicasts. Multicasts are generally aimed at a certain group of receivers within a network, but not all of them:

- For example, video streams are frequently transmitted as multicasts, but not all of the network stations are intended to receive that stream.
- Various applications in the medical field rely on multicasts to send data to certain terminal devices, but this data should not be available to all stations.

A LAN bridge in the LANCOM will have ports to which no multicast recipients are connected. This "unnecessary" transmission of multicasts to ports without any receivers is not an error, but it can compromise overall performance.

- Many stations are unable to reject the unwanted multicasts in their hardware. Instead, the packets are forwarded to higher protocol layers, which leads to an increase in CPU load.
- WLANs are particularly susceptible to bandwidth restrictions due to multicasts if none of the associated WLAN clients want to receive the multicast.

The TCP/IP protocol suite defines a protocol called IGMP that allows network stations to register their desire to receive certain IP multicasts to their router. Stations carry out a multicast registration with their router to subscribe to certain multicast groups which deliver the relevant packets. IGMP makes use of Join messages and Leave messages to register and de-register respectively.

Information about which multicast groups a station can or should join are available from other protocols than IGMP.

As a layer-3 protocol, IGMP only performs multicast guiding/routing for whole IP subnets. However, network devices such as bridges, switches or WLAN access points only forward the packets on layer 2, meaning that IGMP itself does not help in any way to further guide multicast traffic through this substructure. For this reason, the bridges use the multicast registrations between stations and routers to receive additional information for targeting the distribution of multicasts. IP multicasts only need to be forwarded to an interface where a router is located that is capable of multicast routing and therefore of forwarding multicasts to other IP subnets. This method is called IGMP snooping. The bridges, which normally use the MAC on layer 2 for packet forwarding, thus additionally use the layer 3 information in the IP multicast packets.

For more detailed description of the functions of IGMP snooping in LCOS, we have to differentiate between two important terms:

- A port is "member" of a multicast group if at least one station connected to it wishes to receive the packets for a certain multicast address. Multicast registration can be dynamic via IGMP snooping or configured manually.
- A port is a "router port" if it is connected to a router that is capable of multicast routing and therefore of forwarding multicasts to other IP subnets.
- A multicast group is "unregistered" if none of the interfaces attached to the bridge is a member of this multicast group.

A.9.2 IGMP snooping operation

Whenever a packet is received, the bridge initially determines whether it is a unicast, broadcast, or multicast packet. For broadcast and unicast packets, the bridge operates in the usual way, i.e. it floods to all ports or sends to a specific port based on the MAC table entry for the receiver.

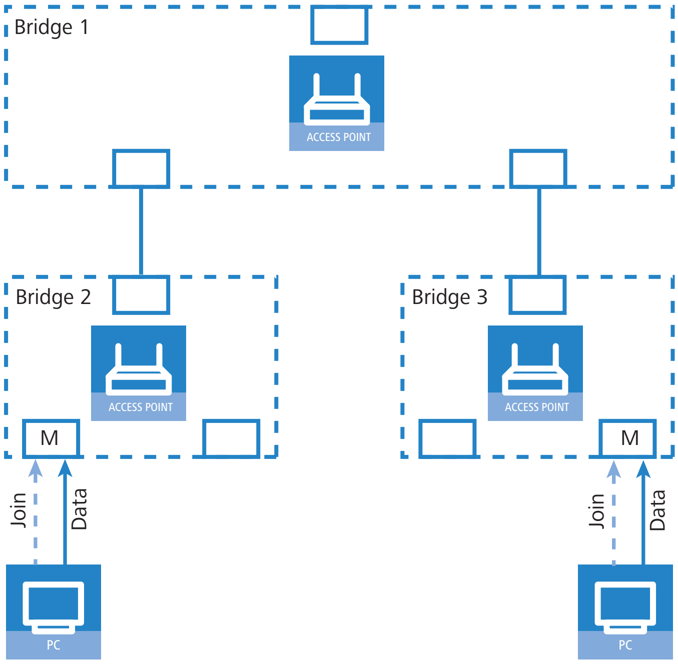
Two types of IP multicast packet are differentiated (whereby packets which are truncated or contain an invalid checksum are discarded entirely):

- IGMP messages are handled in different ways depending on their content:
  - A Join message results in the incoming port becoming member of the respective multicast group. This message is forwarded to router ports only.
  - Similarly, a Leave message results in the incoming port being removed from the multicast group's member list. This message is also forwarded to router ports only.
  - An incoming IGMP query results in the port being marked as a router port. These messages are flooded to all interfaces.
  - All other messages are flooded to all interfaces—no ports experience a change of state.
- If an IP multicast packet does not contain an IGMP message, the IP destination address is examined. Packets for the destination address "224.0.0.x" are flooded to all ports because this is a "reserved" range. For all other packets the destination address is looked up in the IGMP membership table:
  - If the address is found, the packet is forwarded according to the membership stored in the table.
  - If the address is not found, the packet may either be discarded, flooded to all ports, or forwarded exclusively to all router ports (depending on the configuration).

  In either case, packets are forwarded to all router ports.

A.9.3 IGMP snooping through multiple bridges

As described, IGMP snooping only forwards incoming Join or Leave messages via router ports. In a structure with multiple bridges, initially none of the ports are router ports or members of a multicast group. If a station connected to the bridge registers with a multicast group, the port automatically becomes a member of this group. However, none of the ports are router ports at this phase, so the Join messages are not forwarded anywhere. Other bridges thus receive no information about the port's membership with the multicast group.



Consequently, bridges must have router ports in order for membership information to be propagated. Since the ports of a bridge only become router ports in the case of IGMP queries, one of the multicast-capable routers in the network must take over the task of distributing the necessary IGMP queries throughout the network. This router is referred to as the IGMP querier. If the network does not contain a multicast router, the LANCOM access points are capable of simulating a querier. To avoid parallel queries arriving from various queriers, a querier will deactivate itself if it discovers another querier with a lower IP number. The distribution of IGMP information by the querier can be explained with the following example:

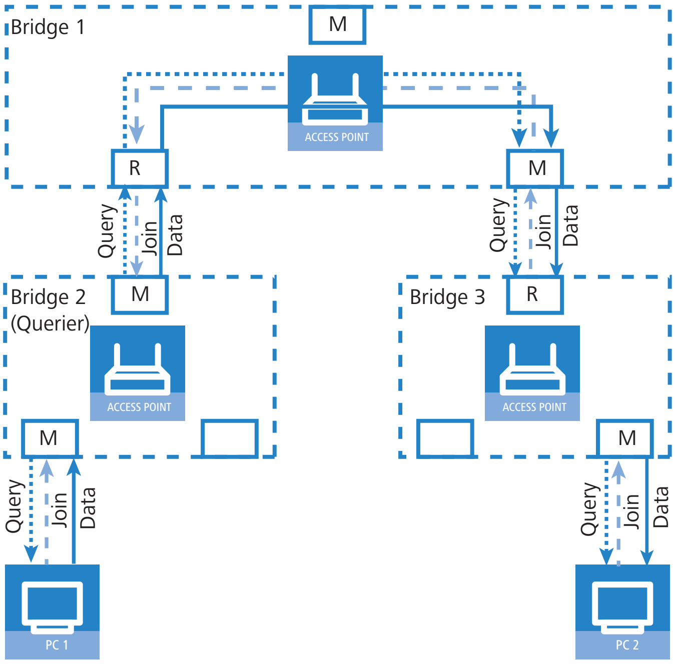
① The querier (Bridge 2 in this example) regularly sends out IGMP queries on all ports of bridge 2 (dotted lines). The next bridge (Bridge 1) receives the query on a port which is then marked as a router port (R). PC 1 responds to this query with a Join message for all multicast groups (light dashed lines) that it wishes to join. The port connecting PC 1 to Bridge 2 then becomes a member of the multicasting group(s).

② In addition to this, Bridge 1 sends the queries on all other ports to the bridges and stations lower down in the structure. In Bridge 3 the port receiving the query becomes a router port (R).

③ The station (PC 2) connected to bridge 3 responds to this query with a Join message for all registered multicast groups. The port connecting PC 2 to Bridge 3 then becomes a member of the multicasting group(s).

④ Bridge 3 forwards this Join message to Bridge 1 over the router port. The receiving port on Bridge 1 thus also takes on membership of the multicast groups that PC 2 has registered for.

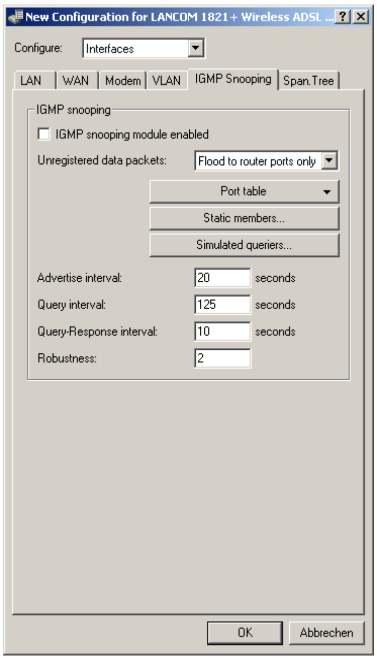
⑤ In the final step, Bridge 1 forwards the Join message from PC 2 via the router port to Bridge 2, where the receiving port also takes on membership of PC 2's multicast groups.



If PC 1 now transmits a multicast for which PC 2 has registered, all of the bridges (2, 1 and then 3) forward the packets to PC 2 via the member port.

A.9.4 Configuration

General settings



Configure: Interfaces

IGMP snooping

□ IGMP snooping module enabled

Unregistered data packets: Flood to router ports only

Advertise interval: 20 seconds

Query interval: 125 seconds

Query-Response interval: 10 seconds

Robustness: 2

LANconfig: Interfaces ▶ IGMP snooping

WEBconfig: LCOS menu tree ▶ Setup ▶ LAN bridge ▶ IGMP snooping

- **Operating**

  Activates or deactivates IGMP snooping in the device and all of the defined querier instances. Without IGMP snooping the bridge functions like a simple switch and forwards all multicasts to all ports.

  Possible values:

  - Yes, No

  Default:

  - No

If this function is deactivated, all IP multicast packets are sent on all ports. If the device operating state changes, the IGMP snooping function is completely reset, i.e. all dynamically learned values are lost (membership, router-port states).

- **Query interval**

  Interval in seconds in which a multicast-capable router (or a simulated querier) sends IGMP queries to the multicast address 224.0.0.1, so prompting the stations to transmit return messages about multicast group memberships. These regular queries influence the time in which memberships age, expire, and are then deleted.

  - After the startup phase, the querier sends IGMP queries in this interval.
  - A querier returns to the querier status after a time equal to "Robustness*Query-Interval+(Query-Response-Interval/2)".
  - A port loses its router-port status after a time equal to "Robustness*Query-Interval+(Query-Response-Interval/2)".

  Possible values:

  - 10-figure number greater than 0.

  Default:

  - 125

The query interval must be greater than the query response interval.

- **Query response interval**

  Interval in seconds influencing the timing between IGMP queries and router-port aging and/or memberships.

Interval in seconds in which a multicast-capable router (or a simulated querier) expects to receive responses to its IGMP queries. These regular queries influence the time in which memberships age, expire, and are then deleted.

Possible values:

- □ 10-figure number greater than 0.

Default:

- □ 10

The query response interval must be less than the query interval.

- ■ **Robustness**

  This value defined the robustness of the IGMP protocol. This option tolerates packet losses of IGMP queries with respect to Join messages.

  Possible values:

  - □ 10-figure number greater than 0.

  Default:

  - □ 2

- ■ **Advertise interval**

  The interval in seconds in which devices send packets advertising themselves as multicast routers. This information makes it quicker for other IGMP-snooping devices to find which of their ports are to operate as router ports. When activating its ports, a switch (for example) can query for multicast routers, and the router can respond to this query with an advertisement of this type. Under some circumstances this method can be much quicker than the alternative IGMP queries.

