1 Configuration and management

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

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

1.1 Configuration tools and approaches

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

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

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

What is the difference between these three possibilities?

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

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

1.2 Configuration software

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

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

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

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

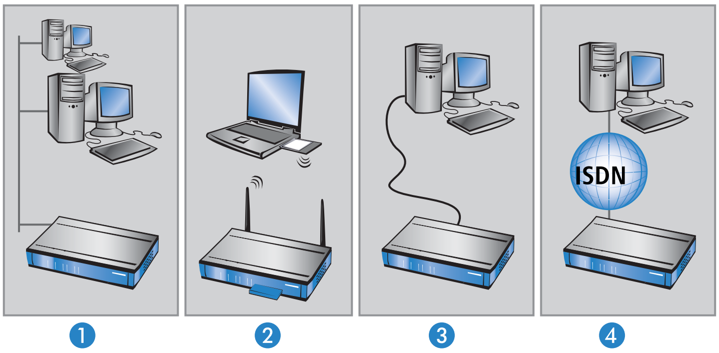
Please note that all procedures access the same configuration data. For example, if you change the settings in LANconfig, this will also have a direct effect on the values under WEBconfig and Telnet.

1.3 Searching and configuring devices

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

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

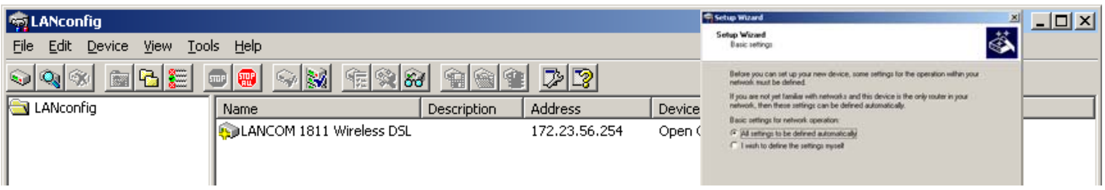
- Via the local network (LAN) ➊.
- Via the wireless network (WLAN) ➋, if the WLAN encryption (e.g. WEP) of a device with a wireless interface and in the configuration PC has been adjusted correctly and/or has been deactivated.
- Via the serial configuration interface ➌.
- Via a ISDN connection ➍



1.4 Configuration with LANconfig

1.4.1 Starting LANconfig

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



Name	Description	Address	Device
LANCOM 1811 Wireless DSL		172.23.56.254	Open (

Setup Wizard
Basic settings

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

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

Basic settings for network operation:

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

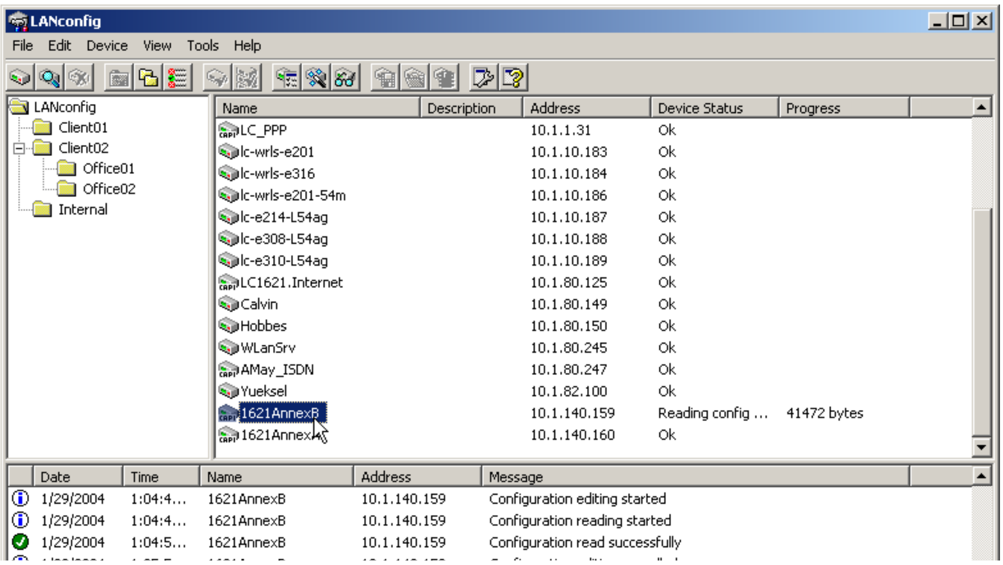
If the firewall is activated the LANconfig might not be able to find the new device in the LAN. In this occasion deactivate the firewill whilst the configuration.

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

Find new devices

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

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



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

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

The expanded range of functions for professionals

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

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

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

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

The integrated Help function

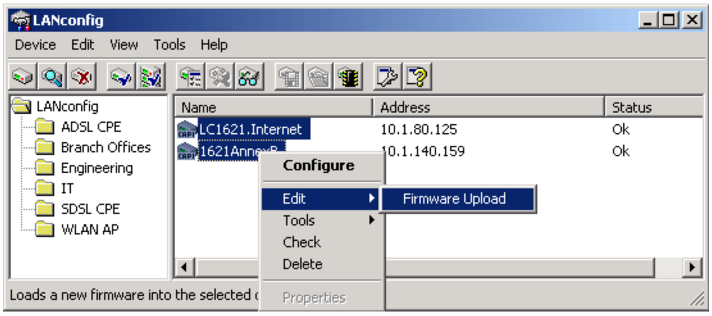
The remainder of the program's operation is self-explanatory or you can use the online help. You can click on the 'Help' button top right in any window or right-click on an unclear term at any time to call up context-sensitive help.

Management of multiple devices

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

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

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

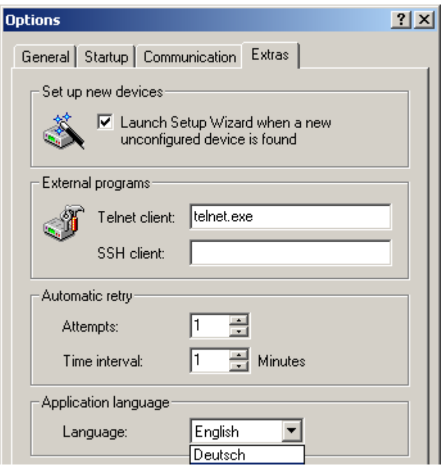


Name	Address	Status
LC1621.Internet	10.1.80.125	Ok
1621AnnexB	10.1.140.159	Ok

Loads a new firmware into the selected (

1.4.2 Switch graphical user interface language

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



Set up new devices

☑ Launch Setup Wizard when a new unconfigured device is found

External programs

Telnet client: telnet.exe

SSH client:

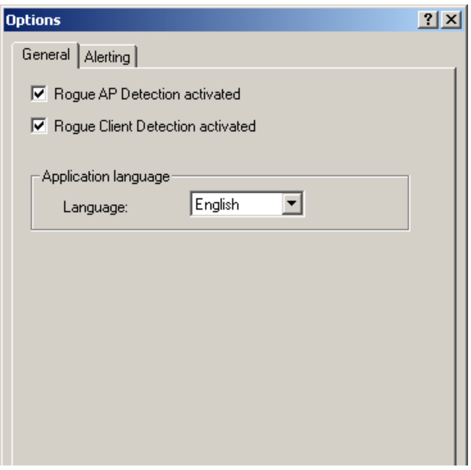
Automatic retry

Attempts: 1

Time interval: 1 Minutes

Application language

Language: English



☑ Rogue AP Detection activated

☑ Rogue Client Detection activated

Application language

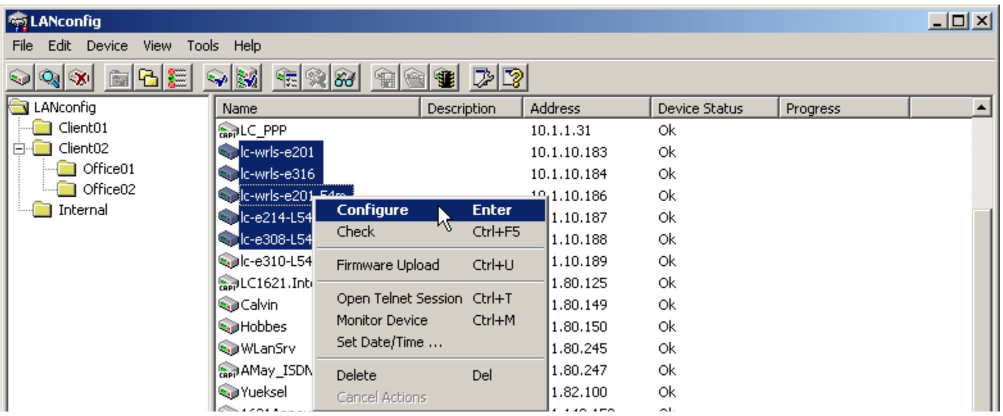
Language: English

LANconfig: Tools ▶ Options ▶ Extras

LANmonitor and WLANmonitor: Tools ▶ Options ▶ General

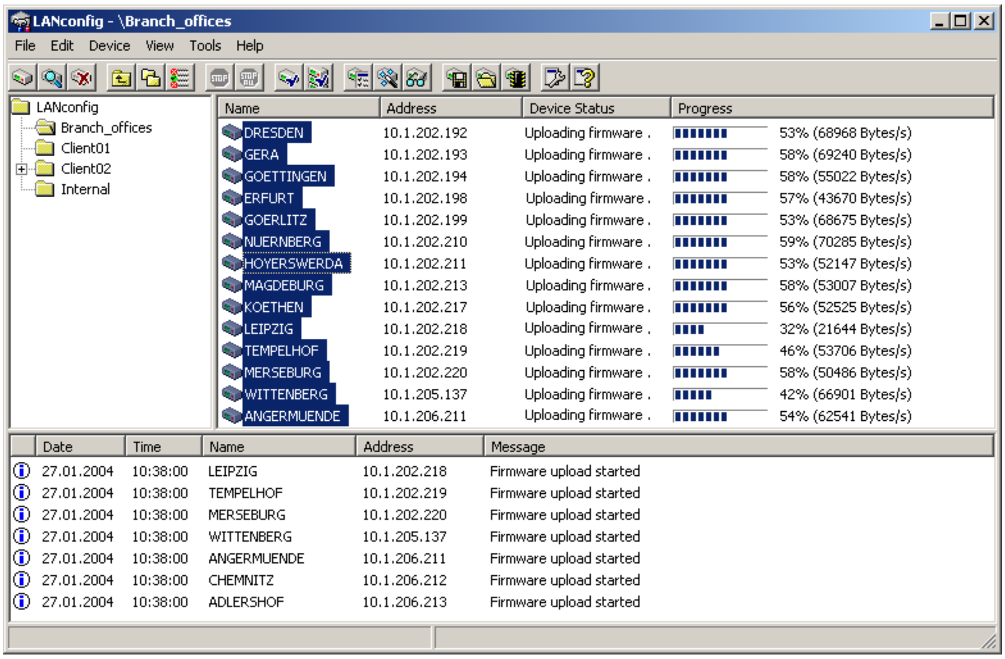
1.4.3 Project management with LANconfig

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



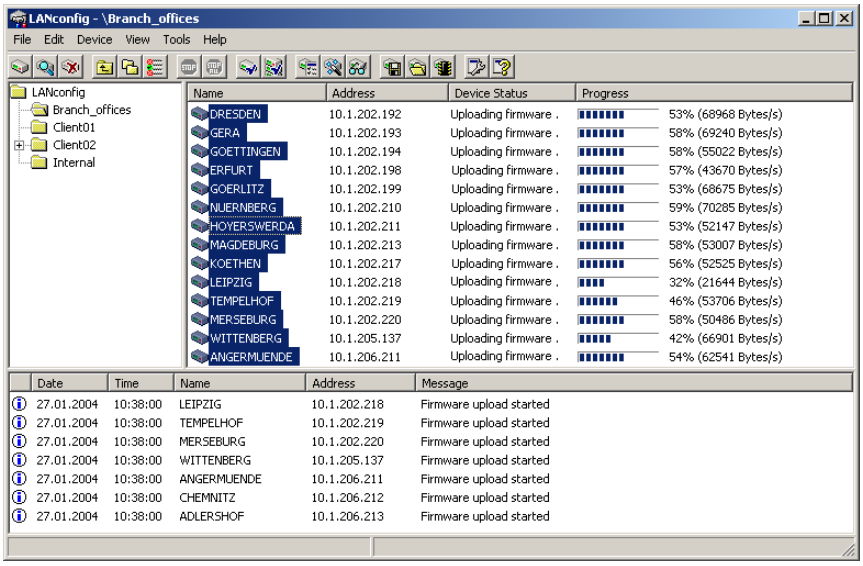
Name	Description	Address	Device Status	Progress
LC_PPP		10.1.1.31	Ok	
lc-wrls-e201		10.1.10.183	Ok	
lc-wrls-e316		10.1.10.184	Ok	
lc-wrls-e201-54		1.10.186	Ok	
lc-e214-L54		1.10.187	Ok	
lc-e308-L54		1.10.188	Ok	
lc-e310-L54		1.10.189	Ok	
LC1621.Int		1.80.125	Ok	
Calvin		1.80.149	Ok	
Hobbes		1.80.150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

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



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

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


LANconfig - \Branch_offices

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

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

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

> ! When setting the time, please observe the functions of the LANCOM as NTP client and NTP server ('Time server for the local net' → page 672).

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

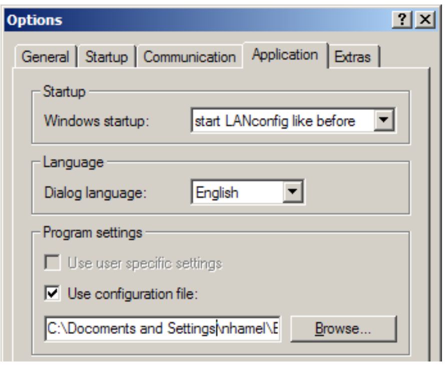
1.4.4 User-specific settings for LANconfig

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

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

- By selecting the user directory, users can save their personal settings even if they don't have a write authorization for the program directory.

- Selecting an alternative storage location can be used, for example, to transfer program settings to any other LANconfig installation, or to save the program settings to a central location in the network for use by multiple users.



Options

General | Startup | Communication | Application | Extras

Startup

Windows startup: start LANconfig like before

Language

Dialog language: English

Program settings

□ Use user specific settings

☑ Use configuration file:

C:\Docoments and Settings\nhamel\E

Browse...

LANconfig: **Options ▶ Application**

- **Use user-specific settings**

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

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

  □ Possible values: On/off

  □ Default: Off

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

- **Use configuration file**

  The activates the usage of the lanconf.ini from the given directory.

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

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

  □ Default: Off

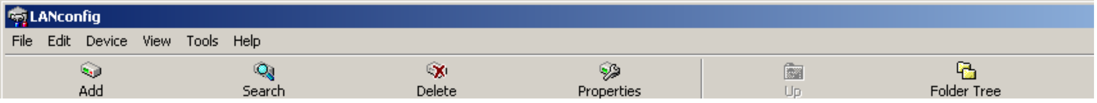
The file you select must be a valid LANconfig settings file.

