



**HIRSCHMANN**

A **BELDEN** BRAND

# User Manual

## Operation and Maintenance Guide BAT54, BAT300

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2011 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement on the enclosed CD applies.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site ([www.beldensolutions.com](http://www.beldensolutions.com)).

Printed in Germany  
Hirschmann Automation and Control GmbH  
Stuttgarter Str. 45-51  
72654 Neckartenzlingen  
Germany  
Tel.: +49 1805 141538

# Contents

	<b>Key</b>	<b>8</b>
<b>1</b>	<b>Project Management with LANconfig</b>	<b>11</b>
1.1	Starting LANconfig	12
	1.1.1 Finding New Devices	13
	1.1.2 Expanding the Functional Display	15
	1.1.3 Using the Integrated Help Function	16
1.2	LANconfig Behavior at Windows Startup	17
1.3	Setting the GUI Language	19
1.4	Managing Multiple Devices	20
1.5	User-Specific Settings for LANconfig	22
1.6	Directory Structure	24
1.7	Increasing the Number of Columns in LANconfig	25
1.8	Searching with QuickFinder	27
	1.8.1 QuickFinder in the LANmonitor	30
	1.8.2 QuickFinder in the WLANmonitor	31
1.9	Multithreading	33
1.10	Password Protection for SNMP Read-Only Access	35
	1.10.1 Requiring a Password for SNMP Read-only Access	35
	1.10.2 Configuring User Information for SNMP Access	36
1.11	Device-Specific Settings for Communication Protocols	38
	1.11.1 Global Settings for Communication Protocols	38
	1.11.2 Device-Specific Settings for Communication Protocols	40
<b>2</b>	<b>Connecting to the Device</b>	<b>43</b>
2.1	Identifying the specified IP address	44
2.2	Making the Initial Connection	45
	2.2.1 Connection Procedure	45
<b>3</b>	<b>Upload Settings to the Device</b>	<b>49</b>
3.1	Uploading Settings in LANconfig	50
3.2	Uploading Settings in WEBconfig	54

<b>4</b>	<b>Working with Device Files</b>	<b>57</b>
4.1	Creating, Editing and Uploading Files	58
4.1.1	Creating, Editing and Printing Files in LANconfig	58
4.1.2	Uploading and Downloading Device Files	59
4.2	Automatic Backup of Files in LANconfig	60
<b>5</b>	<b>Managing Device Configurations with an AutoConfiguration Adapter</b>	<b>63</b>
5.1	Manually Transferring Device Settings to the ACA	64
5.2	Automatically Uploading Settings from the ACA to the Device	67
5.3	Manually Upload Settings from a ACA to the Device	68
<b>6</b>	<b>Rollout Wizard</b>	<b>71</b>
6.1	Settings for the Rollout Wizard	72
6.2	Variables	73
6.3	Actions Executed by the Rollout Wizard	75
6.4	Actions for Managing the Rollout Wizard	77
<b>7</b>	<b>Configuring a Device without an IP Connection</b>	<b>79</b>
7.1	Introducing the LANCOM Layer 2 Management Protocol	80
7.2	Configuring the LL2M Server	81
7.3	LL2M Client Commands	82
<b>8</b>	<b>Resetting and Re-Starting the Device</b>	<b>85</b>
8.1	Default Reset Behavior	86
8.2	Disabling the Reset Button	87
<b>9</b>	<b>Updating Firmware</b>	<b>89</b>
9.1	How FirmSafe Works	90
9.2	How to Load New Firmware	92
9.2.1	LANconfig	92
9.2.2	WEBconfig	93

9.2.3	Terminal Program	94
9.2.4	TFTP	94
9.2.5	Loading the Firmware via the Serial Interface with a Configuration Reset	95
9.3	Searching for New Firmware	97
9.3.1	Automatic Search for Firmware Updates	97
9.3.2	Manually Search for Firmware Updates	99
9.3.3	Viewing All Device Firmware Versions	100
<b>10</b>	<b>Load Files from a TFTP or HTTP Server to the Device</b>	<b>101</b>
10.1	TFTP	102
10.2	Loading Firmware, Device Configuration or Script via HTTP(S)	103
10.3	Loading Firmware, Device Configuration or Script via HTTP(S) or TFTP	104
10.3.1	Examples	105
<b>11</b>	<b>Scripting</b>	<b>107</b>
11.1	Applications	108
11.2	Scripting Function	110
11.3	Generate Script Files	111
11.3.1	Reading Out the Configuration via the Console	111
11.3.2	Reading the Configuration via TFTP from the CLI	112
11.3.3	Reading the Configuration with Hyperterminal	112
11.3.4	Download Script from the Device	113
11.4	Uploading Configuration Commands and Script Files	115
11.4.1	Entering Commands in a Console Session (Telnet, SSH)	115
11.4.2	Upload Script with TFTP Client	116
11.4.3	Upload Script with LANconfig	117
11.4.4	Upload Script with Hyperterminal	118
11.4.5	Multiple Parallel Script Sessions	119
11.4.6	Scripting Commands	119
<b>12</b>	<b>Managing Rights for Administrators</b>	<b>125</b>
12.1	Administrator Rights	126
12.1.1	Access Rights	126
12.1.2	Function Rights	128
12.2	Administrators' Access via TFTP and SNMP	129






