LANCOM reference manual
Addendum to LCOS version 7.6

Revision 1 (December 2008)

LANCOM
Systems

© 2008 LANCOM Systems GmbH, Wuerselen (Germany). All rights reserved.

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

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

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

Trademarks

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

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

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

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

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

This product includes the LZMA SDK written by Igor Pavlov.

This product includes components available in source code as Open Source software with specific licenses and copyrights of various authors. In particular the firmware incorporates components which are subject to the GNU General Public License, version 2 (GPL). The license agreement including the text of the GPL can be found on the product CD in the product folder. The source codes and all license texts can be obtained from LANCOM Systems GmbH FTP server electronically upon request.

The firmware of LANCOM VP-100 incorporates components available in source code as Open Source software with specific licenses and copyrights of various authors. In particular the firmware incorporates components which are subject to the GNU General Public License, version 2 (GPL). The license agreement including the text of the GPL can be found on the product CD in the product folder as LC-VP100-License-EN.txt. The source codes and all license texts can be obtained from LANCOM Systems GmbH FTP server electronically upon request.

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

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom.de

Wuerselen, December 2008

A Addendum to LCOS-Version 7.6

A.1 Overview

This addendum describes the new functions with LCOS version 7.6 and the modifications since release 7.5:

- Configuration
  - Telnet: Enhanced functions for editing commands
  - Telnet: Functions for editing commands
  - WEBconfig: New WEBconfig with comprehensive device status, on-line help, etc.
  - Load files directly from a TFTP or HTTP server into the device
  - Managing rights for different administrators – administrators without trace rights
  - Asymmetric Firmsafe
  - LANconfig: Transferring device configurations to similar models
  - LANconfig: Automatic backup of configuration
  - LANconfig: Customizing the toolbar
  - LANconfig: Object-oriented definition of firewall rules (see Firewall)
  - LL2M: LANCOM Layer 2 Management protocol (LL2M)
- Diagnosis
  - LANmonitor: Saving support files with trace data, device configuration, bootlog and sysinfo
  - LANmonitor: Automatic backup of trace data
  - LANmonitor: Trace configuration with Wizards
  - LANmonitor: Display of Show commands
  - LANmonitor: Display of status information and statistics
  - LANmonitor: SSL-encrypted Telnet connection
  - Display of SYSLOG in LANmonitor and WEBconfig
- WAN
  - Flexible selection of the PPP authentication protocols
  - The Action table
  - GnuDIP support
  - COM port forwarding, using the serial interface in the LAN
  - Flexible definition of WAN-RIP remote stations by using place holders.
  - Interfaces tags for remote sites
- VPN
  - Unlimited number of VPN remote sites
  - Extended Authentication Protocol (XAUTH)
  - Backup via alternative VPN connection
  - Multi-level certificates
- Firewall
  - Object-oriented definition of firewall rules with LANconfig
  - Restricting the firewall rule to backup connections
  - Restricting the firewall rule to one station's connections
  - Specification of a maximum number of connections
  - Specification of a percentage of bandwidth
- Voice over IP

  New parameters for SIP provider lines ans SIP-PBX lines:
  - Local port number
  - (Re-) registration
  - Line monitoring
  - Monitoring interval
  - Trusted
  - Privacy method

  New parameter for ISDN ans SIP users:

- □ CLIR

New parameters for Analog users:

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

- WLAN
  - □ WLAN: Packet forwarding adjustable per SSID
  - □ DFS 2, version 1.4: Release of channels for weather radar
  - □ Central WLAN management: Internal script storage (script management without an HTTP server)
- 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

B Configuration

B.1 Configuration with different tools

B.1.1 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:

Configuration tool	Command (with English set as the console language)
WEBconfig	Expert configuration ▶ Config-Module ▶ Language
Telnet	`set /Setup/Config/Language Deutsch`

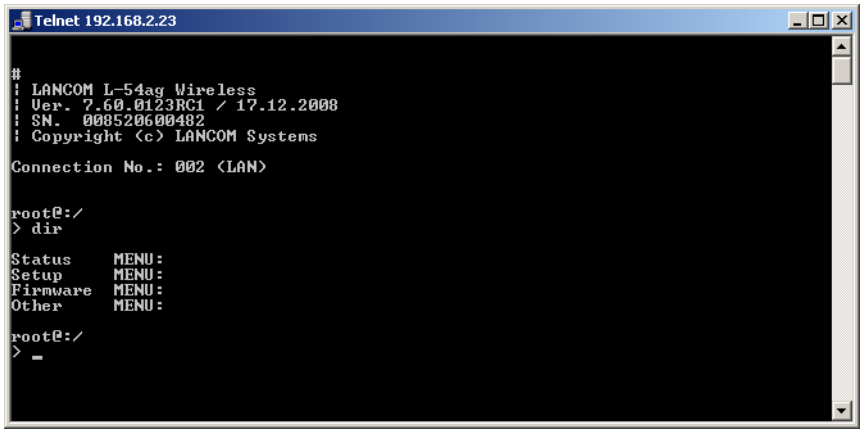
Close the Telnet session

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:



- **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.
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

Command	Description
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 "`cma`". 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.

Function	Esc key sequences	Description
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.

B.1.2 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.

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.

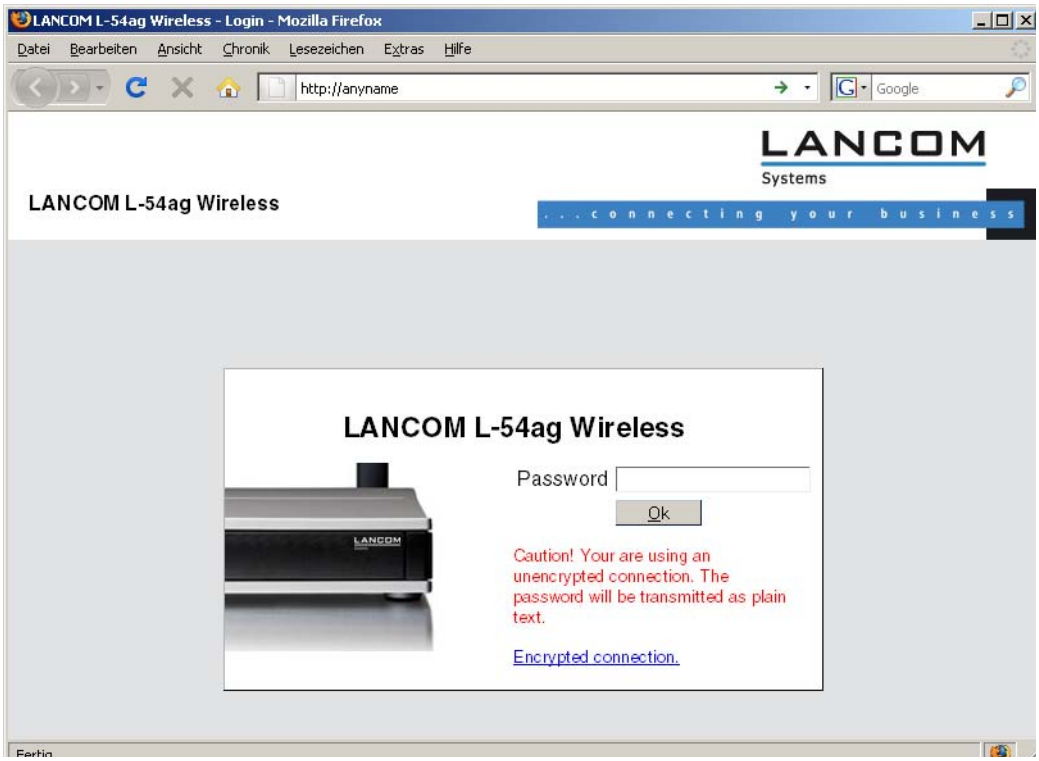
If a LANCOM Wireless Router or LANCOM Access Point is centrally managed from a LANCOM WLAN Controller, the DHCP mode is switched from auto-mode to client mode upon provision of the WLAN configuration.

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.

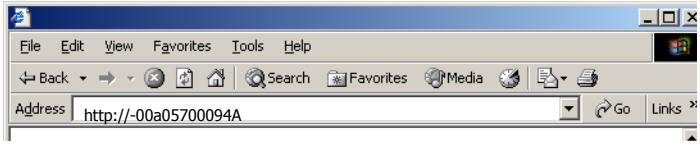


If the configuration computer does not retrieve its IP address from the LANCOM DHCP server, it determines the current IP address of the computer (with**Start** ▶ **Run** ▶ **cmd** and command **ipconfig** at the prompt under Windows 2000 or Windows XP, with **Start** ▶ **Run** ▶ **cmd** and command **winipcfg** 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".



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

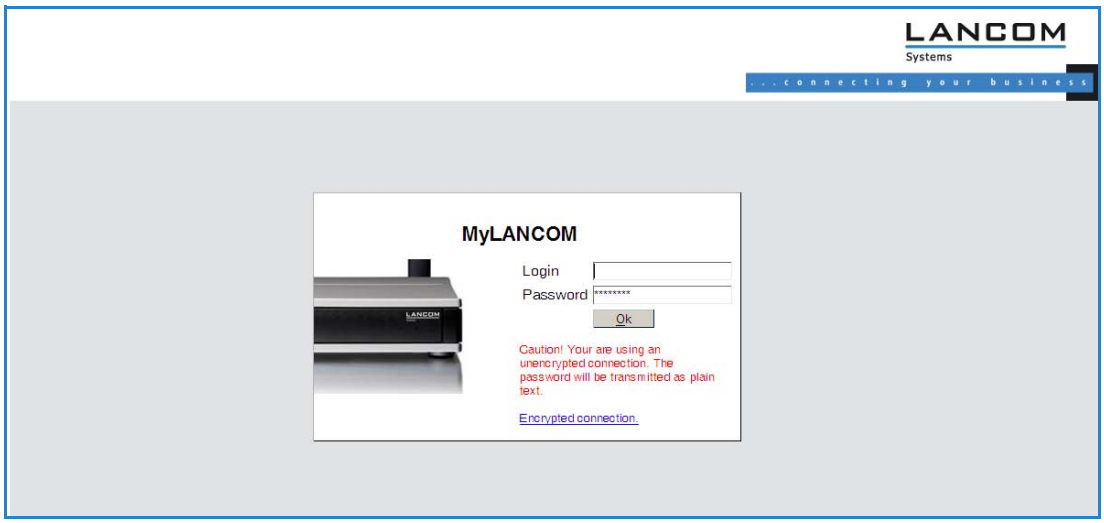
- If there is no DNS server in the LAN, or if it is not coupled to the DHCP server, the device cannot be reached via the name. In this case the following options remain:
  - Use LANconfig's “Find Device” function, or perform WEBconfig's “Device Search” from another yet accessible LANCOM.
  - Use suitable 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.

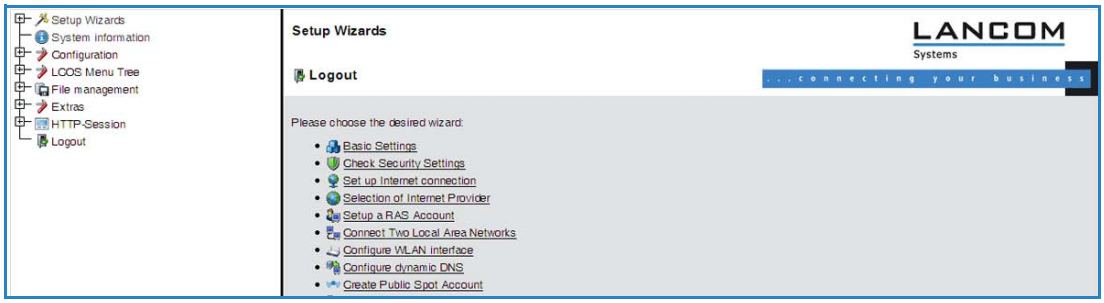
If you used the general configuration access, only enter the corresponding password. The user name field remains blank in this case.

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.



Setup Wizards

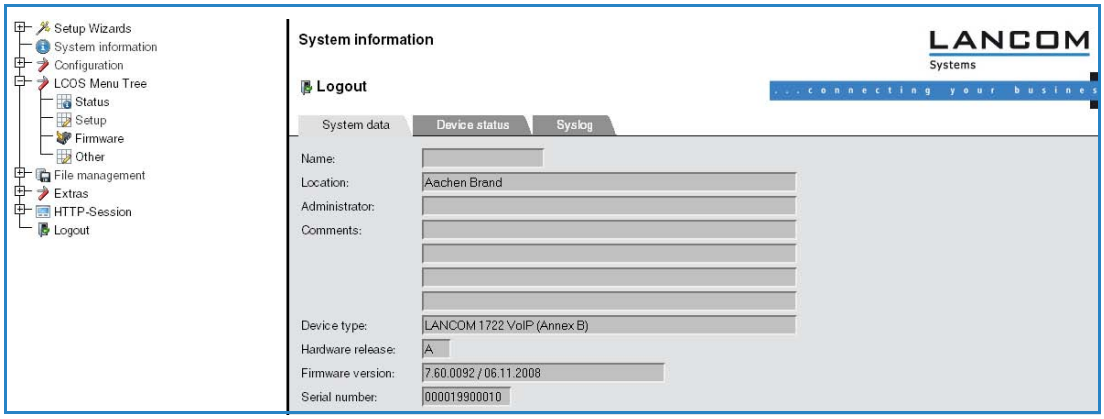
The setup Wizards allow quick and easy configuration of the most common device settings. Select the Wizard and enter the appropriate data on the following screens.



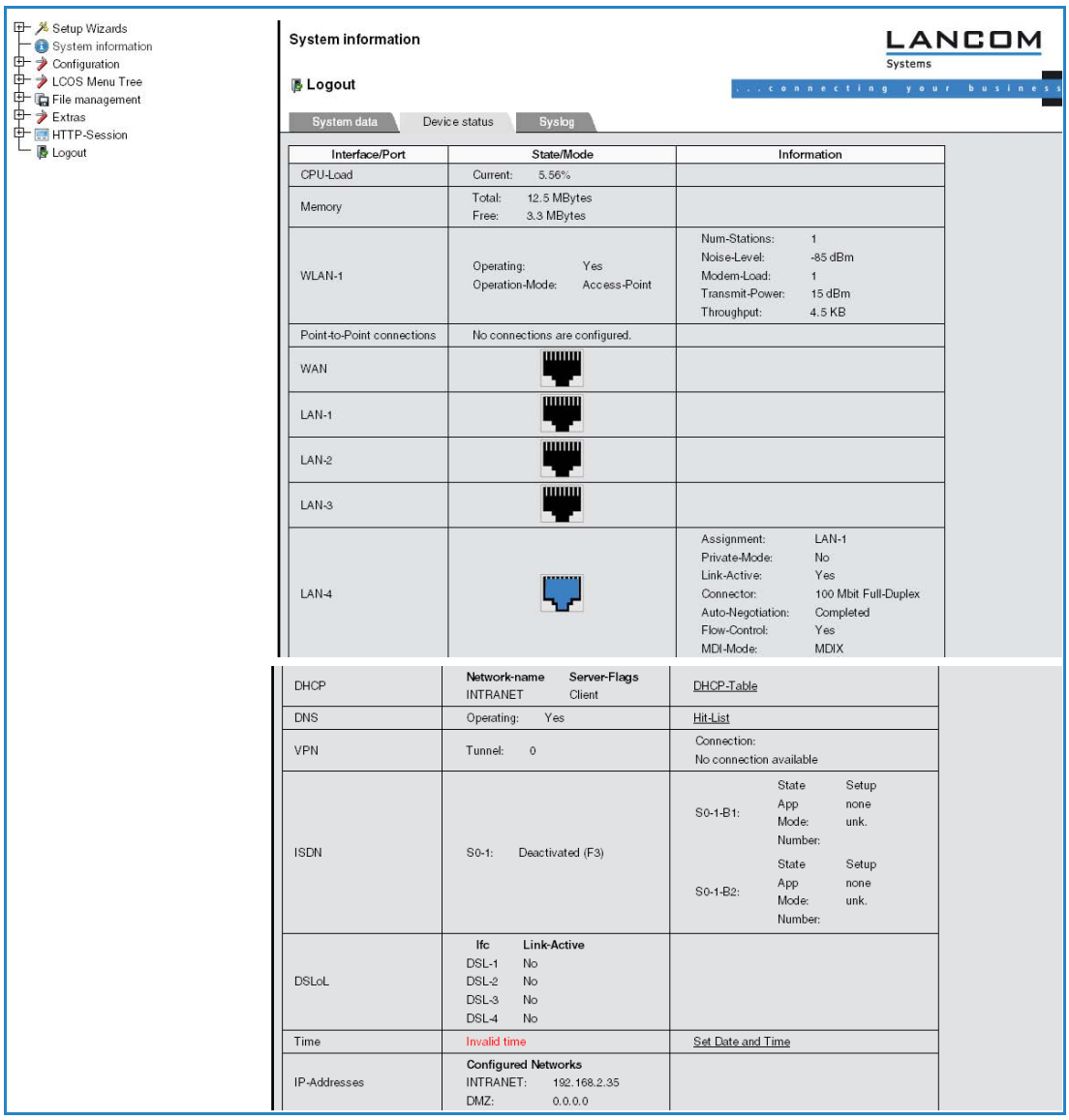
The settings are not stored in the device until inputs are confirmed on the last screen of the Wizard.

System information

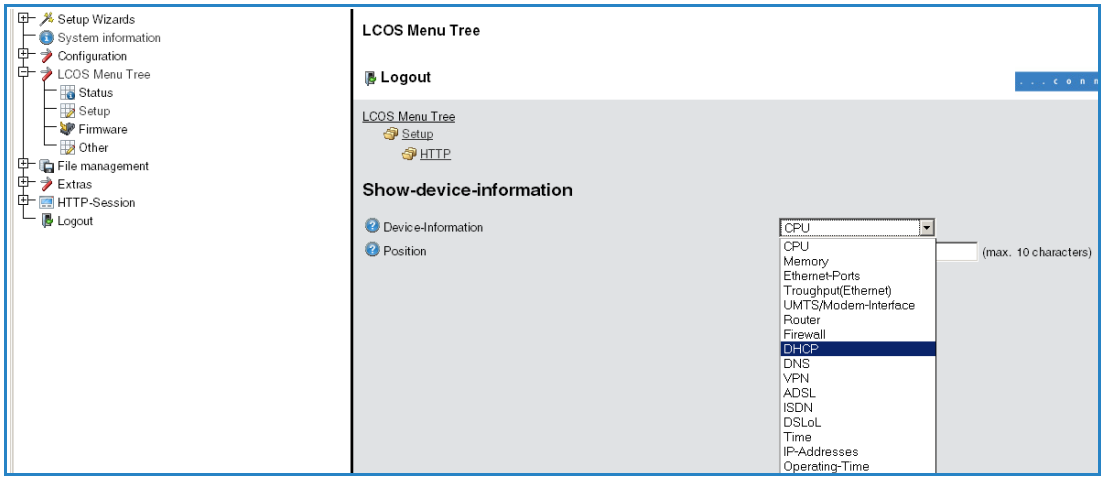
Under the "System Data" tab on the system information screen displays general information on the device including its location, the firmware version, the serial number, etc.



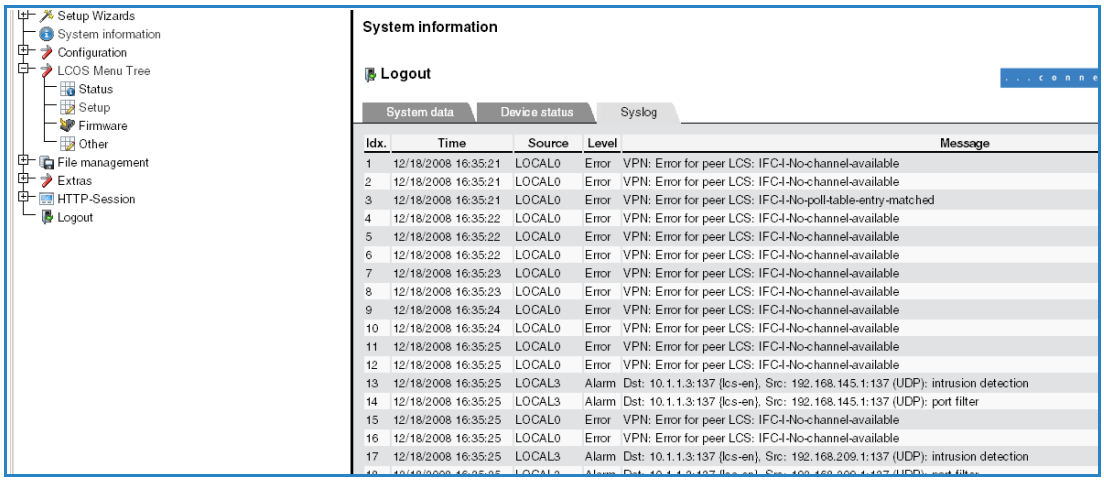
The "Device status" tab contains comprehensive information on the current operating state of the device. This includes, for example, a visual representation of the interfaces with information on the networks active on them. Appropriate links can be used to call up further relevant statistics (such as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



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.



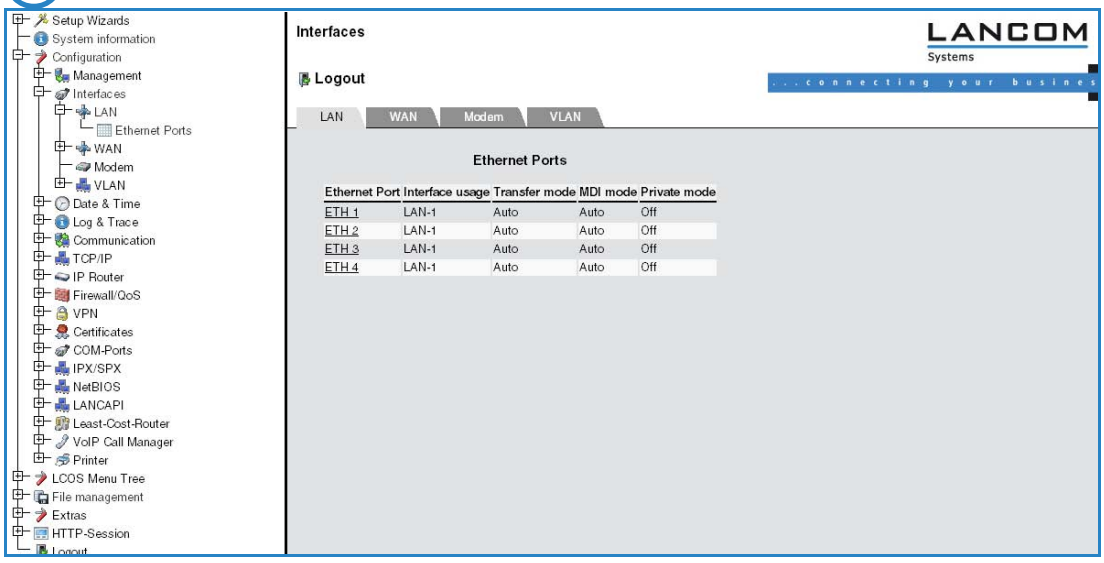
LANCOM devices also store syslog information to the main memory (see Syslog). You can also view the latest syslog entries in WEBconfig under "System information".



Configuration

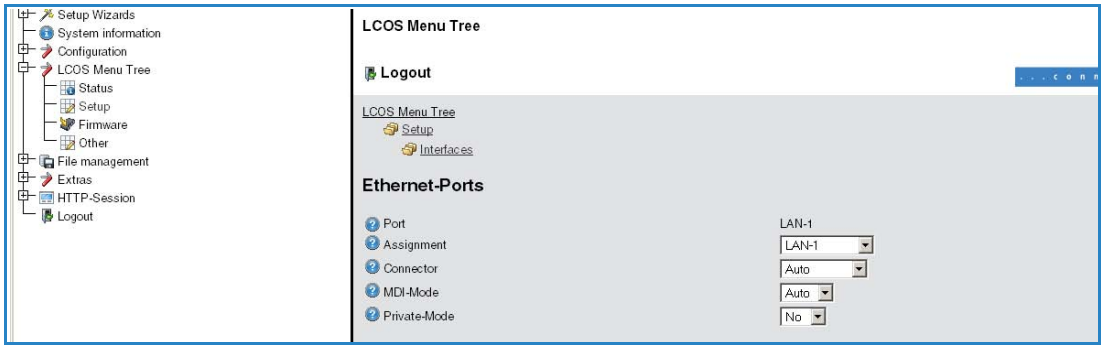
Menu area “Configuration” provides the configuration parameters in the same structure as they are used in LANconfig.

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



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.