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

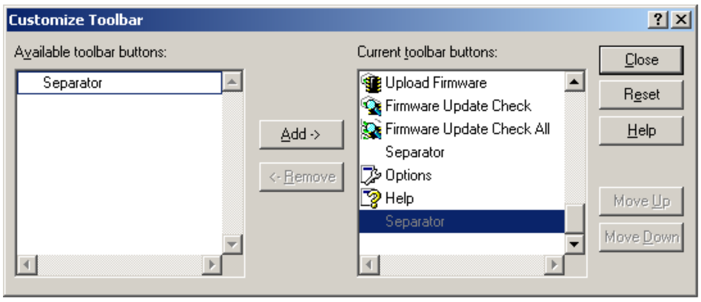
1.4.5 Customizing the toolbar

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

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



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



Available toolbar buttons:
- Separator

Current toolbar buttons:
- Upload Firmware
- Firmware Update Check
- Firmware Update Check All
- Separator
- Options
- Help
- Separator

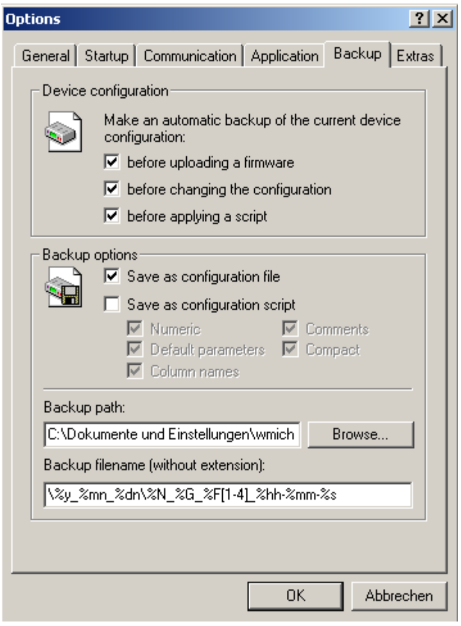
- Reset: Resets the settings for the toolbar to the default values.

1.4.6 Automatic backup of configuration with LANconfig

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

Select the following options here:

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



Device configuration

Make an automatic backup of the current device configuration:

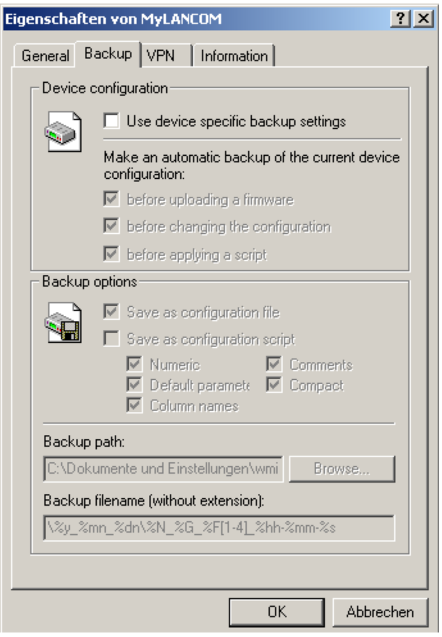
☑ before uploading a firmware
☑ before changing the configuration
☑ before applying a script

Backup options

☑ Save as configuration file
☐ Save as configuration script
☑ Numeric ☑ Comments
☑ Default parameters ☑ Compact
☑ Column names

Backup path: C:\Dokumente und Einstellungen\wmich

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



Device configuration

☐ Use device specific backup settings

Make an automatic backup of the current device configuration:

☑ before uploading a firmware
☑ before changing the configuration
☑ before applying a script

Backup options

☑ Save as configuration file
☐ Save as configuration script
☑ Numeric ☑ Comments
☑ Default paramete ☑ Compact
☑ Column names

Backup path: C:\Dokumente und Einstellungen\wmi

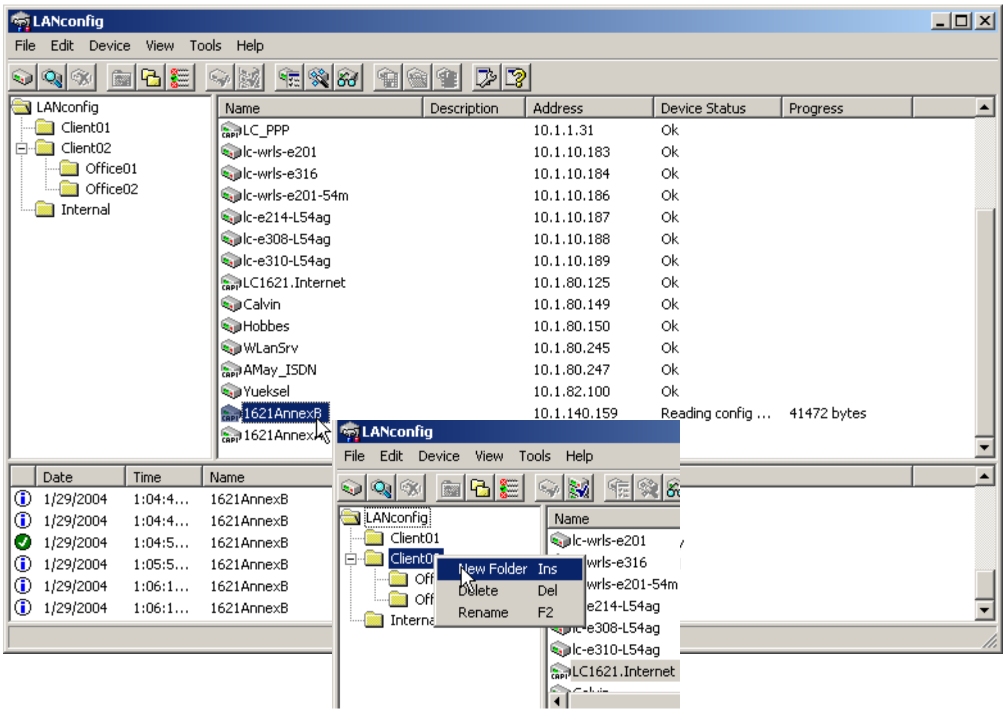
Backup filename (without extension): \%y_%mn_%dn\%N_%G_%F[1-4]_%hh-%mm-%s

1.4.7 Directory structure

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

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

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



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

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

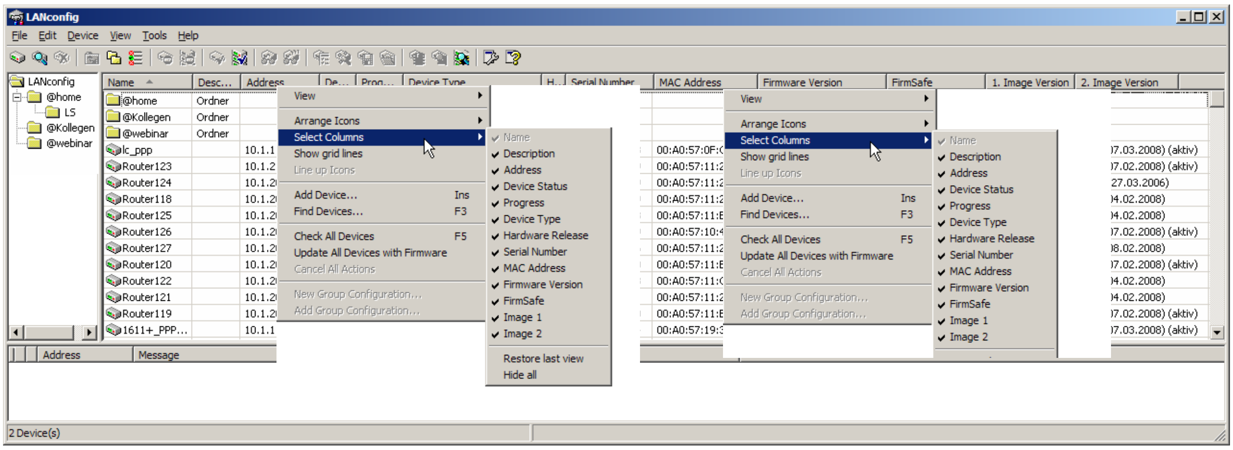
The directory structure in the left margin of the LANconfig window can be switched on and off with the **F6** function key or by using the menu **View** ▶ **Folder Tree**.

1.4.8 Better overview in LANconfig with more columns

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

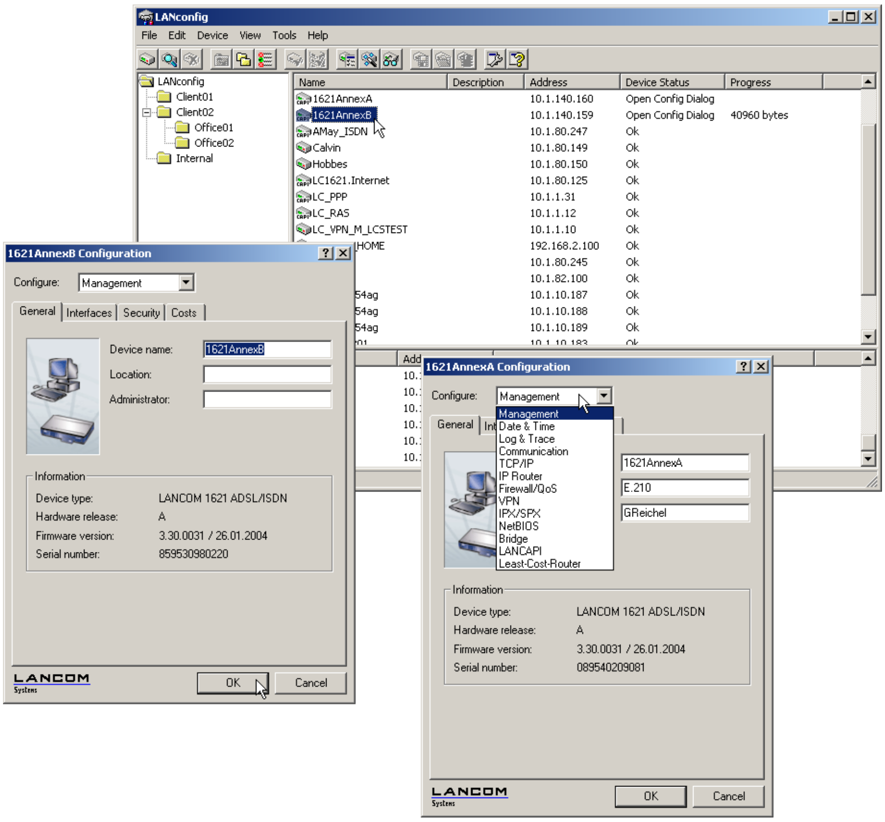
The following details can be displayed in the various columns:

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



1.4.9 Multithreading

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



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

1621AnnexB Configuration:

Device name: 1621AnnexB
Location:
Administrator:

Device type: LANCOM 1621 ADSL/ISDN
Hardware release: A
Firmware version: 3.30.0031 / 26.01.2004
Serial number: 859530980220

1621AnnexA Configuration:

1621AnnexA
E.210
GReichel

Device type: LANCOM 1621 ADSL/ISDN
Hardware release: A
Firmware version: 3.30.0031 / 26.01.2004
Serial number: 089540209081

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

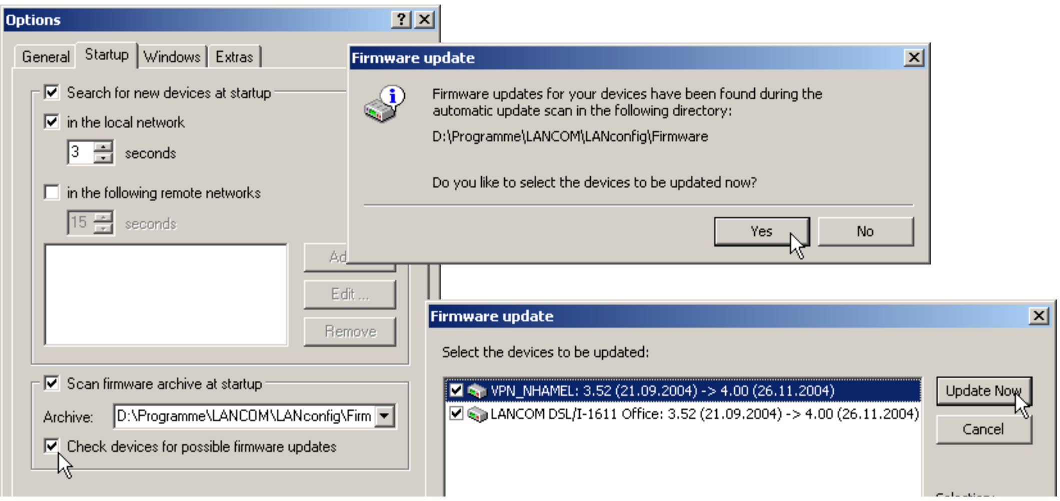
Multithreading allows changes to both the internal configurations of the available devices and to the configuration files. Each configuration is written separately to the file and to the device when the dialog is closed.

1.4.10 Manual and automatic searches for firmware updates

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

Automatic search for firmware updates

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



Options

☑ Search for new devices at startup
☑ in the local network
3 seconds
□ in the following remote networks
15 seconds
☑ Scan firmware archive at startup
Archive: D:\Programme\LANCOM\LANconfig\Firm
☑ Check devices for possible firmware updates

Firmware update

Firmware updates for your devices have been found during the automatic update scan in the following directory:
D:\Programme\LANCOM\LANconfig\Firmware

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

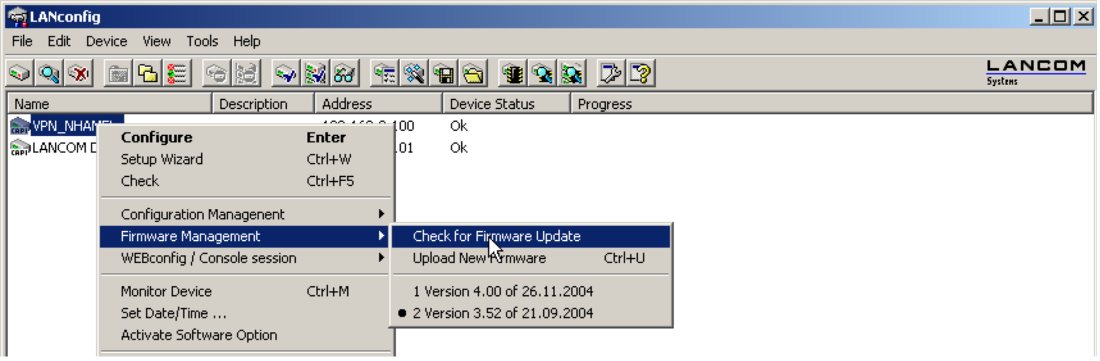
Firmware update

Select the devices to be updated:

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

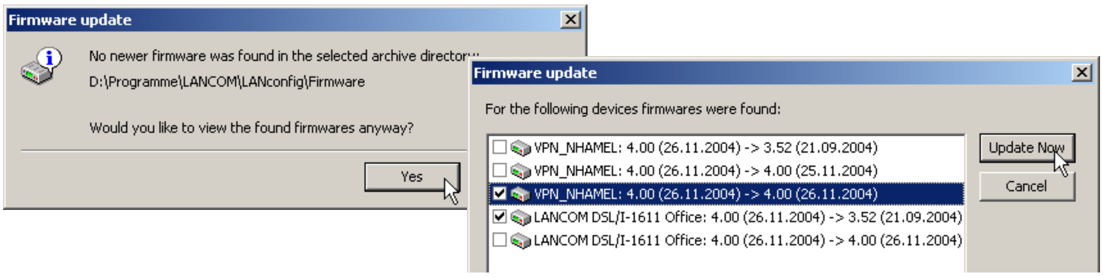
Manual search for firmware updates

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



View a full list of all firmware versions

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



Firmware update

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

Would you like to view the found firmwares anyway?