  Possible values:

  - □ 4 to 180 seconds.

  Default:

  - □ 20

- ■ **Unregistered data packet handling**

  This setting defines the handling of multicast data packets with a destination address outside the 224.0.0.x range and for which neither static memberships were defined nor were dynamic memberships learned.

  Possible values:

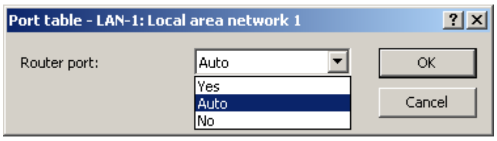
  - □ Router ports only: Sends these packets to all router ports.
  - □ Flood: Sends these packets to all ports.
  - □ Discard: Drops these packets.

  Default:

  - □ Router ports only

Port settings

This table defines the port-related settings for IGMP snooping.


Port table - LAN-1: Local area network 1

Router port: Auto

LANconfig: Interfaces ▶ IGMP snooping ▶ Port table

WEBconfig: LCOS menu tree ▶ Setup ▶ LAN bridge ▶ IGMP snooping ▶ Port settings

- ■ **Port**

  The port for which the settings apply.

  Possible values:

  - □ Selects a port from the list of those available in the device.

  Default:

  - □ N/A

- **Router port**

  This option defines the port's behavior.

  Possible values:

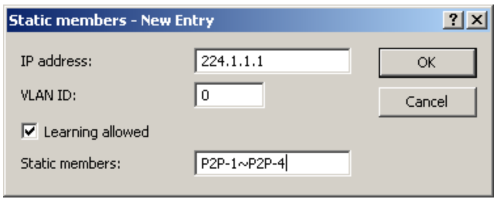
  - □ Yes: This port will always work as a router port, irrespective of IGMP queries or router messages received at this port.
  - □ No: This port will never work as a router port, irrespective of IGMP queries or router messages received at this port.
  - □ Auto: This port will work as a router port if IGMP queries or router messages are received. The port loses this status if no packets are received for the duration of "Robustness*Query-Interval+(Query-Response-Interval/2)".

  Default:

  - □ Auto

Static members

This table enables members to be defined manually, for example if they cannot or should not be learned automatically.



Static members - New Entry

IP address: 224.1.1.1

VLAN ID: 0

☑ Learning allowed

Static members: P2P-1~P2P-4

LANconfig: Interfaces ▶ IGMP snooping ▶ Static members

WEBconfig: LCOS menu tree ▶ Setup ▶ LAN bridge ▶ IGMP snooping ▶ Static members

- **Address**

  The IP address of the manually defined multicast group.

  Possible values:

  - □ Valid IP multicast address.

  Default:

  - □ Blank

- **VLAN ID**

  The VLAN ID which is to support this static member. Each IP multicast address can have multiple entries with different VLAN IDs.

  Possible values:

  - □ 0 to 4096.

  Default:

  - □ 0

  Special values:

  - □ If "0" is selected as VLAN, the IGMP queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

- **Allow learning**

  This option activates the automatic learning of memberships in this multicast group. If automatic learning is deactivated, packets can only be sent via the ports which have been manually defined for the multicast group.

  Possible values:

  - □ Yes, No.

  Default:

  - □ Yes

- **Static members**

  These ports will always be the destination for packets with the corresponding IP multicast address, irrespective of any Join messages received.

  Possible values:

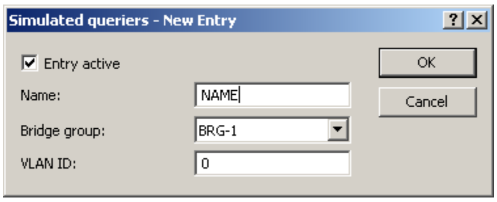
- □ Comma-separated list of the desired ports, max. 215 alphanumerical characters.

Default:

- □ Blank

Simulated queriers

This table contains all of the simulated queriers defined in the device. These units are employed if IGMP functions are required but there is no multicast router in the network. The querier can be limited to certain bridge groups or VLANs by defining multiple independent queriers to support the corresponding VLAN IDs.


Simulated queriers - New Entry

☑ Entry active

Name: NAME

Bridge group: BRG-1

VLAN ID: 0

LANconfig: Interfaces ▶ IGMP snooping ▶ Simulated queriers

WEBconfig: LCOS menu tree ▶ Setup ▶ LAN bridge ▶ IGMP snooping ▶ Simulated queriers

- **Name**

  Name of the querier instance

  Possible values:

  - □ 8 alphanumerical characters.

  Default:

  - □ Blank

- **Operating**

  Activates or deactivates the querier instance

  Possible values:

  - □ Yes, No.

  Default:

  - □ No

- **Bridge group**

  Limits the querier instance to a certain bridge group.

  Possible values:

  - □ Select from the list of available bridge groups.

  Default:

  - □ none

  Special values:

  - □ If bridge group is set to "none", the IGMP queries will the sent via all bridge groups.

- **VLAN ID**

  Limits the querier instance to a certain VLAN.

  Possible values:

  - □ 0 to 4096.

  Default:

  - □ 0

  Special values:

  - □ If "0" is selected as VLAN, the IGMP queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

A.9.5 IGMP status

General statistics

Status messages for IGMP snooping are to be found under the following paths:

WEBconfig: LCOS menu tree ▶ Status ▶ LAN bridge statistics ▶ IGMP snooping

- **Operating**

  Indicates whether IGMP snooping is activated or deactivated.
- **IPv4 packets**

  Shows the number of IPv4 multicast packets received at all ports, whether they were IGMP packets or not.
- **Data packets**

  Shows the number of intact IPv4 multicast packets received at all ports and which were not IGMP packets.
- **Control packets**

  Shows the number of intact IGMP packets received at all ports.
- **Bad packets**

  Shows the number of damaged data or IGMP packets received at all ports. Possible causes for damage to packets may be IP checksum errors or truncated packets.

ⓘ For performance reasons, IP checksums are evaluated for IGMP packets only and not for the data portion of multicast packets. This is why packets with a faulty checksum in the TCP/UDP or IP header are not detected. These packets are counted as data packets.

- **Deleted values**

  This action deletes all statistical entries.

Port status

This table shows all port-related statistics.

WEBconfig: LCOS menu tree ▶ Status ▶ LAN bridge ▶ IGMP snooping ▶ Port status

- **Router port**

  Shows whether the port is currently in use as a router port or not, irrespective of whether this status was configured statically or learned dynamically.
- **IPv4 packets**

  Shows the number of IPv4 multicast packets received at this port, whether they were IGMP packets or not.
- **Data packets**

  Shows the number of intact IPv4 multicast packets received at this port and which were not IGMP packets.
- **Control packets**

  Shows the number of intact IGMP packets received at this port.
- **Bad packets**

  Shows the number of damaged data or IGMP packets received at this port. Possible causes for damage to packets may be IP checksum errors or truncated packets.

ⓘ For performance reasons, IP checksums are evaluated for IGMP packets only and not for the data portion of multicast packets. This is why packets with a faulty checksum in the TCP/UDP or IP header are not detected. These packets are counted as data packets.

Groups

This table displays all the the multicast group memberships known to the device, irrespective of whether they were configured statically or learned dynamically. If both static and dynamic memberships exist for a multicast group, these are shown in separate entries.

WEBconfig: LCOS menu tree ▶ Status ▶ LAN bridge ▶ IGMP snooping ▶ Groups

- **Address**

  Shows the group's IP multicast address.
- **VLAN ID**

  Shows the VLAN ID that this entry applies to.
- **Allow learning**

  Shows whether new memberships for this group can be learned dynamically or not.
- **Static members**

  Shows the list of statically defined members for this group.
- **Dynamic members**

  Shows the list of dynamically learned members for this group.

Simulated queriers

This table shows the status of all defined and active IGMP querier instances.

- **Name**

  Shows the name of the multicast group.

- **Bridge group**

  Shows the bridge group that this entry applies to.

- **VLAN ID**

  Shows the VLAN that this entry applies to.

- **Status**

  Shows the current status of the entry.

  - Initial: The querier instance has just started and is sending IGMP queries in short intervals (four-times faster than the query interval defined).
  - Querier: The querier instance considers itself to be the active querier and is sending IGMP queries in the defined query interval.
  - Non-Querier: Another querier instance with a lower IP address has been detected, and the instance listed here is not sending any IGMP queries.

A.10 TACACS+

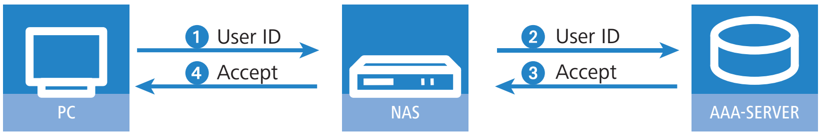
A.10.1 Introduction

Tacacs+ (Terminal Access Controller Access-Control System) is a protocol for authentication, authorization and accounting (AAA). It thus provides access to the network for certain authorized users only, it regulates the rights of those users, and it is a logging mechanism to keep track of user actions. TACACS+ is an alternative to other AAA protocols such as RADIUS.

! TACACS+ must be used in order to meet with PCI compliance (Payment Card Industry).

Modern networks with their numerous types of service and network components present a massive challenge in terms of controlling access rights for the user. In large installations in particular, the overhead would be enormous to keep user data consistent on all devices or for all services. For this reason, user data should be managed on a central server.

As a simple example, a user wishes to register at a router and sends the corresponding login details (user ID) to it. In this case the router functions as a Network Access Server (NAS): It does not check the user data itself; rather, the data is forwarded to the central AAA server, which responds by checking the data and answering with an accept or a reject.



The advanced TACACS+ functions include, among others, the option of requesting user to change their passwords after logging in for the first time, or if the password has expired. The corresponding messages are sent from the NAS to the user.

! Please note that LANconfig cannot process all of the messages in the extended login dialog. Should LANconfig reject a login attempt at a LANCOM even if the correct data is entered, please use an alternative method of configuration (such as WEBconfig or telnet).

TACACS+ is an alternative AAA server to the widespread RADIUS servers. The following table shows some of the major differences between RADIUS and TACACS+:

TACACS+	RADIUS
Connection-orientated data transfer via TCP	Connectionless data transfer via UDP
Fully encrypted data transfer	Password only encrypted, other content remains unencrypted
Complete separation of authentication, authorization and accounting possible	Authentication and authorization combined

- TCP-based communication with TACACS+ is more reliable than RADIUS. Communications between the NAS and AAA server are confirmed, so the NAS is always informed if the AAA server is unavailable.
- TACACS+ encrypts not only the password like RADIUS but the entire payload data (except for the TACACS+ header). This assures the confidentiality of information such as user names or the permitted services. TACACS+ encryption works with a one-time pad based on MD5 hashes.
- The separation of the three AAA functions enables TACACS+ to operate with multiple servers. Whereas RADIUS always combines authentication and authorization, TACACS+ allows these to be separated. In this way, for example, TACACS+ servers can be employed for authentication only, in that only the users are managed but not the permissible commands.

Please note: Even though TACACS+ is used to centrally manage user accounts on an AAA server, you should ensure that you set a secure password for root access to the LANCOM. If no root password is set, access to the device configuration can be blocked for security reasons if no connection is available to the TACACS+ server. In this case, the device may have to be reset to its factory settings in order to regain access to the configuration.

A.10.2 Configuring the TACACS+ parameters

The parameters for configuring TACACS+ are to be found under the following paths:

WEBconfig: LCOS menu tree ▶ Setup ▶ TACACS+

- **Accounting**

  Activates accounting via TACACS+ server. If TACACS+ accounting is activated, all accounting data is transmitted via TACACS+ protocol to the configured TACACS+ server.

  Possible values:

  □ Activated, deactivated

  Default

  □ Deactivated

TACACS+ accounting will only activate if the defined TACACS+ server is available.