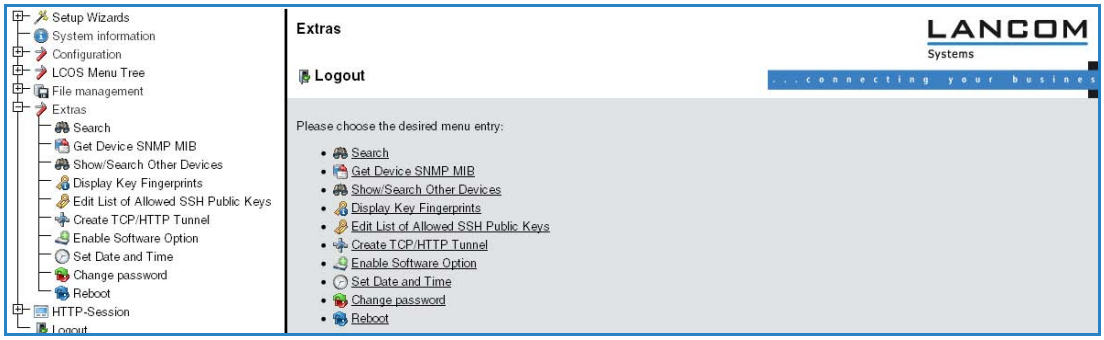
File management

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

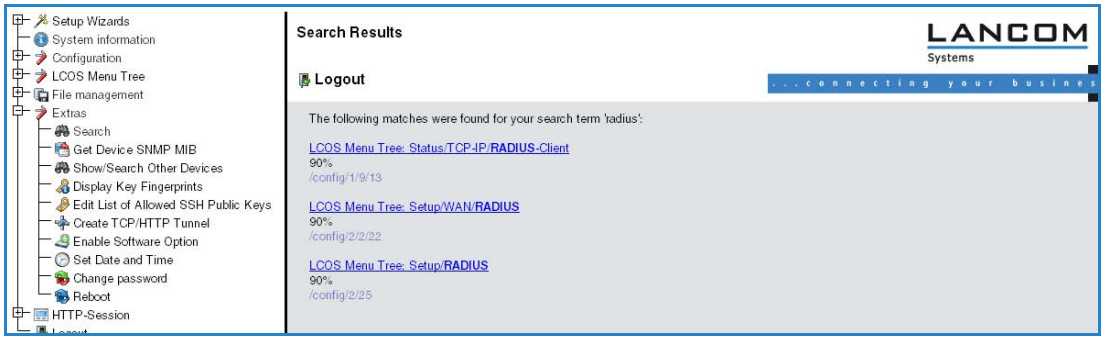
- Uploading new firmware
- Saving configuration
- Uploading configuration
- Using configuration script
- Saving configuration script
- Uploading certificate or file
- Downloading certificate or file

Extras

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



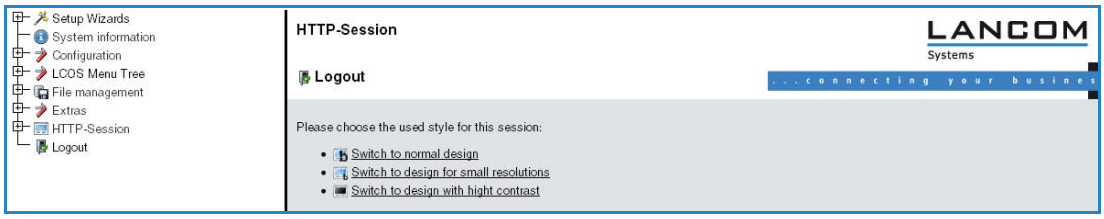
The search function can be used, for example, to search the names for all configuration parameters. If you know the name for a particular configuration parameter, but do not know which menu is used to reach this entry, you can quickly locate the required place in the LCOS menu in this way.



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.

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.



B.2 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.

B.2.1 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 (such as 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:

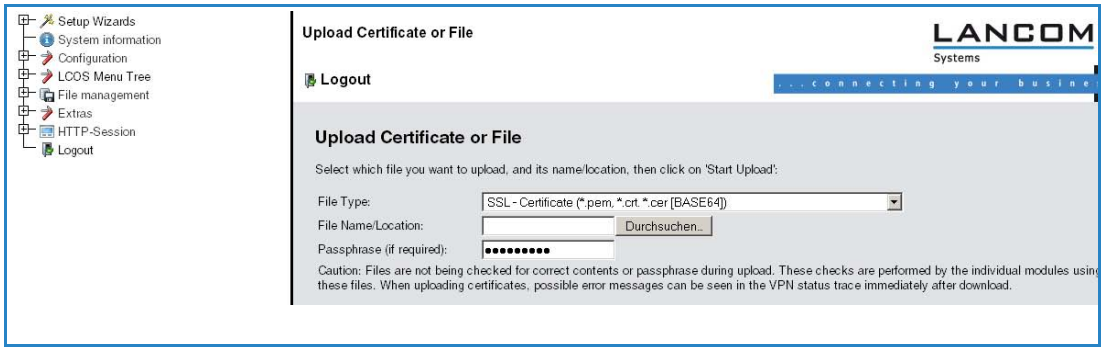
- <Master password><Command> or
- <User name>:<Password>@<Command>

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

B.2.2 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:



B.2.3 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.

B.3 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).

B.3.1 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

B.3.2 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.

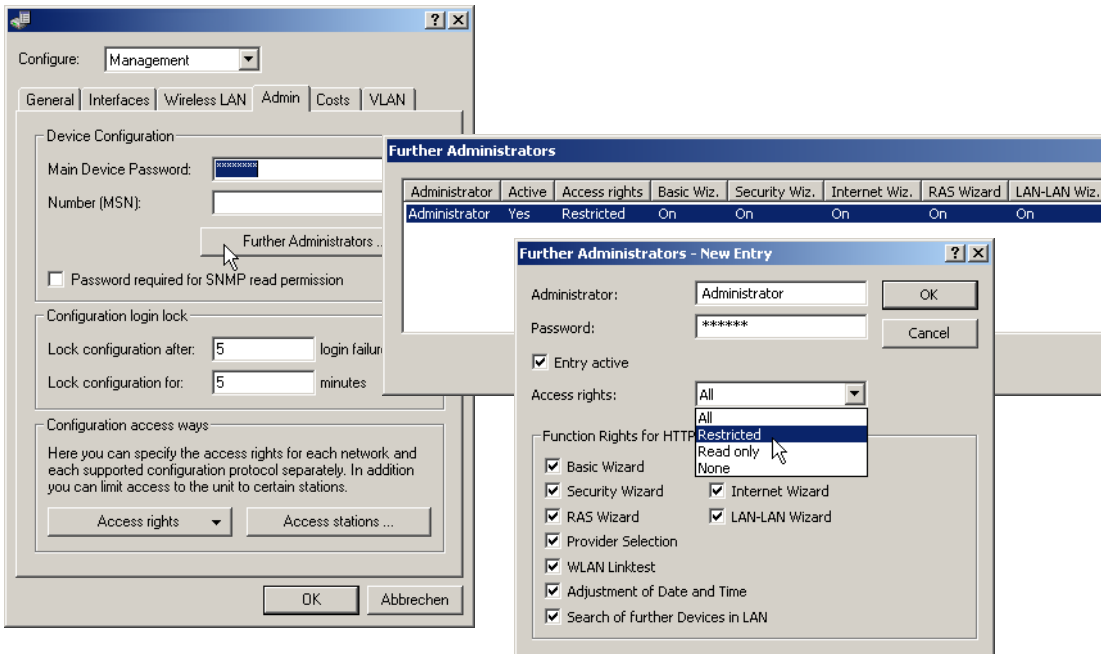
The community 'public' corresponds with the rights of a local administrator with read-only access, as long as the SNMP read access without password is enabled (). If this access is not allowed, then the 'public' community will have access to no menus at all.

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

B.3.3 Configuration of user rights

LANconfig

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



Enter the following values:

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

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

WEBconfig, Telnet or terminal program

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

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

B.3.4 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.

B.3.5 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:

Configuration tool	Call
WEBconfig, Telnet	Expert configuration > Setup > HTTP

- **Max. tunnel connections**

  The maximum number of simultaneously active TCP/HTTP tunnels

- □ Possible values: Max. 255 tunnels.
- □ Default: 3 Tunnels.

■ **Tunnel idle timeout**

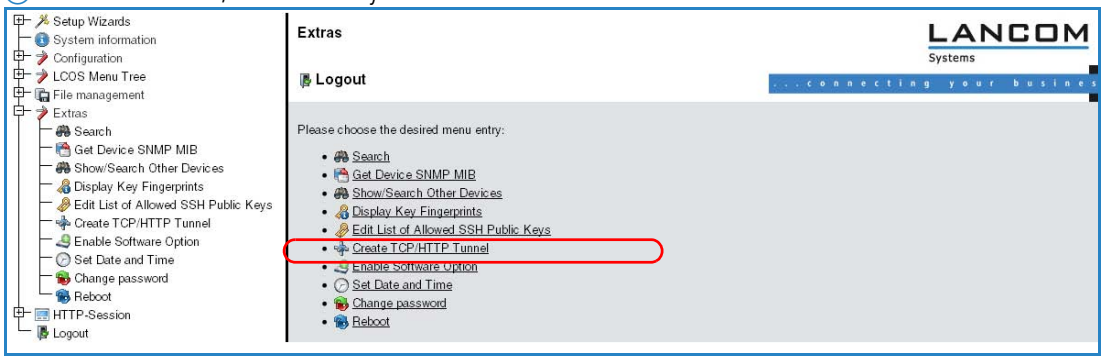
Life-expectancy of an inactive tunnel. After expiry of this time period the tunnel closes automatically unless data transfer is actively taking place.

- □ Possible values: Max. 4294967295 seconds.
- □ Default: 300 seconds.

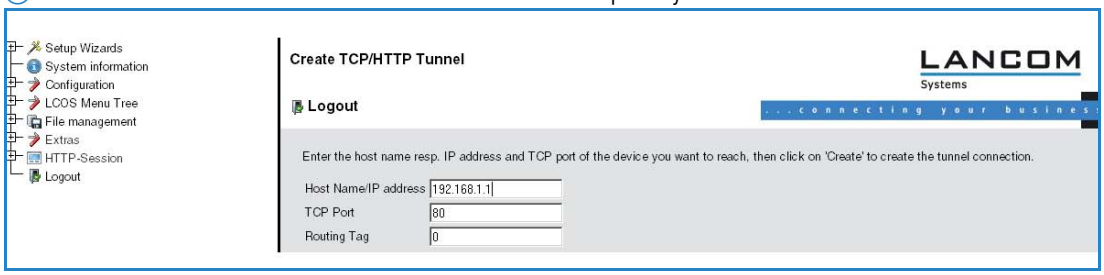
Create the TCP/HTTP tunnel

① HTTP tunnels are set up on the start page of WEBconfig. In WEBconfig log on to the LANCOM Router 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**

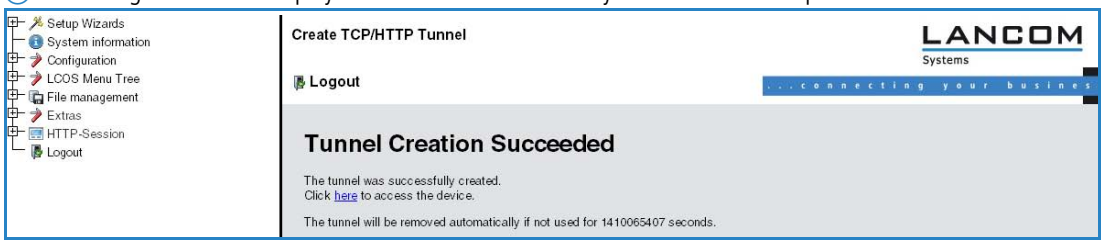


③ Enter the name or IP address of the device that is to be temporarily available via HTTP.



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.



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.

B.4 New firmware with LANCOM FirmSafe

New in LCOS 7.60:

■ Asymmetric Firmsafe

B.4.1 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. 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.

B.5 Project management with LANconfig

New in LCOS 7.60:

- Transferring device configurations to similar models
- Automatic creation of configuration backups before a firmware upload, configuration change and script execution.
- Customizing the toolbar

B.5.1 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.

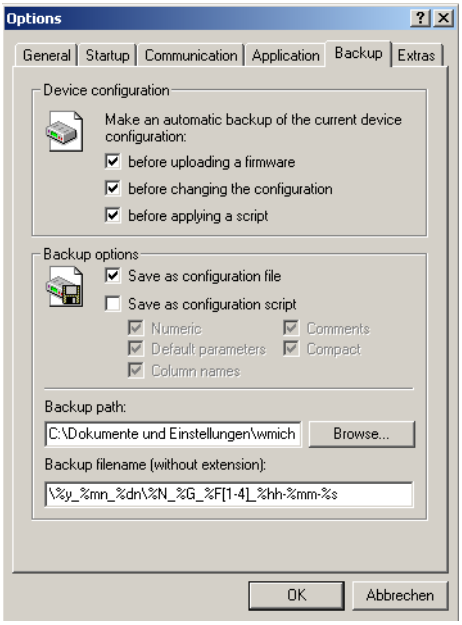
Please note that this function is intended primarily for replacement devices and not for the configuration of new devices to be operated in parallel with the source device in the same network. Because key communication settings, such as the IP address of the device and DHCP settings, are transferred 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.

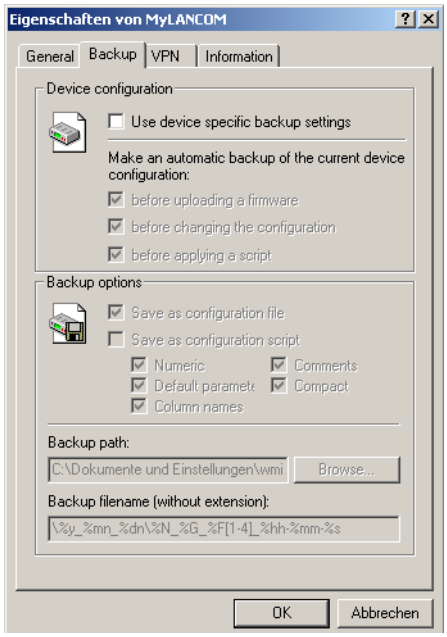
B.5.2 Automatic backup of configuration with LANconfig

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.

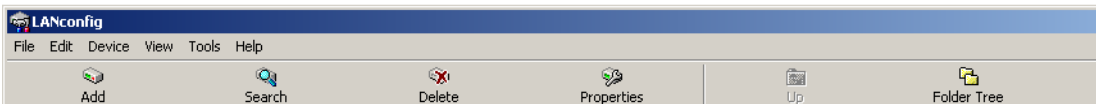




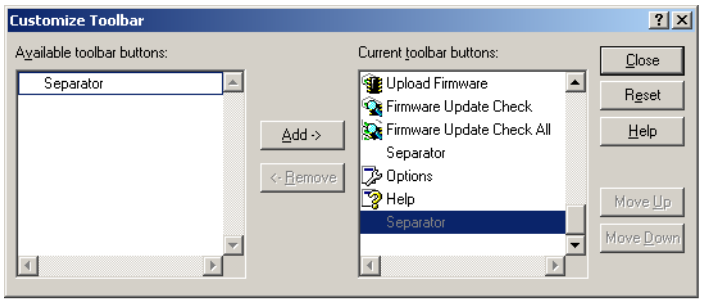
B.5.3 Customizing the toolbar

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.

B.6 LANCOM Layer 2 Management protocol (LL2M)

New with LCOS 7.6:

■ LANCOM Layer 2 Management protocol (LL2M)

B.6.1 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.

B.6.2 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.

B.6.3 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".

C Diagnosis

C.1 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

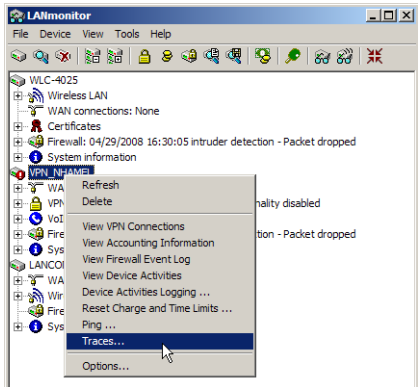
Traces can be executed very easily with LANmonitor. Simply click on the entry for the device with the right-hand mouse key and select **Traces** from the context menu.

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.

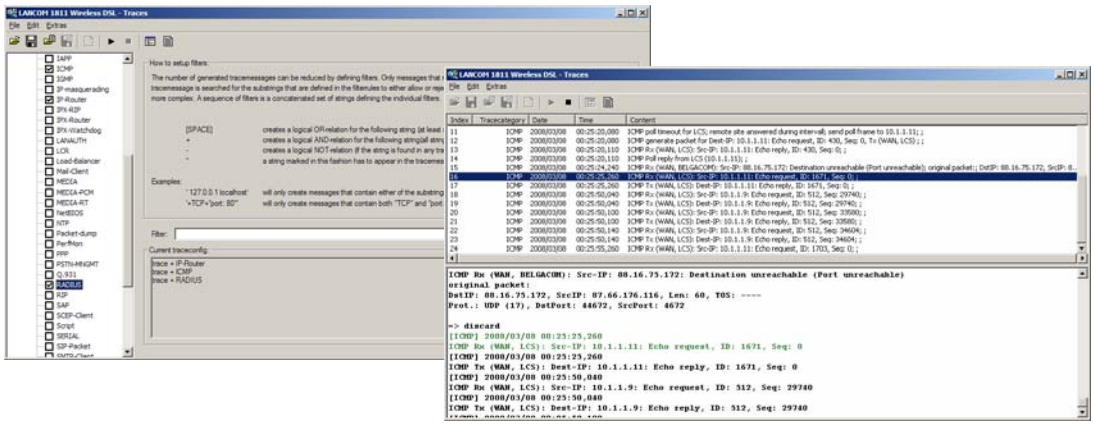
Clears the current display or trace results.

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.

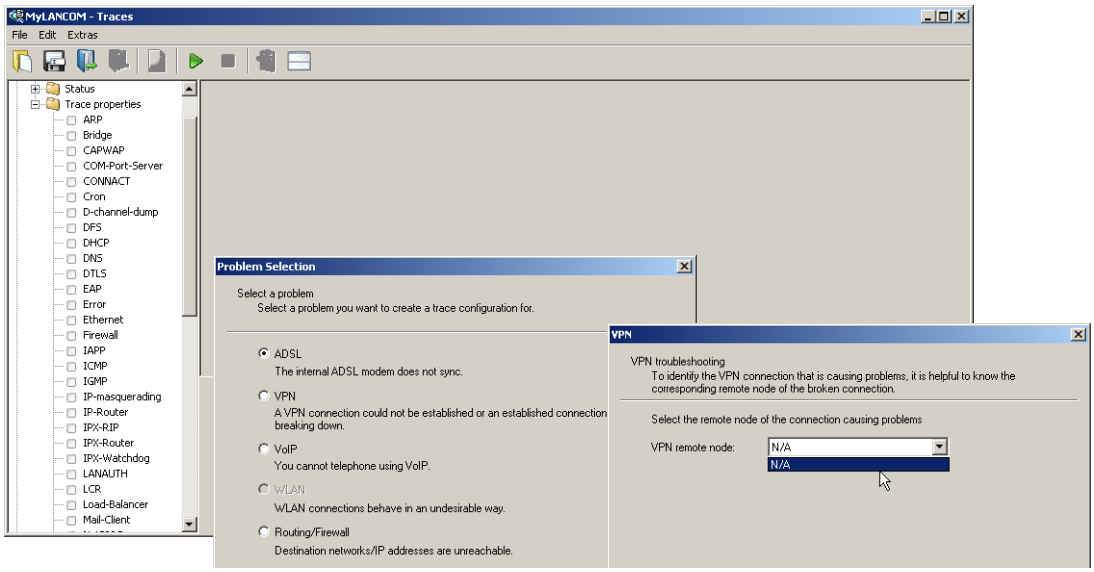
Switches to the mode for displaying the trace output.



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.



Expert configuration of the trace dumps

Going beyond the settings of the Wizard, traces and other displays can be set up precisely using the Expert Configuration. The Expert Configuration is divided into three areas:

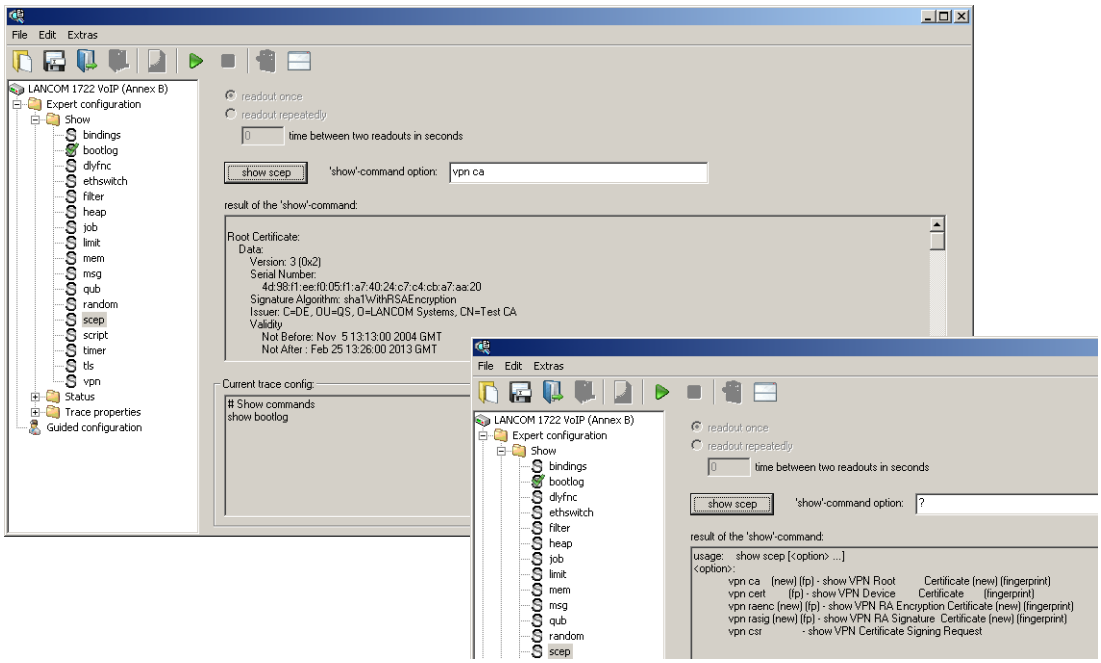
- Show

  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.



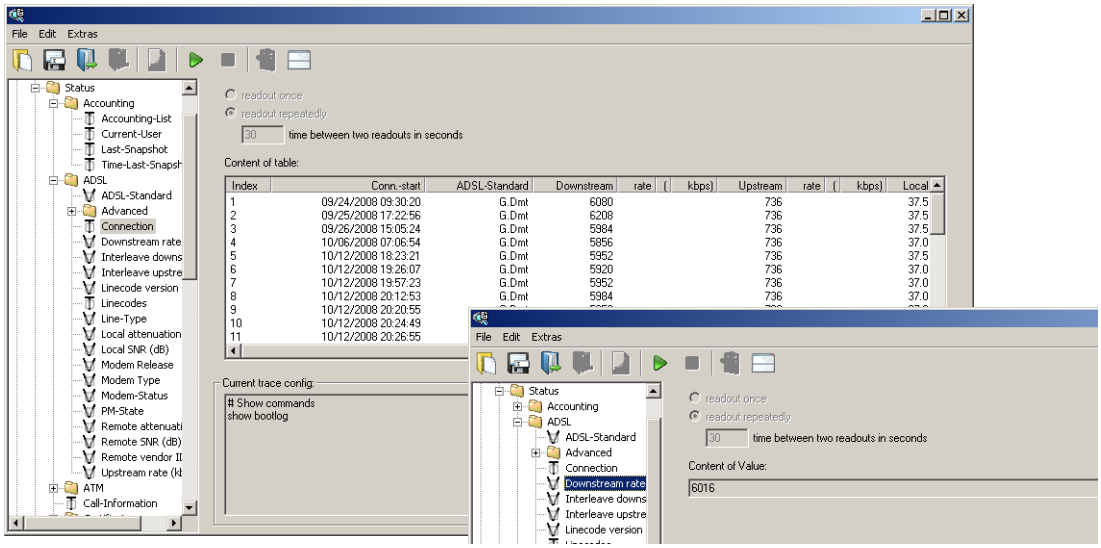
■ Status

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).

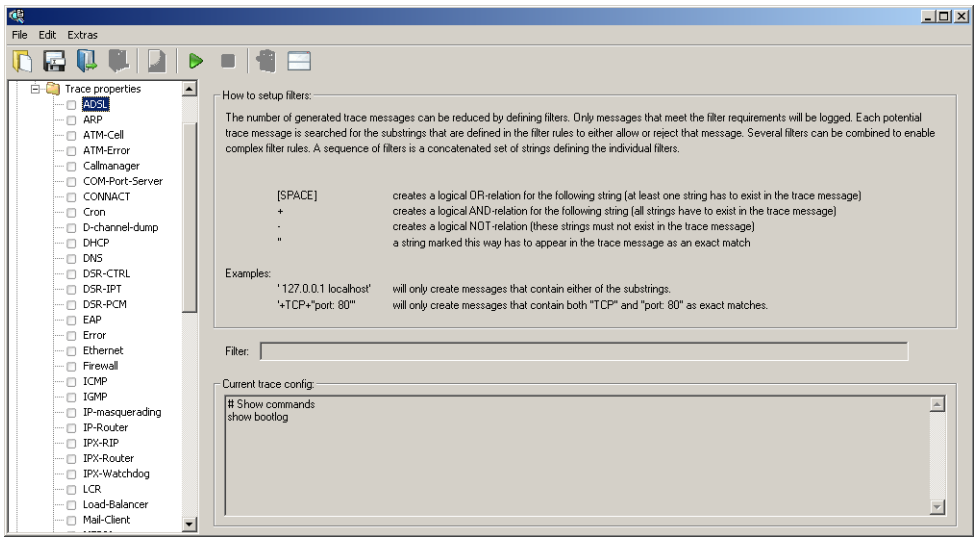
The settings of the Status information are stored in the trace configuration together with the actual trace settings. Status information is stored together with the actual trace data.