Firmware update

For the following devices firmwares were found:

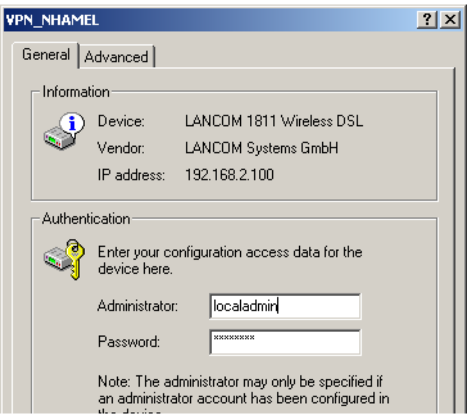
□ VPN_NHAMEL: 4.00 (26.11.2004) -> 3.52 (21.09.2004)
□ VPN_NHAMEL: 4.00 (26.11.2004) -> 4.00 (25.11.2004)
☑ VPN_NHAMEL: 4.00 (26.11.2004) -> 4.00 (26.11.2004)
☑ LANCOM DSL/I-1611 Office: 4.00 (26.11.2004) -> 3.52 (21.09.2004)
□ LANCOM DSL/I-1611 Office: 4.00 (26.11.2004) -> 4.00 (26.11.2004)

1.4.11 Password protection for SNMP read-only access.

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

LANmonitor

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



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

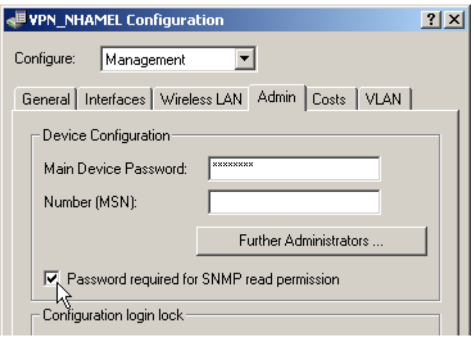
Enter your configuration access data for the device here.

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

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

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

- A supervisor has full access to the information in LANmonitor and can execute actions such as closing a connection, among others.
- A local administrator also has full access to the information in LANmonitor and can execute actions such as closing a connection, among others.
- A user with read-only rights can view the information in LANmonitor but cannot take any actions such as closing a connection.
- A user without rights has no SNMP access to the device's information.



Configure: Management

Main Device Password: ********
Number (MSN):

☑ Password required for SNMP read permission

LANconfig: Management ▶ General

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

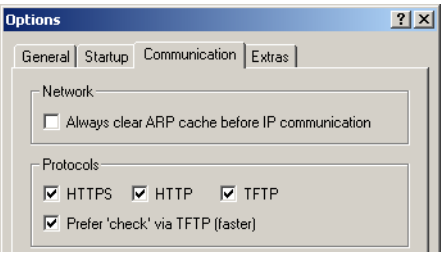
1.4.12 Device-specific settings for communications protocols

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

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

Configuration of the global communication settings

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



☐ Always clear ARP cache before IP communication

☑ HTTPS ☑ HTTP ☑ TFTP

☑ Prefer 'check' via TFTP (faster)

LANconfig: Tools ▶ Options ▶ Communication

- **HTTPS, HTTP, TFPT**

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

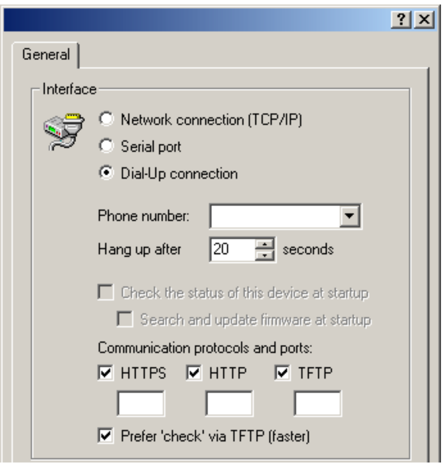
- **Prefer checks via TFTP**

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

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

Configuration of the specific communication settings

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



General

Interface

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

Phone number:
Hang up after 20 seconds

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

Communication protocols and ports:
☑ HTTPS ☑ HTTP ☑ TFTP

☑ Prefer 'check' via TFTP (faster)

- **HTTPS, HTTP, TFPT**

  Select the communications protocols as described in the global settings:

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

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

- **Prefer checks via TFTP**

  Preferred checking via TFTP as described in the global settings.

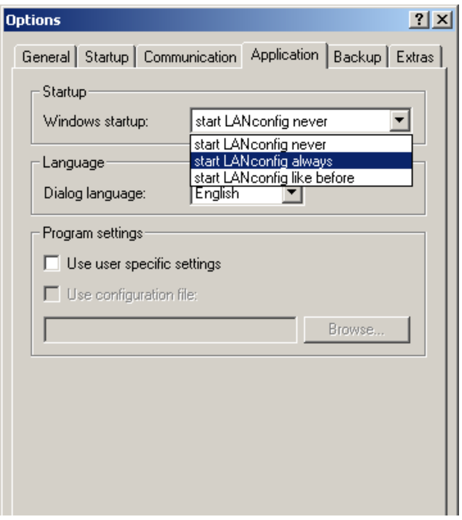
> For all specific communications settings, the global settings are considered to be superordinate. A protocol can therefore only be used for operating a device when it is also activated in the global settings.

1.4.13 LANconfig behavior at Windows startup

LANconfig can be automatically started when the operating system starts.

Configuring the behavior of LANconfig at startup

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



Startup

Windows startup: start LANconfig never

start LANconfig never
start LANconfig always
start LANconfig like before

Language

Dialog language: English

Program settings

□ Use user specific settings

□ Use configuration file:

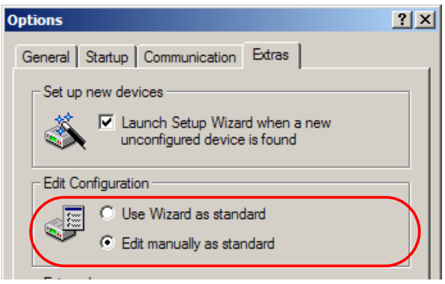
LANconfig: Options ▶ Extras ▶ Application

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

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

1.4.14 Choice of Wizard or configuration dialog

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



Set up new devices

☑ Launch Setup Wizard when a new unconfigured device is found

Edit Configuration

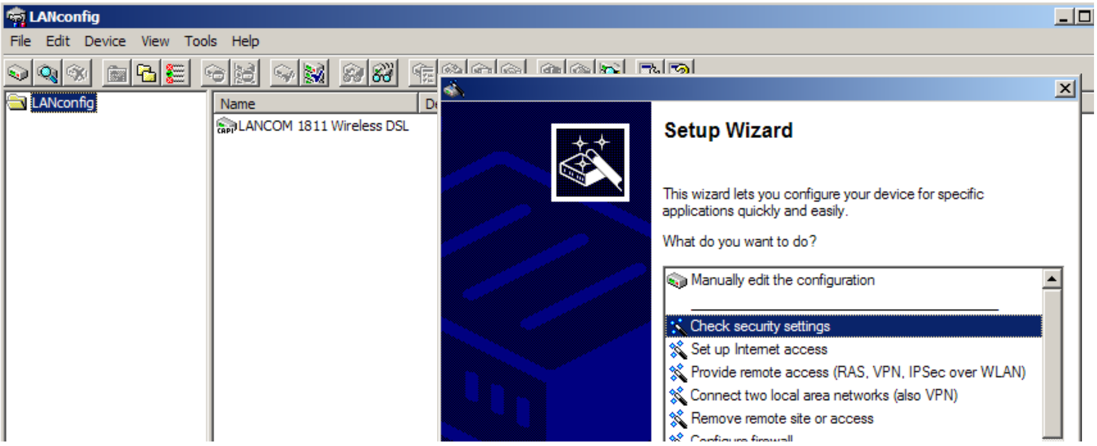
○ Use Wizard as standard

● Edit manually as standard

The standard behavior of LANconfig can be set under:

LANconfig: Tools ▶ Options ▶ Extras

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



LANconfig
File Edit Device View Tools Help
LANconfig
Name
LANCOM 1811 Wireless DSL

Setup Wizard

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

What do you want to do?

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

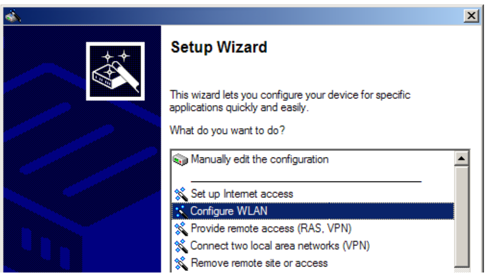
Edit manually as standard: Double-clicking on a device entry in LANconfig will open up a dialog for editing the configuration manually.

1.4.15 WLAN configuration with the wizards in LANconfig

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

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

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



Setup Wizard

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

What do you want to do?

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

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

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

Country settings

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

WLAN module operation

The WLAN modules can be operated in various operating modes:

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

  For further information please refer to section → Client Mode.

Physical WLAN settings

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

Logical WLAN networks

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

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

Point-to-point settings

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

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

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

1.5 Group configuration with LANconfig

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

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

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

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

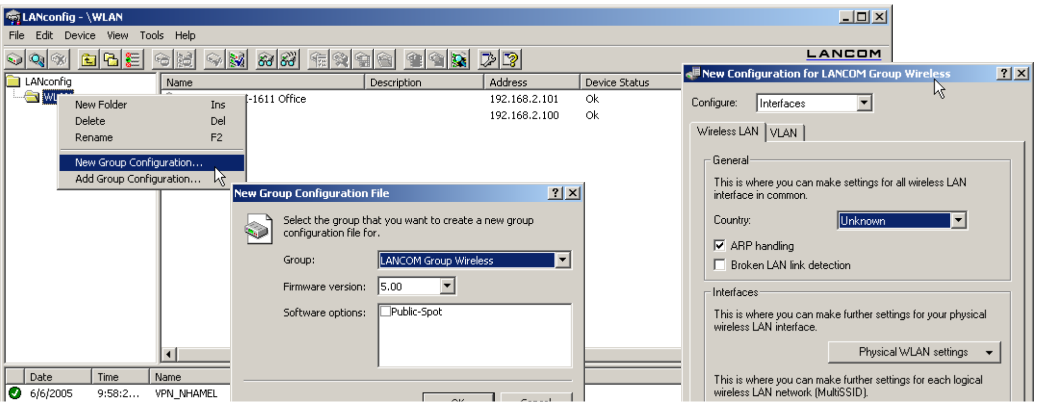
1.5.1 Create a group configuration

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

Group configuration with a new partial configuration file

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

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



192.168.2.101 Ok
192.168.2.100 Ok

6/6/2005 9:58:2... VPN_NHAMEL

New Group Configuration File

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

Group: LANCOM Group Wireless

Firmware version: 5.00

Software options: □ Public-Spot

New Configuration for LANCOM Group Wireless

Configure: Interfaces

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

Country: Unknown

☑ ARP handling

□ Broken LAN link detection

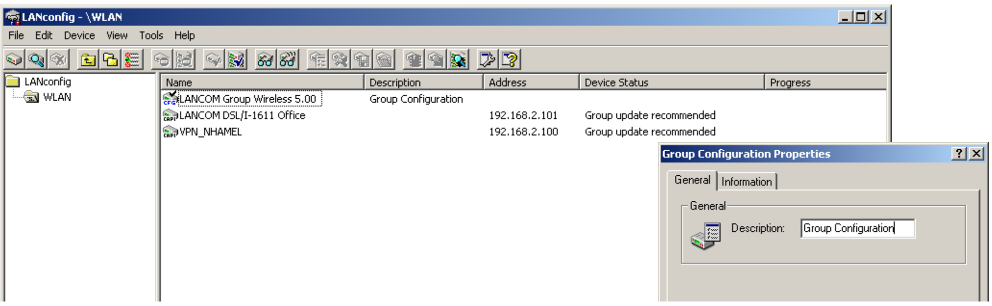
This is where you can make further settings for your physical wireless LAN interface.

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

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

> ! The group configuration then saves all parameters to a partial configuration file. Those parameters which were not changed are also set to the standard values. Use the scripting function ('Scripting' → page 91) to read out non-standard settings from a device and transfer them to other devices, if required.

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



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

Group Configuration Properties

Description: Group Configuration

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

Use an existing partial configuration file

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

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

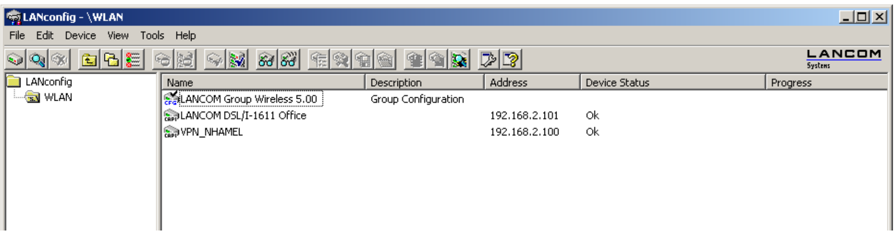
② In the subsequent dialog, select the existing partial configuration file to create a link to this file in the folder.

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

1.5.2 Update device configurations

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

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



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

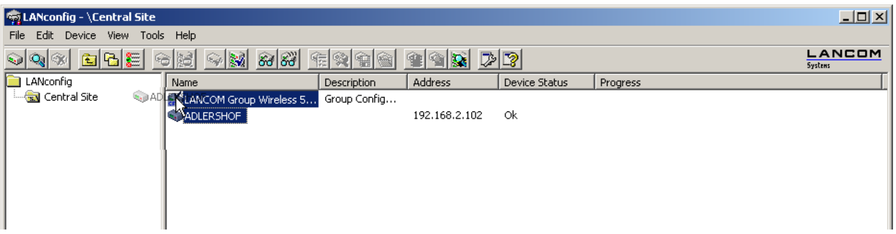
It is also possible to use the partial configuration for a device as a group configuration. Simply drag the device entry onto the group configuration entry.