- **Authentication**

  Activates authentication via TACACS+ server. If TACACS+ authentication is activated, all authentication data is transmitted via TACACS+ protocol to the configured TACACS+ server.

  Possible values:

  □ Activated, deactivated

  Default

  □ Deactivated

TACACS+ authentication will only activate if the defined TACACS+ server is available. Fallback to local users is only possible if a root password has been set for the LANCOM. The fallback to local users must be deactivated for devices without a root password. Otherwise a failure of the network connection (TACACS+ server unavailable) would make the LANCOM accessible without a password.

- **Authorization**

  Activates authorization via TACACS+ server. If TACACS+ authorization is activated, all authorization data is transmitted via TACACS+ protocol to the configured TACACS+ server.

  Possible values:

  □ Activated, deactivated

  Default

  □ Deactivated

TACACS+ authorization will only activate if the defined TACACS+ server is available.
If TACACS+ authorization is activated, the TACACS+ server will be queried for authorization each time a user enters a command. Data traffic during configuration will increase correspondingly. Also, the user rights must be defined in the TACACS+ server.

- **Fallback to local users**

  Should the defined TACACS+ server be unavailable, it is possible to fallback to local user accounts on the LANCOM. This allows for access to the device even if the TACACS+ connection should fail, e.g. when deactivating the usage of TACACS+ or for correcting the configuration.

  Possible values:

  □ Allowed, prohibited

  Default

  □ Allowed

The fallback to local user accounts presents a security risk if no root password is set for the LANCOM. For this reason, TACACS+ authentication with fallback to local user accounts can only be activated if a root password has been set. If no root password is set, access to the device configuration can be blocked for security reasons if no connection is available to the TACACS+ server. In this case, the device may have to be reset to its factory settings in order to regain access to the configuration.

- **Shared secret**

  The password for encrypting the communications between NAS and TACACS+ servers.

  Possible values:

  □ 31 alphanumerical characters

  Default

  □ Blank

The password must be entered identically into the LANCOM and the TACACS+ server. We recommend that you do not operate TACACS+ without encryption.

- **SNMP-GET requests accounting**

  Numerous network management tools use SNMP for requesting information from network devices. LANmonitor also uses SNMP to access the LANCOM devices to display information about current connections, etc., or to execute actions such as disconnecting a connection. SNMP can be used to configure devices. For this reason TACACS+ requires authentication for SNMP access requests. Since LANmonitor regularly queries these values, a large number of unnecessary TACACS+ connections would be established. If authentication, authorization and accounting by TACACS+ are activated, then each request would initiate three sessions with the TACACS+ server.

  This parameter allows the regulation of the behavior of LANCOM devices with regard to SNMP access in order to reduce the number of TACACS+ sessions required for accounting. Authentication via the TACACS+ server remains necessary if authentication for TACACS+ is activated generally.

Entering a read-only community under LCOS menu tree ▶ Setup ▶ SNMP enables authentication by TACACS+ to be deactivated for LANmonitor. The read-only community defined here is then entered into LANmonitor as a user name.

  Possible values:

  □ only_for_SETUP_tree: With this setting, accounting via TACACS+ server is only required for SNMP access via the setup branch of LCOS.

  □ All: With this setting, accounting by TACACS+ server will be carried out for every SNMP access. In case of regular request for status information, for example, the load on the TACACS+ server will increase significantly.

  □ None: With this setting, accounting by TACACS+ server will not be carried out for SNMP accesses.

  Default:

  □ only_for_SETUP_tree

- **SNMP-GET requests authorization**

  This parameter allows the regulation of the behavior of LANCOM devices with regard to SNMP access in order to reduce the number of TACACS+ sessions required for authorization. Authentication via the TACACS+ server remains necessary if authentication for TACACS+ is activated generally.

  Possible values:

  □ only_for_SETUP_tree: With this setting, authorization via TACACS+ server is only required for SNMP access via the setup branch of LCOS.

- □ All: With this setting, authorization by TACACS+ server will be carried out for every SNMP access. In case of regular request for status information, for example, the load on the TACACS+ server will increase significantly.
- □ None: With this setting, authorization by TACACS+ server will not be carried out for SNMP accesses.

Default:

- □ only_for_SETUP_tree

■ **Encryption**

Activates or deactivates the encryption of communications between NAS and TACACS+ servers.

Possible values:

- □ Activated, deactivated

Default

- □ Activated

! We recommend that you do not operate TACACS+ without encryption. If encryption is activated here, the password for encryption entered here must match with the password on the TACACS+ server.

A.10.3 Configuring the TACACS+ server

Two servers can be defined to work with TACACS+ functions. One server acts as a backup in case the other one fails. When logging in via telnet or WEBconfig, the user can select the server to be used.

The parameters for configuring the TACACS+ server are to be found under the following paths:

WEBconfig: LCOS menu tree ▶ Setup ▶ TACACS+ ▶ Server

■ **Server address**

Address of the TACACS+ server to which requests for authentication, authorization and accounting are to be forwarded.

Possible values:

- □ Valid DNS resolvable name or valid IP address.

Default

- □ Blank

■ **Loopback address**

Optionally you can configure a loopback address here.

Possible values:

- □ Name of the IP networks whose addresses are to be used
- □ "INT" for the address of the first intranet.
- □ "DMZ" for the address of the first DMZ.
- □ LB0 to LBF for the 16 loopback addresses
- □ Any valid IP address

Default

- □ Blank

■ **Compatibility mode**

TACACS+ servers are available as open-source or commercial versions, each of which works with different messages. The compatibility mode enables the processing of messages from free TACACS+ servers.

Possible values:

- □ Activated, deactivated

Default

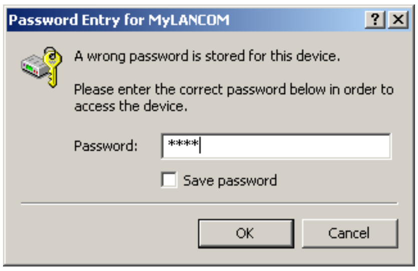
- □ Deactivated

A.10.4 Login to the TACACS+ server

Once TACACS+ has been activated for authentication and/or authorization, all logins to the device are redirected to the TACACS+ server. The remaining login procedure differs according to the access method.

TACACS+ login via LANconfig

Using LANconfig to login to a device with activated TACACS+ authentication is only possible with the user named "root". Correspondingly, the user "root" must be configured on the TACACS+ server. To login via LANconfig, enter the password as configured for the user "root" on the TACACS+ server.


Password Entry for MyLANCOM

A wrong password is stored for this device.

Please enter the correct password below in order to access the device.

Password: ****

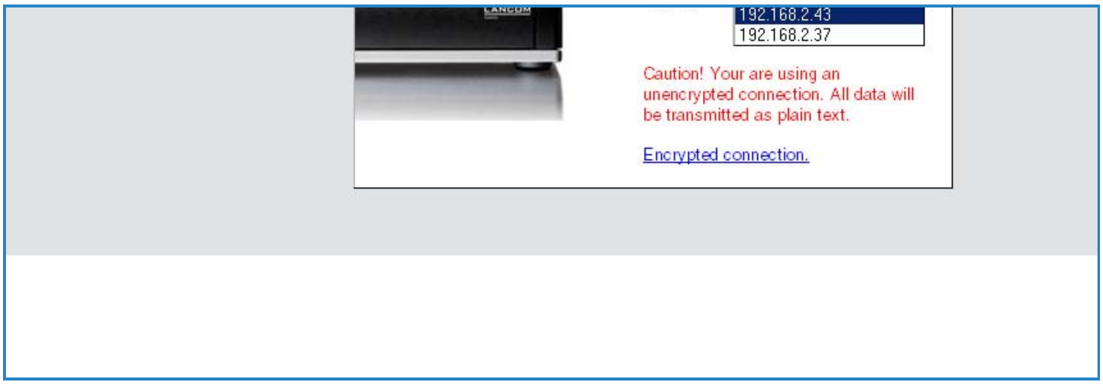
□ Save password

Once authenticated by TACACS+, "root" is the only user automatically assigned with full supervisor rights, and thus able to edit the configuration without having to change privilege level. When authorization is in use, the TACACS+ server decides whether this is allowed or not.

If authorization is activated for the device as well as authentication, the TACACS+ server must permit the commands "readconfig" and "writeconfig" for the user "root" in order for the user to read the configuration from the device and to upload any changes ('Assigning rights under TACACS+' → Page 24).

TACACS+ login via WEBconfig

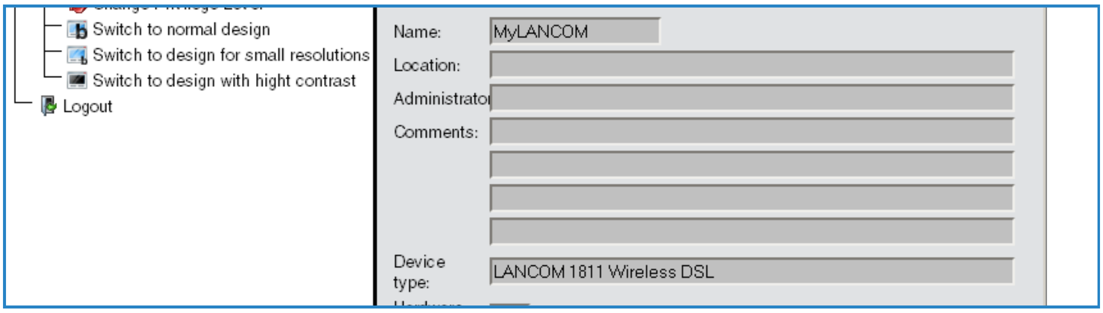
Using WEBconfig to login to a device with activated TACACS+ authentication is possible for any user configured on the TACACS+ server. When logging in with WEBconfig, enter the user name configured on the TACACS+ server and select the server which is to carry out authentication.


192.168.2.43
192.168.2.37

Caution! Your are using an unencrypted connection. All data will be transmitted as plain text.

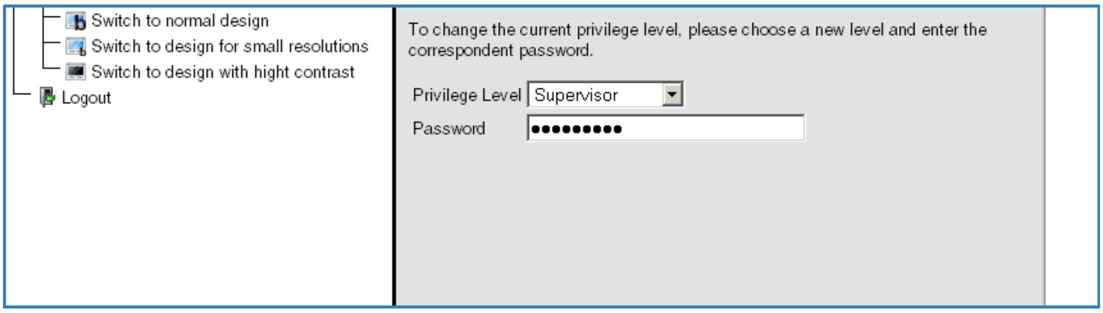
Encrypted connection.

The corresponding password is requested in the following dialog. After logging in, the user initially sees a reduced WEBconfig user interface. If authorization is not being used, all WEBconfig users (except for the user "root") initially have read rights only.


Change Privilege Level
Switch to normal design
Switch to design for small resolutions
Switch to design with hight contrast
Logout

Name: MyLANCOM
Location:
Administrator:
Comments:
Device type: LANCOM 1811 Wireless DSL

To gain further rights, click on the link **Change privilege level** on the left of the screen.


Switch to normal design
Switch to design for small resolutions
Switch to design with hight contrast
Logout

To change the current privilege level, please choose a new level and enter the correspondent password.

Privilege Level: Supervisor

Password: ●●●●●●●●●●

In this dialog you select the required user rights and enter the corresponding password.