■ Trace settings

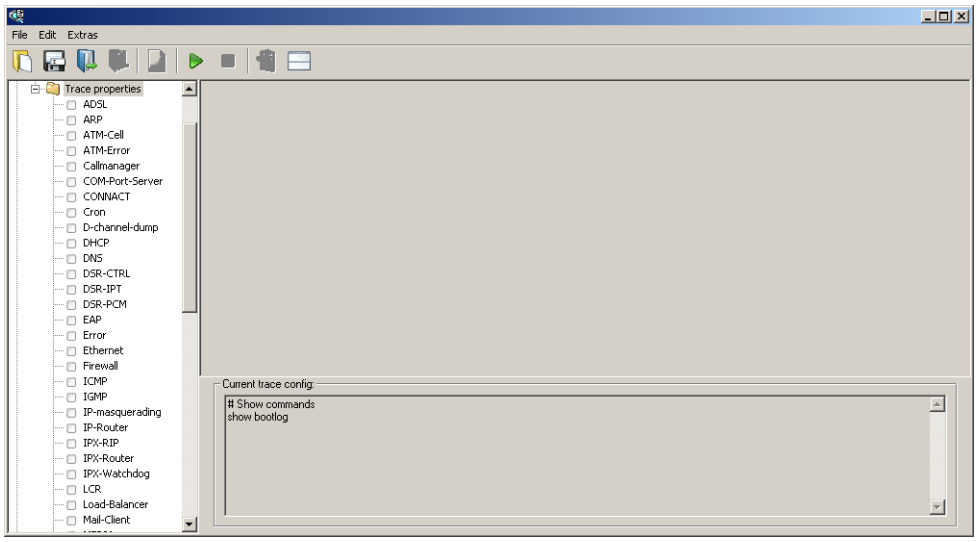
The traces to be dumped for the current device can be enabled in the trace settings area.

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.



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.



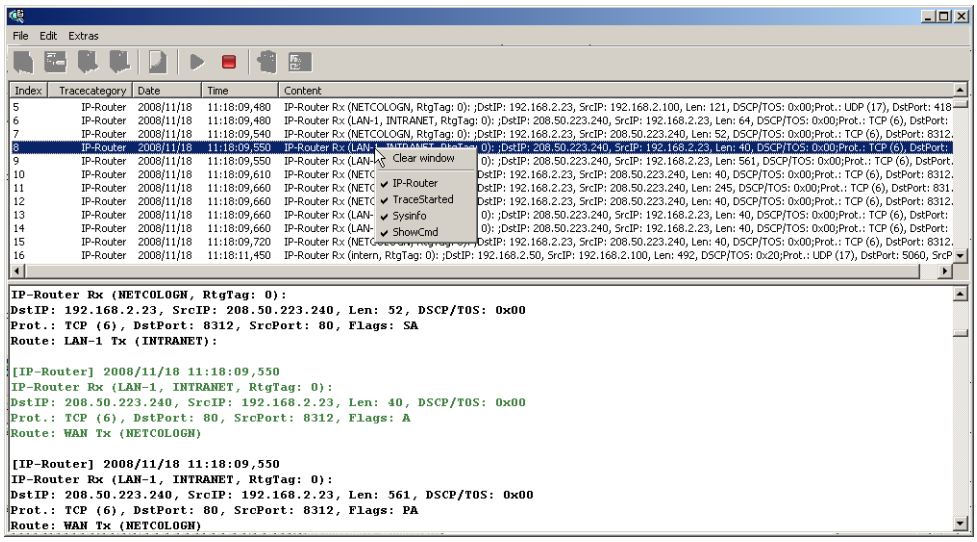
To start the dump of the trace data, change to Display mode with the Start button. The ongoing trace dumps are displayed in this view:

- 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**.



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**.

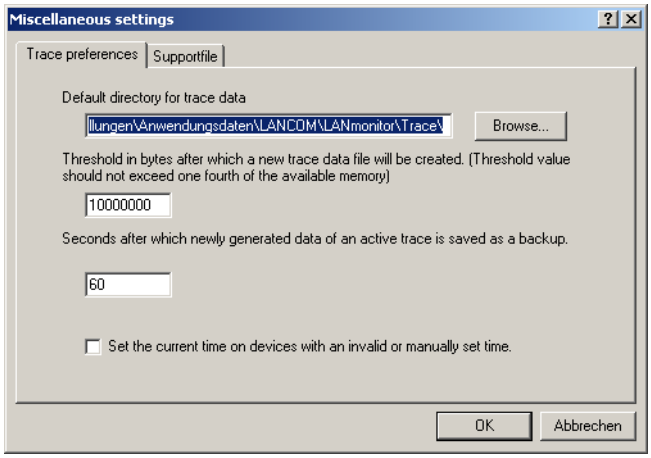
Backing up and restoring the trace data

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.



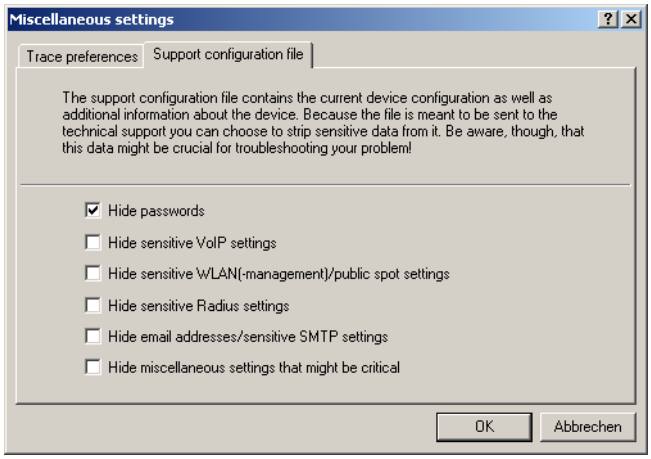
Saving support file

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 file created this way contains text-based information. The file can be opened using an editor or checked for any critical entries.

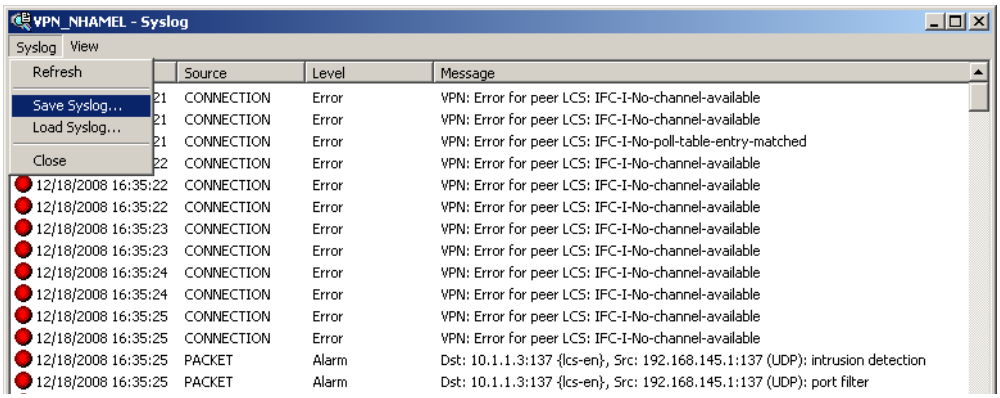
C.2 SYSLOG

C.2.1 Introduction

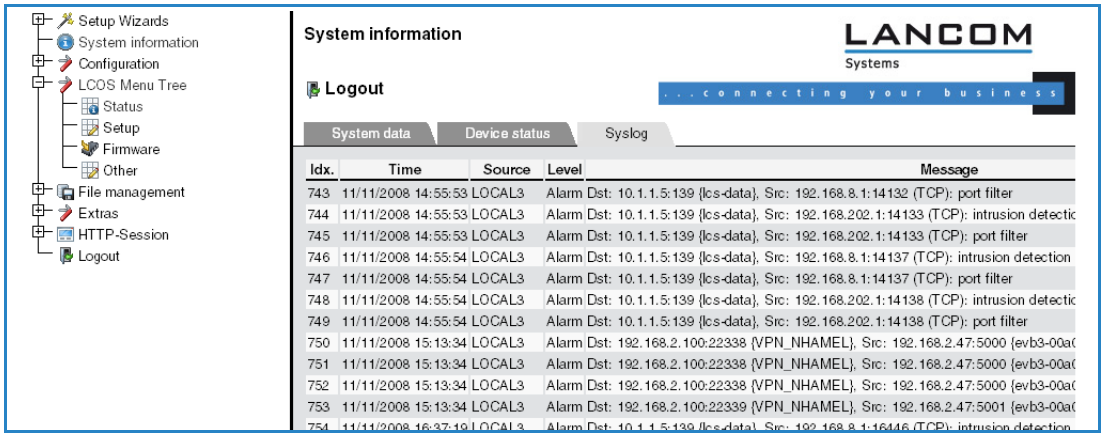
The SYSLOG protocol is used to log the activities of a LANCOM device. This function is especially interesting for system administrators as it records a a complete history of all activities in the device. The information captured in the SYSLOG log can be viewed in different ways:

- 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.



Alternatively you can view the current SYSLOG messages on the first page of WEBconfig on the SYSLOG tab:



C.2.2 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.

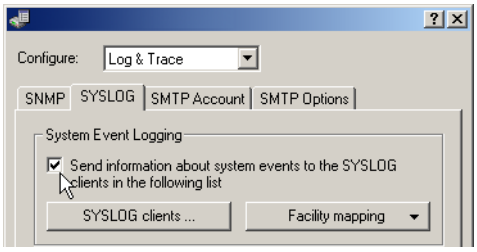
The LANCOM devices must have a valid time stamp for the evaluation of the SYSLOG messages in internal memory.

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.

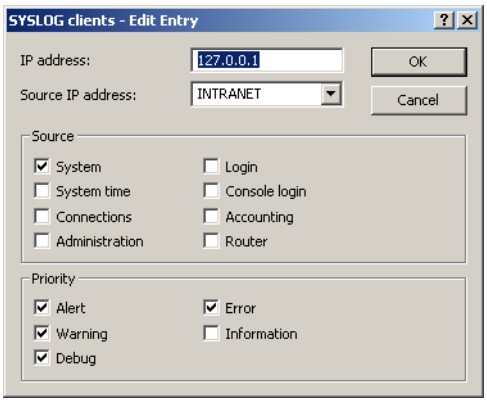
C.2.3 Configuring SYSLOG using LANconfig

You can find the parameters to configure SYSLOG under LANconfig in the configuration area "Log & Trace" on the "SYSLOG" tab.

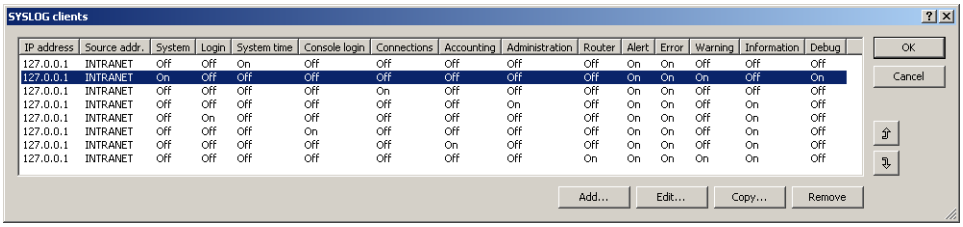


Creating SYSLOG clients

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.



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:

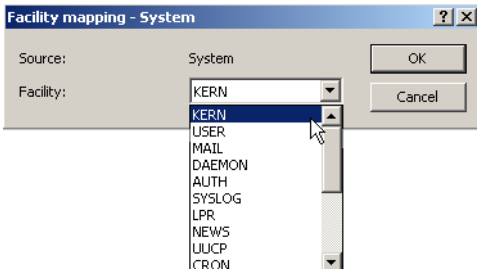


Further information about the meaning of the pre-defined syslog clients and the update options for existing LANCOM devices are to be found in the section "Table of syslog clients" for the configuration of syslog via telnet or WEBconfig.

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.



C.2.4 Configuring SYSLOG using Telnet or WEBconfig

Path: Setup/SYSLOG

- **Active**

  Activates the dispatch of information about system events to the configured SYSLOG client.

  Possible values:

  - Yes, No

  Default:

  - Yes

- **Port**

  Port used for sending SYSLOG messages.

  Possible values:

  - Max. 5 characters

  Default:

  - 514

Facility mapping

Path: Setup/SYSLOG/Facility-Mapper

- **Facility**

  Mapping sources to specific facilities.

  Possible values:

  - KERNEL
  - AUTH
  - CRON

- □ AUTHPRIV
- □ LOCAL0
- □ LOCAL1
- □ LOCAL2
- □ LOCAL3

■ **Source**

Mapping sources to specific facilities.

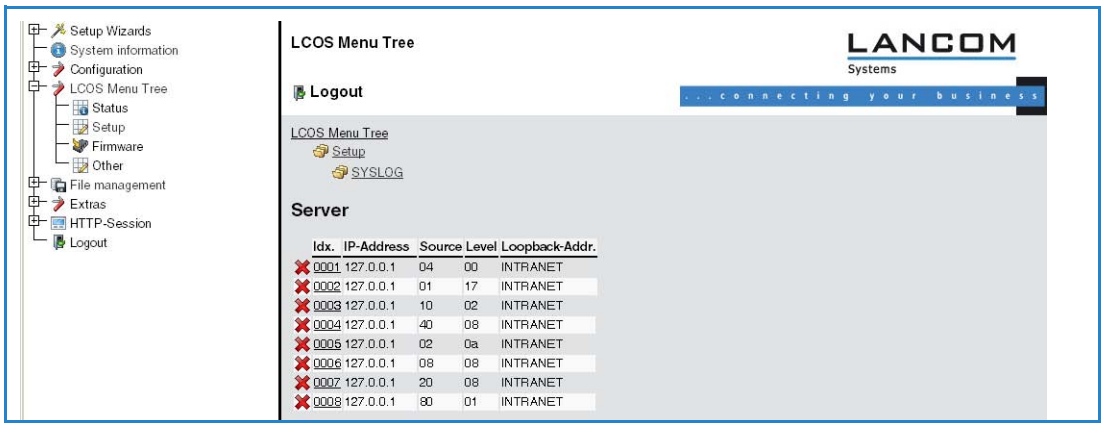
Possible values:

- □ System
- □ Logins
- □ System time
- □ Console logins
- □ Connections
- □ Accounting
- □ Administration
- □ Router

Table of SYSLOG clients

Path: Setup/SYSLOG/Table SYSLOG

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:



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.

Possible values:

□ Valid IP address

Default:

□ Blank

■ **Source**

Source that caused the message to be sent. Each source is represented by a certain code.

Possible values:

□ System: 01
□ Logins: 02
□ System time: 04
□ Console logins: 08
□ Connections: 10
□ Accounting: 20
□ Administration: 40
□ Router: 80

Default:

□ 00

Special values:

□ 00: No source is defined.

■ **Level**

SYSLOG level with which the message is sent. Each level is represented by a certain code.

Possible values:

□ Alert: 01
□ Error: 02
□ Warning: 04
□ Information: 08
□ Debug: 10

Default:

□ 00

Special values:

□ 00: No level is defined.

■ **Loopback address**

This is where you can configure an optional sender address for use instead of that 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.

D WAN

D.1 Flexible selection of the PPP authentication protocols

D.1.1 Introduction

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.

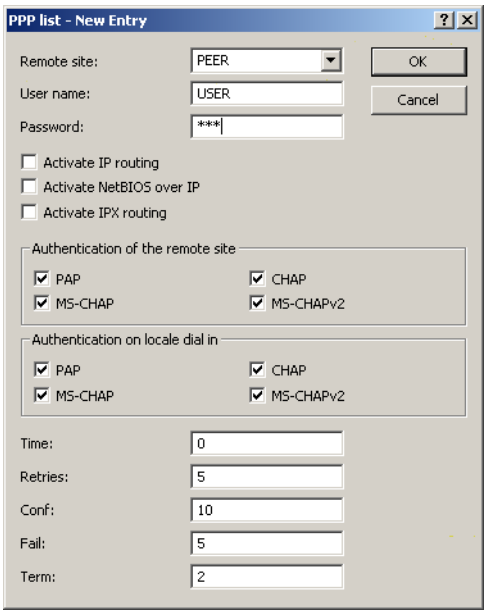
In principle authentication can be repeated while the connection is being negotiated. Another protocol can be selected if, for example, it can only be recognized from the username at the earliest. However, this repeat negotiation is not supported in all scenarios. In particular when dialing in over UMTS, 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.

LANconfig: Communication ▶ Protocols ▶ PPP list



Telnet: Setup ▶ WAN ▶ PPP

D.1.2 Configuration

In the PPP list, you are able to specify you own definition of PPP negotiation for every remote site contacting your network.

- **Remote site**

  Name of the remote site used to log in to your router.

  - □ Possible values: Max. 16 characters
  - □ Default: No entry
  - □ Special values: DEFAULT (see section "The meaning of the DEFAULT remote site")

■ **User name**

Name with which your router logs in to the remote site. If there is no entry here, your router's device name is used.

□ Possible values: Max. 64 characters

□ Default: No entry

■ **Password**

Password passed by your router to the remote site (if requested) or as expected by the remote site during an active authentication of the remote site by the LANCOM.

□ Possible values: Max. 32 characters

□ Default: No entry

■ **Authent.request**

Remote site authentication method.

□ Possible values: PAP, CHAP, MS-CHAP, MS-CHAPv2, none

□ Default: No entry

■ **Authent-response**

Procedures accepted for the passive authentication of the remote site.

□ Possible values: PAP, CHAP, MS-CHAP, MS-CHAPv2, none

□ Default: PAP, CHAP, MS-CHAP, MS-CHAPv2

The LANCOM only uses the protocols enabled here—other negotiations with the remote site are not possible.

■ **Time**

Time between two tests of the connection with LCP (see also LCP). This time is entered in multiples of 10 seconds (e.g. 2 for 20 seconds). The value is also the time between two tests of the connection as per CHAP. This time is entered in minutes.

□ Possible values: Max. 2 characters

□ Default: 0

For remote sites running the Windows operating system the time must be set to 0.

■ **Retries**

Number of retries for the test attempt. Multiple retries reduces the impact from temporary line faults. The connection is only terminated if all tries prove unsuccessful. The interval between two retries is 1/10 of the time between two connections tests and is also the maximum number of "Configure Requests" that the router sends before assuming a line fault and tearing down the connection.

□ Possible values: Max. 2 characters

□ Default: 0

■ **Conf, Fail, Term**

These parameters affect the mode of operation of the PPP. The parameters are defined in RFC 1661 are not described in further detail here. If you are unable to establish PPP connections, this RFC in conjunction with the PPP statistics of the router provides information on fault rectification. The default settings are generally adequate. These parameters can only be changed with LANconfig, SNMP and TFTP.

□ Possible values: Max. 3 characters

□ Default: 0

■ **Rights**

Specifies the protocols that can be routed to this remote site.

□ Possible values: IP, NetBIOS over IP, IPX

□ Default: None

D.1.3 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, authen-

tication 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.

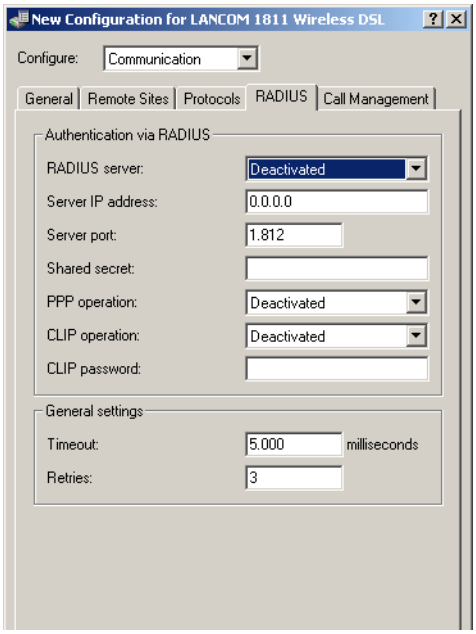
If authentication uses a protocol entered under DEFAULT, but which is not permitted for the remote site, then authentication is repeated with the permitted protocols.

D.1.4 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

LANconfig: Communication ▶ RADIUS



Telnet: Setup ▶ WAN ▶ RADIUS

■ **Active**

Enables the use of an external RADIUS server for the authentication of PPP connections or dial-in access.

Possible values:

□ Yes, No

Default:

□ No

■ **Auth. port**

The TCP/UDP port over which the external RADIUS server can be reached.

Possible values:

□ Valid port number

Default:

□ 1812

■ **Auth. protocols**

Method for securing the PPP connection permitted by the external RADIUS server.

Possible values:

□ PAP, CHAP, MS-CHAP, MS-CHAPv2, none

Default:

□ PAP, CHAP, MS-CHAP, MS-CHAPv2

■ **CLIP operation**

When remote sites dial in, the internal call number list, or alternatively an external RADIUS server, can be used for authentication.

Possible values:

- □ Yes: Enables the use of an external RADIUS server for the authentication of dial-in remote sites. A matching entry in the call number list takes priority however.
- □ No: No external RADIUS server is used for authentication of dial-in remote sites.
- □ Exclusive: Enables the use of an external RADIUS server as the only possibility for authenticating dial-in remote sites. The call number list is ignored.

Default:

- □ No

The dial-in remote sites must be configured in the RADIUS server such that the name of the entry corresponds to the call number of the remote site dialling in.

■ **CLIP password**

Password for the log-in of dial-in remote sites to the external RADIUS server.

Possible values:

- □ Max. 31 characters.

Default:

- □ Blank

The dial-in remote sites must be configured in the RADIUS server such that all the entries for all call numbers use the password configured here.

■ **Loopback address**

Sender address to be used in place of the sender address otherwise selected automatically 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.

■ **PPP operation**

When PPP remote sites dial in, the internal user authentication data from the PPP list, or alternatively an external RADIUS server, can be used for authentication.

Possible values:

- □ Yes: Enables the use of an external RADIUS server for authentication of PPP remote sites. A matching entry in the PPP list takes priority however.
- □ No: No external RADIUS server is used for authentication of PPP remote sites.
- □ Exclusive: Enables the use of an external RADIUS server as the only possibility for authenticating PPP remote sites. The PPP list is ignored.

Default:

- □ No

■ **Protocol**

RADIUS over UDP or RADSEC over TCP with TLS can be used as the transmission protocol for authentication on an external server.

Possible values:

□ RADIUS, RADSEC

Default:

□ RADIUS

■ **Key**

Password that is required for access to the external RADIUS server.

Possible values:

□ Max. 32 characters

Default:

□ Blank

■ **Server address**

Address of the external RADIUS server.

Possible values:

□ Valid IP address

Default:

□ Blank

D.2 The Action table

D.2.1 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.

4.2.2 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”).

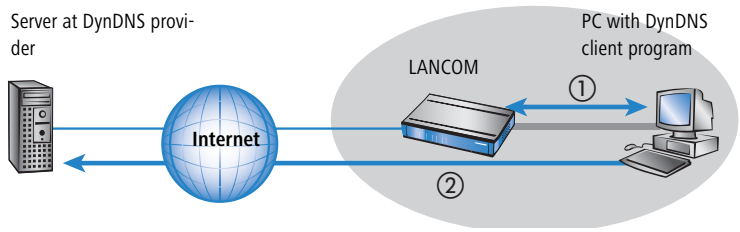
The advantage is obvious: If you wish to carry out remote maintenance via WEBconfig/HTTP, the only information you need is the dynamic DNS name. Also, a DynDNS name can be used to establish VPN connections between remote stations that have changing IP addresses.

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.

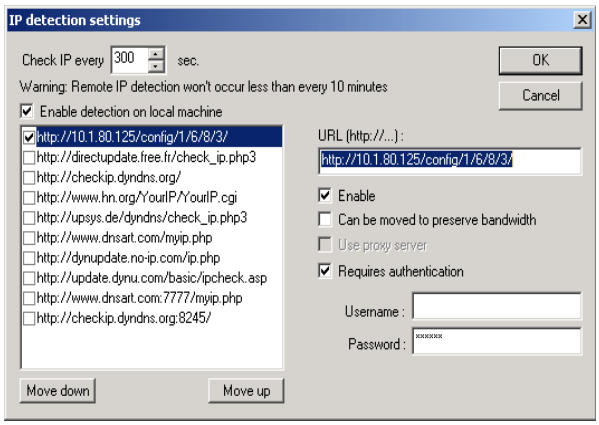
Dynamic DNS client on the workstation

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.