1.5.3 Update group configurations

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

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

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

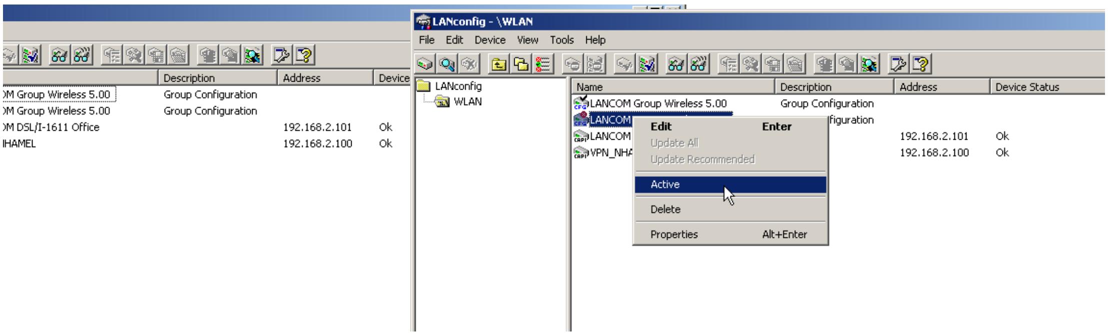


Name	Description	Address	Device Status	Progress
LANCOM Group Wireless 5...	Group Config...			
ADLERSHOF		192.168.2.102	Ok	

1.5.4 Using multiple group configurations

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

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



Name	Description	Address	Device
OM Group Wireless 5.00	Group Configuration		
OM Group Wireless 5.00	Group Configuration		
OM DSL/I-1611 Office		192.168.2.101	Ok
IHAMEL		192.168.2.100	Ok

Name	Description	Address	Device Status
LANCOM Group Wireless 5.00	Group Configuration		
LANCOM	figuration		
LANCOM		192.168.2.101	Ok
VPN_NHA		192.168.2.100	Ok

1.5.5 Transferring device configurations to similar models

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

- If the destination device has the appropriate parameter, and the value lies within the possible range, the value of the source device is taken.
- If the value of a parameter available on the destination device is not supported, the default value is used. Example:

- □ The source device has four Ethernet interfaces.
- □ The destination device only has two Ethernet interfaces.
- □ The interface for an IP network is set to LAN-4 on the source device.
- □ This value is not supported on the destination device. The value is therefore set to default value "LAN-1" on loading the configuration file.

- All destination-device parameters that were not available on the source device retain their respective values.

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

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

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

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

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

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

1.6 LANmonitor—know what's going on

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

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

Explanations about the LANmonitor messages and helpful tips can be found in the appendix under 'Error messages in LANmonitor' → page 700.

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

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

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

1.6.1 Extended display options

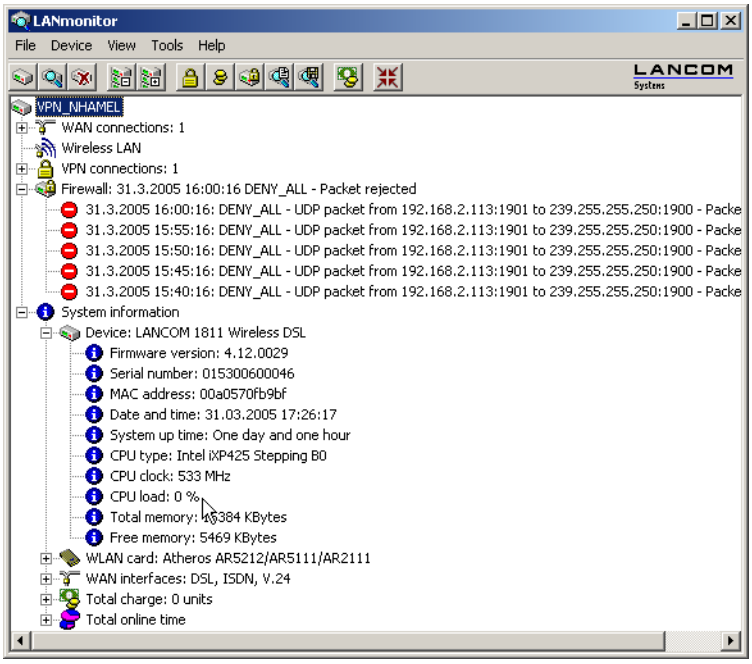
Under **View** ▶ **Show Details** you can activate and deactivate the following display options:

- Error messages
- Diagnostic messages
- System information

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

1.6.2 Enquiry of the CPU and Memory utilization over SNMP

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



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

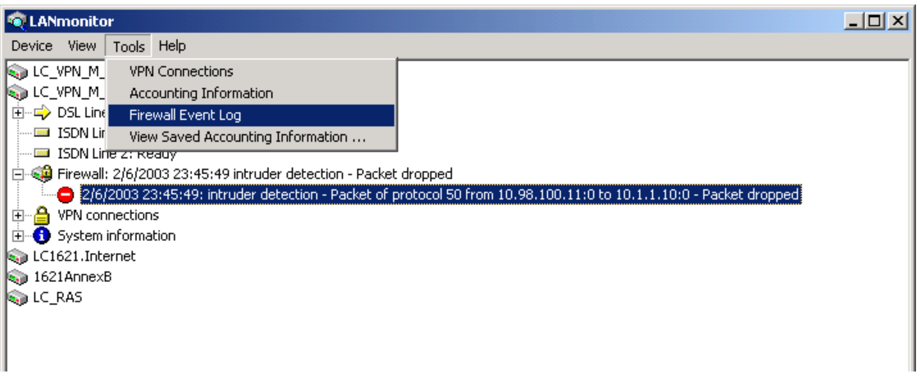
1.6.3 Monitor Internet connection

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

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

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

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



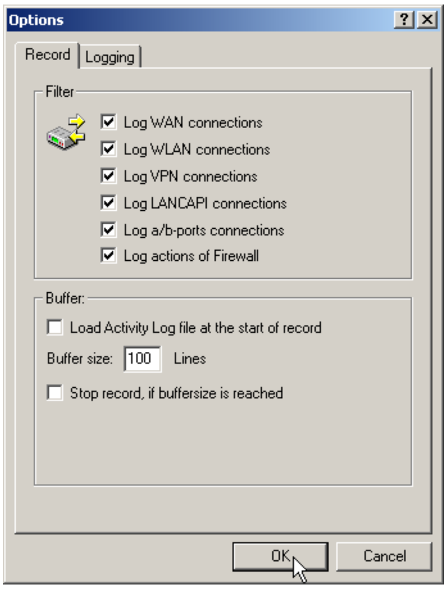
```
LC_VPN_M_
LC_VPN_M_
 ⊞ DSL Line
   ISDN Lir
   ISDN Line 2: Ready
 ⊟ Firewall: 2/6/2003 23:45:49 intruder detection - Packet dropped
     2/6/2003 23:45:49: intruder detection - Packet of protocol 50 from 10.98.100.11:0 to 10.1.1.10:0 - Packet dropped
 ⊞ VPN connections
 ⊞ System information
LC1621.Internet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

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

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

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

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



Filter

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

Buffer:

☐ Load Activity Log file at the start of record

Buffer size: 100 Lines

☐ Stop record, if buffersize is reached

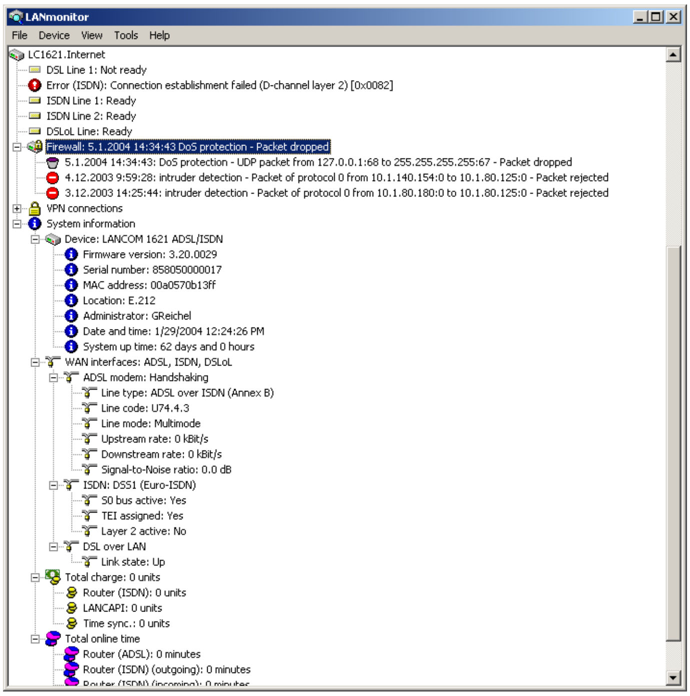
On the 'Protocol' tab you can define whether the following activities should be protocolled:

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

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

1.6.4 Display functions in LANmonitor

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



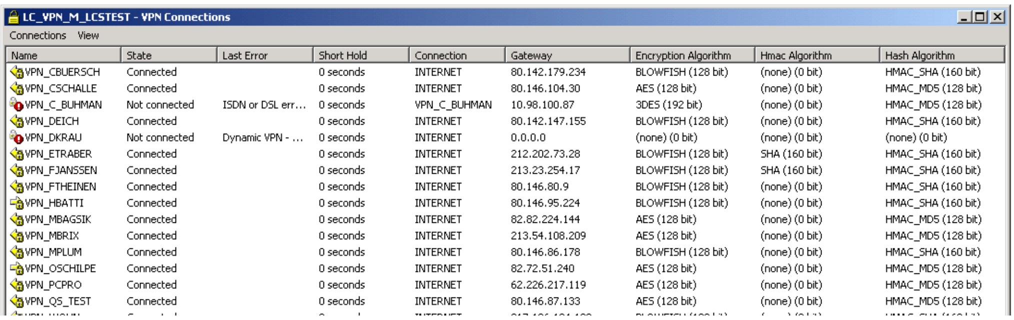
```
LC1621.Internet
    DSL Line 1: Not ready
    Error (ISDN): Connection establishment failed (D-channel layer 2) [0x0082]
    ISDN Line 1: Ready
    ISDN Line 2: Ready
    DSLoL Line: Ready
    Firewall: 5.1.2004 14:34:43 DoS protection - Packet dropped
        5.1.2004 14:34:43: DoS protection -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

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

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

- VPN connections

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

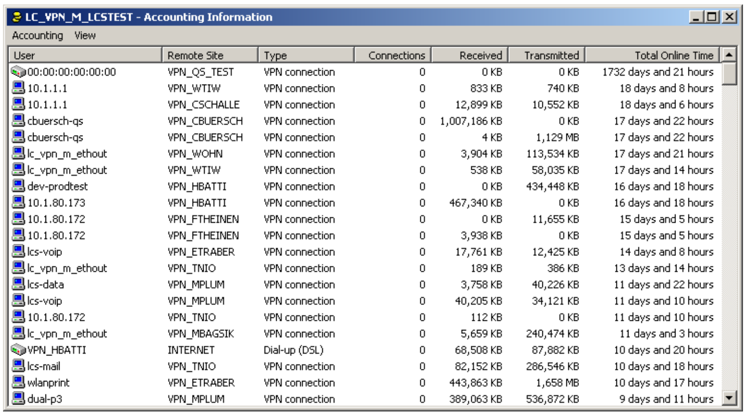


Name	State	Last Error	Short Hold	Connection	Gateway	Encryption Algorithm	Hmac Algorithm	Hash Algorithm
VPN_CBUERSCH	Connected		0 seconds	INTERNET	80.142.179.234	BLOWFISH (128 bit)	(none) (0 bit)	HMAC_SHA (160 bit)
VPN_CSCHALLE	Connected		0 seconds	INTERNET	80.146.104.30	AES (128 bit)	(none) (0 bit)	HMAC_MD5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

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

- Accounting information

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

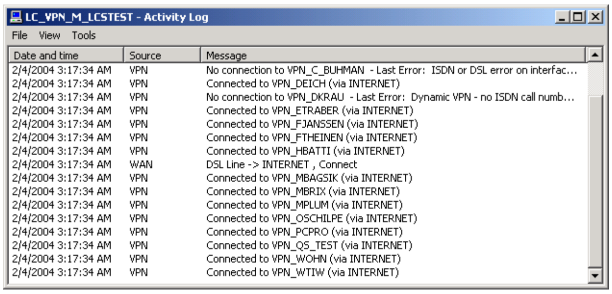


User	Remote Site	Type	Connections	Received	Transmitted	Total Online Time
00:00:00:00:00:00	VPN_QS_TEST	VPN connection	0	0 KB	0 KB	1732 days and 21 hours
10.1.1.1	VPN_WTIW	VPN connection	0	833 KB	740 KB	18 days and 8 hours
10.1.1.1	VPN_CSCHALLE	VPN connection	0	12,899 KB	10,552 KB	18 days and 6 hours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

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

- Activity log

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



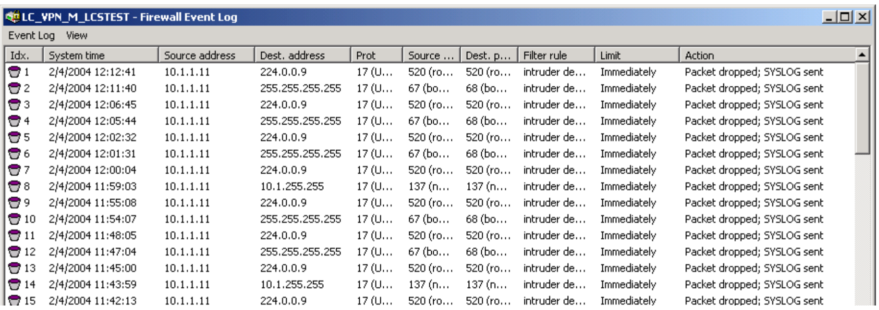
Date and time	Source	Message
2/4/2004 3:17:34 AM	VPN	No connection to VPN_C_BUHMAN - Last Error: ISDN or DSL error on interfac…
2/4/2004 3:17:34 AM	VPN	Connected to VPN_DEICH (via INTERNET)
2/4/2004 3:17:34 AM	VPN	No connection to VPN_DKRAU - Last Error: Dynamic VPN - no ISDN call numb…
2/4/2004 3:17:34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

  - □ Date and time

- □ Source
- □ Message

- ■ Firewall actions log

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



LC_VPN_M_LCSTEST - Firewall Event Log

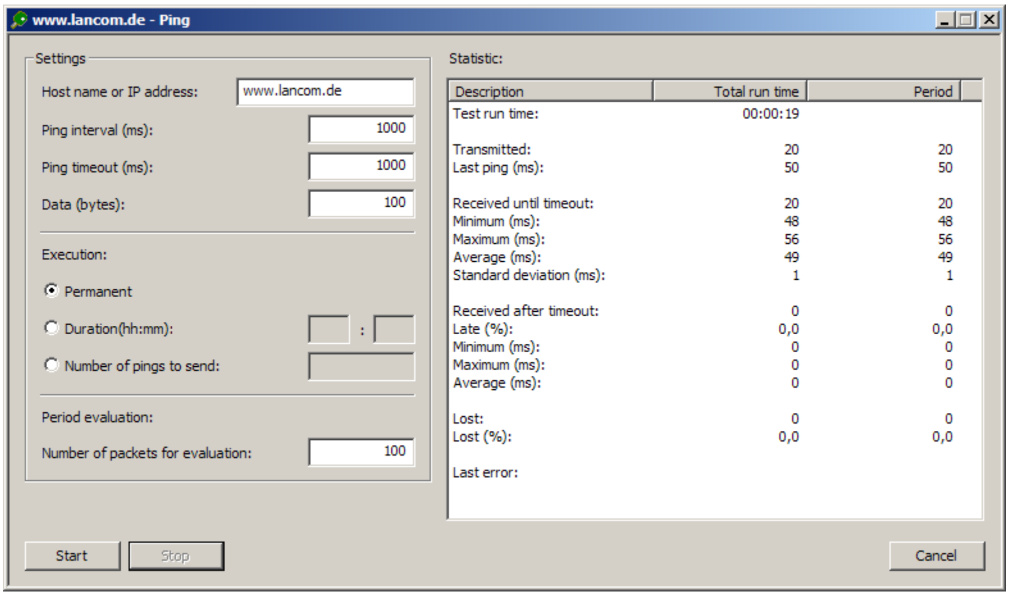
Idx.	System time	Source address	Dest. address	Prot	Source ...	Dest. p...	Filter rule	Limit	Action
1	2/4/2004 12:12:41	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
2	2/4/2004 12:11:40	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder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

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

1.6.5 Connection diagnosis with LANmonitor

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

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



www.lancom.de - Ping

Settings

Host name or IP address: www.lancom.de

Ping interval (ms): 1000

Ping timeout (ms): 1000

Data (bytes): 100

Execution:

● Permanent

○ Duration(hh:mm): :

○ Number of pings to send:

Period evaluation:

Number of packets for evaluation: 100

Statistic:

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

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

Configuring Ping execution

- ■ **Host name or IP address**

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

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

- ■ **Ping interval**

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

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

- **Ping timeout**

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

- **Data**

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

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

- **Execution**

  Repeat mode for the ping command.