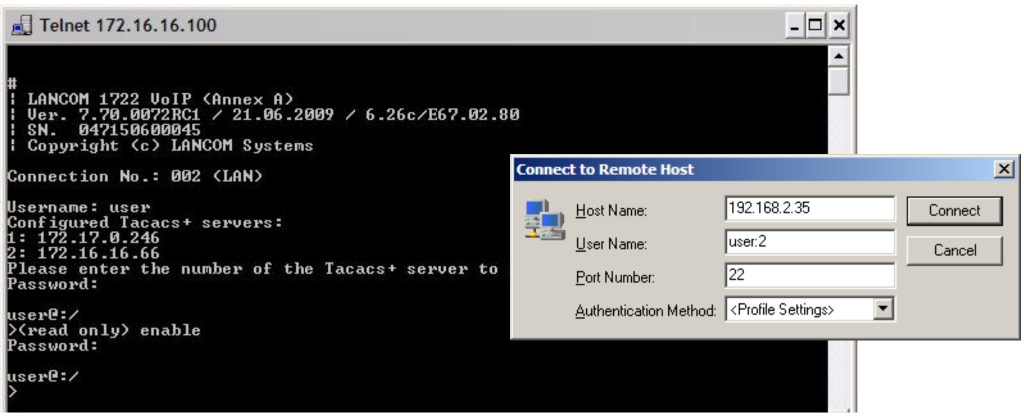
The passwords for individual user rights are configured as "enable" passwords in the TACACS+ server.

If authorization is activated for the device as well as authentication, the TACACS+ server must permit the required commands for each user in order for the user to read and edit the device configuration ('Assigning rights under TACACS+' → Page 24).

TACACS+ login with telnet or SSH

Using tenet or SSH to login to a device with activated TACACS+ authentication is possible for any user configured on the TACACS+ server.

When logging in with telnet, enter the user name configured on the TACACS+ server and select the server which is to carry out authentication. When logging in with SSH, enter the user name followed by a colon and then the server name, i.e. "user:1" or "user:2".



```
#
| LANCOM 1722 VoIP (Annex A)
| Ver. 7.70.0072RC1 / 21.06.2009 / 6.26c/E67.02.80
| SN.  047150600045
| Copyright (c) LANCOM Systems

Connection No.: 002 (LAN)

Username: user
Configured Tacacs+ servers:
1: 172.17.0.246
2: 172.16.16.66
Please enter the number of the Tacacs+ server to
Password:

user@:/
>(read only) enable
Password:

user@:/
>
```

Host Name: 192.168.2.35

User Name: user:2

Port Number: 22

Authentication Method: <Profile Settings>

After login, all users initially have read-rights only (except for the user "root").

To gain further rights, enter the command `enable` and enter the password. Rights will be assigned according to configuration for that password. The parameters for the enable command are the numbers 1-15. 1 is the lowest level, 15 the highest. If no parameter is entered, 15 is taken automatically.

The passwords for individual user rights are configured as "enable" passwords in the TACACS+ server.

If authorization is activated for the device as well as authentication, the TACACS+ server must permit the required commands for each user in order for the user to read and edit the device configuration ('Assigning rights under TACACS+' → Page 24).

A.10.5 Assigning rights under TACACS+

TACACS+ uses privilege levels to separate users into different groups. For the local authorization of users via the "enable" command under telnet/SSH or via privilege levels under WEBconfig, the various administrator rights of LCOS are mapped to the TACACS+ privilege levels:

TACACS+ level	LCOS administrator rights
0	No rights
1	Read only
3	Read-write
5	Read-only limited admin

TACACS+ level	LCOS administrator rights
7	Read-write limited admin
9	Read-only admin
11	Read-write admin
15	Supervisor (root)

A.10.6 Authorizing functions

If authorization is activated for the device as well as authentication, the TACACS+ server must permit the corresponding functions for the user. Enter the required values into the user configuration on the TACACS+ server.

LANconfig

Command	Arguments	Remark
readconfig	none	Read out the entire configuration
writeconfig	none	Write the entire configuration

WEBconfig

Command	Arguments	Remark
delRow	SNMP-ID of the table	Delete row
addRow	SNMP-ID of the table	Add row
editRow	SNMP-ID of the table	Edit row
modifyItem	SNMP-ID of the menu item	Edit a menu item
viewTable	SNMP-ID of the table	View table
viewRow	SNMP-ID of the row	View row
setValue	SNMP-ID of the menu item	Set value of a menu item
listmenu	SNMP-ID of the menu	List sub menu
action	SNMP-ID of the action	Execute an action
reboot	none	Restart device
$URL	none	Display a certain URL

When working with WEBconfig, all URLs sent to the TACACS+ server during configuration must be enabled. For example, the URL "config2" under WEBconfig provides access to the configuration branch of the LCOS menu tree. Additionally, the individual parameters which the user may edit must also be enabled. You can view the URLs sent by WEBconfig to the TACACS+ server with the trace "trace+ tacacs".

Telnet/SSH

Command	Arguments	Remark
dir	SNMP-ID of the directory	View directory content
list	SNMP-ID of the directory	View directory content
ls	SNMP-ID of the directory	View directory content
llong	SNMP-ID of the directory	View directory content
del	SNMP-ID of the table	Delete row
delete	SNMP-ID of the table	Delete row
rm	SNMP-ID of the table	Delete row
cd	SNMP-ID of the target directory	Change directory
add	SNMP-ID of the table	Add row
tab	SNMP-ID of the table	Changes the order of the columns for adding values
do	SNMP-ID of the action	Execute action
show	Parameter name	View information
trace	Parameter name	Execute trace
time	Parameter name	Time
feature	Parameter name	Add function
repeat	Parameter name	Repeat the command
readmib	none	Read-out SNMP-MIB
readconfig	none	Read out the entire configuration
readstatus	none	Read-out status menu
writefiash	none	Update firmware
activateimage	Parameter name	Activate another firmware image
ping	Parameter name	Start ping
wakeup	Parameter name	Sends wakeup packet
linktest	Parameter name	WLAN link test
writeconfig	none	Write the entire configuration
ll2mdetect	none	Start LL2M detection
ll2mexec	Parameter name	Execute LL2M command
scp	Parameter name	Secure copy
rcp	Parameter name	Secure copy
readscript	Parameter name	Read-out script
beginscript	none	Start script
endscript	none	Stop script
flash	Parameter name	Activate/deactivate flash mode

For telnet access, all of the parameters that the user may edit must be enabled. You can view the values sent by telnet to the TACACS+ server with the trace "trace+ tacacs".

SNMP

Command	Arguments	Remark
get	SNMP-ID of the menu item	Read-out value
set	SNMP-ID of the menu item	Set value

A.11 Sending attachments with the mailto command

E-mails with information on device status can be sent automatically if certain events occur. To do this, just include the mailto command into entries in the action table or cron table.

Attachments can be sent with the e-mails. This allows the results of console commands executed on the device before sending the mail to be sent as an attachment. In this way, the content of tables or menus (e.g. detailed status messages) can be sent by e-mail.

- **Action (action table) or command (cron table) (max. 250 characters)**

  Here you describe the action that is be executed at a certain time or when a change in the status of the WAN connection occurs. Only one action can be triggered per entry.

  Possible values for the actions (max. 250 characters):

  □ mailto: – This prefix causes an e-mail to be sent.

  Optional variables for the actions:

  □ attach=`console command`

  Any console command can be entered which outputs useful information. The console command is enclosed in "backquotes" also known as backticks. This character is produced with the aid of the "accent grave" key.

  The output of the console command is written to a text file for attachment to the mail. This text file is headed by the command and a time/date stamp, followed by the output.

  Default:

  □ Blank

  Examples:

  The following action enables you to sent the ADSL status by e-mail:
  mailto:admin@mycompany.com?subject=ADSL_status?attach=`dir /status/adsl`.

  An action can be used to send mutliple console commands:
  mailto:admin@mycompany.com?subject=Status_reports?attach=`dir /status/adsl`?attach=`dir /status/config`
  The attached files are named 'cmd1.txt', 'cmd2.txt', etc.

A.12 Firmware upload for the UMTS module in the LANCOM 1751 UMTS

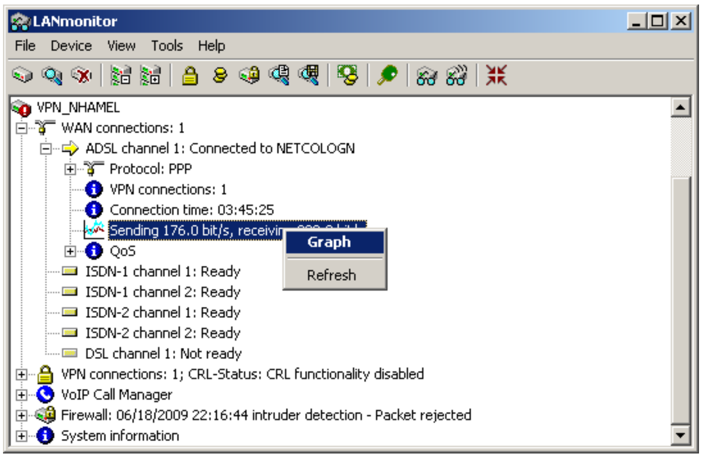
The firmware of the UMTS module in the LANCOM 1751 UMTS can be updated easily as of LCOS version 7.70. Firmware for the UMTS module is available in UPX format and can be uploaded to the LANCOM 1751 UMTS in the same manner as the LANCOM firmware.

A.13 Performance monitoring with LANmonitor

LANmonitor logs various parameters in the devices and displays these graphically:

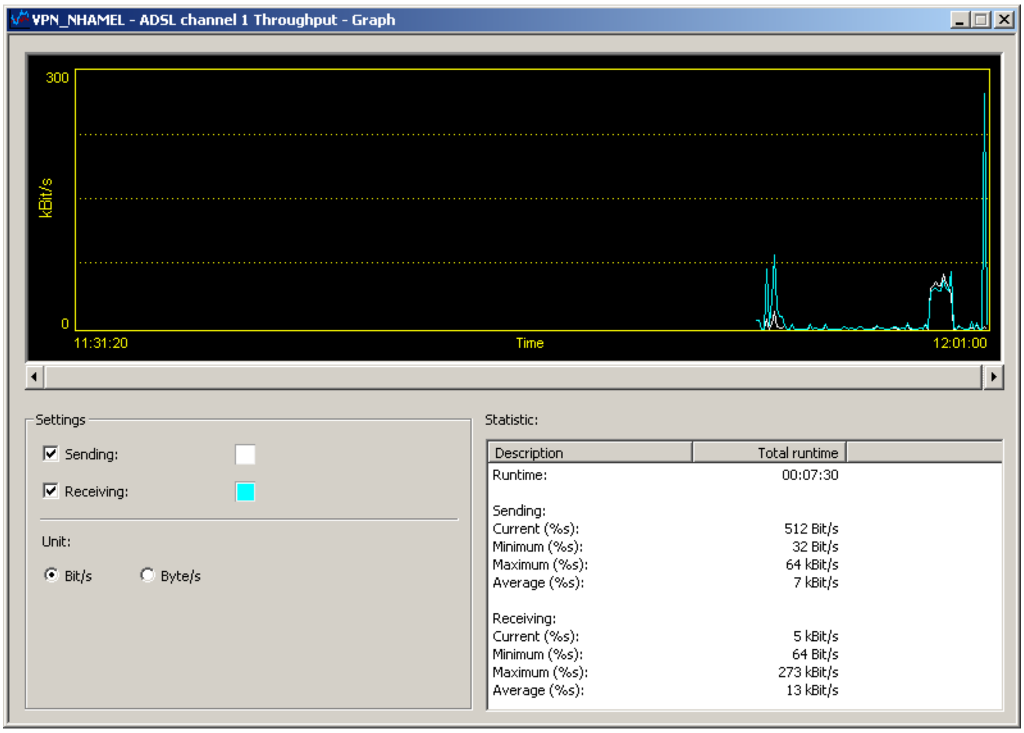
- Transmit and receive rates for WAN connections
- Transmit and receive rates for point-to-point connections
- Signal reception strength for point-to-point connections
- Link signal strength for point-to-point connections
- Throughput for point-to-point connections
- CPU load
- Free memory
- Temperature (not available on all models)

LANmonitor displays the current values directly in the corresponding groups.



```
VPN_NHAMEL
  WAN connections: 1
    ADSL channel 1: Connected to NETCOLOGN
      Protocol: PPP
      VPN connections: 1
      Connection time: 03:45:25
      Sending 176.0 bit/s, receivi
      QoS
    ISDN-1 channel 1: Ready
    ISDN-1 channel 2: Ready
    ISDN-2 channel 1: Ready
    ISDN-2 channel 2: Ready
    DSL channel 1: Not ready
  VPN connections: 1; CRL-Status: CRL functionality disabled
  VoIP Call Manager
  Firewall: 06/18/2009 22:16:44 intruder detection - Packet rejected
  System information
```

A click on the **Graph** item in the context menu opens a new window which displays these parameters over time.