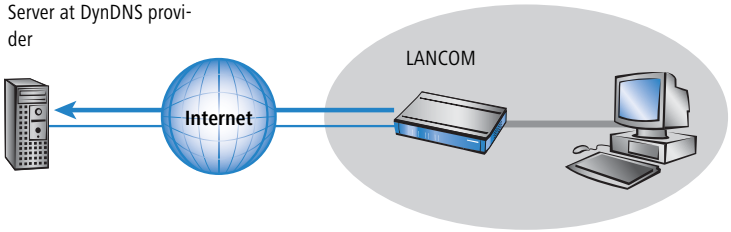
The current WAN-side IP address of a LANCOM can be read from the following address and entered into a client program:

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



Dynamic-DNS client in the LANCOM via HTTP

Alternatively the LANCOM can transmit the current WAN IP to the DynDNS provider directly:

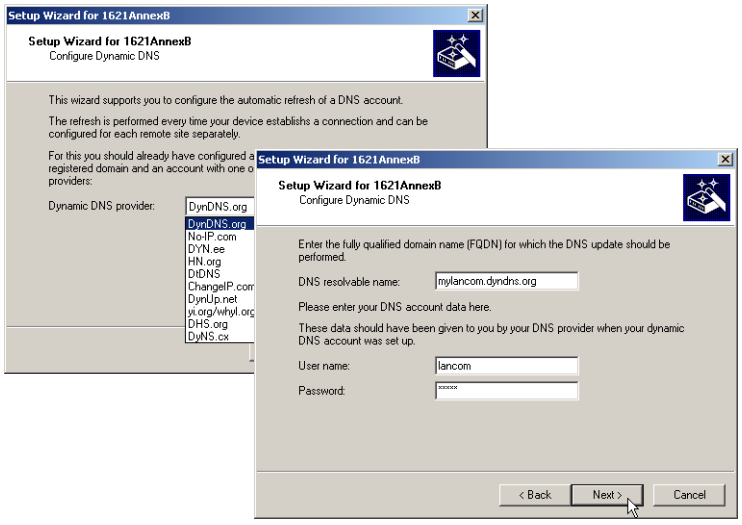


An action is defined for this which, for example, automatically sends an HTTP request to the DynDNS server each time a connection is established. The necessary information is transferred via the DynDNS account, so triggering an update of the registration. An HTTP request of this type from DynDNS.org 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:



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.

D.2.3 Further example actions

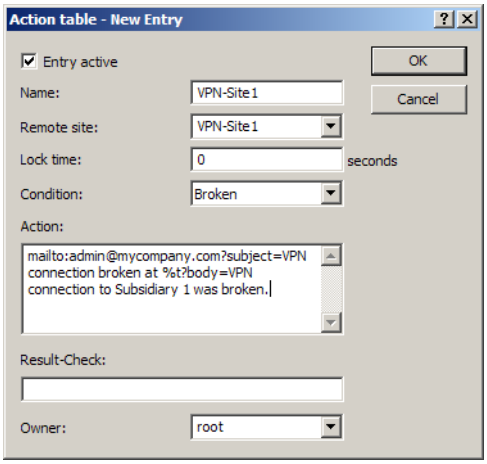
Broken connection alert as an SMS to a mobile telephone

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**.



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.

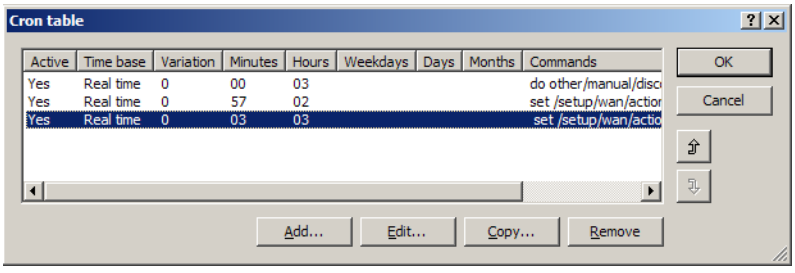
For complex scenarios with several subsidiaries, each of the remote sites is given a corresponding entry in the central LANCOM. For monitoring the central device itself, an action is entered into a device at one of the subsidiaries. In this way the administrator receives an alert even if the VPN gateway 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.



D.2.4 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.

LANconfig: Communication ▶ General ▶ Action table

Telnet: 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 infuences 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.

Possible values:

□ Max. 10 characters

Default:

□ 0

■ **Active**

Activates or deactivates this entry.

Possible values:

□ Yes

□ No

Default:

□ Yes

■ **Host name**

Action name. This name can be referenced in the fields "Action" and "Check for" with the place holder %h (host name).

Possible values:

□ Max. 64 characters

Default:

□ Blank

■ **Remote site**

A change in status of this remote site triggers the action defined in this entry.

Possible values:

□ Max. 16 characters

Default:

□ Blank

■ **Lock time (max. 10 characters)**

Prevents this action from being repeated within the period defined here in seconds.

Possible values:

□ Max. 10 characters

Default:

□ 0

■ **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.

Default:

- □ Structure

■ **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 numer 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.

Default:

□ Blank

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.

Possible values:

□ Select from the administrators defined in the device. Maximum 16 characters.

Default:

□ root

D.3 Using the serial interface in the LAN

D.3.1 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.

D.3.2 Operating modes

A COM port server has two operating modes:

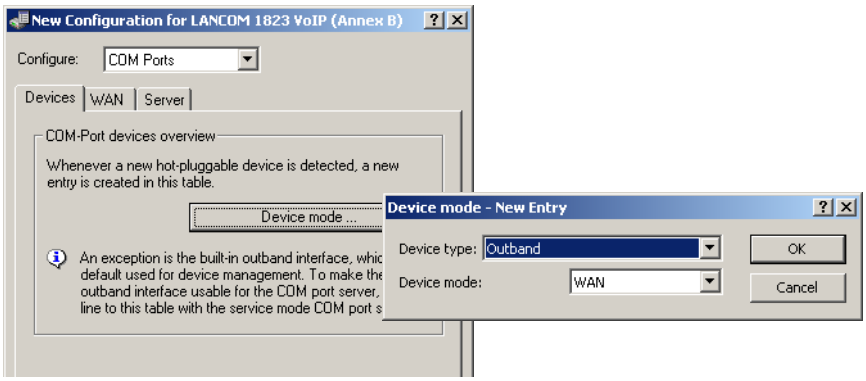
- Server mode: The COM port server waits for requests from a defined TCP port to establish TCP connections. The mode is used for remote maintenance, for example.
- Client mode: As soon as a device connected to the serial interface becomes active, the COM port client opens a TCP connection to a preset 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.

D.3.3 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.

LANconfig: COM ports ▶ Devices ▶ Device operating mode



Telnet: Setup ▶ COM-Ports ▶ Devices

■ **Device type**

Selects a serial interface from the list of those available in the device.

□ Possible values: All of the serial interfaces available in the device.

□ Default: Outband

■ **Service**

Activation of the port in the COM port server.

□ Possible values: WAN, COM-port server.

□ Default: WAN

D.3.4 Configuring the COM port server

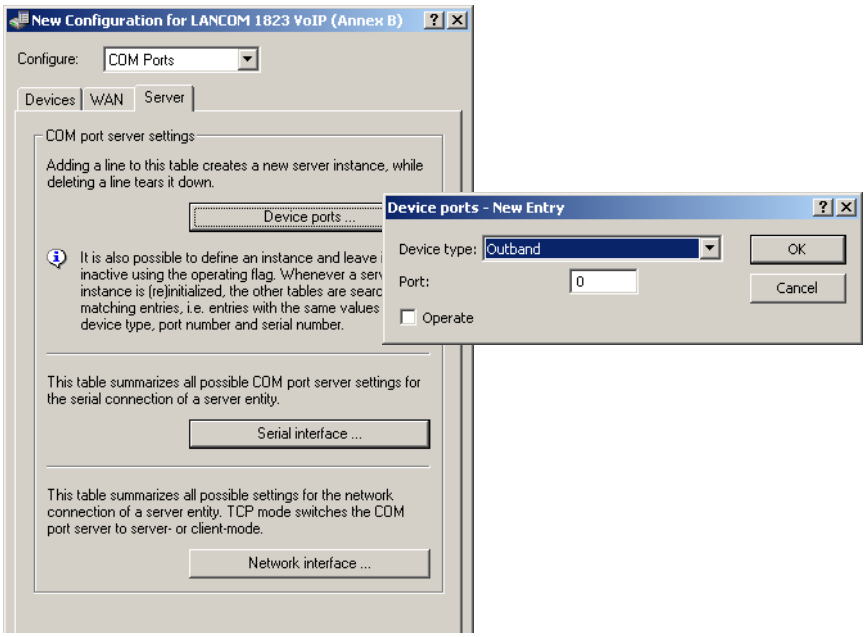
Configuring the COM port server involves three tables. What all three tables have in common is that a certain port at a serial interface is identified by the values for device type and port number. Because some serial devices such as a CardBus card have multiple ports, the port to be used must be specified 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.

LANconfig: COM ports ▶ Server ▶ Device ports



Telnet: Setup ▶ COM-Ports ▶ COM-Port-Server ▶ Devices

■ **Device type**

Selects a serial interface from the list of those available in the device.

□ Possible values: All of the serial interfaces available in the device.

□ Default: Outband

■ **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.

□ Possible values: Max. 10 characters

□ Default: 0

□ Special values: 0 for serial interfaces with just one port, e. g. outband.

■ **Operating**

Activates the COM port server on the selected port of the selected interface.

□ Possible values: No, yes

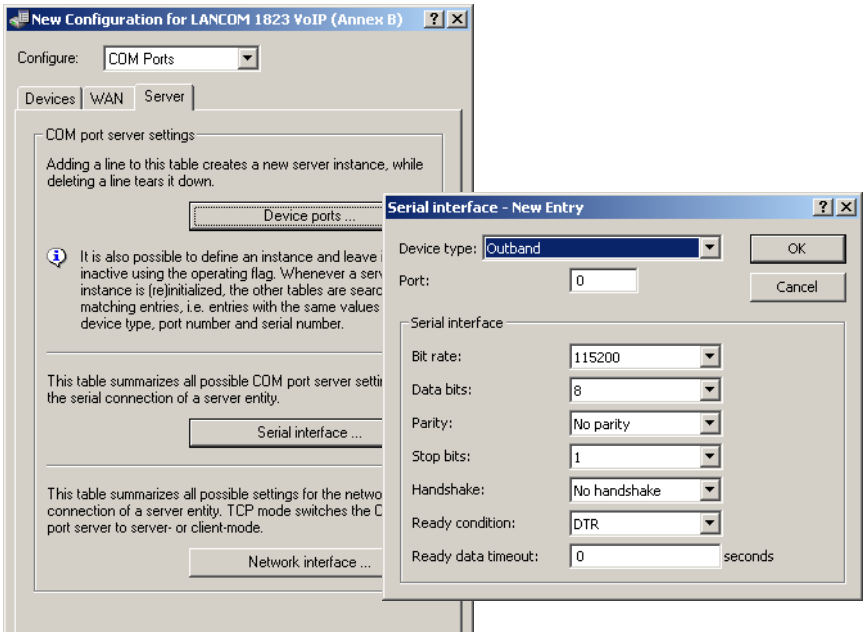
□ Default: No

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.

LANconfig: COM ports ▶ Server ▶ Serial interface



Telnet: Setup ▶ COM-Ports ▶ COM-Port-Server ▶ COM-Port-Settings

■ **Device type**

Selects a serial interface from the list of those available in the device.

□ Possible values: All of the serial interfaces available in the device.

□ Default: Outband

■ **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.

□ Possible values: Max. 10 characters

□ Default: 0

□ Special values: 0 for serial interfaces with just one port, e. g. outband.

■ **Bitrate**

Bitrate used on the COM port

- □ Possible values: Common values for bitrate vary from 110 to 230400
- □ Default: 9600

■ **Data bits:**

Number of data bits.

- □ Possible values: 7, 8
- □ Default: 8

■ **Parity**

The checking technique used on the COM port.

- □ Possible values: None, odd, even
- □ Default: None

■ **Stop bits**

Number of stop bits.

- □ Possible values: 1, 2
- □ Default: 1

■ **Handshake**

The data-flow control used on the COM port.

- □ Possible values: None, RTS/CTS
- □ Default: RTS/CTS

■ **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.

- □ Possible values: DTR, data
- □ Default: DTR

■ **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.

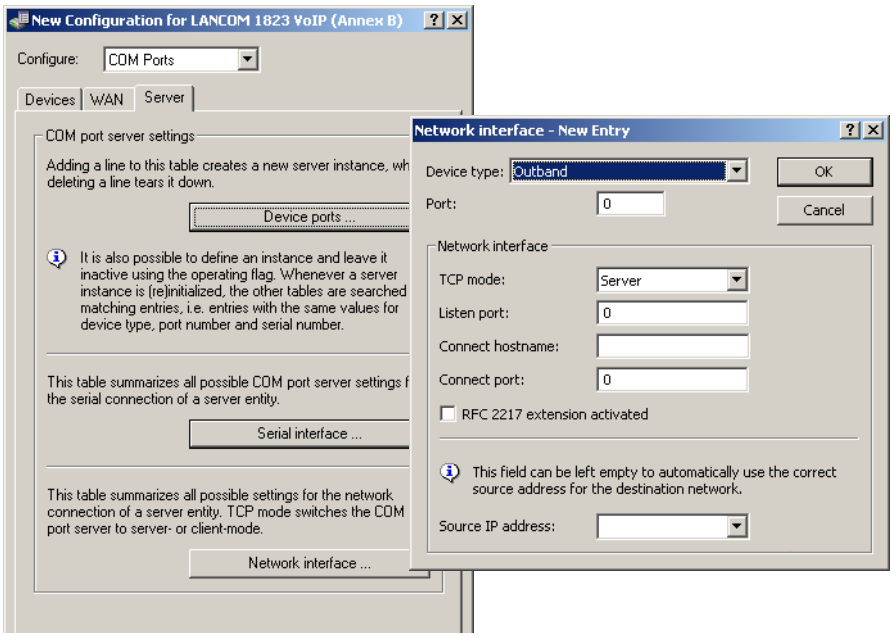
- □ Possible values: Max. 10 characters
- □ Default: 0
- □ Special values: 0 switches the Ready-data-timeout off.

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.

LANconfig: COM ports ▶ Server ▶ Network interface



Telnet: Setup ▶ COM-Ports ▶ COM-Port-Server ▶ Network settings

■ **Device type**

Selects a serial interface from the list of those available in the device.

□ Possible values: All of the serial interfaces available in the device.

□ Default: Outband

■ **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.

□ Possible values: Max. 10 characters

□ Default: 0

□ Special values: 0 for serial interfaces with just one port, e. g. outband.

■ **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.

□ Possible values: Server, Client

□ Default: Server

■ **Listen port**

The TCP port where the COM port in TCP server mode expects incoming connections.

□ Possible values: Max. 10 characters

□ Default: 0

■ **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.

□ Possible values: Max. 48 characters The host can be specified either as a DNS name or as an IP address.

□ Default: Blank

■ **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.

□ Possible values: Max. 10 characters

□ Default: 0

■ **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.

- □ Possible values: Max. 16 characters
- □ Default: Blank

■ **RFC2217 extensions**

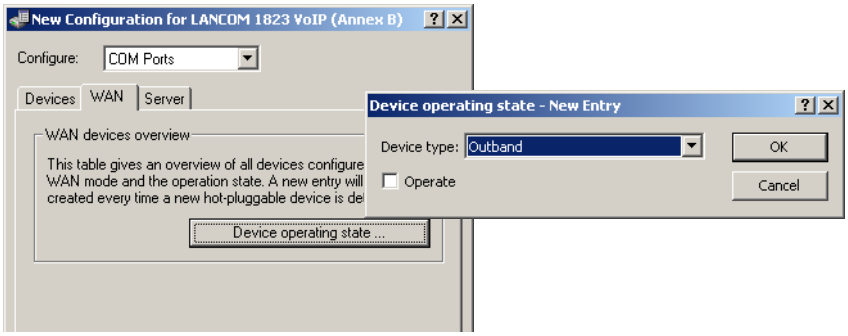
The RFC2217 extensions can be activated for both TCP modes. With these extensions activated, the LANCOM uses the IAC DO COM-PORT-OPTION sequence to signal that it will accept Telnet control sequences. The COM port subsequently works with the corresponding options; the configured default values are overwritten. 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.

- □ Possible values: No, yes
- □ Default: No

D.3.5 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.

LANconfig: COM ports ▶ WAN ▶ Device operating state



Telnet: Setup ▶ COM ports ▶ WAN ▶ Devices

■ **Device type**

List of serial interfaces available in the device.

- □ Possible values: All of the serial interfaces available in the device.

■ **Active**

Status of connected device:

- □ Possible values: No, yes

D.3.6 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 not 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
- □ Possible values: Common values for bitrate vary from 110 to 230400

■ **Data bits:**
Number of data bits.
- □ Possible values: 7, 8

■ **Parity**
The checking technique used on the COM port.
- □ Possible values: None, odd, even

■ **Stop bits**
Number of stop bits.
- □ Possible values: 1, 2

■ **Handshake**
The data-flow control used on the COM port.
- □ Possible values: None, RTS/CTS

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.

D.3.7 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

D.4 RIP

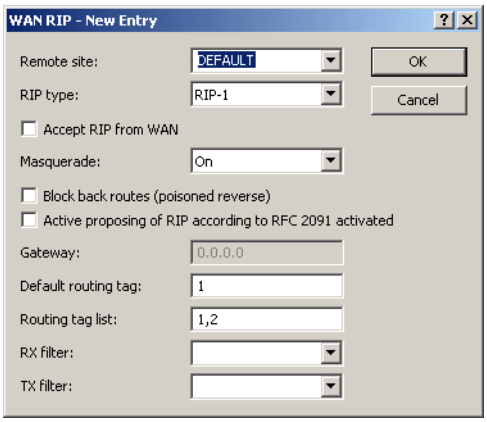
D.4.1 WAN RIP

New with LCOS 7.6:

- Flexible definition of WAN-RIP remote stations by using place holders.

In order for statically defined routes and routes learned from RIP to be broadcast across the WAN, or for routes to be learned from the WAN, the respective remote sites can be entered into the WAN RIP table.

LANconfig: IP-Router ▶ General ▶ WAN RIP



WEBconfig: Setup ▶ IP-Router ▶ RIP ▶ WAN table

- **Remote site**

  Name of the remote site for exchanging routing information via RIP.

  Possible values:

  - Selection from the list of defined remote sites (max. 16 characters).

  Default:

  - Blank

  Special values:

  - Multiple remote sites can be configured in one entry by using * as a place holder. If for example multiple remote stations are to exchange dynamic routing information via WAN RIP, while the networks for all other users and branch offices are defined statically, the appropriate remote stations can be given names with the

prefix "RIP_". To configure all of the remote stations, the WAN RIP table requires just a single entry for remote station "RIP_*".

■ **RIP type**

The RIP type details the RIP version with which the local routes are propagated.

Possible values:

- □ Off
- □ RIP-1
- □ RIP-1 compatible
- □ RIP-2

Default:

- □ Off

■ **RIP learning**

The column RIP-Accept specifies whether RIP is accepted from the WAN and whether routes should be learned from this remote site. The RIP type must be set for this.

Possible values:

- □ On/off

Default:

- □ Off

■ **Masking**

The column Masquerade lists whether or not masquerading is performed on the connection and how it is carried out. This entry makes it possible to start WAN RIP even in an empty routing table.

Possible values:

- □ Auto: The masquerade type is taken from the routing table. If there is no routing entry for the remote site, then masquerading is not performed.
- □ To: All IP connections to this remote site are masqueraded.
- □ Intranet: IP connections from intranet networks are masqueraded, IP connections from the DMZ pass through transparently

■ **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.

Possible values:

- □ Yes/No

Default:

- □ No

■ **RFC 2091**

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 (triggered updates).

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.

Possible values:

- □ Yes/No

Default:

- □ No

■ **Gateway**

IP address of the nearest available router in the context of RFC 2091.

Possible values:

□ Valid IP address

Default:

□ 0.0.0.0

Special values:

□ If 0.0.0.0 is entered, the gateway address is determined from PPP negotiation.

In a router at the central location, RFC 2091 can be switched off and the gateway can remain on 0.0.0.0 because the central location always observes the requests from the subsidiaries.

The LANCOM automatically reverts to standard RIP if the indicated gateway does not support RFC 2091.

■ **Dft-Rtg-Tag**

The column Default tag lists the valid "Default touting tag" for the WAN connection. All untagged routes are tagged with this tag when sent on the WAN.

Possible values:

□ 0 to 65535

Default:

□ 0

■ **Rtg-Tag-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.

Possible values:

□ Maximum 33 characters

Default:

□ Blank

■ **Rx-Filter**

Here you define the filter to be used when receiving RIP packets.

Possible values:

□ Select from the list of defined RIP filters (max. 16 characters).

Default:

□ Blank

■ **Tx-Filter**

Here you define the filter to be used when sending RIP packets.

Possible values:

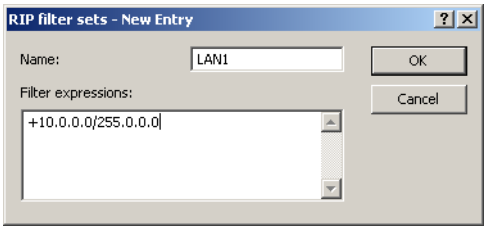
□ Select from the list of defined RIP filters (max. 16 characters).

Default:

□ Blank

D.4.2 RIP-Filter

LANconfig: IP-Router ▶ General ▶ RIP filter sets



Telnet: Setup ▶ IP-Router ▶ 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.

- **Name**

  Name of the filter.

  Possible values:

  - 18 alphanumerical characters. The last two characters must combine a digit with the hash symbol (e.g. #1). Consequently, the assignment to LAN and WAN networks can only use 16 characters.

  Examples:

  - LAN#1, LAN#2, WAN1, etc.

The hash symbol # can be used to combine multiple entries into a single filter. Taken together the entries LAN#1 and LAN#2 make up a filter "LAN" that can be called from the RIP table.

- **Filter**

  Comma-separated list of networks that are to be accepted (+) or rejected (-).

  - Example of an accepted network: +10.0.0.0/255.0.0.0
  - Example of an unaccepted network: -192.168.0.0/255.255.0.0
  - Possible values: 64 characters from `,+-/0123456789.`

The plus-sign for accepted networks is optional.

Filters defined in the filter table can be referenced in the columns for RX filter and TX filter in the LAN RIP and WAN RIP tables. RX defines the networks from which routes can be learned or blocked, and TX defines the networks to which propagation should be allowed or blocked.

Filtering by routing tags is unaffected, i.e. if a tag for a route indicates that it is not to be learned or propagated, then this cannot be forced by means of the filter table.

D.5 Advanced Routing and Forwarding

D.5.1 Interfaces tags for remote sites

New with LCOS 7.6:

- Assignment of interfaces tags via the remote site

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:

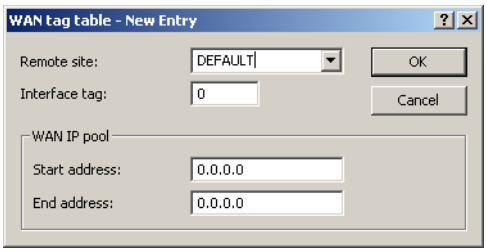
- By using appropriate firewall rules that only capture data packets from particular remote sites, IP addresses or ports
- Based on the routing table
- Via an explicit assignment of tags to remote sites.

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



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	Distance	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.

Assignment of interface tags via the tag table

The tag table enables inbound data packets to be directly assigned with an interface tag that depends on the remote site.

■ Telnet: Setup ▶ IP router ▶ Tag table

■ **Remote site**

Name of the remote site whose packets are to be given interface tags when received at the WAN side.

Possible values:

- □ Selection from the list of defined remote sites (max. 16 characters).

Default:

- □ Blank

Special values:

- □ Multiple remote sites can be configured in one entry by using * as a place holder. If, for example , several remote sites (RAS users) of a company are to be tagged, all appropriate remote sites can be given a name

with the prefix "Company1_". To configure all of the remote sites, just one entry with remote site "Company1_*" can be included in the tag table.

■ **Rtg tag**

This interface tag is assigned to the inbound packets of the remote site.

Possible values:

□ 0 to 65535

Default:

□ 0

■ **Start WAN pool**

The start WAN pool represents the beginning of the address pool for the remote site or group of remote sites (when using placeholders to specify remote site). When RAS users dial in, the remote site is assigned an address from the address pool defined here.

Possible values:

□ Max. 15 characters

Default:

□ 0.0.0.0

Special values:

□ If the pool is empty (start and end addresses are 0.0.0.0), the global pool is used.

■ **End WAN pool**

The end WAN pool represents the end of the address pool for the remote site or group of remote sites (when using placeholders to specify remote site). When RAS users dial in, the remote site is assigned an address from the address pool defined here.

Possible values:

□ Max. 15 characters

Default:

□ 0.0.0.0

Special values:

□ If the pool is empty (start and end addresses are 0.0.0.0), the global pool is used.

E VPN

E.1 Unlimited number of VPN remote sites

Some tables in LCOS can be converted to allow dynamic sizing, for example to enable any number of remote sites to be entered into the VPN setup table. Unchanged is the number of simultaneous connections possible. This depends on the license.

E.2 Extended Authentication Protocol (XAUTH)

E.2.1 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).