Evaluation

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

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

The following information is displayed for evaluation:

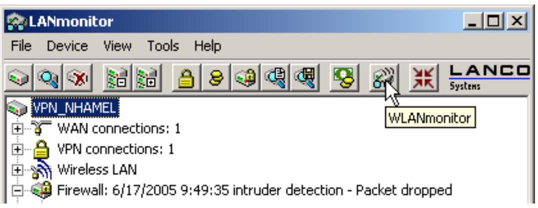
- **Test run time**
  - The total run time [hr./ min./ sec.]
- **Transmitted**
  - Total number of pings sent
  - Run time of the last ping [ms]
- **Received until timeout**
  - The number of pings answered in the timeout period
  - Minimum runtime
  - Maximum runtime
  - Average
  - Standard deviation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

1.7 Visualization of larger WLANs with WLANmonitor

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

1.7.1 Start the LANCOM WLANmonitor

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



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

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

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

1.7.2 Search for access points

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

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

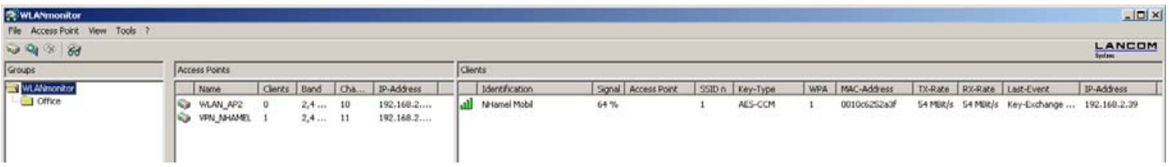
The right-hand column (client list) lists the clients that are logged in to the selected access point. The following information is shown for each client:

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

  LANconfig: WLAN Security ▶ Stations ▶ Stations

  Telnet: Setup/WLAN/Access-List

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



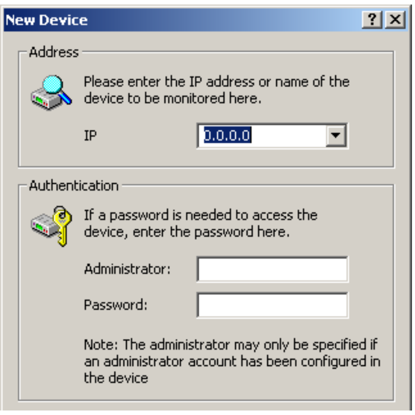
Name	Clients	Band	Cha...	IP-Address
WLAN_AP2	0	2,4 ...	10	192.168.2....
VPN_NHAMEL	1	2,4 ...	11	192.168.2....

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

1.7.3 Add access points

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

.



Address

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

IP: 0.0.0.0

Authentication

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

Administrator:

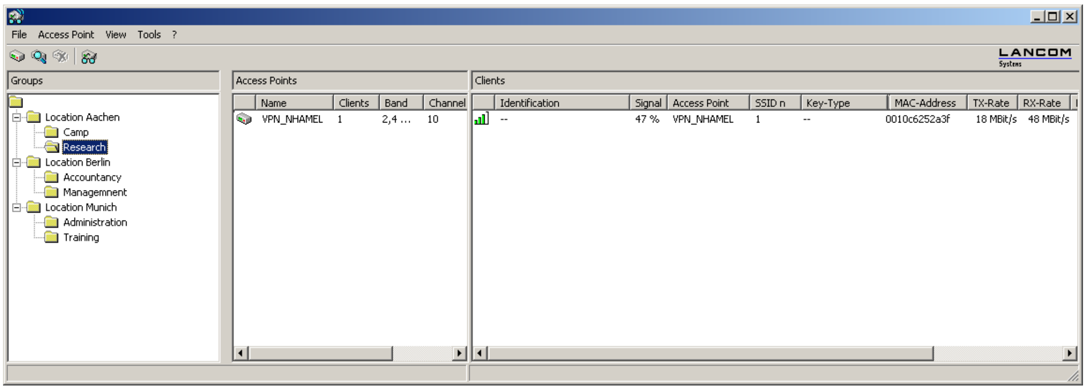
Password:

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

1.7.4 Organize access points

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

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



- Location Aachen
  - Camp
  - Research
- Location Berlin
  - Accountancy
  - Managemnent
- Location Munich
  - Administration
  - Training

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

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

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

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

1.7.5 Rogue AP and rogue client detection with the WLANmonitor

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

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

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

Further information can be found under 'Background WLAN scanning' → page 25.

Rogue AP detection

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

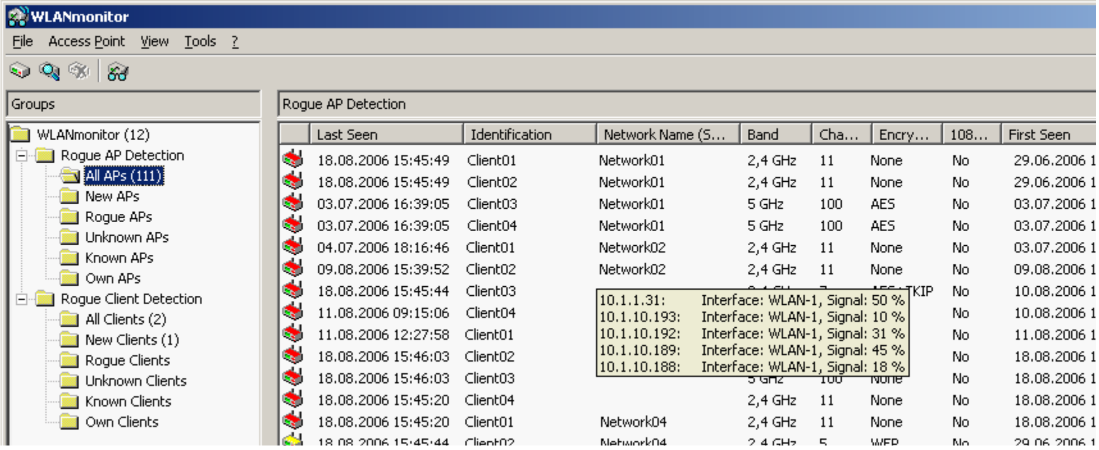
- Time of first and last detection
- BSSID, the MAC addresse of the AP for this WLAN network
- Network name
- Type of encryption used
- Frequency band used
- Radio channel used
- Use of 108Mbps mode

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

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

- All APs: List of all scanned WLAN networks grouped as follows
- New APs: New unknown and unconfigured WLAN networks are automatically grouped here (APs displayed in yellow)
- Rogue APs: WLAN networks identified as rogue and in need of urgent observation (APs displayed in red)
- Unknown APs: WLAN networks which are to be further analyzed (APs displayed in gray)
- Known APs: WLAN networks which are not a threat (APs displayed in gray)
- Own APs: New affiliated WLAN networks from access points monitored by WLANmonitor are automatically grouped here (APs displayed in green)

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



Last Seen	Identification	Network Name (S...	Band	Cha...	Encry...	108...	First Seen
18.08.2006 15:45:49	Client01	Network01	2,4 GHz	11	None	No	29.06.2006 1
18.08.2006 15:45:49	Client02	Network01	2,4 GHz	11	None	No	29.06.2006 1
03.07.2006 16:39:05	Client03	Network01	5 GHz	100	AES	No	03.07.2006 1
03.07.2006 16:39:05	Client04	Network01	5 GHz	100	AES	No	03.07.2006 1
04.07.2006 18:16:46	Client01	Network02	2,4 GHz	11	None	No	03.07.2006 1
09.08.2006 15:39:52	Client02	Network02	2,4 GHz	11	None	No	09.08.2006 1
18.08.2006 15:45:44	Client03		2,4 GHz	7	AES+TKIP	No	10.08.2006 1
11.08.2006 09:15:06	Client04					No	10.08.2006 1
11.08.2006 12:27:58	Client01					No	11.08.2006 1
18.08.2006 15:46:03	Client02					No	18.08.2006 1
18.08.2006 15:46:03	Client03		5 GHz	100	None	No	18.08.2006 1
18.08.2006 15:45:20	Client04		2,4 GHz	11	None	No	18.08.2006 1
18.08.2006 15:45:20	Client01	Network04	2,4 GHz	11	None	No	18.08.2006 1
18.08.2006 15:45:44	Client02	Network04	2,4 GHz	5	WEP	No	29.06.2006 1

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

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

Rogue client detection

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

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

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

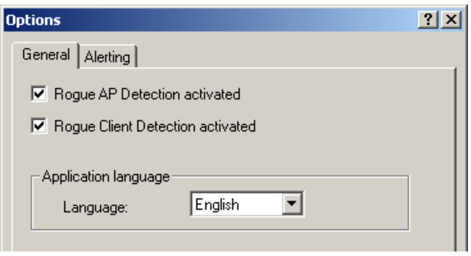
The WLANmonitor uses the following groups for sorting the clients that are found:

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

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

Activating rogue-AP and rogue-client detection

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



☑ Rogue AP Detection activated

☑ Rogue Client Detection activated

Application language

Language: English

:WLANmonitor: Tools ▶ Options ▶ General

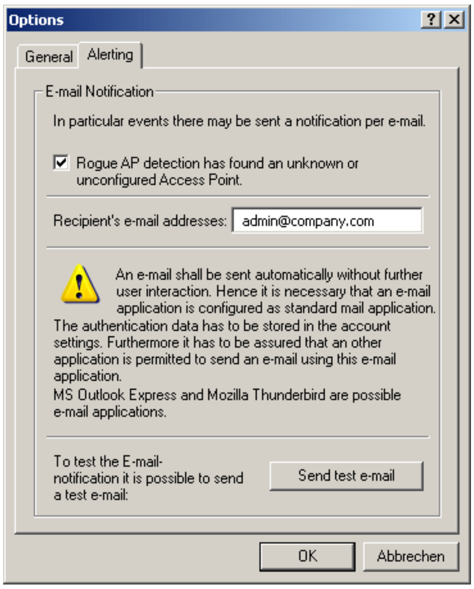
- **Rogue AP detection activated**

  Activate this option if WLANmonitor is to display unknown or unconfigured access points.
- **Rogue client detection activated**

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

Configuring the alert function in the WLANmonitor

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



E-mail Notification

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

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

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

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

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

WLANmonitor: Tools ▶ Options ▶ Alerts

- **E-mail messaging**

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

- **Recipient e-mail addresses**

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

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

- **Send a test e-mail**

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

1.8 Configuration with WEBconfig

New with LCOS 7.6:

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

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

Secure with HTTPS

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

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

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

Access with WEBconfig

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

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

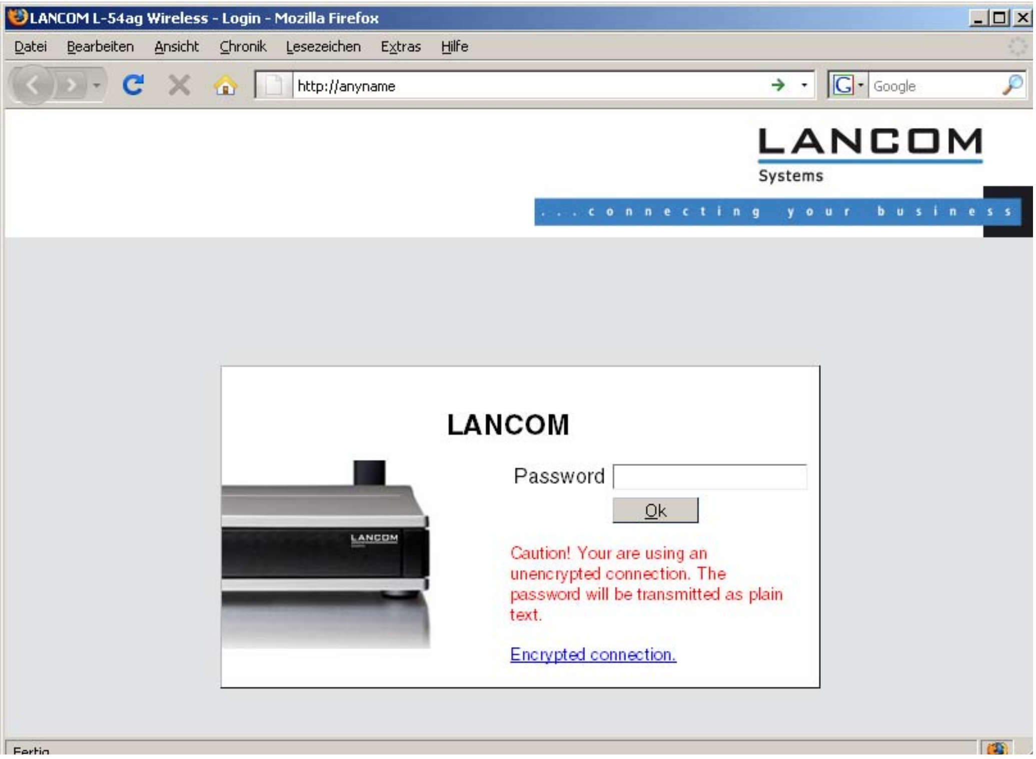
If a LANCOM Wireless Router or LANCOM Access Point is centrally managed from a LANCOM WLAN Controller, the DHCP mode is switched from auto-mode to client mode upon provision of the WLAN configuration.