Settings

☑ Sending: □

☑ Receiving: 🟦

Unit:

● Bit/s ○ Byte/s

Statistic:

Description	Total runtime
Runtime:	00:07:30
Sending:	
Current (%s):	512 Bit/s
Minimum (%s):	32 Bit/s
Maximum (%s):	64 kBit/s
Average (%s):	7 kBit/s
Receiving:	
Current (%s):	5 kBit/s
Minimum (%s):	64 Bit/s
Maximum (%s):	273 kBit/s
Average (%s):	13 kBit/s

You can use the left-hand mouse key to mark any period in the graph, and these statistical values will be displayed separately.

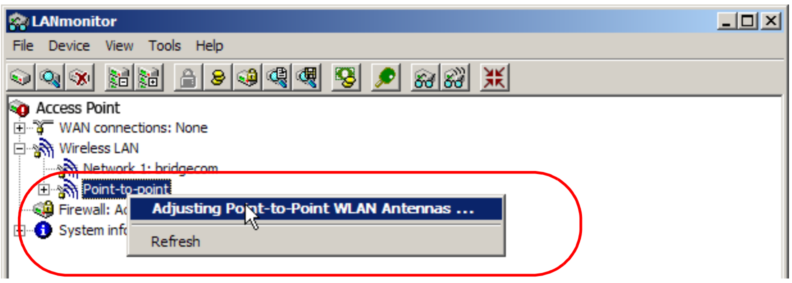
This dialog displays the values collected over the last 24 hours.

Please note that the values on display are deleted when the dialog is closed. For monitoring over a longer period, leave the window open.

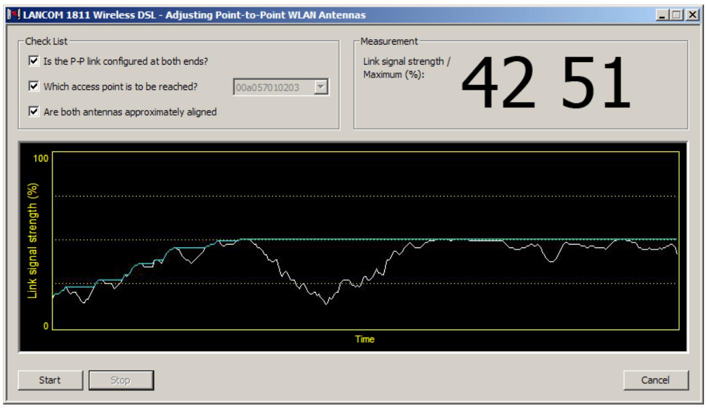
A.14 Setting up point-to-point connections with LANmonitor

To find the best possible alignment for point-to-point connection antennas, the current signal quality over a P2P connection can be displayed on the device's LEDs or in LANmonitor. LANmonitor provides not only an optical display of link strength, but an acoustic signal as well.

In LANmonitor the connection quality display is opened with the context menu. Right-clicking with the mouse on 'Point-to-point' activates the option 'Adjusting Point-to-Point WLAN Antennas...'



Once signal monitoring has commenced, the P2P dialog displays the absolute values for the current signal strength and the maximum value since starting the measurement. The development of the signal strength over time and the maximum value are displayed in a diagram, too.


LANCOM 1811 Wireless DSL - Adjusting Point-to-Point WLAN Antennas

Check List

☑ Is the P-P link configured at both ends?

☑ Which access point is to be reached? 00a057010203

☑ Are both antennas approximately aligned

Measurement

Link signal strength / Maximum (%): 42 51

Initially only one of the two antennas should be adjusted until a maximum value is achieved. This first antenna is then fixed and the second antenna is then adjusted to attain the best signal quality.

An acoustic signal can be activated to help align the antennas precisely. With this option, the PC can emit a tone which varies according to signal strength. Maximum signal strength over the link is signaled by a constant tone. If the signal strength drops below the maximum, tones are emitted at intervals indicating the difference from the former maximum. The shorter the interval, the closer the current link signal strength is to the maximum.

A Addendum to LCOS Version 7.8

A.1 Overview

A.2 DHCP cluster

A.2.1 Introduction

If multiple DHCP servers are active in a network, the stations "divide" themselves equally between them. However, the DNS server in LANCOM devices can only properly resolve the name of the station which was assigned the address information by the DHCP server. In order for the DNS server to be able to resolve the names of other DHCP servers, these can be operated in a cluster. In this operating mode, the DHCP server monitors all DHCP negotiations in the network. It additionally supplements its table with the stations which are registered at the other DHCP servers in the cluster.

A.2.2 Configuration

A DHCP server's operation in the cluster can be activated or deactivated for each individual ARF network with the associated DHCP settings.

WEBconfig: LCOS menu tree ▶ Setup ▶ DHCP ▶ Network list

- **Cluster**

  This setting defines whether the DHCP server for this ARF network is to be operated separately or in the cluster.

  Possible values:

  □ Yes: With cluster mode activated, the DHCP server monitors all of the ongoing DHCP negotiations in the network, and it additionally supplements its table with the stations which are registered at the other DHCP servers in the cluster. These stations are flagged as "cache" in the DHCP table.

  □ No: The DHCP server manages information only for the stations connected to it.

  Default:

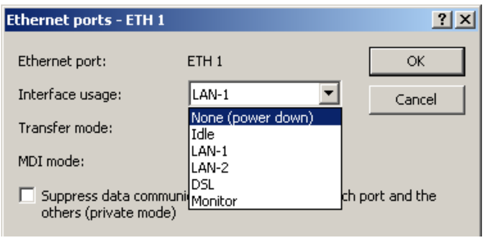
  □ No

If the lease time for the information supplied by DHCP expires, the station requests a renewal from the DHCP server which supplied the original information.
If the original DHCP server does not respond, the station then emits its rebinding request as a broadcast to all available DHCP servers.
DHCP servers in a cluster ignore renew requests, which forces a rebinding. The resulting broadcast is used by all of the DHCP servers to update their entries for the station.
The only DHCP server to answer the rebind request is the one with which the station was originally registered. If a station repeats its rebind request, the all DHCP servers in the cluster assume that the original DHCP server is no longer active in the cluster, and they respond to the request. The responses received by

the station will have the same IP address, but the gateway and DNS server addresses may differ. From these responses, the station selects a new DHCP server to connect with, and it updates its gateway and DNS server (and other relevant parameters) accordingly.

A.3 Deactivating Ethernet interfaces

The Ethernet interfaces on any publicly accessible LANCOM device can potentially be used by unauthorized persons to gain physical access to a network. The Ethernet interfaces on the device can be disabled to prevent this.



Ethernet ports - ETH 1

Ethernet port: ETH 1

Interface usage: LAN-1

Transfer mode:

MDI mode:

☐ Suppress data communi... ch port and the others (private mode)

LANconfig: Interfaces ▶ LAN ▶ Interface settings

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces

- **Interface usage**

  Here you select how this interface is to be used.

  Possible values:

  - None (power down): The interface is deactivated.
  - Idle: The interface is not allocated to any particular task, but it remains physically active.
  - LAN-1 to LAN-n: The interface is allocated to a logical LAN.
  - DSL-1 to DSL-n: The interface is allocated to a DSL interface.
  - Monitor: The port is a monitor port, i.e. everything received at the other ports is output via this port. A packet sniffer such as Wireshark / Ethereal can be connected to this port, for example.

  Default:

  - Depends on the particular interface or the hardware model.

A.4 ARF network for IAPP

Access points use the IAPP protocol to communicate and pass information about the handovers of associated WLAN clients which are roaming. Access points regularly send out multicast announcements to inform the devices about the BSSIDs and IP addresses of the other access points. A roaming WLAN client initiates a handover by informing a new access point about its former AP. The access point uses the information supplied by the IAPP protocol to inform the former access point to remove the WLAN client from its list of associated clients.

Where an access point supports multiple ARF networks, the IAPP announcements are transmitted on all ARF networks. To limit these multicasts to one particular ARF network, it is possible to define an IAPP IP network.

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN

- **IAPP-IP network**

  Here you select the ARF network which is to be used as the IAPP-IP network.

  Possible values:

  - Selection from the list of ARF networks defined in the device; max. 16 alphanumerical characters

  Default:

  - Blank

  Special values:

  - Blank: If no IAPP-IP network is defined, IAPP announcements are transmitted on all of the defined ARF networks.

A.5 Routing of local services/ARP handling switchable

A.5.1 Introduction

Response packets for internal services (such as telnet, http/https, tftp, etc.) from the LANCOM to recipients in the Ethernet (LAN or WAN) were, prior to LCOS version 7.80, always sent directly to the corresponding requester. This meant, among other things, that devices could be detected from within any LAN.

As of LCOS version 7.80, a switch provides the option to initiate an ARP request to determine a specific route, instead of using the direct address.

If, for example, a LANCOM router should be detected by LANconfig without any knowledge of the LAN topology, then the older method would be preferable. In this case, the sender of the TFTP broadcast (in this case LANconfig/ device search) receives a direct unicast response from the router.

In scenarios where LANs use changing virtual MAC and IP addresses (e.g. when VRRP components are used in the LAN), direct addressing may lead to errors if the redundancy protocol has adjusted the MAC/IP assignments. In such cases it is preferable to activate the "route internal services" option.

A.5.2 Configuration

The appropriate settings for IP routing can be used to route the LANCOM's internal services via the router.

WEBconfig: LCOS menu tree ▶ Setup ▶ IP router ▶ Routing method

- **Route internal services**

  This is where you select whether the internal services are to be directed via the router.

  Possible values:

  □ Yes: Packets for internal services are directed via the router.

  □ No: Packets are returned straight to the sender.

  Default:

  □ No

A.6 XAUTH with external RADIUS servers

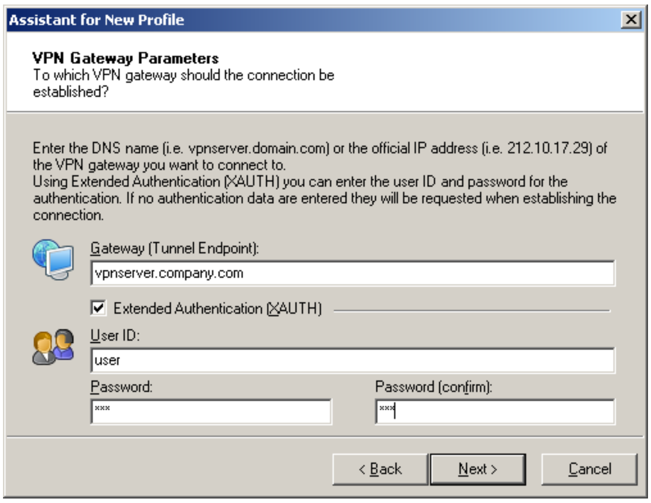
As of LCOS version 7.60, LANCOM devices can identify and authenticate remote stations with the Extended Authentication Protocol (XAUTH). Authentication referred to the user data in the PPP list.