E.2.2 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:

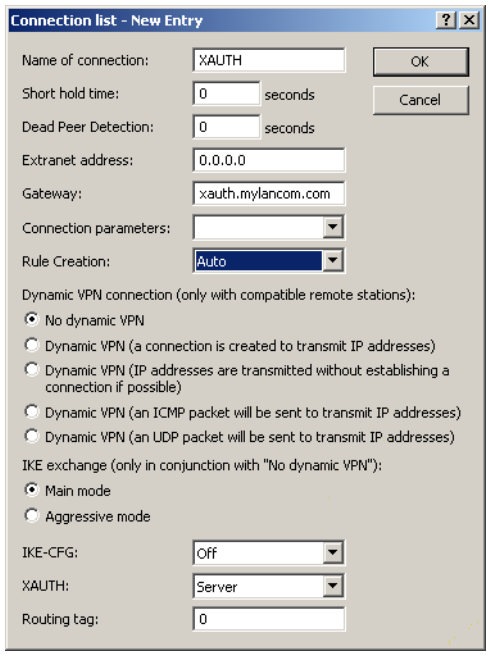
XAUTH operating mode	Server	Client
XAUTH user name	Remote site from the PPP table. The PPP-table entry is selected for which the PPP remote site corresponds to the transferred XAUTH user name. The PPP remote site must also match the VPN remote site used.	User name from the PPP table. The entry selected 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.

E.2.3 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



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

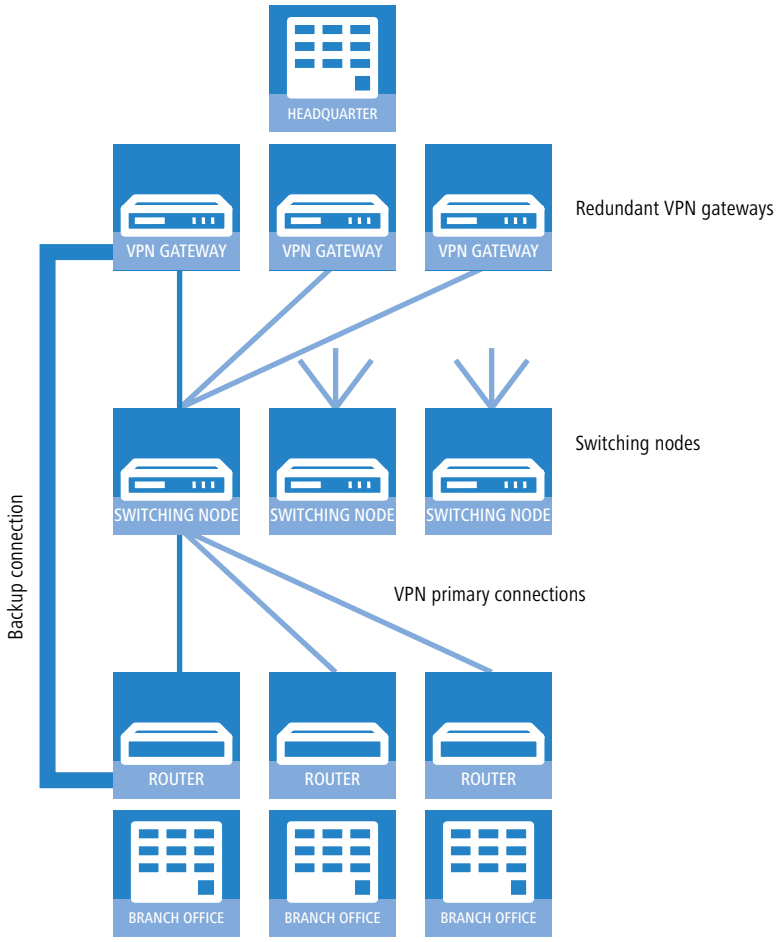
If XAUTH authentication is enabled for a VPN remote site, the IKE-CFG option must be set to the same value.

E.3 Backup via alternative VPN connection

E.3.1 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.

E.3.2 Backup-capable network infrastructure

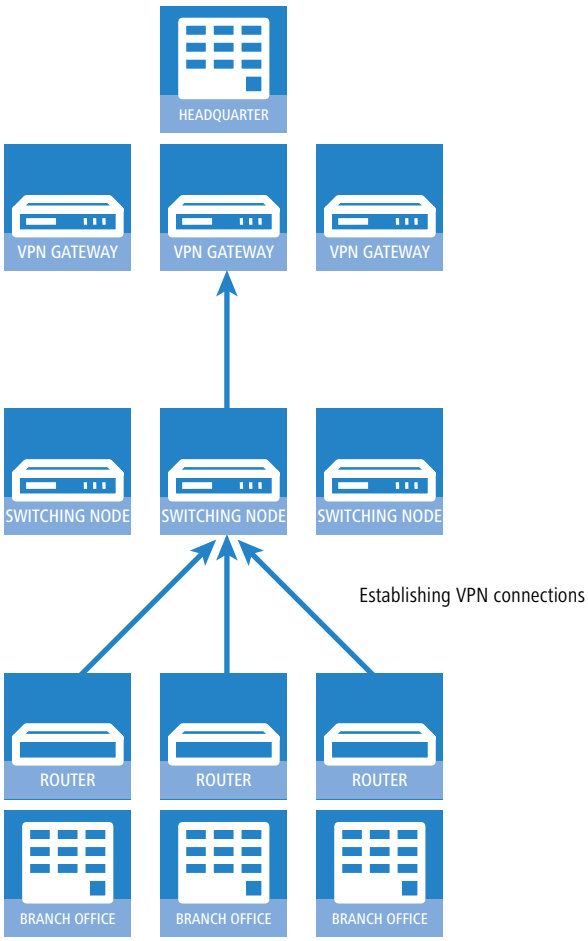
In order to also build up an operational backup solution for these applications, the points described in the following sections must be satisfied.

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.

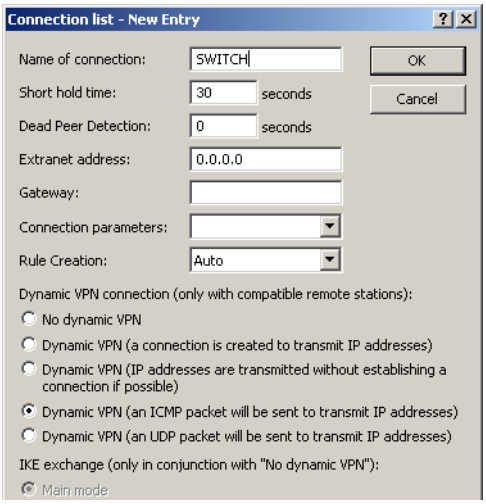
To prevent this, initial "Dynamic VPN" negotiations with the primary connection's remote site are performed. If these negotiations are successful, the primary connection can be reestablished. To this end, the backup connection is disconnected and the backup status is reset. This prevents the backup connection 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.

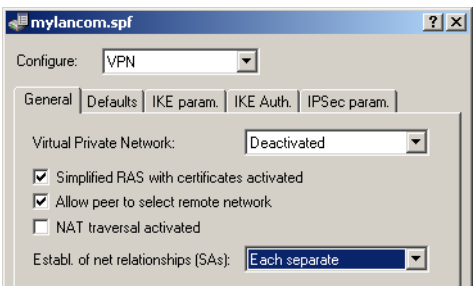
E.3.3 Configuring the VPN backup

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.



  - 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.



- 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.

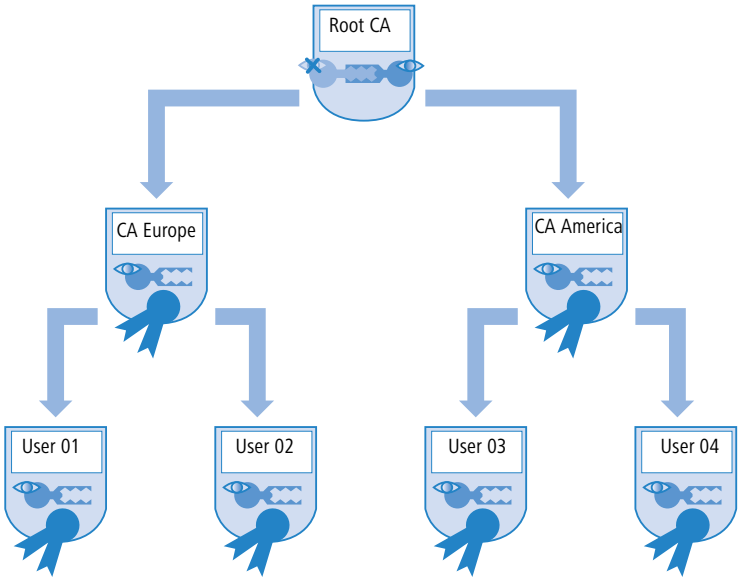
E.4 Multi-level certificates for SSL/TLS

New with LCOS 7.6:

- Multi-level certificates for SSL/TLS

E.4.1 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.

E.4.2 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.

E.4.3 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.

F Firewall

F.1 Configuring the firewall with LANconfig

New in LCOS 7.60:

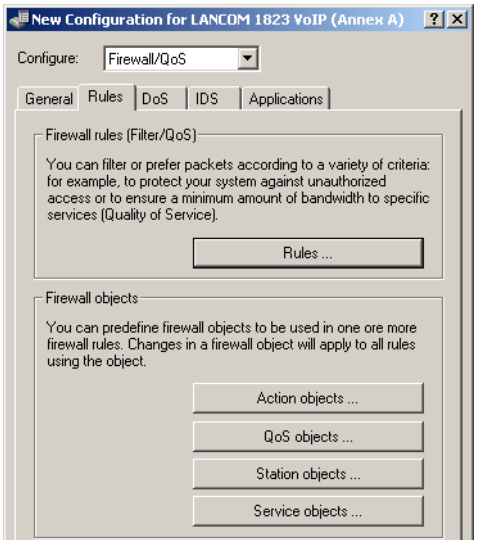
- Object-oriented definition of firewall rules

F.1.1 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.

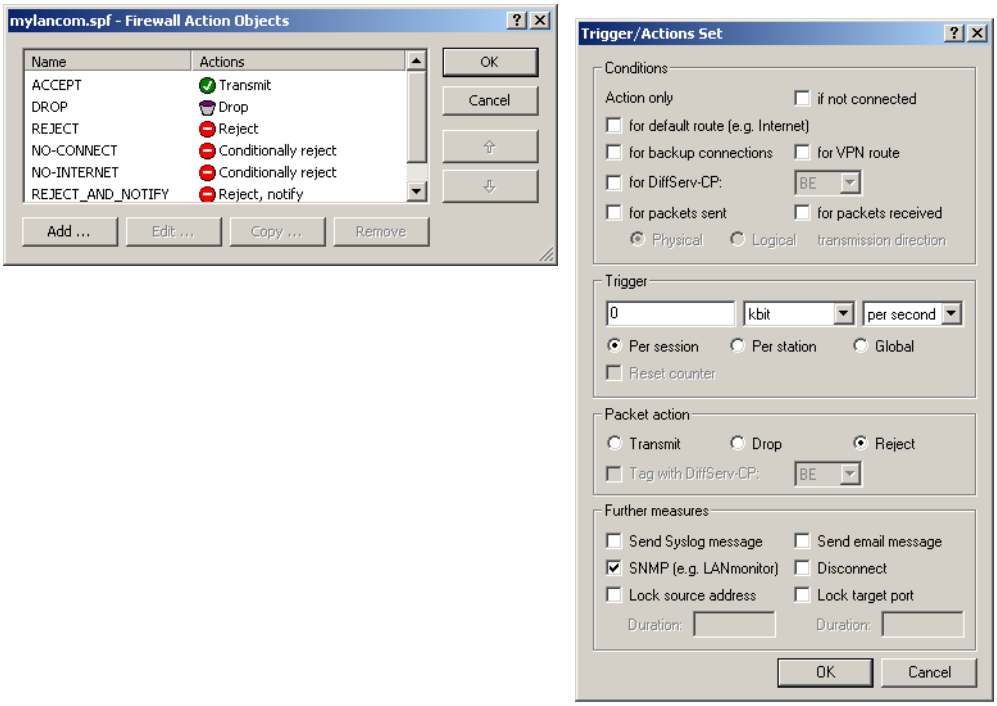
Please note that a change to firewall objects affects all of the firewall rules that use this object. For this reason, all firewall rules that also use these objects are displayed when you make changes to firewall objects.

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.



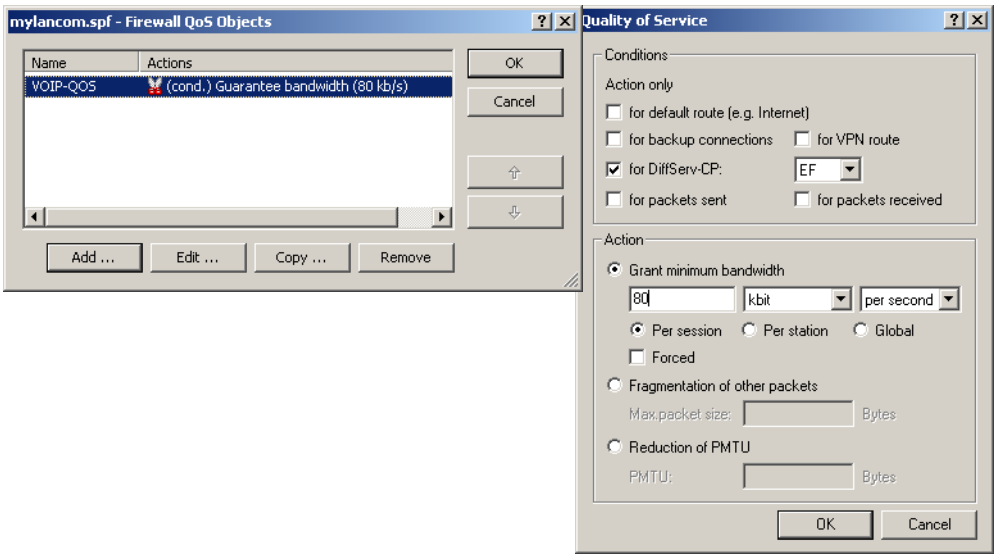
Action objects

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.



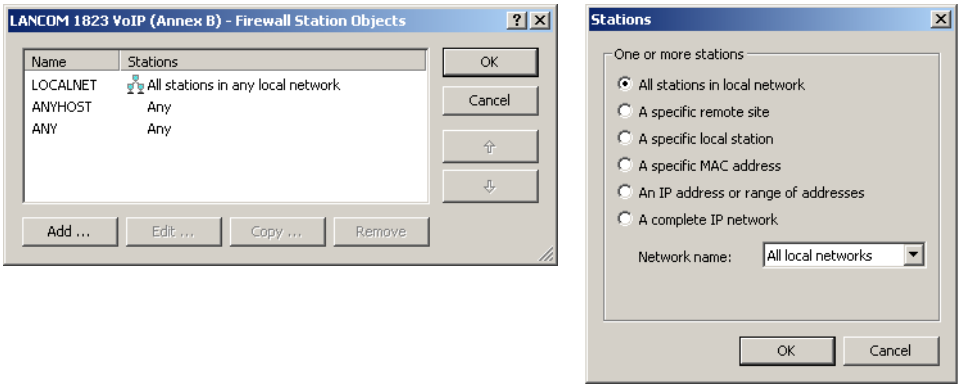
QoS objects

Here you set the minimum bandwidths that the firewall rules allocate to data packets.



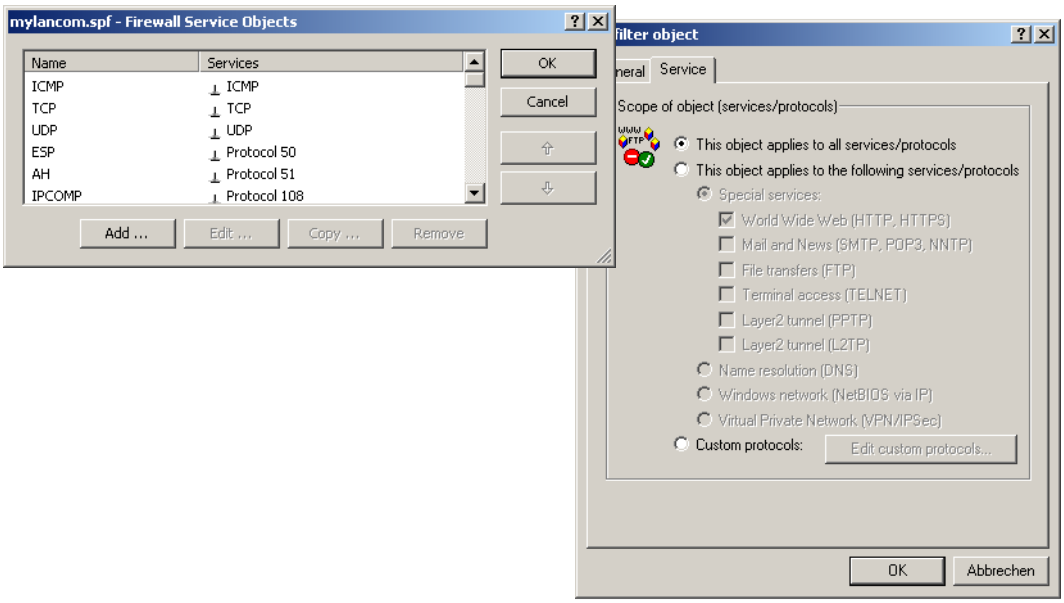
Station objects

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.



Service objects

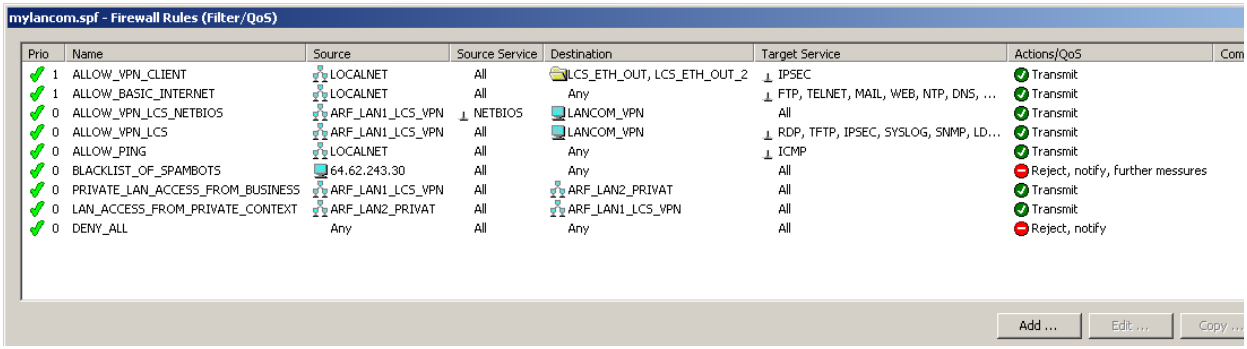
The IP protocols and the source/destination ports to be used by the firewall rules are defined here.



F.1.2 Defining firewall rules

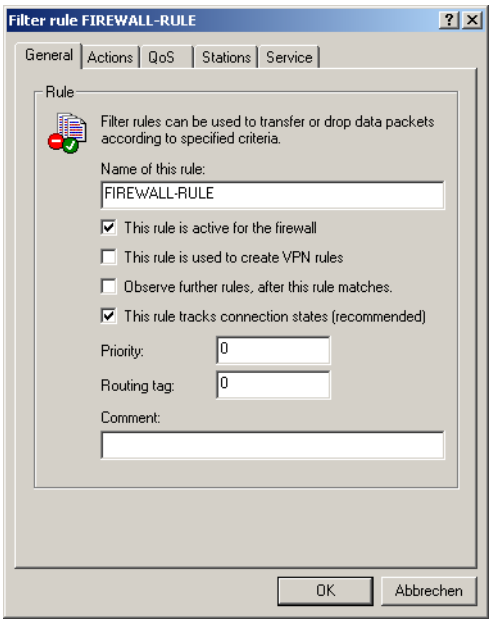
The firewall rules are shown in a clearly laid-out table containing the following information:

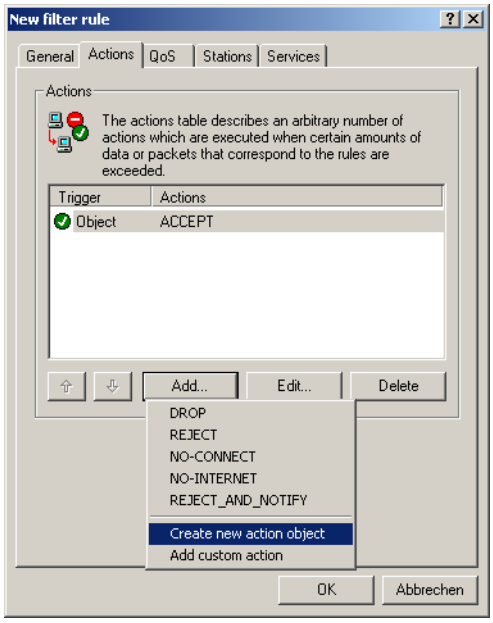
- In the left-most column, icons indicate the status of the firewall rule:
  - Green check-mark: Firewall rule is enabled.
  - Red cross: Firewall rule is disabled.
  - Lock: Firewall rule is used to create VPN rules manually.
  - Two interlinked arrows: If this firewall rule applies, please observe other rules.
- Name of firewall rule
- Source
- Destination
- Source and destination service
- Action/QoS
- Comment



Adding a new firewall rule

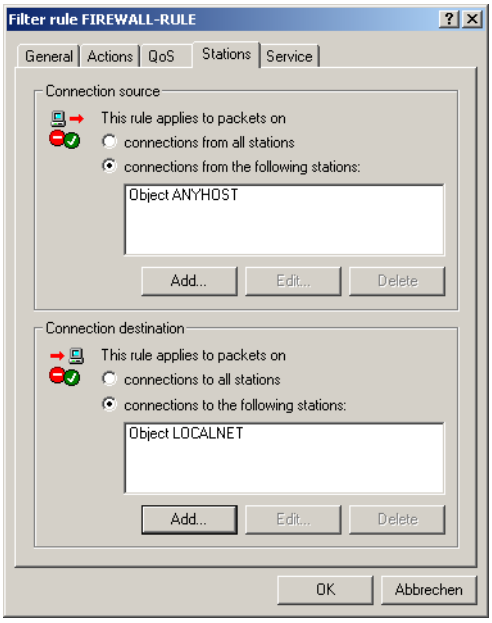
When creating a new firewall rule, the general data is entered first. Objects already defined can be selected directly from the tabs for Actions, QoS, Stations and Services. New objects that can also be used in other rules can be created here, as can user-defined entries that are only to be used in the active firewall rule.

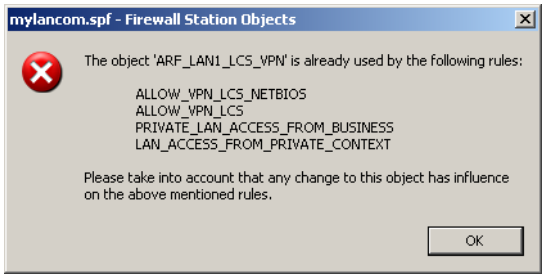




Editing firewall rules

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.





F.2 Configuring firewall rules with WEBconfig or Telnet

Changes with LCOS 7.6:

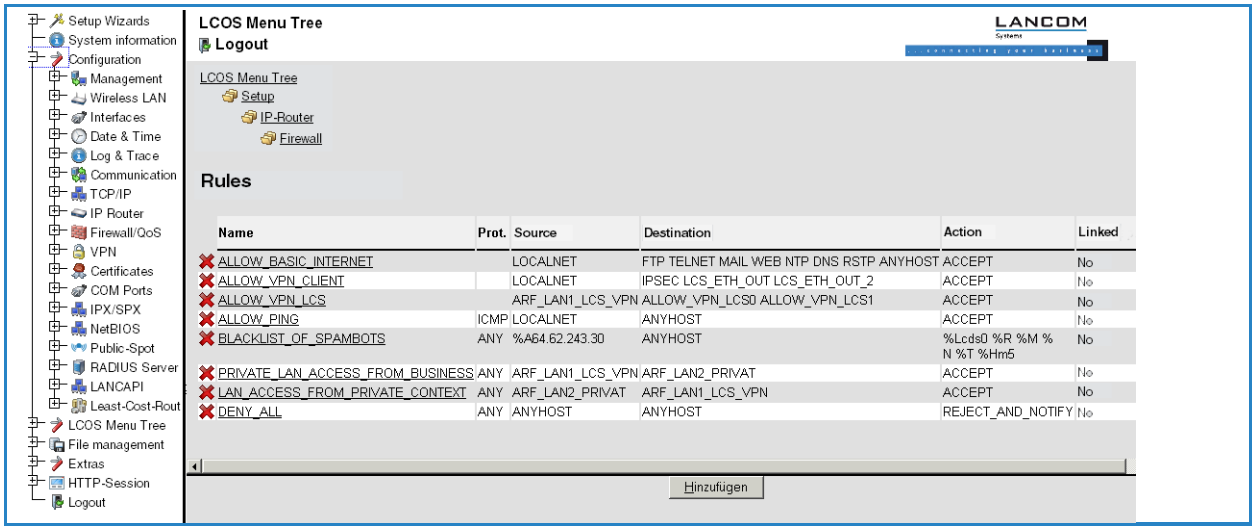
- New condition @b for restricting the firewall rule to backup connections
- New limit %u for restricting the firewall rule to one station's connections
- New limit %i for the specification of a maximum number of connections
- New limit %b for the specification of a percentage of bandwidth
- Object-oriented definition of firewall rules

F.2.1 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.