Network without a DHCP server

Not for centrally managed LANCOM Wireless Routers or LANCOM Access Points

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

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


LANCOM L-54ag Wireless - Login - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://anyname
Google
LANCOM
Systems
...connecting your business
Fertig

LANCOM

Password

Ok

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

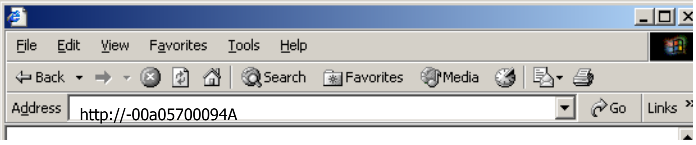
Encrypted connection.

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”.


File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links

http://-00a05700094A

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

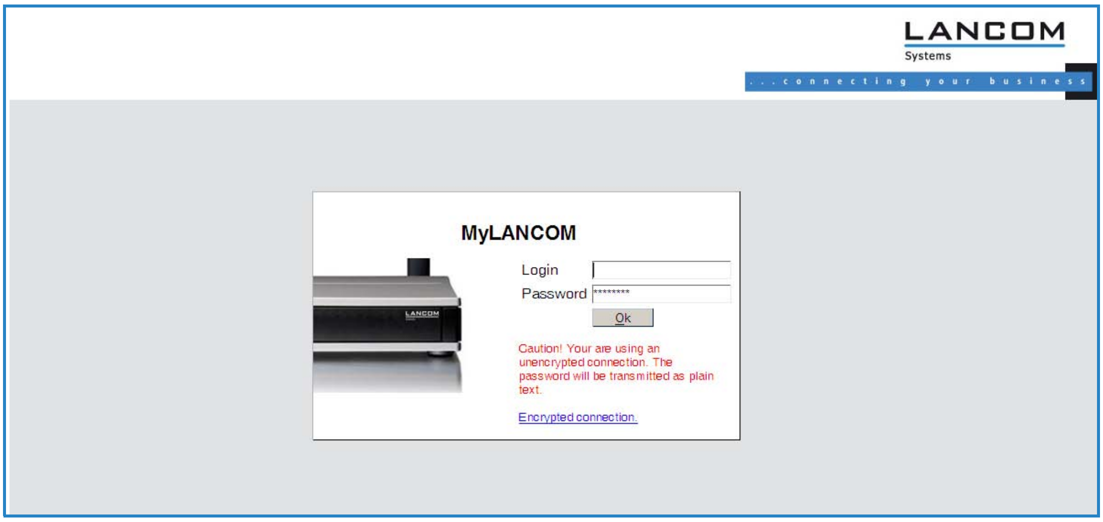
- If there is no DNS server in the LAN, or if it is not coupled to the DHCP server, the device cannot be reached via the name. In this case the following options remain:
  - □ Use LANconfig's “Find Device” function, or perform WEBconfig's “Device Search” from another yet accessible LANCOM.
  - □ Use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

Login

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

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

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



MyLANCOM

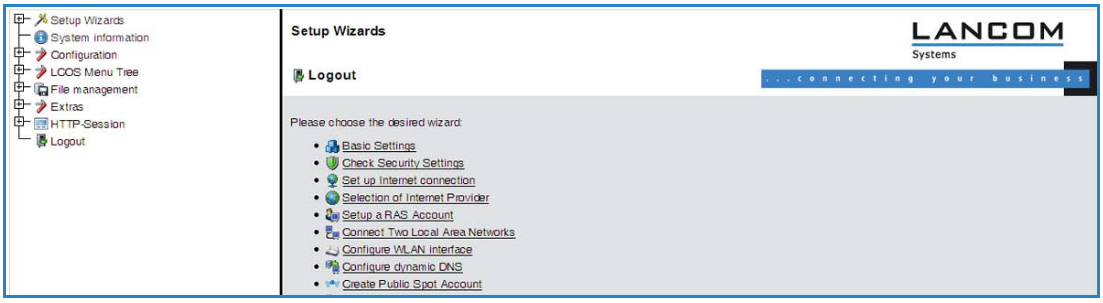
Login
Password ********
Ok

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

Encrypted connection.

Setup Wizards

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



Setup Wizards

Logout

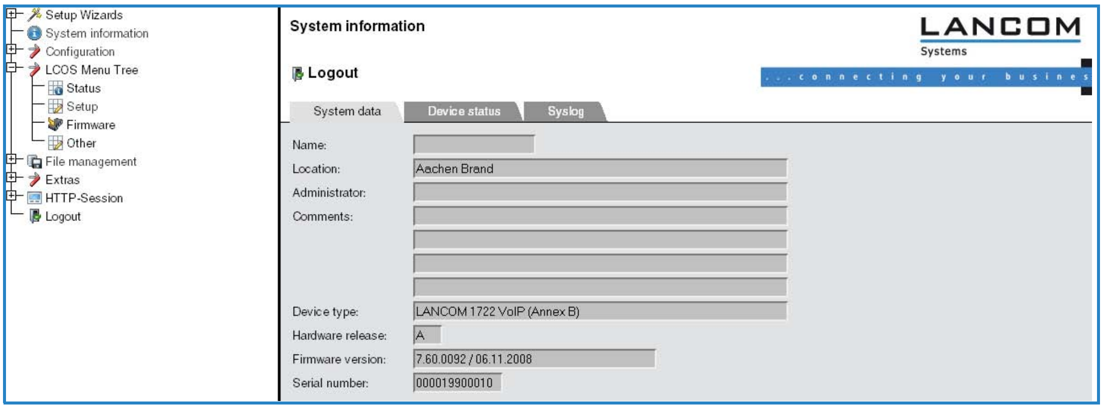
Please choose the desired wizard:

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

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

System information

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

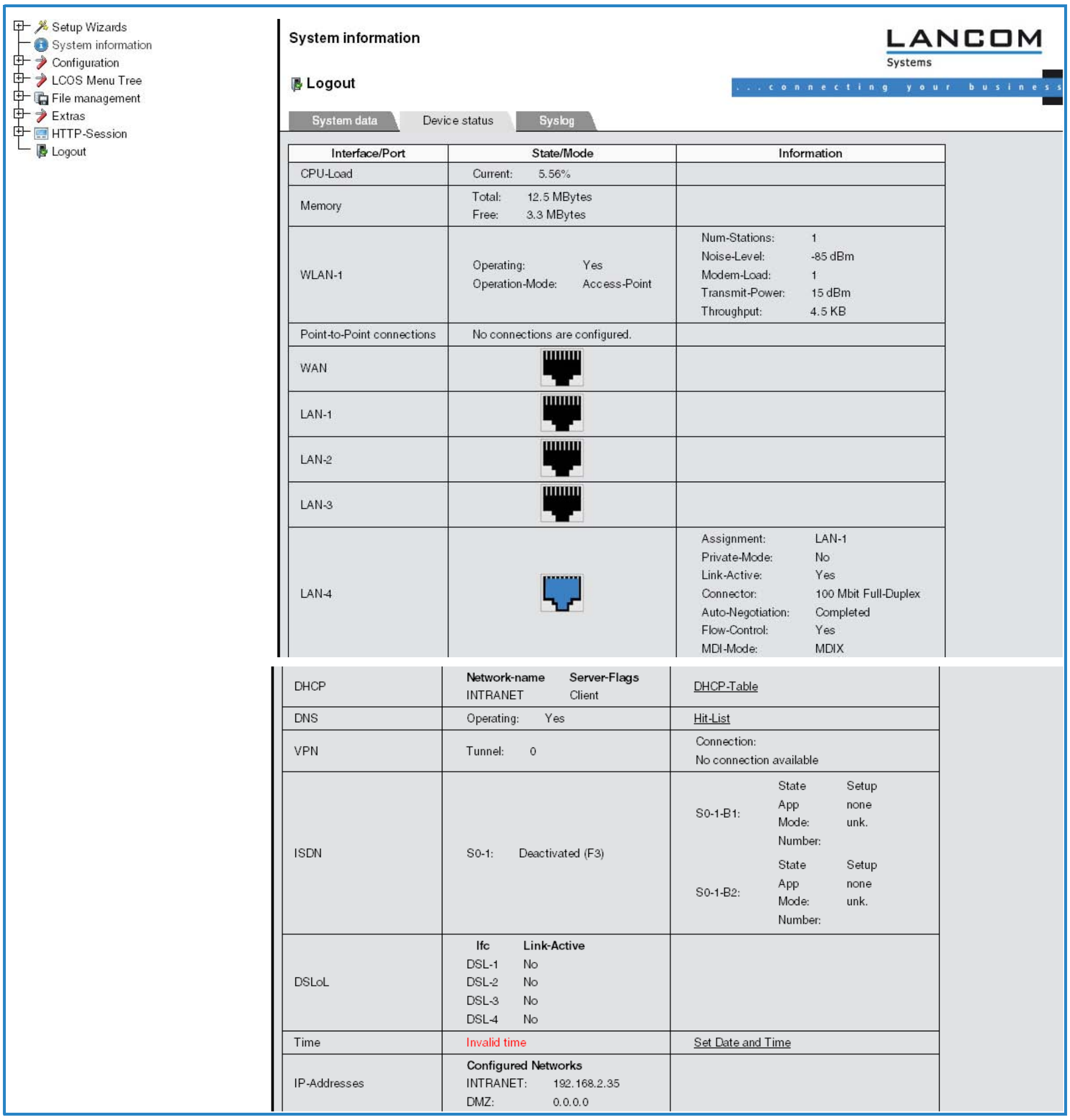


System information

Logout

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

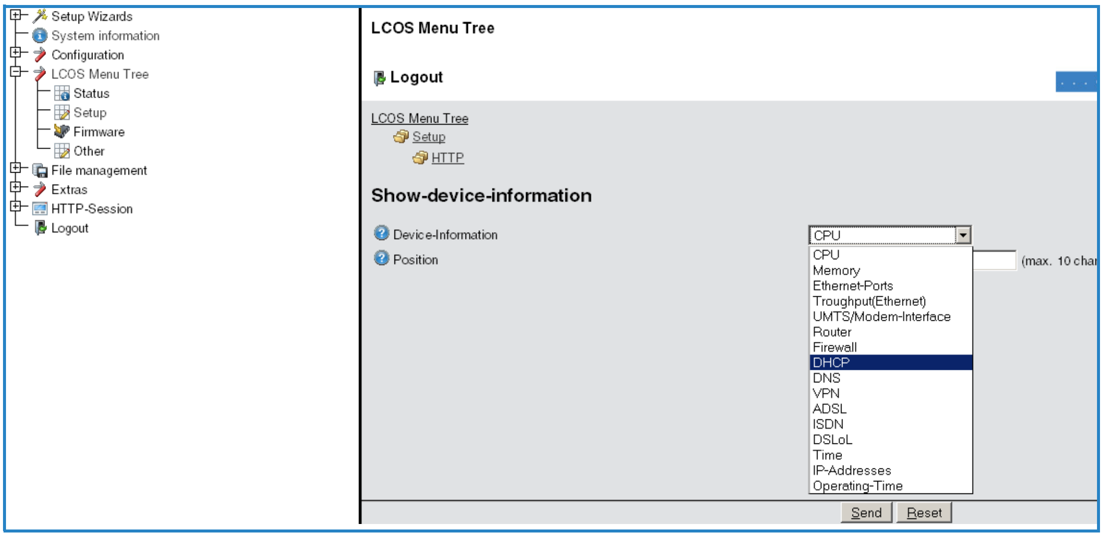
The "Device status" tab contains comprehensive information on the current operating state of the device. This includes, for example, a visual representation of the interfaces with information on the networks active on them. Appropriate links can be used to call up further relevant statistics (such as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



System information

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

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



LCOS Menu Tree

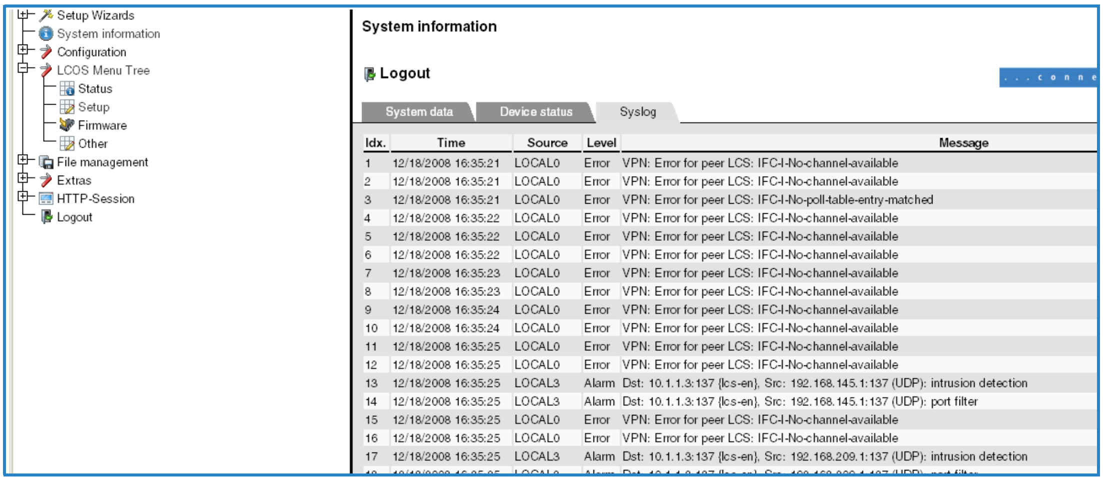
LCOS Menu Tree
Setup
HTTP

Show-device-information

Device-Information: CPU

Position: (max. 10 char

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

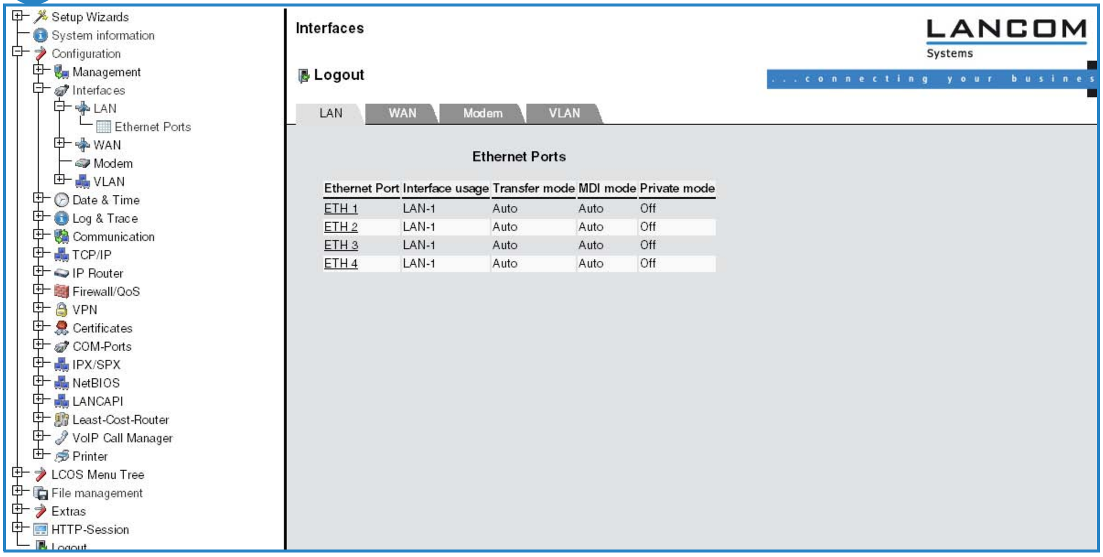


Idx.	Time	Source	Level	Message
1	12/18/2008 16:35:21	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-channel-available
2	12/18/2008 16:35:21	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-channel-available
3	12/18/2008 16:35:21	LOCAL0	Error	VPN: Error for peer LCS: IFC-I-No-poll-table-entry-matched
4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