As of LCOS version 7.80, XAUTH authentication can also be handled by an (external) RADIUS server. For example, this allows reference to existing RAS user data on the RADIUS server, assuming that RADIUS-authenticated dial-in via PPP has been set up for VPN with XAUTH.

To supplement VPN dial-in with XUTH for authentication, please proceed as follows:

① Set up a VPN dial-in account, for example with the LANconfig Setup Wizard.

② Activate XAUTH in the VPN client at the station which is to dial in. The user name and password are the same as those stored on the RADIUS server.



Assistant for New Profile

VPN Gateway Parameters
To which VPN gateway should the connection be established?

Enter the DNS name (i.e. vpnserver.domain.com) or the official IP address (i.e. 212.10.17.29) of the VPN gateway you want to connect to.
Using Extended Authentication (XAUTH) you can enter the user ID and password for the authentication. If no authentication data are entered they will be requested when establishing the connection.

Gateway (Tunnel Endpoint): vpnserver.company.com

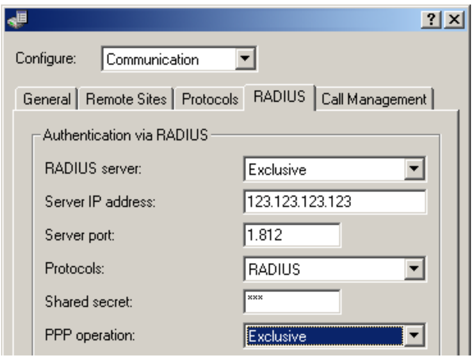
☑ Extended Authentication (XAUTH)

User ID: user

Password: ***

Password (confirm): ***

③ Activate the authentication of dial-in remote stations via the XAUTH protocol on an external RADIUS server. In LANconfig, access the configuration area **Communication** and the **RADIUS** tab to activate the "Exclusive" operating mode for the RADIUS server. With this setting, all incoming XAUTH requests are authenticated by the RADIUS server.



Configure: Communication

Authentication via RADIUS

RADIUS server: Exclusive

Server IP address: 123.123.123.123

Server port: 1.812

Protocols: RADIUS

Shared secret: ***

PPP operation: Exclusive

④ You should also specify the IP address, the port, and the key for the external RADIUS server.

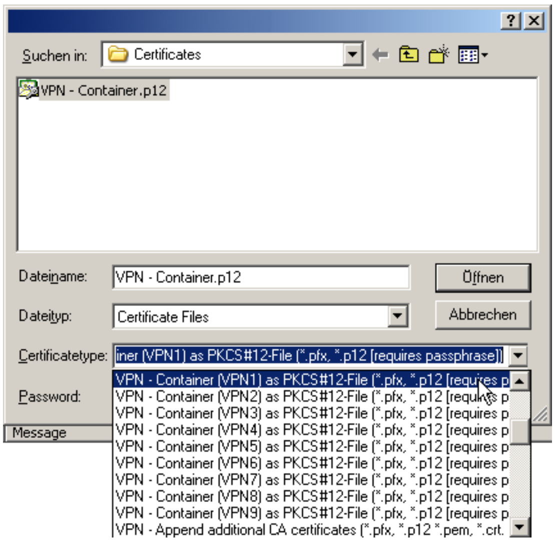
⑤ Also set PPP operation to "Exclusive" so that incoming XAUTH requests are authenticated by the RADIUS server only.

A.7 Enhanced certificate support

In order to support multiple certificate heirarchies, LCOS as of version 7.80 allows up to nine PKCS#12 files to be uploaded to the device. Also, further files with individual additional CA certificates can be uploaded, which enclose the certificates either individually or as PKCS#12 containers. All certificate hierarchies can be managed manually or with SCEP, and they can use CRLs.

LANconfig: Device ▶ Configuration management ▶ Upload certificate from file

WEBconfig: File management ▶ Upload certificate or file


Öffnen
Abbrechen
VPN - Container (VPN1) as PKCS#12-File (*.pfx, *.p12 [requires p
VPN - Container (VPN2) as PKCS#12-File (*.pfx, *.p12 [requires p
VPN - Container (VPN3) as PKCS#12-File (*.pfx, *.p12 [requires p
VPN - Container (VPN4) as PKCS#12-File (*.pfx, *.p12 [requires p
VPN - Container (VPN5) as PKCS#12-File (*.pfx, *.p12 [requires p
VPN - Container (VPN6) as PKCS#12-File (*.pfx, *.p12 [requires p
VPN - Container (VPN7) as PKCS#12-File (*.pfx, *.p12 [requires p
VPN - Container (VPN8) as PKCS#12-File (*.pfx, *.p12 [requires p
VPN - Container (VPN9) as PKCS#12-File (*.pfx, *.p12 [requires p
VPN - Append additional CA certificates (*.pfx, *.p12 *.pem, *.crt,
Message

Suchen in: Certificates

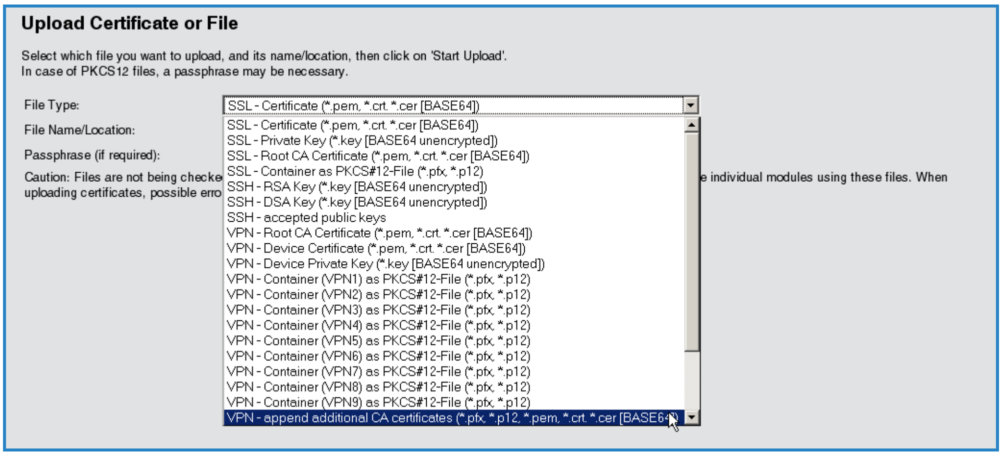
VPN - Container.p12

Dateiname: VPN - Container.p12

Dateityp: Certificate Files

Certificatetype: iner (VPN1) as PKCS#12-File (*.pfx, *.p12 [requires passphrase])

Password:


SSL - Certificate (*.pem, *.crt, *.cer [BASE64])
SSL - Private Key (*.key [BASE64 unencrypted])
SSL - Root CA Certificate (*.pem, *.crt, *.cer [BASE64])
SSL - Container as PKCS#12-File (*.pfx, *.p12)
SSH - RSA Key (*.key [BASE64 unencrypted])
SSH - DSA Key (*.key [BASE64 unencrypted])
SSH - accepted public keys
VPN - Root CA Certificate (*.pem, *.crt, *.cer [BASE64])
VPN - Device Certificate (*.pem, *.crt, *.cer [BASE64])
VPN - Device Private Key (*.key [BASE64 unencrypted])
VPN - Container (VPN1) as PKCS#12-File (*.pfx, *.p12)
VPN - Container (VPN2) as PKCS#12-File (*.pfx, *.p12)
VPN - Container (VPN3) as PKCS#12-File (*.pfx, *.p12)
VPN - Container (VPN4) as PKCS#12-File (*.pfx, *.p12)
VPN - Container (VPN5) as PKCS#12-File (*.pfx, *.p12)
VPN - Container (VPN6) as PKCS#12-File (*.pfx, *.p12)
VPN - Container (VPN7) as PKCS#12-File (*.pfx, *.p12)
VPN - Container (VPN8) as PKCS#12-File (*.pfx, *.p12)
VPN - Container (VPN9) as PKCS#12-File (*.pfx, *.p12)
VPN - append additional CA certificates (*.pfx, *.p12, *.pem, *.crt, *.cer [BASE64

Upload Certificate or File

Select which file you want to upload, and its name/location, then click on 'Start Upload'.
In case of PKCS12 files, a passphrase may be necessary.

File Type: SSL - Certificate (*.pem, *.crt, *.cer [BASE64])

File Name/Location:

Passphrase (if required):

Caution: Files are not being checke … e individual modules using these files. When uploading certificates, possible erro

The certificates in the device can be viewed in the status area:

WEBconfig: Status ▶ Status ▶ Certificates ▶ Device certificates

The internal file system for the device classifies the device certificates as applications "VPN1" to "VPN9".

To use the certificate, either the certificate subject or this abbreviation can be used as "local identity" in the IKE keys of type ASN.1-Distinguished Name.

Using this abbreviation to reference the certificates allows subjects containing special characters to be used, such as German umlauts. This is not usually possible when working with the command-line interface configuration.

The abbreviation is entered as "Application" when configuring the certificates for the SCEP client.

A.8 Wildcard matching of certificates

A.8.1 Introduction

Generally speaking, the local identity and remote identity for certificate-based VPN connections are the certificate subjects. In the VPN configuration, these are stored in the form of (often complex) ASN.1 Distinguished Names (DN). During VPN negotiation, the local identity is used to select the certificate which is to be transmitted to the remote station, whereas the local value for the remote identity is compared with the received identity of the remote station and the subject of the received certificate.

Until now, the local and the remote identities had to be entered in full into the VPN configuration. Not only is this prone to error, it is sometimes desirable to specify only a part of the certificate subject. This is practical where different certificates with similar subjects are to be accepted automatically, for example where certificates can change, or where multiple parallel certificate hierarchies operate simultaneously.

This is facilitated by flexible identity comparison. The certificate subjects have to contain the components of an ASN.1 Distinguished Name (DN) (Relative Distinguished Names – RDNs) as included in the configured identities. The RDNs can be in any order. Also, the RDN values can include the wildcards '?' and '*'. If the RDNs are to include wildcards, these must be entered in the form '\?' or '*'. Examples:

- Subject = '/CN=John Doe/O=*ACME*', DN = '/CN=John?Doe*'
- Subject = '/CN=John Doe/O=*ACME*', DN = '/O=*ACME*'

A.8.2 Configuration

This flexible method of identification comparison is activated or deactivated in the VPN configuration.

WEBconfig: LCOS menu tree ▶ Setup ▶ VPN

- **Flexible ID comparison**

  Possible values:

  □ Yes, No

  Default:

  □ No

Flexible identity comparison is used when checking the (received) remote identity and also for selecting the certificate based on the local identity.

A.9 Multiple WLAN profiles in client mode

A.9.1 Introduction

If a device equipped with an Ethernet interface is to be connected to a wireless LAN, a LANCOM access point can be switched into client mode, causing it to act as conventional wireless LAN client and not as an access point.

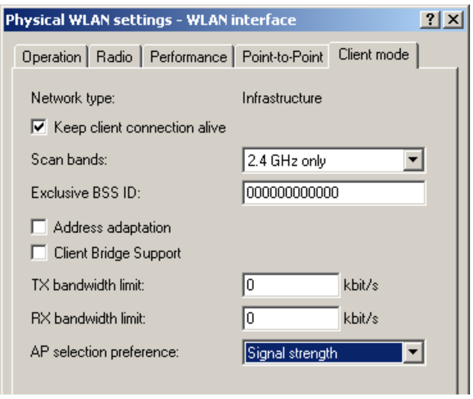
WLAN clients such as notebooks are generally able to save and manage various profiles which allow different access points to be selected depending on the environment (e.g. for a company WLAN or for another WLAN at home). These profiles store various information such as the WLAN SSID and the associated key. The WLAN client automatically selects the profile fitting to the strongest available or preferred WLAN.