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.

- **Name**

  Specify here a unique name for this firewall rule.

  - Possible values: Max. 32 characters

- **Prot.**

  Specification of the protocol that is to apply for this entry (assuming that protocols have not been defined in source and destination along with the ports/services).

  - Possible values: Max. 10 characters Direct input observing the LCOS syntax as defined in the object table or references to an entry in the object table.

- **Source**

  Specification of the source objects (one or more networks, stations, protocols and ports) for which this entry is to apply.

  - Possible values: Max. 40 characters Direct input observing the LCOS syntax as defined in the object table or references to an entry in the object table.

- **Destination**

  Specification of the destination objects (one or more networks, stations, protocols and ports) for which this entry is to apply.

  - Possible values: Max. 40 characters Direct input observing the LCOS syntax as defined in the object table or references to an entry in the object table.

If protocols and ports entered in a source or destination object are mixed, these ports apply for all protocols listed in the rule!

Example: Destination = FTP, DNS with the object definitions FTP = TCP, port 21 and NTP = UDP, port 123. The resulting rule releases ports 21 and 123 for UDP and TCP (UDP port 21 and 123 and TCP port 21 and 123).

For standard values this is rarely a problem, since the well-known ports are mostly defined both for TCP and UDP (see www.iana.org/assignments/port-numbers).

If this behavior is undesirable for detailed controls, then only objects with the same protocol can be used in a rule, or a rule has to be defined for each service/protocol object.

- **Action**

  Action to be run if the firewall rule applies to a packet.

  - Possible values: Max. 40 characters. Direct input observing the LCOS syntax as defined in the action table or references to an entry in the action table.

- **Linked**

  Links the rule to other rules.

  - Possible values: Yes, No
  - Default: No

- **Prio**

  Priority of the rule.

  - Possible values: 0 to 255

- **Active**

  Switches the rule on/off.

- □ Possible values: Yes, No
- □ Default: Yes

■ **VPN rule**

Activates the rule for creating VPN rules manually.

- □ Possible values: Yes, No
- □ Default: No

■ **Stateful**

When this option is enabled, a check is performed as to whether a connection is being established correctly. Erroneous packets are discarded whilst the connection is being established. If this option is disabled, all packets for which this rule applies are accepted (simple packet-filter firewall).

By tracking the connection status, whereby each packet is allocated to a certain session, the filter effectively becomes direction-dependent, so that the commencing session's data traffic can only flow from the specified source to the destination. Ports for the answer packets of a defined session are opened dynamically.

Furthermore, this option is enabled for the automatic protocol recognition for FTP, IRC, PPTP necessary to be able to open a port in the firewall for each data connection.

The test for portscans/SYN flooding is also enabled/disabled with this option. This can exclude particular, heavily-frequented servers from the test, meaning that limits for half-open connections (DOS) or port requests (IDS) do not have to be set so high that they effectively become useless.

- □ Possible values: Yes, No
- □ Default: Yes

■ **Rtg tag**

Routing tag for the rule.

Possible values:

- □ 0 to 65535

Default:

- □ 0

■ **Comment**

Comment for this entry.

- □ Possible values: Max. 64 characters

F.2.2 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.

■ **Name**

Specify here a unique name for this object.

- □ Possible values: Max. 32 characters

■ **Description**

The stations and services can be defined in the objects table.

Possible values:

- □ %L: local network
- □ %H: Remote sites – name must be in DSL/ISDN/PPTP or VPN remote site list
- □ %D: Host name – note information on host names
- □ %E: MAC address – 00:A0:57:01:02:03
- □ %A: IP address – %A10.0.0.1, 10.0.0.2; %A0 (all addresses)

- □ %M: Network mask – %M255.255.255.0
- □ %P: Protocol (TCP/UDP/ICMP, etc.) – %P6 (for TCP)
- □ %S: Service (port) – %S20-25 (for ports 20 to 25)

Special values:

- □ Definitions of the same type can be created as comma-separated lists, such as host lists/address lists (%A10.0.0.1, 10.0.0.2) or with ranges separated by hyphens, such as port lists (%S20-25).
- □ Specifying '0' or an empty string denotes the Any object.

For configuration from the console (Telnet or terminal application), the combined parameters (port, destination, source) must be enclosed with quotation marks (").

Host names can only be used if the LANCOM can resolve the names into IP addresses. To this end, 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. One entry in the IP routing table can assign a complete network to a host name.

F.2.3 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.

■ **Name**

Specify a unique name for this action.

- □ Possible values: Max. 32 characters

■ **Description**

In the actions table, firewall actions are combined as any combination of conditions, limits, packet actions and other measures.

Conditions

Conditions can be used to restrict the effectiveness of a firewall rule.

Possible values for the conditions:

- □ @c: Connect filter – the filter is active if there is no physical connection to the destination of the packet.
- □ @d (plus DSCP): DiffServ filter – the filter is active if the packet contains the specified Differentiated Services Code Point (DSCP).
- □ @i: Internet filter – the filter is active if the packet was received, or is to be sent, via the default route.
- □ @v: VPN filter – the filter is active if the packet was received, or is to be sent, via a VPN connection.
- □ @b: Backup filter – the filter is active if either the direct remote site is in the backup state or one of the stacked protocols was built-up in a protocol stack (e.g. VPN via PPTP over DSL) over a backup connection. If, for example, the Internet connection is in the backup state, a VPN connection established over it is classified by the firewall as a backup connection.

Special values for the conditions:

- □ If no further action is specified for the "Connect" or "Internet" filter, a combination of these filters is implicitly adopted with the "Reject" action.

Limits

The limit (or trigger) denotes a quantified threshold that must be exceeded on a defined connection before the filter captures a data packet. A limit comprises the values for the unit (kbit, Kbyte, packets, number of sessions or % of bandwidth), the amount (data rate or number) and reference value (per second, per minute, per hour or absolute) and possible other parameters (such as period and size).

It can also be agreed for the limit whether it refers to a logical session/station or to all connections together (existent between the specified destination and source stations via the related services). This controls whether the filter takes effect when, for example, the total of all user HTTP connections in the LAN exceeds the limit or whether it is sufficient when just one parallel HTTP connection exceeds the threshold.

For absolute values, you can define whether the associated counter should be reset in the event that the limit is exceeded.

Data is always transferred until the limit is reached. When the amount is "0", the rule immediately comes into effect if data packets are pending for transmission on the connection.

Possible values for the limits:

- %c: Connection – the limit refers to the individual connection.
- %u: User – the limit refers to all of the user's connections (of the station, identified via the IP address).
- %g: Global – the limit refers to all connections that match the sources/destinations and protocols/services defined for this firewall rule.
- %d: Data – number of kilobytes after which the action is run.
- %p: Packet – number of packets after which the action is run.
- %i: Interconnection – number of connections (sessions) after which the action is run.
- %b: Based – percentage of bandwidth after which the action is run.
- %s, %m, %h: second, minute, hour – time in seconds, minutes, hours after which the action is run.
- %r: Receive option – restriction of the limit to the receive direction.
- %t: Transmit option – restriction of the limit to the transmit direction.
- Amount - amount of data, number of packets/connections or percentage of bandwidth after which the action is run.

Limit objects are generally initiated with %L, followed by a combination of the possible limit parameters.

Special values for the limits:

- Limit %i for the number of connections is only useful with user-related (%u) and global rules (%g).

If a firewall rule is specified without a limit, a packet limit is used that is immediately exceeded on the first packet.

Packet actions

Packet actions can be combined with one another in any way. For nonsensical or ambiguous actions (such as Accept + Drop), the more secure one is taken - "Drop" in this example.

Possible values for the packet actions:

- %a: Accept – the packet is accepted
- %r: Reject – the packet is rejected with an appropriate error message
- %d: Drop – the packet is dropped silently

Other measures

The firewall is not only used to discard or allow through filtered data packets. It can also take additional measures when a data packet is captured by the filter. The measures are divided into two functions - "Logging/Notification" and "Prevention of further attacks":

Possible values for other measures:

- %s: Syslog – provides a detailed message via Syslog
- %m: Mail – sends an e-mail to the administrator
- %n: SNMP – sends an SNMP trap
- %p: Close port – closes the destination port of the packet for a configurable time
- %h: Deny host – blocks the sender address of the packet for a configurable time
- %t: Disconnect – disconnects the physical connection to the remote site over which the packet was received or is to be sent.
- %z: Zero-limit – resets the limit counter to 0 if trigger threshold is exceeded.
- %f: Fragmentation – forces the fragmentation of all packets not matching the rule

Possible values for other measures:

- When the "Close port" action is run, an entry is made in a block list with which all packets sent to the respective computer and port are discarded. For the "Close port" object, a block time in seconds, minutes or hours can be specified. This is noted directly behind the object ID. This time is made up of the identifier for the time unit (h, m, s for hour, minute, second) as well as the actual time specification. For example, %pm10 blocks the port for 10 minutes. "Minutes" is used as the unit if no time unit is specified. (%p10 is therefore equivalent to %pm10)
- If the "Deny host" action is run, the sender of the packet is entered into a block list. From this moment on, all packets received from the blocked computer are discarded. The "Deny host" object can also be given a block time, formed as described for the "Close port" option.

G Voice over IP

G.1 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

G.1.1 Configuration of users

Local users are the terminal equipment/telephones that are connected to the LANCOM VoIP Router. There is a difference between:

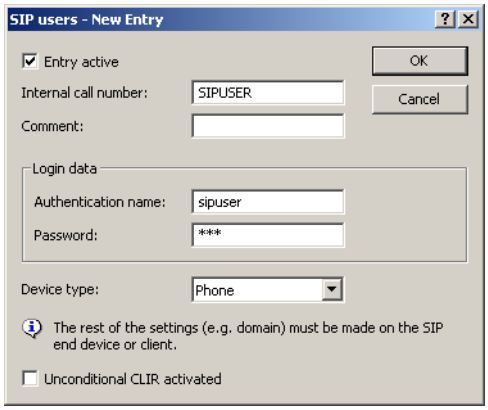
- SIP users: Users who are connected to the LAN by means of a SIP telephone. For the user configuration, it does not matter whether the LAN is connected directly to LANCOM, or whether it is connected via a VPN (over the Internet).
- ISDN users: Users who are connected by ISDN. They use the SIP gateway 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.

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



WEBconfig: 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).

  Possible values:

  - Maximum 16 alphanumerical characters.

Default:

- □ Blank

■ **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).

Possible values:

- □ Maximum 64 alphanumerical characters

Default:

- □ Blank

■ **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).

Possible values:

- □ Maximum 64 alphanumerical characters.

Default:

- □ Blank

■ **Device type**

Type of device connected.

Possible values:

- □ Telephone
- □ Fax
- □ Telephone/fax

Default:

- □ Telephone

■ **CLIR**

Switches the transmission of the calling-line identifier on/off.

Possible values:

- □ Yes: Transmission of the calling-line identifier is suppressed whatever the setting in the user's device.
- □ No: Transmission of the calling-line identifier is not suppressed in the device; the settings in the user's terminal device control the transmission of the calling-line identifier.

Default:

- □ No

■ **Active**

Activates or deactivates the entry.

Possible values:

- □ Yes, No

Default:

- □ Yes

■ **Comment**

Comment on this entry

Possible values:

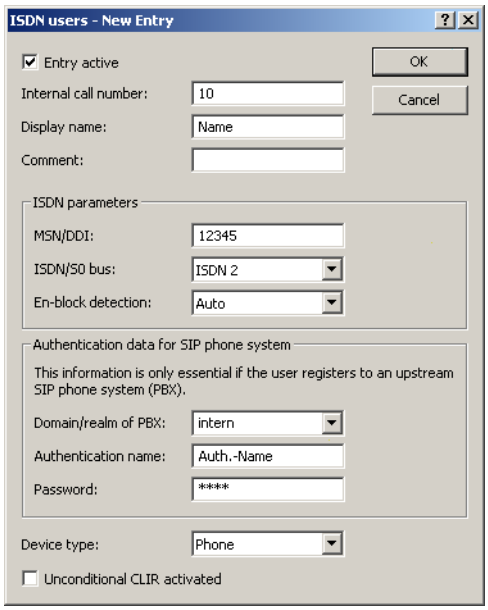
- □ Maximum 64 alphanumerical characters.

Default:

- □ Blank

ISDN users

LANconfig: VoIP Call Manager ▶ Users ▶ ISDN users



WEBconfig: Setup ▶ Voice Call Manager ▶ Users ▶ ISDN users

■ **Number/Name**

Internal number of the ISDN telephone or name of the user (SIP URI).

Possible values:

□ Maximum 16 alphanumerical characters.

Default:

□ Blank

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.

Possible values:

□ One or more of the S0 buses available in the device

Default:

□ Blank

■ **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.

Possible values:

□ Maximum 16 characters (numbers and # characters).

Default:

□ Blank

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.

Possible values:

□ Maximum 64 alphanumerical characters.

Default:

□ Blank

■ **Display name**

Name for display on the telephone being called.

Possible values:

□ Maximum 64 alphanumerical characters

Default:

□ Blank

■ **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).

Possible values:

□ Maximum 64 alphanumerical characters

Default:

□ Blank

■ **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.

Possible values:

□ Maximum 63 alphanumerical characters

Default:

□ Blank

■ **Device type**

Type of device connected.

Possible values:

□ Telephone

□ Fax

□ Telephone/fax

Default:

□ Telephone

■ **DialCompl**

En-block dial detection.

Possible values:

□ Auto: Block dialing is detected automatically (for example, with speed dial or repeat dialing), so that the call is established more quickly. Suffix dialing is not possible.

□ Manual: No block dialing; the number can be marked as complete with '#' and the call can be initiated.

Default:

□ Auto

■ **CLIR**

Switches the transmission of the calling-line identifier on/off.

Possible values:

□ Yes: Transmission of the calling-line identifier is suppressed whatever the setting in the user's device.

- □ No: Transmission of the calling-line identifier is not suppressed in the device; the settings in the user's terminal device control the transmission of the calling-line identifier.

Default:

- □ No

■ **Active**

Activates or deactivates the entry.

Possible values:

- □ Yes, No

Default:

- □ Yes

■ **Comment**

Comment on this entry.

Possible values:

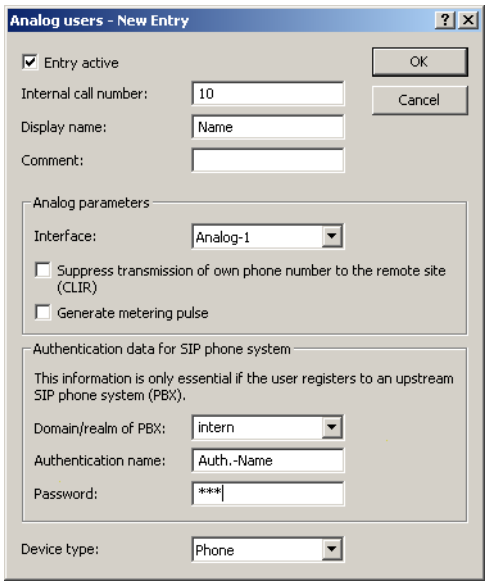
- □ Maximum 64 alphanumerical characters

Default:

- □ Blank

Analog users

LANconfig: VoiP Call Manager ▶ Users ▶ Analog users



WEBconfig: Setup ▶ Voice Call Manager ▶ Users ▶ Analog users

■ **Number/Name**

Internal number of the analog telephone or name of the user (SIP URI).

Possible values:

- □ Maximum 16 alphanumerical characters

Default:

- □ Blank

■ **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.

Possible values:

- □ Maximum 64 alphanumerical characters

Default:

- □ Blank

■ **Display name**

Name for display on the telephone being called.

Possible values:

□ Maximum 64 alphanumerical characters

Default:

□ Blank

■ **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).

Possible values:

□ Maximum 64 alphanumerical characters

Default:

□ Blank

■ **Ifc**

Analog interface that should be used to establish the connection.

Possible values:

□ One of the available analog interfaces in the device.

Default:

□ Analog-1

■ **CLIR**

Switches the transmission of the calling-line identifier on/off.

Possible values:

□ Yes: Transmission of the calling-line identifier is suppressed whatever the setting in the user's device.

□ No: Transmission of the calling-line identifier is not suppressed in the device; the settings in the user's terminal device control the transmission of the calling-line identifier.

Default:

□ No

■ **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.

Possible values:

□ Yes, No

Default:

□ No

■ **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.

Possible values:

□ Maximum 63 alphanumerical characters

Default:

□ Blank

■ **Device type**

Type of device connected.

Possible values:

□ Telephone

- □ Fax
- □ Telephone/fax

Default:

- □ Telephone

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.

Possible values:

- □ Yes, No

Default:

- □ Yes

■ **Comment**

Comment on this entry

Possible values:

- □ Maximum 64 alphanumerical characters.

Default:

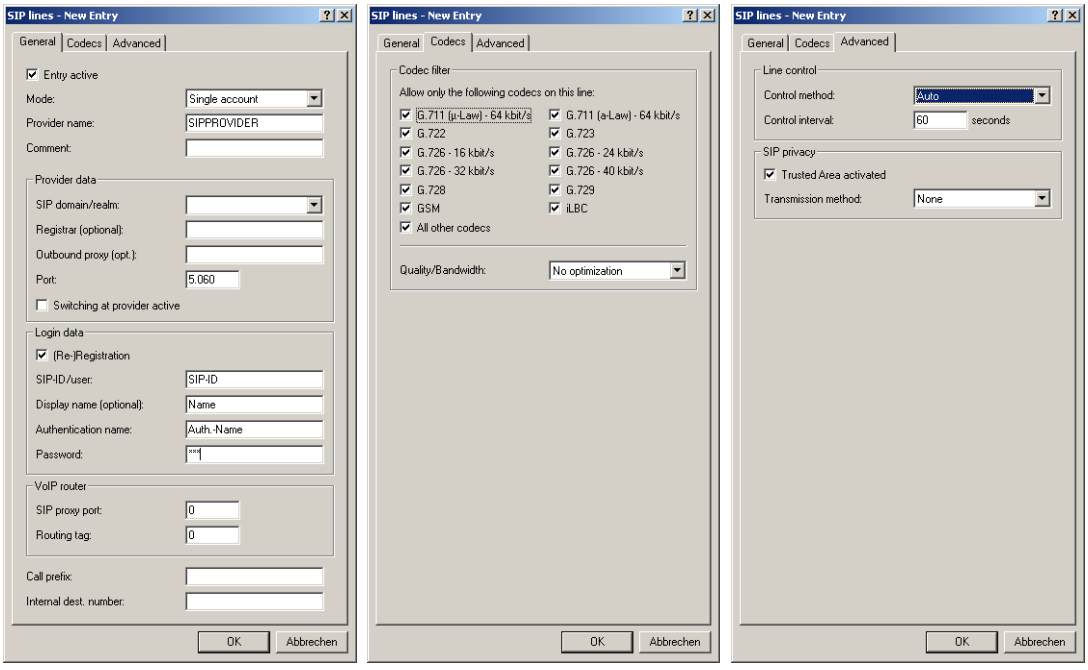
- □ Blank

G.1.2 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. Up to 16 SIP lines can be entered.

LANconfig: VoIP Call Manager ▶ Lines ▶ SIP lines



WEBconfig: 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.

Possible values:

- □ Maximum 16 alphanumerical characters

Default:

□ Blank

■ **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:"

Default:

□ Single account

■ **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.

Possible values:

□ Maximum 64 alphanumerical characters

Default:

□ Blank

■ **Rtg tag**

Routing tag for selecting a certain route in the routing table for connections to this SIP provider.

Possible values:

□ Maximum 64 characters

Default:

□ 0

■ **Port**

TCP/UDP port that the SIP provider uses as the target port for SIP packets.

Possible values:

□ Any available TCP/IP port

Default:

□ 5060

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).

Possible values:

□ Maximum 64 alphanumerical characters

Default:

□ Blank

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).

Possible values:

□ Maximum 64 alphanumerical characters

Default:

□ Blank

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.

Possible values:

□ Maximum 64 alphanumerical characters

Default:

□ Blank

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.

Possible values:

□ Maximum 64 alphanumerical characters

Default:

□ Blank

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.

Possible values:

□ Maximum 63 alphanumerical characters

Default:

□ Blank

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.

Possible values:

□ Maximum 64 alphanumerical characters

Default:

□ Blank

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.

Possible values:

□ Maximum 9 characters

Default:

□ Blank

■ **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.

Possible values:

□ Maximum 64 alphanumerical characters

Default:

□ Blank

■ **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.

Possible values:

□ Select from the list of available codecs.

Default:

□ All

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.

Possible values:

□ No optimization: Leaves the order of the codecs unchanged

□ Best quality: Changes the order of the codecs that are offered to achieve the best voice quality possible.

□ Minimum bandwidth: Changes the order of the codecs that are offered to achieve the lowest bandwidth possible.

Default:

□ No optimization

■ **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).

Possible values:

□ Yes: Switching is passed on to the provider

□ No: Switching is retained within the device.

Default:

□ No

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.

Possible values:

□ 1 to 65536

Default:

□ 0

Special values:

□ 0: Dynamic port selection; the port is automatically selected from the pool of available port numbers.

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.

Possible values:

□ Yes, No

Default:

□ Yes

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.

Default:

□ Auto

■ **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.

Possible values:

□ Max. 5 numbers.

Default:

□ 60

Special values:

□ Values less than 60 seconds are automatically set to 60 seconds.

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.

Possible values:

- □ Yes: Trusted
- □ No: Not trusted

Default:

- □ Yes

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.

Possible values:

- □ None
- □ RFC3325: Via P-Preferred-Id/P-Asserted-Id
- □ IETF-Draft-Sip-Privacy-04: Via RPID (Remote Party ID)

Default:

- □ None

■ **Active**

Activates or deactivates the entry.

Possible values:

- □ Yes, No

Default:

- □ Yes

■ **Comment**

Comment on this entry.

Possible values:

- □ Maximum 64 alphanumerical characters

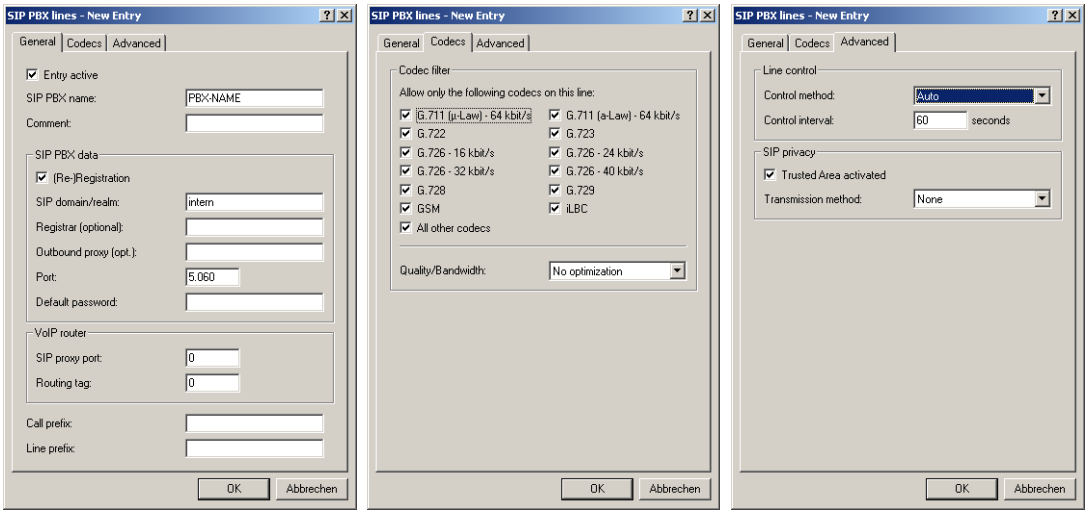
Default:

- □ Blank

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



WEBconfig: 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.

Possible values:

□ Maximum 16 alphanumerical characters

Default:

□ Blank

■ **Domain**

SIP domain/realm of the upstream SIP PBX.

Possible values:

□ Maximum 64 alphanumerical characters

Default:

□ Blank

■ **Rtg tag**

Routing tag for selecting a certain route in the routing table for connections to this SIP PBX.

Possible values:

□ Maximum 64 characters

Default:

□ 0

■ **Port**

TCP/UDP port of the upstream SIP PBX to which the LANCOM device sends the SIP packets.

Possible values:

□ Any available TCP/IP port.

Default:

□ 5060

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.

Possible values:

□ Maximum 64 alphanumerical characters

Default:

□ Blank

■ **Registrar**

The SIP registrar is the point that accepts the login with the configured authentication data for this account in the SIP PBX.

Possible values:

□ Maximum 63 alphanumerical characters

Default:

□ Blank

■ **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.

Possible values:

□ Maximum 9 characters

Default:

□ Blank

■ **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.