Configuration

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

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

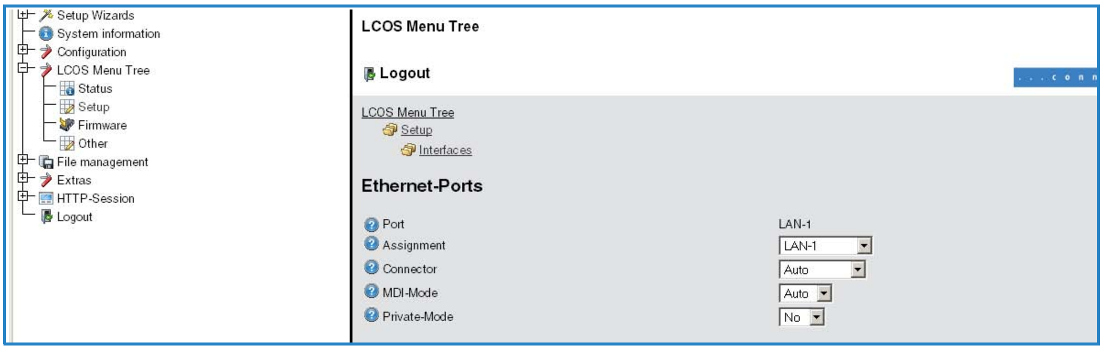


Ethernet Ports

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

LCOS menu tree

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



Ethernet-Ports

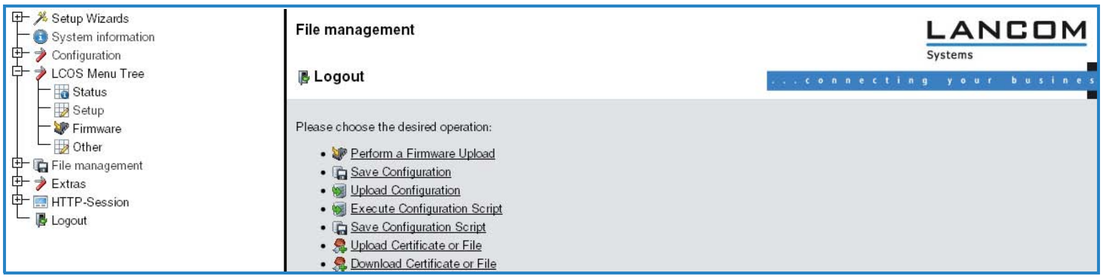
Port	LAN-1
Assignment	LAN-1
Connector	Auto
MDI-Mode	Auto
Private-Mode	No

File management

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

- Uploading new firmware
- Saving configuration

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

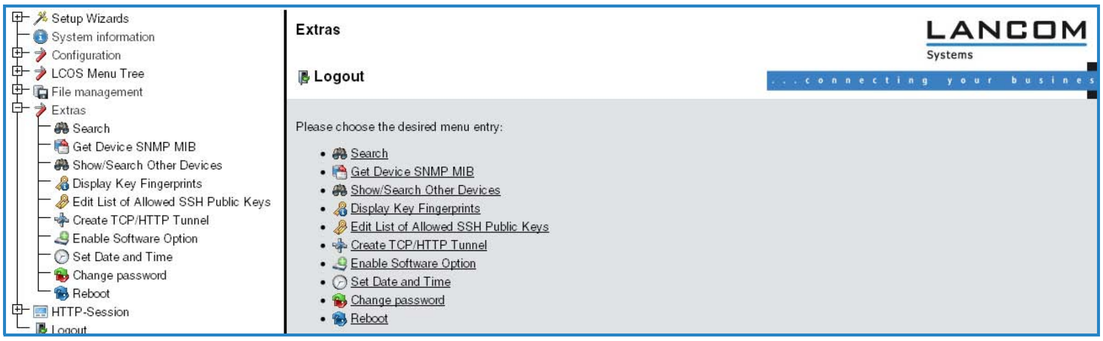


File management

Please choose the desired operation:

Extras

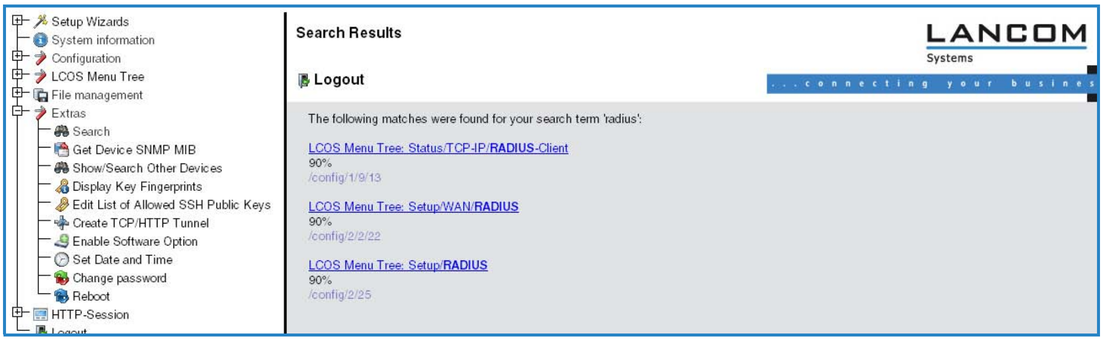
The menu area "Extras" contains a few functions that simplify device configuration.



Extras

Please choose the desired menu entry:

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



Search Results

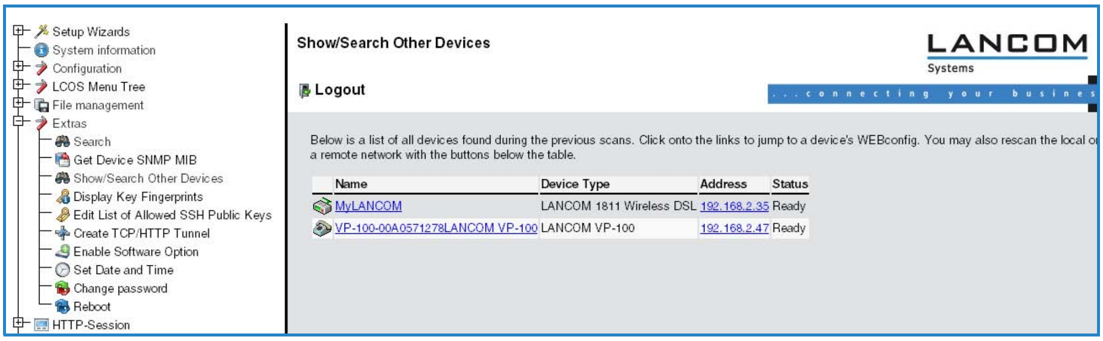
The following matches were found for your search term 'radius':

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

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

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

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



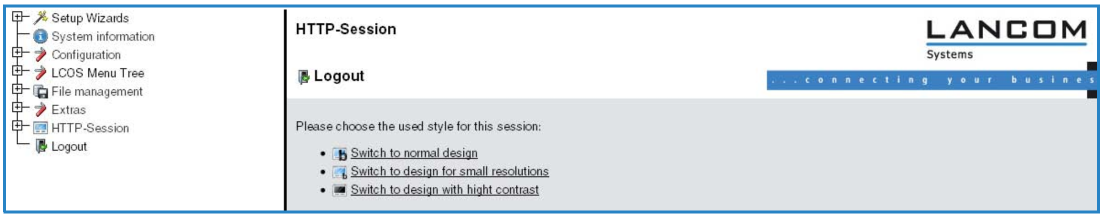
Show/Search Other Devices

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

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

HTTP session

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



Please choose the used style for this session:

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

1.9 Configuration with other tools

1.9.1 Telnet

New with LCOS 7.6:

- Extended functions for editing commands
- Function keys

Open Telnet session

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

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

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

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

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

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

Changing the console language

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

WEBconfig: LCOS menu tree ▶ Config-Module ▶ Language

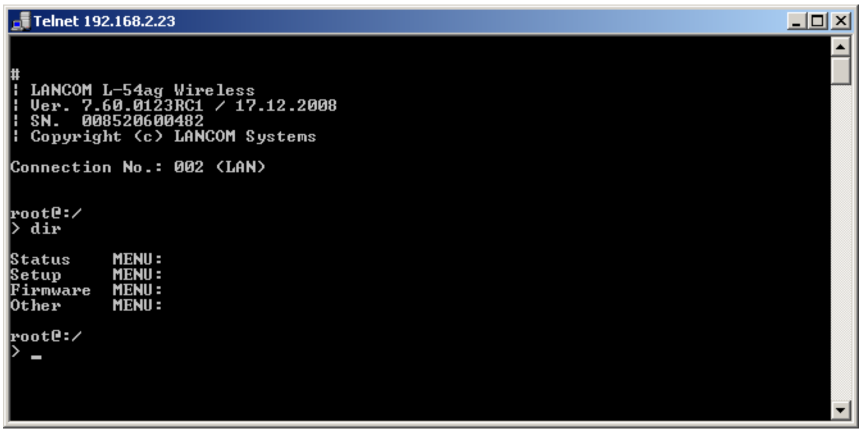
Close the Telnet session

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

```
C:\>exit
```

Structure of the command-line interface

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



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

Connection No.: 002 (LAN)


root@:/
> dir

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

root@:/
> _
```

- **Status**
  Contains the status and statistics of all internal modules in the device
- **Setup**
  Contains all adjustable parameters of all internal modules in the device

- **Firmware**
  Contains the firmware management
- **Others**
  Contains actions for establishing and terminating connections, reset, reboot and upload.

Command-line commands

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

Supervisor rights are necessary to execute some commands.

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

Command	Description
printenv	Display the entire environment
show <options>	Display of special internal data. show ? displays all available information, such as most recent boot processes ('bootlog'), firewall filter rules ('filter'), VPN rules ('VPN') and memory usage ('mem' and 'heap')
sysinfo	Display of system information (e.g. hardware/software version)
testmail	Sends an e-mail. See 'testmail ?' for parameters
time	Set time (DD.MM.YYYY hh:mm:ss)
trace [...]	Configuration of the diagnostics display.
who	List active sessions
writeconfig	Load a new configuration file in the device syntax. All subsequent lines are interpreted as configuration values until two blank lines occur
writeflash	Load a new firmware file (only via TFTP)
!!	Repeat last command
!<num>	Repeat command <num> times
!<prefix>	Repeat last command beginning with <prefix>
#<blank>	Comment

- PATH:
  - Path name for a menu or parameter, separated by / or \
  - .. means one level higher
  - . means the current level
- VALUE:
  - Possible input value
  - "" is a blank input value
- NAME:
  - Sequence of characters (made up of _ 0..9 A..Z)
  - First character cannot be a digit
  - Case insensitive
- All commands and directory/parameter names can be entered using their short-forms as long as they are unambiguous. For example, command "`sysinfo`" can be shortened to "`sys`" and "`cd Management`" to "`c ma`". Input "`cd /s`" is not valid, however, since it corresponds to both "`cd /Setup`" and "`cd /Status`".
- Names that contain spaces must be enclosed within quotation marks ("").
- A command-specific help function is available for actions and commands (call the function with a question mark as the parameter). For example, '`ping ?`' shows the options of the integrated ping command.
- Enter '`?`' on the command line for a complete listing of the console commands available.

Functions for editing commands

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

Function	Esc key sequences	Description
Up arrow	ESC [A	In the list of commands last run, jumps one position up (in the direction of older commands).
Down arrow	ESC [B	In the list of commands last run, jumps one position down (in the direction of newer commands).
Right arrow	Ctrl-F ESC [C	Moves the insert cursor one position to the right.
Left arrow	Ctrl-B ESC [D	Moves the insert cursor one position to the left.
Home or Pos1	Ctrl-A ESC [A ESC [1˜ (	Moves the insert cursor to the first character in the line.
End	Ctrl-E ESC [F ESC OF ESC [4˜	Moves the insert cursor to the last character in the line.
Ins	ESC [ESC [2˜	Switches between input and overwrite modes.
Del	Ctrl-D ESC <BS>ESC [3˜	Deletes the character at the current position of the insert cursor or ends the Telnet session if the line is blank.

Function	Esc key sequences	Description
erase	<BS><DEL>	Deletes the next character to the left of the insert cursor.
erase-bol	Ctrl-U	Deletes all characters to the left of the insert cursor.
erase-eol	Ctrl-K	Deletes all characters to the right of the insert cursor.
Tabulator		Completes the input from the current position of the insert cursor for a command or path of the LCOS menu structure: ■ If there is only one possibility of completing the command/path, this is accepted by the line. ■ If there is more than one possibility of completing the command/path, this is indicated by an audible sound when pressing the Tab key. Pressing the Tab key again displays a list of all possibilities to complete the entry. Then enter another character, for example, to allow unambiguous completion of the input. ■ If there is no possibility of completing the command/path, this is indicated by an audible sound when pressing the Tab key. No further actions are run.

Function keys for the command line

- Telnet: Setup ▶ Config ▶ Function keys

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

- **Key**

  Name of function key.

  Possible values:

  □ Selection from function keys F1 to F12.

  Default:

  □ F1

- **Mapping**

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

  Possible values:

  □ All commands/shortcuts possible in the command line

  Default:

  □ Blank

  Special values:

  □ The caret symbol ^ is used to represent special control commands with ASCII values below 32.^a

  □ ^A stands for Ctrl-A (ASCII 1)

  □ ^Z stands for Ctrl-Z (ASCII 26)

  □ ^[stands for Escape (ASCII 27)

  □ ^^ A double caret symbol stands for the caret symbol itself.

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

1.9.2 SNMP

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

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

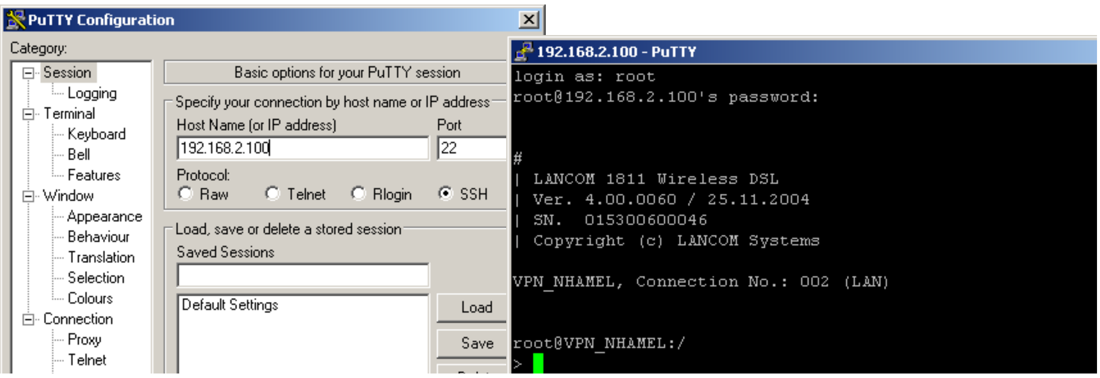
Your LANCOM can export a so-called device MIB file (**M**anagement **I**nformation **B**ase) for use in SNMP programs.

WEBconfig: Extras ▶Get Device SNMP MIB

1.9.3 Encrypted configuration with SSH access

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

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



Host Name (or IP address): 192.168.2.100

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

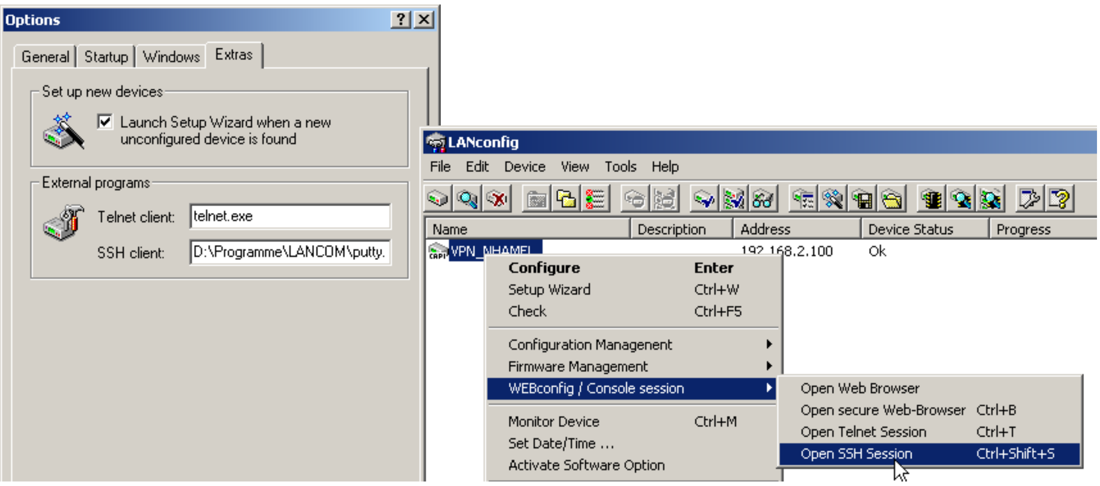
```
login as: root
root@192.168.2.100's password:

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

VPN_NHAMEL, Connection No.: 002 (LAN)

root@VPN_NHAMEL:/
>
```

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



☑ Launch Setup Wizard when a new unconfigured device is found

Telnet client: telnet.exe

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

Name	Description	Address	Device Status	Progress
VPN_NHAMEL		192.168.2.100	Ok	

The configuration is carried out with the same commands as used under Telnet or other terminal program ('Command line reference' → page 33).

1.9.4 SSH authentication

The SSH protocol generally allows two different authentication mechanisms:

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

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

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

Generating key pairs

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

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

Entering users into the public key

The public keys are generated in the following syntax:

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

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

Installing the private key on the SSH client

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

Load public key into the LANCOM Router

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

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

Configuring the authentication methods

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

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

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

Certificate check on SSH access

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

1.9.5 ISDN Remote configuration via Dial-Up Network

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

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

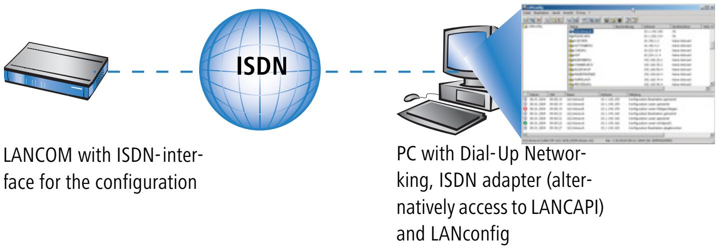
You can also reserve a special calling number for remote configuration. Then the support technician can always access the router even if it is really no longer accessible due to incorrect settings.

This is what you need for ISDN remote configuration

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

The first remote connection using Dial-Up Networking

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


ISDN
LANCOM with ISDN-interface for the configuration
PC with Dial-Up Networking, ISDN adapter (alternatively access to LANCAPI) and LANconfig

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

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

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

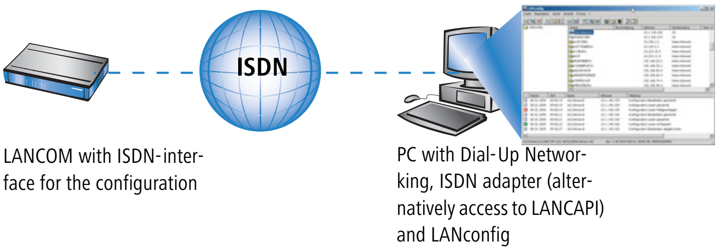
When an entry in the device list is deleted, the related connection in the Windows Dial-Up Network is also deleted.

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

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

The first remote connection using a PPP client and Telnet

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


ISDN
LANCOM with ISDN-interface for the configuration
PC with Dial-Up Networking, ISDN adapter (alternatively access to LANCAPI) and LANconfig

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

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

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

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

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

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

```
passwd
```

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

The default layer for remote field installations

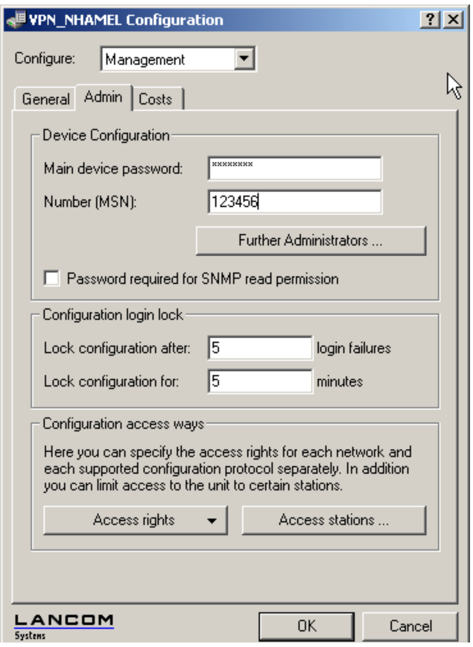
The PPP connection of any other remote site to the router, of course, will only succeed if the device answers every call with the corresponding PPP settings. This is the case using the factory default settings because the default protocol (default layer) is set to PPP.

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

The administrator access for ISDN remote management

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

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


VPN_NHAMEL Configuration

Configure: Management

General | Admin | Costs

Device Configuration

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

Number (MSN): 123456

Further Administrators ...

□ Password required for SNMP read permission

Configuration login lock

Lock configuration after: 5 login failures

Lock configuration for: 5 minutes

Configuration access ways

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

Access rights | Access stations ...

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

Alternatively, enter the following command:

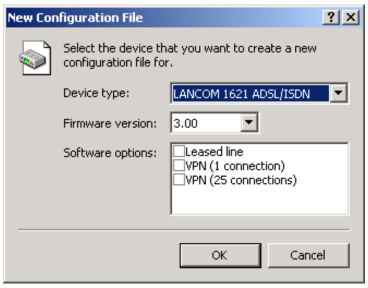
```
set /setup/config/Farconfig 123456
```

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

1.10 Working with configuration files

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

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



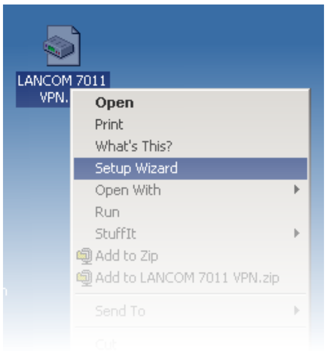
New Configuration File

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

Device type: LANCOM 1621 ADSL/ISDN

Firmware version: 3.00

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



Backup copies of configuration

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

Convenient series configuration

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

Running function

LANconfig:

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

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

1.11 New firmware with FirmSafe

New with LCOS 7.60:

- Asymmetric firmsafe

1.11.1 This is how FirmSafe works

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

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

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

with **Device ▶ Firmware Management ▶ Activate Firmware running in Test Mode**, using Telnet under 'firmware/firmsafe table' with the command 'set # active' (# is the position of the firmware in the firmsafe table). Using WEBconfig you can find the firmsafe table under **LCOS menu tree▶ Firmware**.

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

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

1.11.2 Asymmetric Firmsafe

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

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

Switching over to asymmetric Firmsafe

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

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

Firmware upgrade with asymmetric Firmsafe

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

1.11.3 How to load new software

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

- LANconfig
- WEBconfig
- Terminal program
- TFTP

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

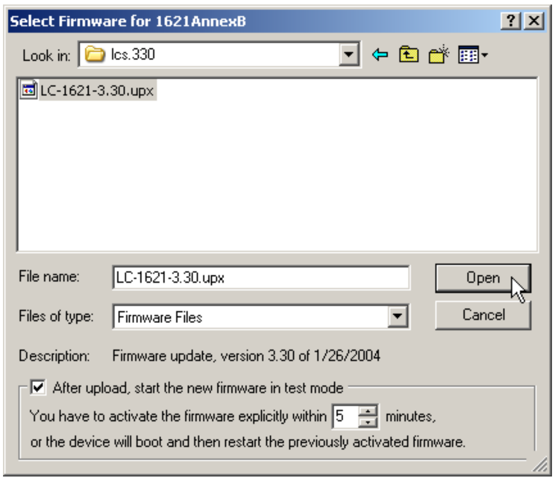
If the newly installed release contains parameters which are not present in the device's current firmware, the device will add the missing values using the default settings.

LANconfig

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

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

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



Look in: lcs.330

LC-1621-3.30.upx

File name: LC-1621-3.30.upx

Files of type: Firmware Files

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

☑ After upload, start the new firmware in test mode

You have to activate the firmware explicitly within 5 minutes,

or the device will boot and then restart the previously activated firmware.

WEBconfig

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

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

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

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

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

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

TFTP

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

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

Firmware upload via the serial interface with configuration reset

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

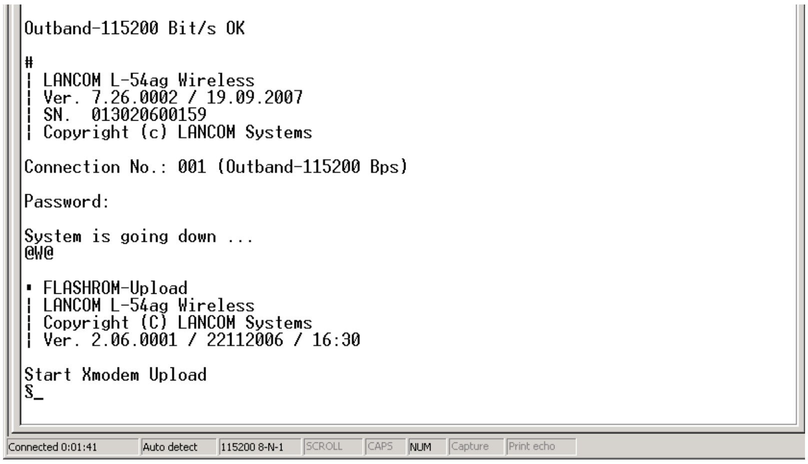
① Use the serial configuration cable to connect the device to a computer.

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

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

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

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



```
Outband-115200 Bit/s OK

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

Connection No.: 001 (Outband-115200 Bps)

Password:

System is going down ...
@W@

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

Start Xmodem Upload
§_
```

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

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

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

New in LCOS 7.60:

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

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

1.12.1 TFTP

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

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

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

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

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

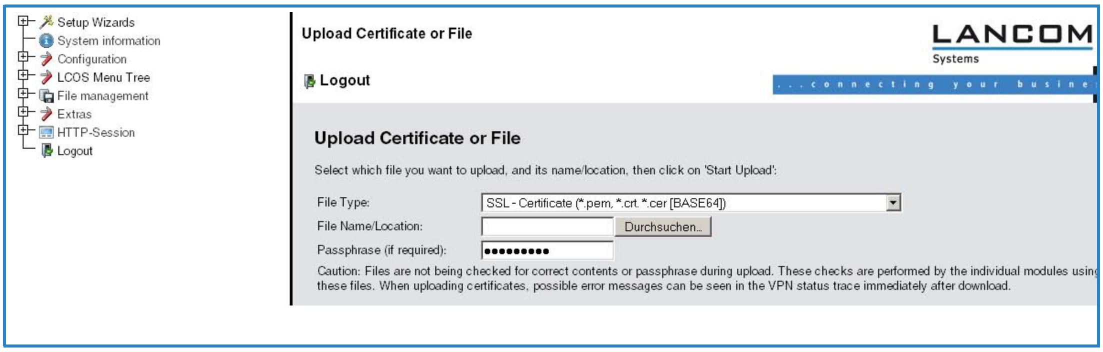
- <Master password><Command> or
- <User name>:<Password>@<Command>

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

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

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

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



Upload Certificate or File

Logout

Upload Certificate or File

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

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

File Name/Location: Durchsuchen...

Passphrase (if required): ●●●●●●●●●●

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

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

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

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

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

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

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

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

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

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

  - `-c <Certificate name>`

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

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

Examples:

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

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

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

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

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

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

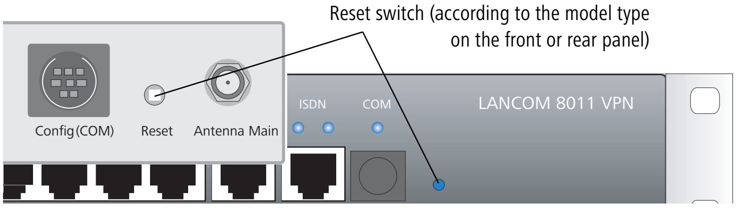
If the parameters `-s` and/or `-f` are not specified, the device uses default values set in path `/setup/config/TFTP-Client`:

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

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

1.13 How to reset the device?

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


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

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

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

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

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

WEBconfig: LCOS Menu Tree ▶ Setup ▶ Config

- **Reset button**

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

  - Ignore: The button is ignored.

Please observe the following notice: The settings 'Ignore' or 'Boot only' makes it impossible to reset the configuration to the factory settings using the reset button. If the password is lost for a device with this setting, there is no way to access the configuration! In this case the serial communications interface can be used to upload a new firmware version to the device-this resets the device to its factory settings, which results in the deletion of the former configuration. Instructions on firmware uploads via the serial configuration interface are available here (→ Seite 1-44).

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

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

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