LANCOM access points can store up to eight different WLAN profiles for use in client mode. The profile in client mode activates the networking and transmission parameters, and also the encryption settings for the logical WLAN.

Please observe that a WLAN module in client mode only connects to one access point at a time, even if multiple WLAN profiles have been defined.

A.9.2 Configuration

Not only can networking, transmission and encryption parameters be defined separately for each WLAN module, but also which criteria are to be used to select the client profile.



Network type: Infrastructure

☑ Keep client connection alive

Scan bands: 2.4 GHz only

Exclusive BSS ID: 000000000000

□ Address adaptation

□ Client Bridge Support

TX bandwidth limit: 0 kbit/s

RX bandwidth limit: 0 kbit/s

AP selection preference: Signal strength

LANconfig: Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Client mode

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ Client modes ▶ WLAN-1

- **AP selection preference**

  Here you select how this interface is to be used.

  Possible values:

  - Signal strength: Selects the profile for the WLAN offering the strongest signal. This setting causes the WLAN module in client mode to automatically switch to a different WLAN as soon as it offers a stronger signal.
  - Profile: Selects the profile for available WLANs in the order that they have been defined (WLAN index, e.g. WLAN-1, WLAN-2, etc.), even if another WLAN offers a stronger signal. In this setting, the WLAN module in client mode automatically switches to a different WLAN as soon as a WLAN with a lower WLAN index is detected (irrespective of signal strengths).

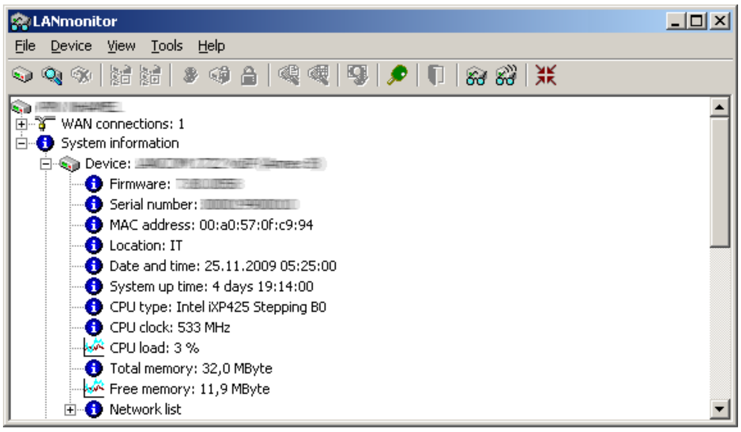
  Default:

  - Signal strength.

A.10 Averaging of CPU- load display

A.10.1 Introduction

The current CPU load for the device can be output in various ways (LANmonitor, WEBconfig, or CLI in the status area; some models have an integrated display).



[redacted]
WAN connections: 1
System information
Device: [redacted]
Firmware: [redacted]
Serial number: [redacted]
MAC address: 00:a0:57:0f:c9:94
Location: IT
Date and time: 25.11.2009 05:25:00
System up time: 4 days 19:14:00
CPU type: Intel IXP425 Stepping B0
CPU clock: 533 MHz
CPU load: 3 %
Total memory: 32,0 MByte
Free memory: 11,9 MByte
Network list

A.10.2 Configuration

You can set the time interval for averaging the value for the displayed CPU load.

WEBconfig: LCOS menu tree ▶ Setup ▶ Config

- **CPU-load interval**

  You can select the time interval for averaging the CPU load. The CPU load displayed in LANmonitor, in the status area, in the display (if fitted), or by SNMP tools is a value which is averaged over the time interval set here. The status area under WEBconfig or CLI additionally display the CPU load values for all four of the optional averaging periods.

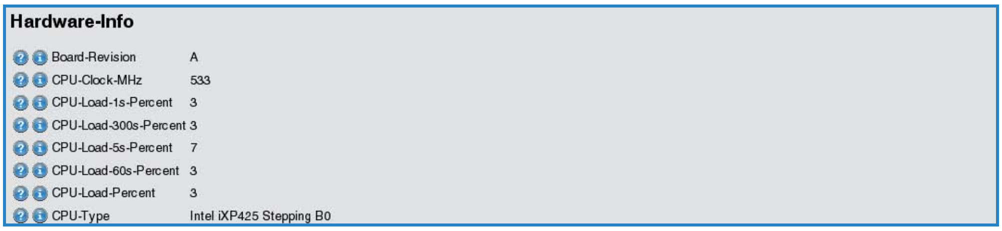
Possible values:

□ 1, 5, 60 or 300 seconds.

Default:

□ 60 seconds.

The default period of 60 seconds is specified by the HOST-RESOURCES-MIB, which is used by many SNMP tools to display CPU load in a tacho display. Please consider this specification when altering the CPU-load interval.



Hardware-Info

Board-Revision	A
CPU-Clock-MHz	533
CPU-Load-1s-Percent	3
CPU-Load-300s-Percent	3
CPU-Load-5s-Percent	7
CPU-Load-60s-Percent	3
CPU-Load-Percent	3
CPU-Type	Intel iXP425 Stepping B0

A.11 Bypassing TACACS+

A.11.1 Introduction

TACACS+ enables every change to a network-device configuration to be subject to special authorization. TACACS+ accounting enables each of these steps to be logged. TACACS+ is a requirement for systems used in electronic payment (PCI compliance).

Strict monitoring of this type leads to an increase in traffic to and from the TACACS+ server(s). In large-scale scenarios, the TACACS+ communications caused when using scripts for centralized configuration changes or if CRON commands are run regularly could lead to an overload of the TACACS+ server.

A.11.2 Configuration

To avoid overloading the TACACS+ server when carrying out automatic configuration changes, it is possible to exclude CRON, action tables and scripts from the authorization and accounting by TACACS+.

WEBconfig: LCOS menu tree ▶ Setup ▶ TACACS+

- **Bypass-Tacacs-for-CRON/scripts/action-table**

  You can activate or deactivate the bypassing of TACACS+ authorization and TACACS+ accounting for various actions.

  Possible values:

  □ Activated, deactivated.

  Default:

  □ Disabled.

Please observe that this option influences the TACACS+ function for the entire system. Be sure that you restrict the use of CRON, the action tables, and scripts only to an absolutely trustworthy circle of administrators!

A.12 Serial COM-port enhancements

A.12.1 Introduction

The COM-port configuration has been enhanced with a number of parameters.

A.12.2 Configuration

The additional parameters are located in the network settings for the COM port.

WEBconfig: LCOS menu tree ▶ Setup ▶ COM ports ▶ COM-port server ▶ Network settings

- **Assume binary mode**

  Some network devices connected to a serial COM port transmit data structures which may be interpreted as control characters (CR/LF – carriage return / line feed). In the default setting, the COM-ports in LANCOM devices process this information to control the data flow. "Binary mode" instructs a COM port to forward the data in binary format and ignore any control characters.

  Possible values:

  □ Yes, No.

  Default:

  □ No.

- **Newline conversion**

  Here you select the character to be output by the serial port when binary mode is activated.

  This setting is independent of the application communicating via the serial port. If the port is connected to another LANCOM device, you can either enter CRLF here or just CR. This is because the outband interface of these devices expects a "carriage return" for the automatic determination of data-transfer speed. However, some Unix applications interpret CRLF as a prohibited double line feed character. In these cases enter either CR or LF.

  Possible values:

  □ CRLF, CR, LF

  Default:

  □ CRLF

This setting is only relevant if binary mode is **deactivated** for this port.

- **TCP keepalive**

  The RFC 1122 sets down a method of checking the availability of TCP connections, called TCP keepalive. An inactive transmitter queries the receive status from the remote station. If the TCP session to the remote site is available, then the remote responds with its receive status. If the TCP session to the remote site is not available, then the query is repeated for as long as it takes for the remote to respond with its receive status (after which a longer interval comes into play). As long as the basic connection functions, but the TCP session to the remote station is not available, then the remote station sends an RST packet which triggers the establishment of the TCP session by the requesting application.

  Possible values:

  □ Inactive: TCP keepalive is not used.

  □ Active: TCP keepalive is active; only RST packets cause the disconnection of TCP sessions.

  □ Proactive: TCP keepalive is active, but the request for the receive status from the remote site is only repeated for the number of times defined under "TCP retry count". If this number of requests expires without a response with the receive status, then the TCP sessions is classified as "not available" and the application is informed. If an RST packet is received during the wait time, the TCP session will be disconnected prematurely.

  Default:

  □ Inactive

The setting "active" is recommended for server applications.

- **TCP keepalive interval**

  This value defines the interval between sending requests for receive status if the first request is not affirmed. The associated timeout is defined as being interval/3 (max. 75 sec.).

  Possible values:

  □ Maximum 10 characters

  Default:

  □ 0

  Special values:

  □ 0 activates the RFC 1122 default values (interval 7200 seconds, timeout 75 seconds).

- **TCP retransmit timeout**

  Maximum time for the retransmission timeout. This timeout defines the the interval between checking TCP-connection status and reporting the result to the application using the TCP connection.

  Possible values:

  - □ 0 to 99 seconds.

  Special values:

  - □ 0 activates the RFC 1122 default value (60 seconds).

  Default:

  - □ 0

The maximum duration of the TCP-connection check is the product of TCP-retransmit-count and TCP-retry-count. The TCP application is only informed after the timeout for all attempts has expired. With the default values of 60 seconds timeout and max. 5 attempts, it can take up to 300 seconds before the application is informed about an inactive TCP connection.

- **TCP retry count**

  The maximum number of attempts for checking TCP-connection status and reporting the result to the application using the TCP connection.

  Possible values:

  - □ 0 to 9

  Special values:

  - □ 0 activates the RFC 1122 default value (5 attempts).

  Default:

  - □ 0

The maximum duration of the TCP-connection check is the product of TCP-retransmit-count and TCP-retry-count. The TCP application is only informed after the timeout for all attempts has expired. With the default values of 60 seconds timeout and max. 5 attempts, it can take up to 300 seconds before the application is informed about an inactive TCP connection.

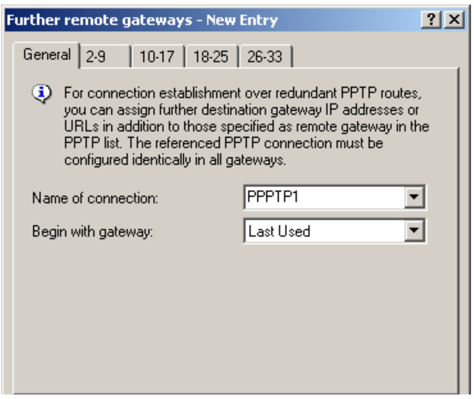
A.13 32 additional gateways for PPTP connections

A.13.1 Introduction

Up to 32 additional gateways can be configured to assure the availability of any PPTP remote station. Consequently, each PPTP remote station can use a total of up to 33 gateways.

A.13.2 Configuration

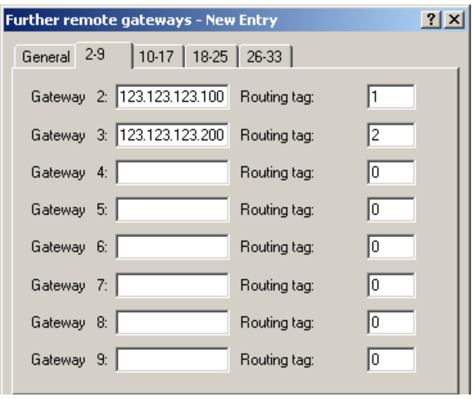
The additional PPTP gateways are defined in a separate list.



For connection establishment over redundant PPTP routes, you can assign further destination gateway IP addresses or URLs in addition to those specified as remote gateway in the PPTP list. The referenced PPTP connection must be configured identically in all gateways.