Possible values:

□ Maximum 19 characters

Default:

□ Blank

■ **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.

Possible values:

□ Select from the list of available codecs.

Default:

□ All

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.

Possible values:

□ No optimization: Leaves the order of the codecs unchanged

□ Best quality: Changes the order of the codecs that are offered to achieve the best voice quality possible.

□ Minimum bandwidth: Changes the order of the codecs that are offered to achieve the lowest bandwidth possible.

Default:

□ No optimization

■ **Local port number**

This is the port used by the LANCOM proxy to communicate with the upstream SIP PBX.

Possible values:

□ 1 to 65536

Default:

□ 0

Special values:

□ 0: Dynamic port selection; the port is automatically selected from the pool of available port numbers.

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.

Possible values:

□ Yes, No

Default:

□ Yes

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.

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.

Default:

- □ Auto

■ **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.

Possible values:

- □ Max. 5 numbers.

Default:

- □ 60

Special values:

- □ Values less than 60 seconds are automatically set to 60 seconds.

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.

Possible values:

- □ Yes: Trusted
- □ No: Not trusted

Default:

- □ Yes

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.

Possible values:

- □ None
- □ RFC3325: Via P-Preferred-Id/P-Asserted-Id
- □ IETF-Draft-Sip-Privacy-04: Via RPID (Remote Party ID)

Default:

- □ None

■ **Active**

Activates or deactivates the entry.

Possible values:

- □ Yes, No

Default:

- □ Yes

■ **Comment**

Comment on this entry.

Possible values:

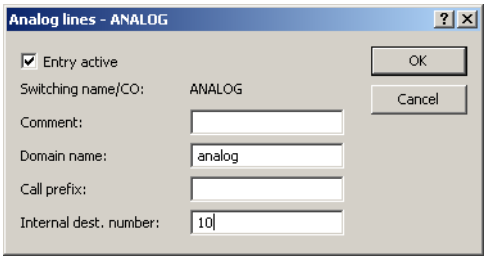
- □ Maximum 64 alphanumerical characters

Default:

- □ Blank

Analog line

LANconfig: VoIP Call Manager ▶ Lines ▶ Analog lines



WEBconfig: Setup ▶ Voice Call Manager ▶ Lines ▶ Analog

■ **Name**

Name of the line; may not be identical to another line that is configured in the device.

Possible values:

- □ Maximum 16 alphanumerical characters

Default:

- □ Blank

■ **Domain**

The analog line's domain name used for addressing in SIP.

Possible values:

- □ Maximum 64 alphanumerical characters

Default:

- □ analog

■ **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.

Possible values:

- □ Maximum 9 characters

Default:

- □ Blank

■ **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).

Possible values:

- □ Maximum 64 alphanumerical characters

Default:

- □ Blank

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.

Possible values:

□ Yes, No

Default:

□ Yes

■ **Comment**

Comment on this entry.

Possible values:

□ Maximum 64 alphanumerical characters

Default:

□ Blank

■ **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).

Possible values:

□ Default: This setting causes the standard value for the country where the device is operated to be taken.

□ FSK: Transfer of the Caller ID with the Frequency Key Shifting method.

□ DTMF: Transfer of the Caller ID with the Dual Tone Multi Frequency method.

Default:

Country-specific default values:

□ The Netherlands: DTMF

□ All other countries: V.23 (FSK)

■ **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.

Default:

Country-specific default values:

□ Austria: During-Ringing

□ Belgium: Ringing Pulse Alerting Signal, RP-AS

□ France: During-Ringing

□ Italy: During-Ringing

□ Switzerland: During-Ringing

□ The Netherlands: Line reversal

□ Spain: Ringing Pulse Alerting Signal, RP-AS

□ United Kingdom: Line reversal

□ Germany: During-Ringing

H WLAN

H.1 Configuration of WLAN parameters

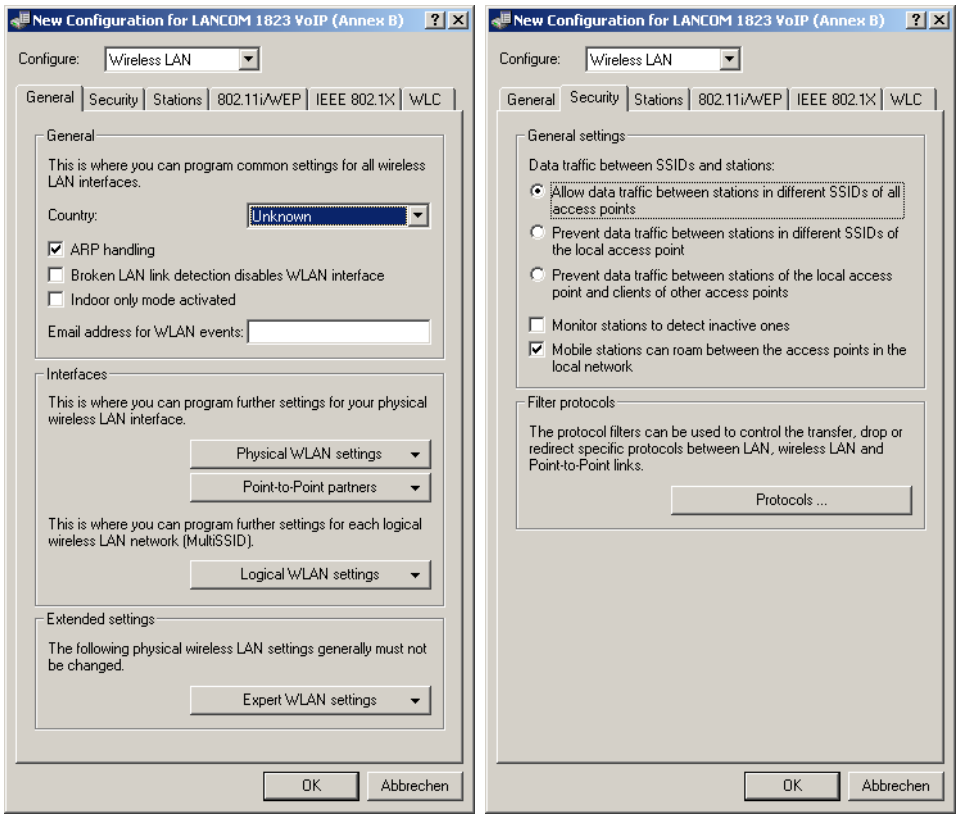
H.1.1 General WLAN settings

Changes with LCOS 7.6:

- Inter-SSID traffic adjustable for the whole WLAN.

LANconfig: Wireless LAN ▶ General

LANconfig: Wireless LAN ▶ Security



WEBconfig: Setup ▶ WLAN

- **Broken link detection**

  The wireless LAN interface is deactivated if the LAN connection (link) is lost (Broken link detection)

  Possible values:

  □ Yes, No

  Default:

  □ No

For WLAN devices with multiple LAN interfaces, this parameter relates to the first LAN interface, LAN-1.

- **Spare heap**

  The heap reserve specifies how many blocks in the LAN heap can be reserved for direct communication (Telnet) with the device. If the number of blocks in the heap is below the specified value, then received packets are rejected immediately (except for TCP packets sent directly to the device).

  Possible values:

  □ Max. 3 numbers

  Default:

  □ 10

■ **IAPP protocol**

Access points use the Access Point Protocol (IAPP) to exchange information about their associated clients. This information is used in particular when clients roam between different access points. The new access point informs the former one of the handover, so that the former access point can delete the client from its station table.

Possible values:

□ Yes, No

Default:

□ Yes

■ **IAPP announce interval**

This is the interval (in seconds) with which the access points broadcast their SSIDs.

Possible values:

□ Max. 10 numbers.

Default:

□ 120

■ **IAPP handover timeout**

If the handover is successful, the new access point informs the former access point that a certain client is now associated with another access point. This information enables the former access point to delete the client from its station table. This stops packets being (unnecessarily) forwarded to the client. For this time space (in milliseconds) the new access point waits before contacting the former access point again. After trying five times the new access point stops these attempts.

Possible values:

□ Max. 10 numbers

Default:

□ 1000

■ **Country**

The device needs to be set with the country where it is operating in order for the WLAN to use the parameters approved for the location.

□ Select from the list of countries.

Default:

□ Blank

■ **Indoor-only operation**

If indoor-only operation is activated, the 5-GHz-band channels are limited to the 5.15 - 5.25 GHz spectrum (channels 36-48) in ETSI countries. Radar detection (DFS) is switched off and the mandatory interruption after 24 hours is no longer in effect. This mode reduces the risk of interruption due to false radar detections. In the 2.4-GHz band in France, the channels 8 to 13 are also permitted, meaning that more channels are available.

Possible values:

□ Yes, No

Default:

□ No

Indoor operation may only be activated if the base station and all other stations are operated within an enclosed space.

■ **Mail address**

This e-mail addressed is used to send information about events in the WLAN.

Possible values:

□ Valid e-mail address

Default:

□ Blank

An SMTP account must be set up to make use of the e-mail function.

■ **Card reinit cycle**

In this interval (in seconds) the internal WLAN cards in older access points are reinitialized in order for point-to-point connections to remain active. This function is handled by the "Alive-Test" in newer models.

Possible values:

□ Max. 10 numbers.

Default:

□ 0

Special values:

□ 0: Deactivates this function.

■ **Noise calibration cycle**

WLAN cards fitted with the Atheros chipset measure noise levels on the medium in this interval (in seconds).

Possible values:

□ Max. 10 numbers

Default:

□ 10

Special values:

□ 0: Deactivates this function.

Please note that deactivating the noise-calibration cycle for these cards means that they cannot react to changes in noise levels. This measurement is mandatory when DFS is being used (automatic interval of 10 seconds). In these cases a shorter interval may be set, but the function should not be deactivated.

■ **Therm. recal. cycle**

In this interval (in seconds) WLAN cards fitted with the Atheros chipset adjust their transmission power to compensate for thermal variations.

Possible values:

□ Max. 10 numbers

Default:

□ 20

Special values:

□ 0: Deactivates this function.

Please note that deactivating the thermal recalibration cycle for these cards means that they cannot react to changes in temperature.

■ **Trace-MAC**

The output of trace messages for the WLAN-Data-Trace can be set for a certain client. The corresponding MAC address is entered here.

Possible values:

□ Max. 12 hexadecimal characters

Default:

□ 000000000000

Special values:

□ 000000000000: Deactivates this function and outputs trace messages for all clients.

■ **Trace level**

The output of trace messages for the WLAN-Data-Trace can be limited to contain certain content only. The messages are entered in the form of a bit mask for this.

Possible values:

□ 0 to 255.

□ 0: Reports that a packet has been received/sent

□ 1: Adds the physical parameters for the packets (data rate, signal strength...)

□ 2: Adds the MAC header

□ 3: Adds the Layer3 header (e.g. IP/IPX)

- □ 4: Adds the Layer4 header (TCP, UDP...)
- □ 5: Adds the TCP/UDP payload

Default:

- □ 255

■ **Idle timeout**

Inactive time (in minutes) after a client is disconnected from the access point. This time is reset when packets are received from the client (not when packets are sent).

Possible values:

- □ 0 to 65535 (5 characters)

Default:

- □ 60

Special values:

- □ 0: Switches the Timeout off

■ **Supervise stations**

In particular for public WLAN access points (public spots), the charging of usage fees requires the recognition of stations that are no longer active. Monitoring involves the access point regularly sending packets to logged-in stations. If the stations do not answer these packets, then the charging systems recognizes the station as no longer active.

Possible values:

- □ Yes, No

Default:

- □ No

■ **ARP handling**

A station in the LAN attempting to establish a connection to a WLAN station which is in power-save mode will often fail or only succeeds after a considerable delay. The reason is that the delivery of broadcasts (such as ARP requests) to stations in power-save mode cannot be guaranteed by the base station.

If you activate ARP handling, the base station responds to ARP requests on behalf of the stations associated with it, thus providing greater reliability in these cases.

Possible values:

- □ Yes, No

Default:

- □ Yes

■ **Access mode**

A way of limiting data traffic between the wireless LAN and its local network is to exclude certain stations from transferring data, or you can approve selected stations only.

Possible values:

- □ Positive: Data from listed stations is filtered out; data from all other stations is transmitted
- □ Negative: Transfer data from the listed stations, authenticate all others via RADIUS or filter them out.

■ **Inter-SSID traffic**

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.

Possible values:

- □ Yes, No

Default:

- □ Yes

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.

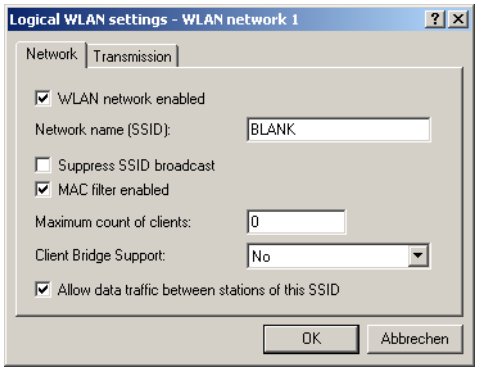
H.1.2 Wireless LAN networks

Changes with LCOS 7.6:

- Inter-Station-Traffic can be set separately for each logical WLAN.

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.

LANconfig: Wireless LAN ▶ General ▶ Logical WLAN settings



WEBconfig: Setup ▶ Interfaces ▶ WLAN ▶ Network

- **Ifc**

  Select from the logical WLAN interfaces.

  Possible values:

  - WLAN-1 to WLAN-1-8, WLAN-2 to WLAN-2-8

- **Active**

  Switches the logical WLAN on or off separately.

  Possible values:

  - Yes, No

  Default:

  - Yes

- **Network name**

  Define an unambiguous SSID (the network name) for each of the necessary logical wireless LANs. Only network cards that have the same SSID can register with this wireless network.

  Possible values:

  - Max. 32 characters

  Default:

  - Blank

- **MAC filter**

  The MAC addresses of the clients allowed to associate with a WLAN are stored in the MAC filter list. With the 'MAC filter' switch, use of the MAC filter list can be switched off 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.

  Possible values:

  - Yes, No

  Default:

  - No

- **RADIUS accounting**

  Activates RADIUS accounting for this logical WLAN, e.g. to record IP addresses and data volumes used by the associated clients. RADIUS packets for the accounting are sent to the server that has been specified for RADIUS accounting.

  Possible values:

  - Yes, No

Default:

□ No

■ **Closed network**

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

Activate the closed network mode if you wish to prevent WLAN clients using the SSID 'ANY' from registering with your network.

Possible values:

□ Yes, No

Default:

□ No

■ **Maximum stations**

Here you set the maximum number of clients that may associate with this access point. Additional clients wanting to associate will be rejected.

Possible values:

□ Max. 10 characters

Default:

□ 0

Special values:

□ 0: No limitation on the maximum number of associated clients.

■ **Cl.-Brg. support**

Whereas address adjustment in client mode allows only the MAC address of the immediately connected devices to be visible to the access point, client-bridge support provides transparency; all MAC addresses of the LAN stations behind the client stations are transferred.

Activate this option for the logical WLAN if the clients are to be provided with this operating mode.

Possible values:

□ Yes, No, Exclusive

Default:

□ No

Special values:

□ Exclusive: This setting means that only clients that support this operating mode are accepted.

Client-bridge mode can only be used between two LANCOM devices.

■ **Inter-station traffic**

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. Individual settings can be made for every logical WLAN as to whether clients in this SSID can exchange data with one another.

Possible values:

□ Yes, No

Default:

□ Yes

Communications between clients in different logical WLANs is controlled centrally by the general WLAN settings (Inter-SSID traffic).

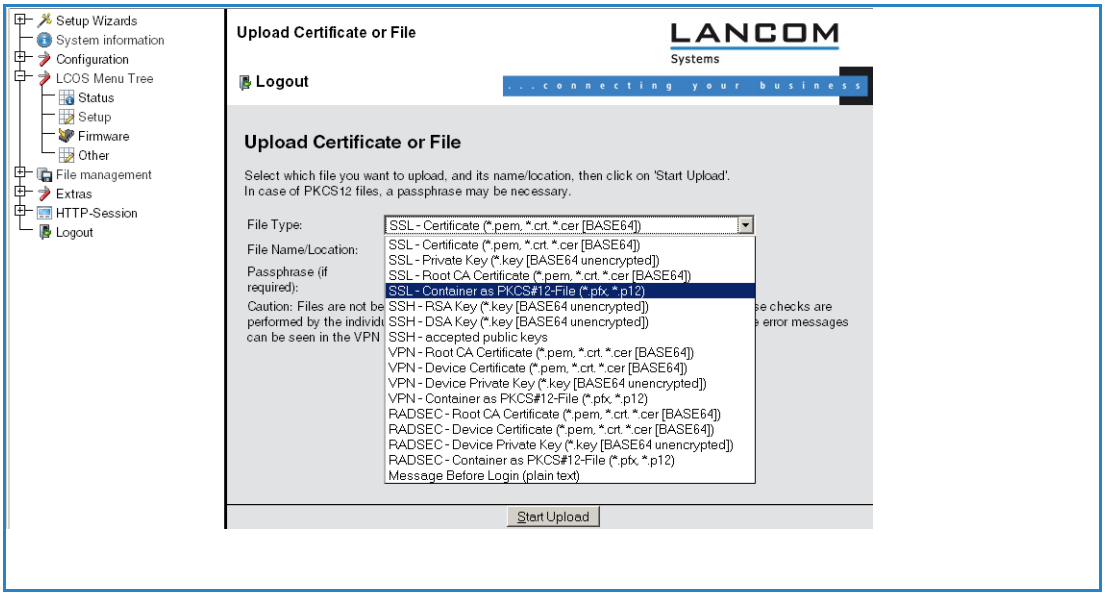
H.2 Multi-level certificates for PublicSpots

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:



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.

H.3 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.

H.4 Central firmware and script management

New with LCOS 7.6:

- Internal script storage (script management without an HTTP server)

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.

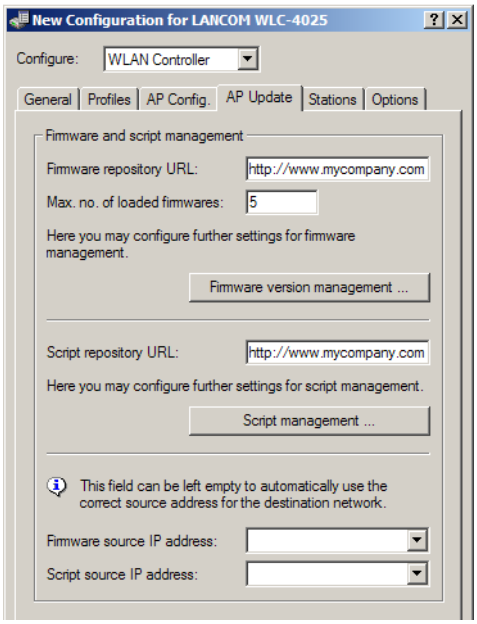
To acheive this, the firmware and script files are stored on a Web server (firmware as *.upx files, scripts and *.lcs files). The WLAN-Controller checks once daily, or on user request, to compare the available files with those on the devices. Alternatively, this procedure can be handled by a cron job—overnight, 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.



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 pupose.

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.

I Messaging

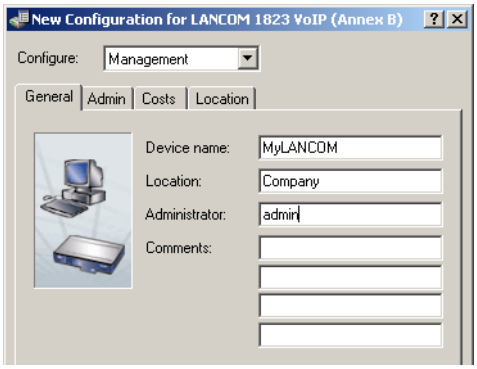
I.1 SNMP traps

New in LCOS 7.60:

- SNMP traps: Trap version can be configured

I.1.1 General SNMP settings

LANconfig: Management ▶ General



WEBconfig: Setup ▶ SNMP

- **Send traps**

  When serious errors occur, for example when an unauthorized attempt is made to access the device, it can send an error message to one or more SNMP managers automatically. For this, activate the option and enter the IP addresses in the IP trap table of those computers where the SNMP managers are installed.

  Possible values:

  - Yes, No

  Default:

  - No

- **Administrator**

  Name of the device administrator. For display purposes only.

  Possible values:

  - Max. 255 characters

  Default:

  - Blank

- **Location**

  Location information for this device. For display purposes only.

  Possible values:

  - Max. 255 characters

  Default:

  - Blank

- **Register monitor**

  This allows SNMP agents to log in to the device in order to receive subsequent SNMP traps. The command is specified together with the IP address, the port and the MAC address of the SNMP agent. Both values can be replaced with the wildcard *, in which case the device ascertains the values from the packets received from the SNMP agent.

  Possible values:

  - <IP address|*>:<Port|*> <MAC address|*> <W>

  Special values:

  - <W> at the end of the command is necessary if registration is to be effected over a wireless LAN connection.

A LANmonitor need not be explicitly logged in to the device. LANmonitor automatically transmits the login information to the device when scanning for new devices.

■ **Delete monitor**

This action allows registered SNMP agents to be removed from the monitor list. The command is specified together with the IP address and the port of the SNMP agent. All three values can be replaced with the wildcard *, in which case the device ascertains the values from the packets received from the SNMP agent.

Possible values:

□ <IP address|*>:<Port|*>

■ **Password required for SNMP read access**

This option allows you to specify that a password is required to read SNMP messages using an SNMP agent (e. g. LANmonitor). If this option is activated, the device password (or username:password) must be used as community.

Possible values:

□ Yes, No

Default:

□ No

■ **Comment 1**

Comment on this device. For display purposes only.

Possible values:

□ Max. 255 characters

Default:

□ Blank

■ **Comment 2**

Comment on this device. For display purposes only.

Possible values:

□ Max. 255 characters

Default:

□ Blank

■ **Comment 3**

Comment on this device. For display purposes only.

Possible values:

□ Max. 255 characters

Default:

□ Blank

■ **Comment 4**

Comment on this device. For display purposes only.

Possible values:

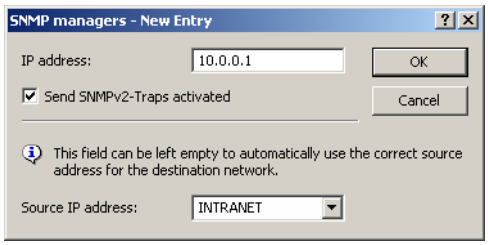
□ Max. 255 characters

Default:

□ Blank

I.1.2 The IP traps table

LANconfig: Log & Trace ▶ SNMP ▶ SNMP managers



WEBconfig: Setup ▶ SNMP ▶ IP traps

■ **Trap IP**

Enter the IP address of the computer where an SNMP manager is installed.

Possible values:

□ Valid IP address

Default:

□ Blank

■ **Loopback address**

This is where you can configure an optional sender address for use instead of that 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.

■ **Version**

Indicates SNMP version that should be used for the traps sent to this receiver.

Possible values:

□ SNMPv1, SNMPv2

Default:

□ SNMPv2

I.1.3 The monitor table

The monitor table shows all SNMP agents registered with the device.

■ **Remote site**

Name of the remote station from where an SNMP agent accesses the device.

■ **IP address**

IP address of the remote station from where an SNMP agent accesses the device.

■ **Loopback address**

Loopback address of the remote station from where an SNMP agent accesses the device.

■ **MAC address**

MAC address of the remote station from where an SNMP agent accesses the device.

■ **Port**

Port used by the remote device to access the local device with an SNMP agent.

■ **Timeout**

Timeout in minutes until the remote device is removed from the monitor table.

■ **VLAN ID**

ID of the VLAN used by the remote device to access the local device with an SNMP agent.

■ **Ethernet port**

Ethernet port used by the remote device to access the local device with an SNMP agent.

■ **LAN Ifc**

LAN Ifc used by the remote device to access the local device with an SNMP agent.

J Server functions

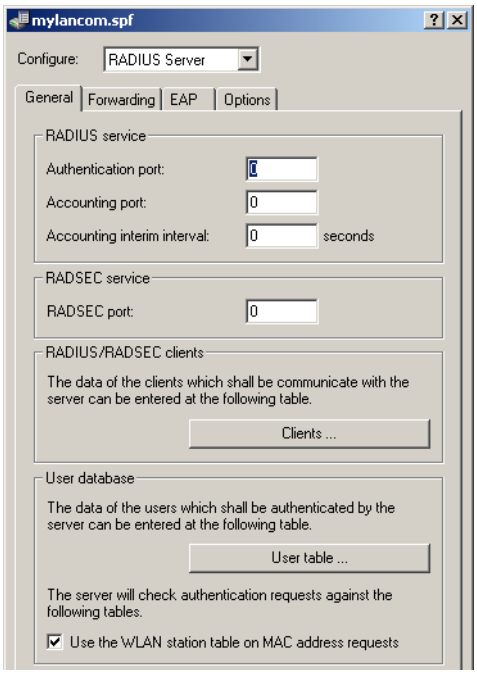
J.1 RADIUS server

New in LCOS 7.60:

- VLAN ID in the table for RADIUS users
- Masking of calling stations and/or called RADIUS clients (e.g. access points) in the RADIUS-user table

J.1.1 Global settings for the RADIUS server

LANconfig: RADIUS server ▶ General



WEBconfig: Setup ▶ RADIUS ▶ Server

- **Authentication port**

  Specify here the port used by the RADIUS client to communicate with the RADIUS server in the device. Port 1812 is normally used.