Name of connection: PPPTP1

Begin with gateway: Last Used



Gateway 2:	123.123.123.100	Routing tag:	1
Gateway 3:	123.123.123.200	Routing tag:	2
Gateway 4:		Routing tag:	0
Gateway 5:		Routing tag:	0
Gateway 6:		Routing tag:	0
Gateway 7:		Routing tag:	0
Gateway 8:		Routing tag:	0
Gateway 9:		Routing tag:	0

LANconfig: Communication ▶ Protocols ▶ Further remote gateways

WEBconfig: LCOS menu tree ▶ Setup ▶ DHCP ▶ Additional PPTP gateways

- **Name of connection**

  Here you select the PPTP remote site that this entry applies to.

Possible values:

- □ Select from the list of defined PPTP remote stations.

Default:

- □ Empty.

- ■ **Begin with**

  Here you select the order in which the entries are to be tried.

  Possible values:

  - □ Last used: Selects the entry for the connection which was successfully used most recently.
  - □ First: Selects the first of the configured remote sites.
  - □ Random: Selects one of the configured remote sites at random. This setting provides an effective measure for load balancing between the gateways at the headquarters.

  Default:

  - □ Last used

- ■ **Gateway 2 to 33**

  Enter the IP addresses of the additional gateways to be used for this PPTP remote station.

  Possible values:

  - □ IP address or 63 alphanumerical characters.

  Default:

  - □ Empty.

- ■ **Routing tag**

  Enter the routing tag for setting the route to the relevant remote gateway.

  Possible values:

  - □ Maximum 5 characters.

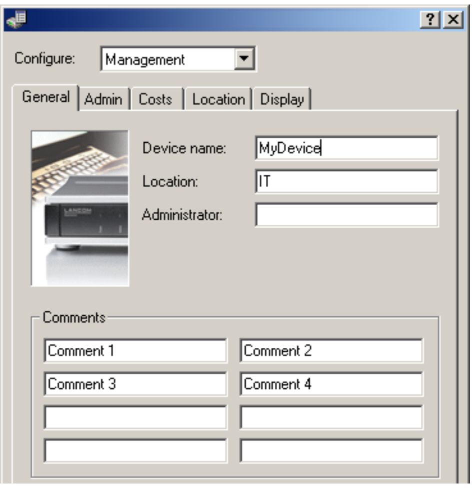
  Default:

  - □ 0.

If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

A.14 Additional commentary fields for describing the devices

Up to eight comments can be entered to describe the LANCOM devices.



Configure: Management

Device name: MyDevice

Location: IT

Administrator:

Comment 1

Comment 2

Comment 3

Comment 4

LANconfig: Management ▶ General

WEBconfig: LCOS menu tree ▶ Setup ▶ SNMP

- ■ **Comment 1 to 8**

  Enter a comment here.

  Possible values:

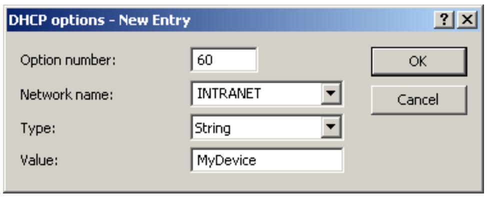
  - □ Maximum 255 alphanumerical characters.

Default:

- □ Blank

A.15 DHCP options with LANconfig

DHCP options can be used to send additional configuration parameters to the clients. The vendor class ID (DHCP option 60) shows e. g. the type of device. This table allows additional options for DHCP operations to be defined.


DHCP options - New Entry

Option number: 60

Network name: INTRANET

Type: String

Value: MyDevice

LANconfig: Management ▶ General

WEBconfig: LCOS menu tree ▶ Setup ▶ DHCP ▶ Additional options

- **Option number**

  Number of the option that should be sent to the DHCP client. The option number describes the transmitted information. For example "17" (root path) is the path to a boot image that a PC without its own hard disk uses to obtain its operating system via BOOTP.

  Possible values:

  - □ Maximum 3 characters.

  Default:

  - □ Blank

You can find a list of all DHCP options in RFC 2132 – "DHCP Options and BOOTP Vendor Extensions" of the Internet Engineering Task Force (IETF).

- **Network name**

  Name of the IP network where this DHCP option is to be used.

  Possible values:

  - □ Selection from the list of IP networks defined in the device; max. 16 characters

  Default:

  - □ Blank

- **Type**

  Entry type. This value depends on the respective option. For option "35" according to RFC 1232, e.g. the ARP cache time is defined as follows:

```
ARP cache timeout option

   This option specifies the timeout in seconds for ARP cache entries.

   The time is specified as a 32-bit unsigned integer.

   The code for this option is 35, and its length is 4.

    Code   Len           Time

   +-----+-----+-----+-----+-----+-----+

   |  35 |  4  |  t1 |  t2 |  t3 |  t4 |

   +-----+-----+-----+-----+-----+-----+
```

  This description tells you that this the type "32-bit integer" is used for this option.

  Possible values:

  - □ String, Integer8, Integer16, Integer32, IP address

  Default:

  - □ String

You can find out the type of the option either from the corresponding RFC or from the manufacturer's documentation of their DHCP options.

- **Value**

  This field defines the contents of the DHCP option.

  IP addresses are specified with the usual notation for IPv4 addresses, e.g. as "123.123.123.100", integer types are entered as normal decimal numbers, and strings as simple text.

  Multiple values in a single field are separated with commas, e.g. "123.123.123.100, 123.123.123.200".

  Possible values:

  □ Maximum 128 characters.

  Default:

  □ Blank

You can find out the possible length of the option value either from the corresponding RFC or from the manufacturer's documentation of their DHCP options.

A.16 Setting the routing tag for local routes

The definition of interface tags in Advanced Routing and Forwarding (ARF) facilitates the use of virtual routers, which only use a part of the overall routing table. The interface tag for a packet received from another local router is set according to the following procedure:

① If the a packet's sender address is recognized as coming from an IP network which is defined in the device, then the interface tag for that IP address is used.

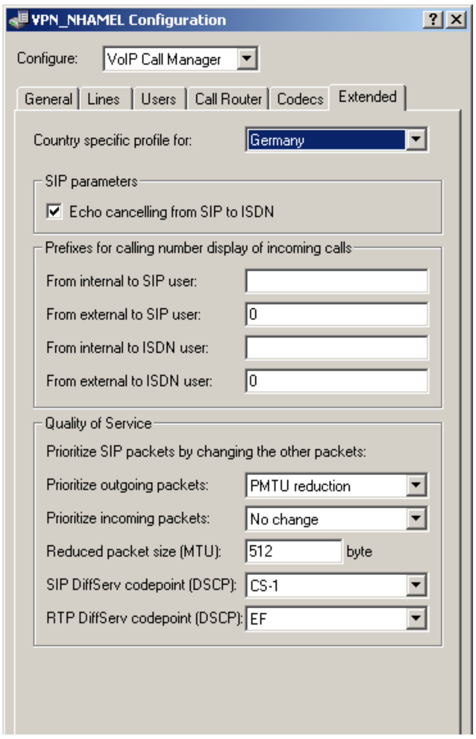
② If the interface receiving the packet is connected to just one IP network, then the interface tag for that IP network is used.

③ If there is no unique result from steps ① and ②, the device attempts to use the MAC address to determine the IP address of the next hop (reverse ARP lookup). The devices uses this IP address in an attempt to identify the relevant IP network, and thus the corresponding interface tag.

④ If there is no unique result from options ① to ③, then the device attempts to identify the relevant IP network (and interface tag) from the routing table.

A.17 Global settings, DiffServ for SIP & RTP

The Voice Call Manager marks SIP and RTP packets with DiffServ CodePoints (DSCP), which enables other hardware to recognize and prioritize these packets.


VPN_NHAMEL Configuration

Configure: VoIP Call Manager

General | Lines | Users | Call Router | Codecs | Extended

Country specific profile for: Germany

SIP parameters

☑ Echo cancelling from SIP to ISDN

Prefixes for calling number display of incoming calls

From internal to SIP user:

From external to SIP user: 0

From internal to ISDN user:

From external to ISDN user: 0

Quality of Service

Prioritize SIP packets by changing the other packets:

Prioritize outgoing packets: PMTU reduction

Prioritize incoming packets: No change

Reduced packet size (MTU): 512 byte

SIP DiffServ codepoint (DSCP): CS-1

RTP DiffServ codepoint (DSCP): EF

LANconfig: Voice Call Manager ▶ Advanced

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ General

- **SIP DiffServ CodePoint (DSCP)**

  This defines which DiffServ CodePoints (DSCP) the SIP packets (for call signaling) are to be marked with.

  Possible values:

  □ BE, CS-0, CS-1, CS-2, CS-3, CS-4, CS-5, CS-6, CS-7, AF-11, AF-12, AF-13, AF-21, AF-22, AF-23, AF-31, AF-32, AF-33, AF-41, AF-42, AF-43, EF

  Default:

  □ CS-1

The option CS-1 is actually outdated now, but it is set as the default value to ensure backwards compatibility. Common values for modern VoIP installations are CS-3, AF-31 or AF-41. We recommend using CS-3, one of the most widespread settings on the market.

- **RTP DiffServ CodePoint (DSCP)**

  This defines which DiffServ CodePoints (DSCP) the RTP packets (voice data stream) are to be marked with.

  Possible values:

  □ BE, CS-0, CS-1, CS-2, CS-3, CS-4, CS-5, CS-6, CS-7, AF-11, AF-12, AF-13, AF-21, AF-22, AF-23, AF-31, AF-32, AF-33, AF-41, AF-42, AF-43, EF

  Default:

  □ EF

With DSCP set to BE or CS-0 the packets are sent unmarked.
Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

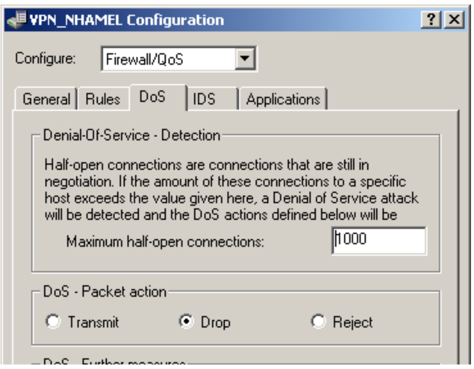
A.18 Increased DoS threshold value for central devices

Denial-of-Service attacks take advantage of inherent weaknesses in the TCP/IP protocol in combination with poor implementations.

- Attacks which target these inherent weaknesses include SYN Flood and Smurf.
- Attacks which target erroneous implementations include those operating with erroneously fragmented packets (e.g. Teardrop) or with fake sender addresses (e.g. Land).

Your device detects most of these attacks and reacts with appropriate countermeasures. Detecting these attacks relies on counting the number of connections which are concurrently under negotiation (half-open connections). If the number of half-open connections exceeds a certain threshold value, then the device assumes that a DoS attack is underway. The actions and measures which are taken in this case can be defined, similar to firewall rules.

Central devices are connected to a large number of users, so it is possible for a large number of half-open connections to exist without being caused by a DoS attack. For this reason, a higher default threshold value is required for the accurate detection of DoS attacks.



Configure: Firewall/QoS

Half-open connections are connections that are still in negotiation. If the amount of these connections to a specific host exceeds the value given here, a Denial of Service attack will be detected and the DoS actions defined below will be

Maximum half-open connections: 1000

○ Transmit ● Drop ○ Reject

LANconfig: Firewall/QoS ▶ DoS

WEBconfig: LCOS menu tree ▶ Setup ▶ IP router ▶ Firewall

- **Maximum half-open connections**

  Specifies the number of half-open connections which triggers DoS-attack countermeasures.

  Possible values:

- 0 to 9999

Default:

- 100
- 1000 for central-site devices such as the 7100, 7111, 8011, 9100, 4025(+), 4100.