  Possible values:

  □ Max. 4 numbers

  Default:

  □ 0

  Special values:

  □ 0: Switches the RADIUS server off.

- **Accounting Interim Interval**

  Enter the value that the RADIUS server should output as "Accounting interim interval" after successful authentication. Provided the requesting device supports this attribute, this value determines the intervals (in seconds) at which an update of the accounting data is sent to the RADIUS server.

  Possible values:

  □ Max. 4 numbers

  Default:

  □ 0

  Special values:

  □ 0: Switches the use of this function off.

- **Accounting port**

  Enter the port used by the RADIUS server to receive accounting information. Port '1813' is normally used.

  Possible values:

□ Max. 4 numbers

Default:

□ 1813

Special values:

□ 0: Switches the use of this function off.

■ **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.

Possible values:

□ Max. 24 characters

Default:

□ Blank

■ **Empty realm**

This realm is used when the user name supplied does not contain a realm.

Possible values:

□ Max. 24 characters

Default:

□ Blank

■ **RADSEC port**

Enter the (TCP) port used by the server to accept accounting or authentication requests encrypted using RADSEC. Port 2083 is normally used.

Possible values:

□ Max. 4 numbers

Default:

□ 2083

Special values:

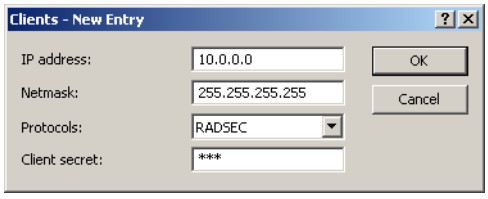
□ 0: Deactivates RADSEC in the RADIUS server.

J.1.2 Table of RADIUS clients

Clients that can communicate with the RADIUS server are entered in the clients table.

The managed Access Points created by a WLAN-Controller are not explicitly included in the list of RADIUS clients. It is not necessary to make manual entries here:

LANconfig: RADIUS server ▶ General ▶ RADIUS clients



WEBconfig: Setup ▶ RADIUS ▶ Server ▶ Clients

■ **IP network**

IP network (IP address range) of RADIUS clients for which the password defined in this entry applies.

Possible values:

□ Valid IP address

Default:

□ Blank

■ **IP netmask**

IP network mask of the RADIUS client.

Possible values:

□ Valid IP network mask

Default:

- □ Blank

■ **Protocols**

Protocol for communication between the internal RADIUS server and the clients.

Possible values:

- □ RADSEC, RADIUS, all

Default:

- □ RADIUS

■ **Secret**

Password required by the client for access to the internal RADIUS server.

Possible values:

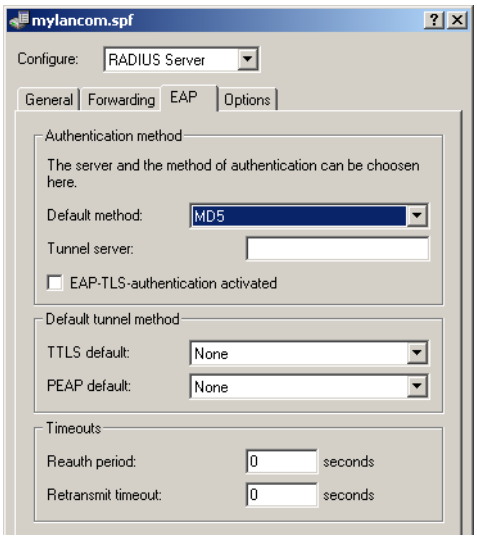
- □ Max. 32 characters

Default:

- □ Blank

J.1.3 EAP settings

LANconfig: RADIUS server ▶ EAP



WEBconfig: Setup ▶ RADIUS ▶ Server ▶ EAP

■ **PEAP default tunnel method**

Two authentication methods are negotiated when PEAP is used. A secure TLS tunnel is first negotiated using EAP. Then a second authentication method is negotiated in this tunnel. In each of these negotiating processes the server offers a method that the client can either accept (ACK) or reject (NAK). The the client rejects it, it sends the server a proposal for a method that it would like to use. If enabled in the server, the method proposed by the client is will be used. Otherwise the server breaks off negotiation.

This parameter is used to determine the method that the server offers to clients for authentication in the TLS tunnel. The value specified here can help to avoid rejected proposals and thus speed up the process of negotiation.

Possible values:

- □ None, MD5, GTC, MSCHAPv2

Default:

- □ MSCHAPv2

■ **Reauth period**

When the internal RADIUS server responds to a client request with an ACCEPT (negotiation of authentication method completed successfully), the RADIUS server can inform the authenticator how long it should wait (in seconds) before triggering repeat authentication of the client.

Possible values:

- □ Max. 10 numbers

Default:

□ 0

Special values:

□ 0: No timeout is sent to the RADIUS client.

The function is not supported by all RADIUS clients.

■ **Retransmit timeout**

When the internal RADIUS server responds to a client request with a CHALLENGE (negotiation of authentication method not yet completed), the RADIUS server can inform the authenticator how long it should wait (in seconds) for a response from the client before issuing a new CHALLENGE.

Possible values:

□ Max. 10 numbers.

Default:

□ 0

Special values:

□ 0: No timeout is sent to the RADIUS client.

The function is not supported by all RADIUS clients.

■ **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.

Possible values:

□ Yes, No

Default:

□ No

■ **TTLS default tunnel method**

Two authentication methods are negotiated when TTLS is used. A secure TLS tunnel is first negotiated using EAP. Then a second authentication method is negotiated in this tunnel. In each of these negotiating processes the server offers a method that the client can either accept (ACK) or reject (NAK). The the client rejects it, it sends the server a proposal for a method that it would like to use. If enabled in the server, the method proposed by the client is will be used. Otherwise the server breaks off negotiation.

This parameter is used to determine the method that the server offers to clients for authentication in the TLS tunnel. The value specified here can help to avoid rejected proposals and thus speed up the process of negotiation.

Possible values:

□ None, MD5, GTC, MSCHAPv2

Default:

□ MD5

■ **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.

Possible values:

□ Max. 24 characters

Default:

□ Blank

If the field remains empty the local RADIUS server assumes responsibility for the request. This means that the local RADIUS server performs internal and external EAP authentication.

■ **Default method**

This value specifies which method the RADIUS server should offer to the client outside of a possible TTLS/PEAP tunnel.

Possible values:

□ None, MD5, GTC, MSCHAPv2, TLS, TTLS, PEAP

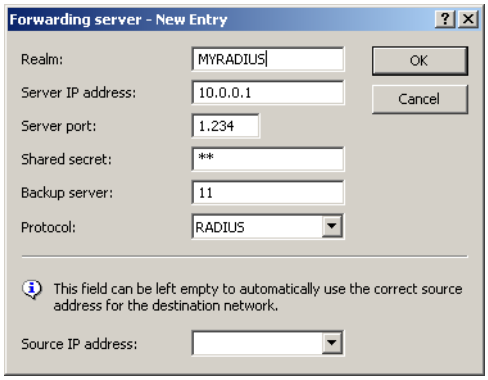
Default:

□ MD5

J.1.4 Table of forwarding servers

The table of forwarding servers contains up to 16 realms with the associated forwarding destinations.

LANconfig: RADIUS server ▶ Forwarding ▶ Forwarding server



WEBconfig: Setup ▶ RADIUS ▶ Server ▶ Forward servers

■ **Realm**

Character string identifying the forwarding destination.

Possible values:

□ Max. 24 characters

Default:

□ Blank

■ **IP address**

IP address of the RADIUS server to which the request is to be forwarded.

Possible values:

□ Valid IP address

Default:

□ Blank

■ **Port**

Open port for communications with the forwarding server.

Possible values:

□ Max. 4 numbers

Default:

□ 0

■ **Secret**

Password required for accessing the forwarding server.

Possible values:

□ Max. 32 characters

Default:

□ Blank

■ **Loopback address**

This is where you can configure an optional sender address for use instead of that 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.

■ **Protocol**

Protocol for communication between the internal RADIUS server and the forwarding server.

Possible values:

- □ RADSEC, RADIUS, all

Default:

- □ RADIUS

■ **Backup**

Alternative forwarding server in case the first forwarding server is not available.

Possible values:

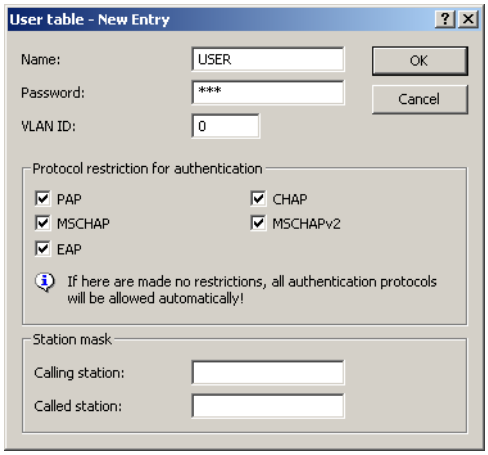
- □ Max. 24 characters

Default:

- □ Blank

J.1.5 Table of RADIUS users

LANconfig: RADIUS server ▶ General ▶ User table



WEBconfig: Setup ▶ RADIUS ▶ Server ▶ Clients

■ **User name**

User name.

Possible values:

- □ Max. 48 characters

Default:

- □ Blank

■ **Calling Station ID Mask**

This mask is used to restrict the validity of the entry to certain IDs that are communicated by the calling station (wireless LAN client). When authenticating via 802.1x the calling Access Point's MAC address is transmitted in ASCII format (capital letters only), with a hyphen separating pairs of characters (for example "00-10-A4-23-19-C0")

Possible values:

- □ Max. 48 characters

Default:

- □ Blank

Special characters:

- □ The wildcard * can be used to include whole groups of IDs and define them as mask.

■ **Called Station ID Mask**

This mask is used to restrict the validity of the entry to certain IDs that are communicated by the called station (access point's BSSID and SSID). When authenticating via 802.1x the called Access Point's MAC addresses (BSSID) are transmitted in ASCII format (capital letters only), with a hyphen separating pairs of characters. The SSID is appended using a colon as separator (for example "00-10-A4-23-19-C0:AP1")

Possible values:

- □ Max. 48 characters

Default:

- □ Blank

Special values:

- □ The wildcard * can be used to include whole groups of IDs and define them as mask. The mask "*:OFFICE1", for example, defines an entry that applies to a client in a radio cell with the name "OFFICE1" irrespective of the access point that the client uses to log in. This allows the client to switch (roam) from one access point to the next while always using the same authentication data.

■ **Limit auth. methods**

This option allows you to place limitations on the authentication methods permitted for the user.

Possible values:

- □ PAP, CHAP, MS-CHAP, MS-CHAPv2, all

Default:

- □ Blank

■ **Password**

User password.

Possible values:

- □ Max. 32 characters

Default:

- □ Blank

■ **VLAN ID**

This option allows a certain VLAN ID to be assigned to the user on successful authorization.

Possible values:

- □ 0 to 4094

Default:

- □ 0

Special values:

- □ 0: This is used if the SSID has been globally assigned with a VLAN ID.
- □ All other values: The user-specific VLAN ID overwrites a globally defined VLAN ID or SSID.

J.2 Automatic IP address management 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)

J.2.1 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.

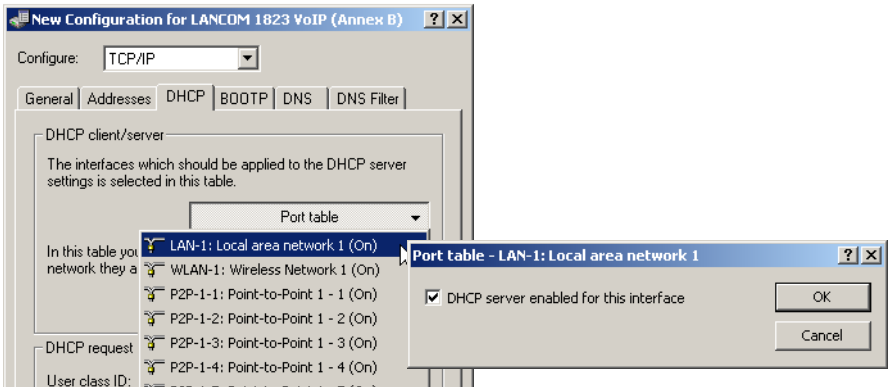
BOOTP

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.

J.2.2 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.



Configuring DHCP networks

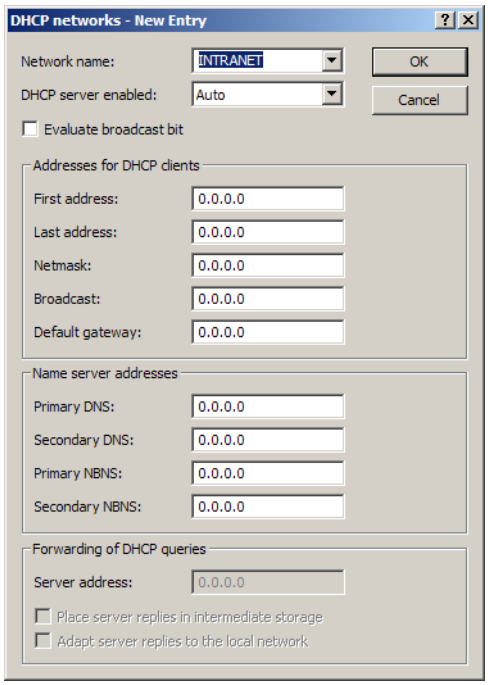
The appropriate DHCP settings can be specified separately for any IP network defined in the device. You can find the parameters for defining DHCP networks in LANconfig in the configuration area "TCP/IP" on the "DHCP" tab.

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.



■ 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.

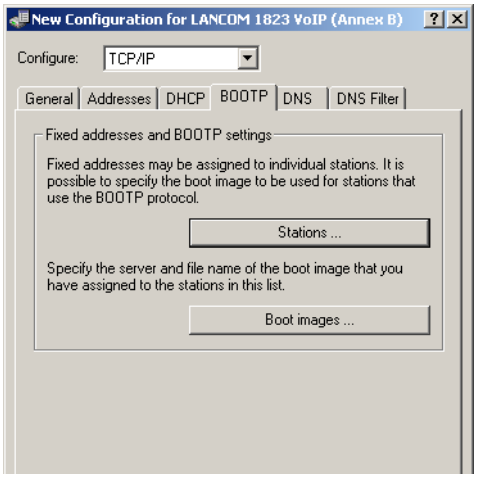
- **Assigning DNS and NBNS servers**

IP address of the DNS and NBNS name servers to which DNS and NBNS requests should be forwarded.

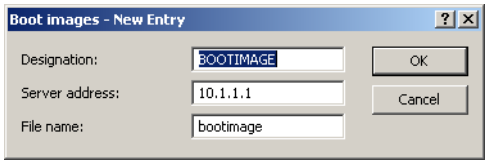
If no server is defined in the relevant fields, the router will forward its own IP network address as DNS or NBNS address if the DNS server has been enabled for the network in question. If the DNS server is not active for this network, then the IP address in the global TCP/IP settings is communicated as the DNS server.

Configuring the assignment of fixed IP addresses to specific clients

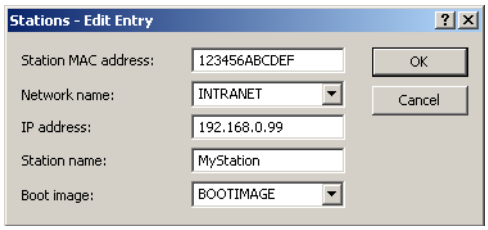
You can find the parameters for configuring BOOTP in LANconfig in the configuration area "TCP/IP" on the "BOOTP" tab.



Optionally: You can define a boot image in the list of boot images that you wish to assign to a client.



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.



J.2.3 Configuring DHCP parameters with telnet or WEBconfig

General DHCP settings

■ **User class identifier**

□ Path: Setup/DHCP

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.

Possible values:

□ Max. 63 characters

Default:

□ Blank

■ **Default lease minutes**

□ Path: Setup/DHCP

When a client requests an address without asking for a specific lease, the address will be assigned the value set here as lease.

Possible values:

□ Max. 5 characters

Default:

□ 500

■ **Max. lease minutes**

□ Path: Setup/DHCP

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.

Possible values:

□ Max. 5 characters

Default:

□ 6000

Alias list

The alias list defines the names for the boot images that are used to reference the images in the hosts table.

□ Path: Setup/DHCP/Alias list

■ **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.

Possible values:

□ Max. 16 characters

Default:

□ Blank

■ **Image server**

Enter the IP address of the server that provides the boot image.

Possible values:

□ Valid IP address

Default:

□ 0.0.0.0

■ **Image file**

Enter the name of the file on the server containing the boot image.

Possible values:

□ Max. 60 characters

Default:

□ Blank

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.

□ Path: Setup/DHCP/DHCP table

■ **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.

- □ Path: Setup/DHCP

■ **MAC address**

Enter the MAC address of the workstation to which an IP address is to be assigned.

Possible values:

- □ Valid MAC address

Default:

- □ Blank

■ **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.

Possible values:

- □ Max. 16 characters

Default:

- □ Blank

Special values:

- □ Blank: The IP address will be assigned if the IP address defined in this field belongs to the range of addresses for the IP network where the requesting client is located.

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.

Possible values:

- □ Valid IP address

Default:

- □ 0.0.0.0

■ **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..

Possible values:

- □ Max. 30 characters

Default:

- □ Blank

■ **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.

Possible values:

□ Max. 16 characters

Default:

□ Blank

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.

□ Path: Setup/DHCP/Network list

■ **Network name**

The name of the network which the DHCP server settings apply to.

Possible values:

□ Name of a defined IP network, max. 16 characters

Default:

□ Blank

■ **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.

Possible values:

□ Yes, No

Default:

□ No

■ **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).

Possible values:

□ Valid IP address

Default:

□ 0.0.0.0

■ **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).

Possible values:

□ Valid IP address

Default:

□ 0.0.0.0

■ **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.

Possible values:

□ Valid IP network mask

Default:

□ 0.0.0.0

■ **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.

Possible values:

□ Valid IP address

Default:

□ 0.0.0.0

Special values:

□ 0.0.0.0: broadcast address is determined automatically.

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.

Possible values:

□ Valid IP address

Default:

□ 0.0.0.0

Special values:

□ 0.0.0.0: the IP address of the LANCOM in this network communicated as the gateway.

■ **DNS default**

IP address of the DNS name server for the forwarding of DNS requests.

Possible values:

□ Valid IP address

Default:

□ 0.0.0.0

Special values:

- □ 0.0.0.0: The IP address of the LANCOM in this network is communicated as the DNS server if the DNS server is activated for this network. 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.

■ **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.

Possible values:

- □ Valid IP address

Default:

- □ 0.0.0.0

Special values:

- □ 0.0.0.0: The IP address from the global TCP/IP settings is communicated as the backup DNS server.

■ **NBNS default**

IP address of the NetBIOS name server for the forwarding of NetBIOS requests.

Possible values:

- □ Valid IP address

Default:

- □ 0.0.0.0

Special values:

- □ 0.0.0.0: The IP address of the LANCOM in this network is communicated as the NBNS server if the NetBIOS proxy is activated for this network. If the NetBIOS proxy is not active for this network, then the IP address in the global TCP/IP settings is communicated as the NBNS server.

■ **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.

Possible values:

- □ Valid IP address

Default:

- □ 0.0.0.0

Special values:

- □ 0.0.0.0: The IP address from the global TCP/IP settings is communicated as the backup NBNS server.

■ **Server address**

This is where the IP address for the superordinate DHCP server is entered when the mode 'Relay requests' is selected.

Possible values:

- □ Valid IP address

Default:

- □ 0.0.0.0

■ **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.

Possible values:

- □ Yes, No

Default:

- □ No

■ **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.

Possible values:

- □ Yes, No

Default:

- □ No

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.

Possible values:

- □ Select from the list of logical devices in this device, e. g. LAN-1, WLAN-1, P2P-1-1 etc.

Default:

- □ N/A

■ **Enable DHCP**

Enables or disables the DHCP server for the selected logical interface.

Possible values:

- □ Yes, No

Default:

- □ Yes

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.

- □ Path: 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 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).

Possible values:

- □ Max. 3 characters

Default:

- □ Blank

■ **Network name**

Name of the IP network where this DHCP option is to be used.

Possible values:

- □ Selection from the list of defined IP networks (max. 16 characters).

Default:

- □ Blank

Special values:

- □ Blank: If no network name is specified the DHCP option defined in this entry will be used in all IP networks.

■ **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.

Possible values:

□ String of max. 128 characters

Default:

□ Blank

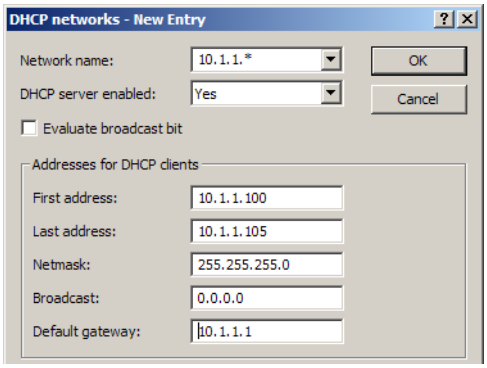
The maximum possible length value depends on the selected option number. RFC 2132 lists the maximum length allowed for each option.

10.2.4 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:



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.

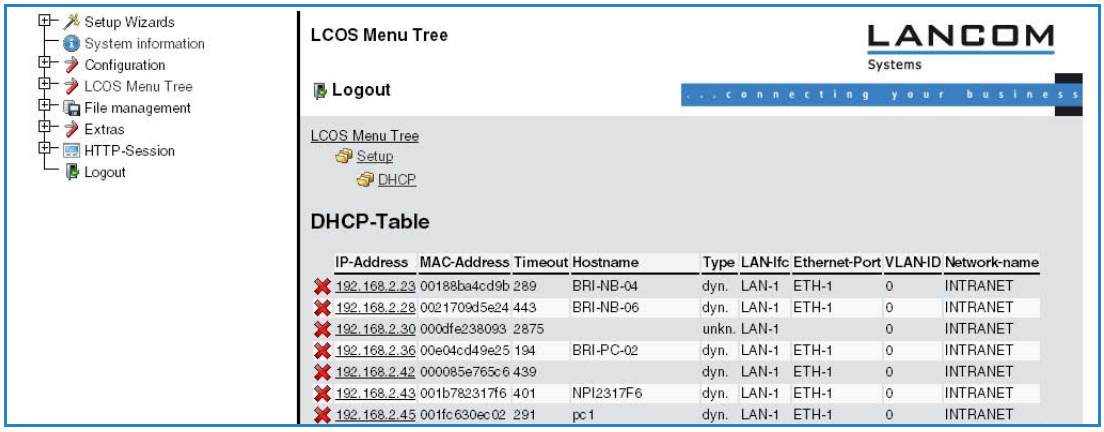
J.2.5 Configuring clients

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.

J.2.6 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.



J.3 Other changes

J.4 Access lists with routing tags

J.4.1 Introduction

LANCOM devices use various access lists to restrict access for certain functions to a specific group of workstations or networks. These access lists are used for the following modules:

- TCP/IP: Configuration access to the device via TCP/IP
- LANCAPI: Use of the LANCAPI function
- Printer: Use of the printer attached to the device

Authorization for a range of workstations is specified in the relevant access list using an IP address and a network mask.

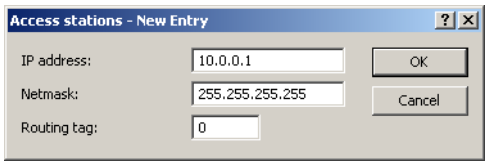
An optional routing tag can also be specified that restricts access for the function to those workstations in the corresponding IP network (please refer to Advanced Routing and Forwarding). Specifying routing tags in the access list can be useful when, for example, several IP networks exist in a network structure with the same IP address range but which are separated by routing tables.

J.4.2 Configuring the access lists

LANconfig: Management ▶ Admin ▶ Access stations

LANconfig: CAPI ▶ Options ▶ Access list

LANconfig: Printer ▶ General ▶ Access list



WEBconfig: Setup ▶ TCP-IP ▶ Access list

WEBconfig: Setup ▶ LANCAPI ▶ Access list

WEBconfig: Setup ▶ Printer ▶ Access list

- **IP address**

  Enter the IP of the workstation that is to be given access to the function.

  Possible values:

  - Valid IP address

  Default:

  - 0.0.0.0

■ **IP netmask**

Enter the IP mask of the network that is to be given access to the function. Enter 255.255.255.255 here if you wish to authorize just a single workstation with the specified IP address. If you wish to authorize a whole IP network, enter the corresponding netmask.

Possible values:

□ Valid IP network mask

Default:

□ 0.0.0.0

■ **Routing tag**

Enter the routing tag of the network that is to be given access to the function.

Possible values:

□ 0 to 65535

Default:

□ 0

Special values:

□ 0: Allows access to this function for all routing tags; access checking is performed on the IP address only.