12.2.1	TFTP Access	129
12.2.2	SNMP Access	130
12.2.3	Configuring User Rights	131
12.2.4	TCP Port Tunnel	133
<b>13</b>	<b>Managing Networks with Loopback Addresses</b>	<b>137</b>
13.1	Loopback Addresses with ICMP Polling	139
13.2	Loopback Addresses for Time Servers	142
13.3	Loopback Addresses for SYSLOG Servers	144
<b>14</b>	<b>Monitoring the LAN</b>	<b>147</b>
14.1	Display Functions in LANmonitor	148
14.2	Expanded Display Options	151
14.3	Querying CPU and Memory Utilization via SNMP	153
14.4	Connection Diagnosis with LANmonitor	154
14.4.1	Ping Configuring	155
14.4.2	Ping Evaluation	156
14.5	Monitoring Internet Connections	157
<b>15</b>	<b>Monitoring WLANs with WLANmonitor</b>	<b>159</b>
15.1	Starting WLANmonitor	160
15.2	Searching for Access Points	161
15.3	Adding Access Points	163
15.4	Organize Access Points	164
15.5	Detecting Rogue Access Points and Clients with WLANmonitor	165
15.5.1	Rogue Access Point Detection	166
15.5.2	Rogue Client Detection	167
15.5.3	Activating Rogue Access Point and Client Detection	168
15.5.4	Configuring the Alert Function with WLANmonitor	169
<b>16</b>	<b>Device Diagnostics</b>	<b>171</b>
16.1	Starting a Trace in Telnet	172
16.1.1	Code Key Overview	172
16.1.2	Trace Parameters	172
16.1.3	Combination Commands	174

16.1.4	Trace Filters	174
16.1.5	Trace Examples	175
16.2	Recording Traces with HyperTerminal	176
16.3	Tracing with LANmonitor	179
16.3.1	Creating Traces with the Trace Configuration Wizard	182
16.3.2	Manually Creating Trace Configurations	183
16.3.3	Displaying Trace Data	188
16.3.4	Backing Up and Restoring Trace Configurations	189
16.3.5	Saving and Restoring Trace Data	190
16.3.6	Back-Up Settings for Traces	190
16.3.7	Saving Support File	192
16.4	Performance Monitoring with LANmonitor	193
16.5	SYSLOG	196
16.5.1	Accessing SYSLOG Data	196
16.5.2	Structure of SYSLOG Messages	198
16.5.3	Configuring SYSLOG with LANconfig	200
16.5.4	Configuring SYSLOG with Telnet or WEBconfig	204
16.6	The Ping Command	206
16.7	Cable Testing	208
<b>A</b>	<b>Index</b>	<b>211</b>
<b>B</b>	<b>Further Support</b>	<b>213</b>






---

# Key

The designations used in this manual have the following meanings:

	List
	Work step
	Subheading
<a href="#">Link</a>	Indicates a cross-reference with a stored link
<b>Note:</b>	A note emphasizes an important fact or draws your attention to a dependency.
<i>Courier</i>	ASCII representation in user interface
	Execution in the Web-based Interface user interface
	Execution in the Command Line Interface user interface

Symbols used:








	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch

---



# Key

---

	Bridge
	Hub
	A random computer
	Configuration Computer
	Server
	PLC - Programmable logic controller
	I/O - Robot



# **1 Project Management with LANconfig**

## 1.1 Starting LANconfig

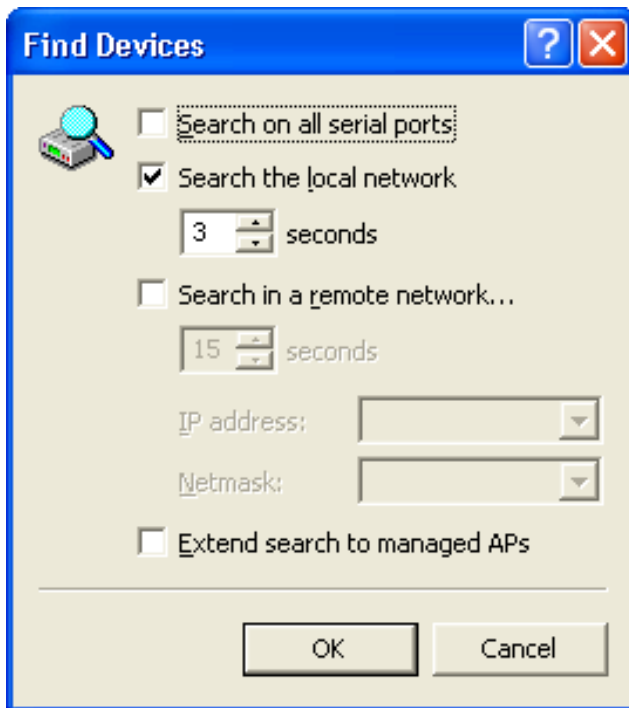
When you first start-up LANconfig, it automatically searches for devices on the local network. If it discovers an unconfigured device on the local area network (LAN), LANconfig automatically launches the setup wizard for that device.

**Note:** If a firewall is activated on your PC, LANconfig might not be able to find a new device in the LAN. In this case, deactivate the firewall during device discovery and configuration.

### 1.1.1 Finding New Devices

You can manually instruct LANconfig to initiate a search for new LAN devices. To begin a search:

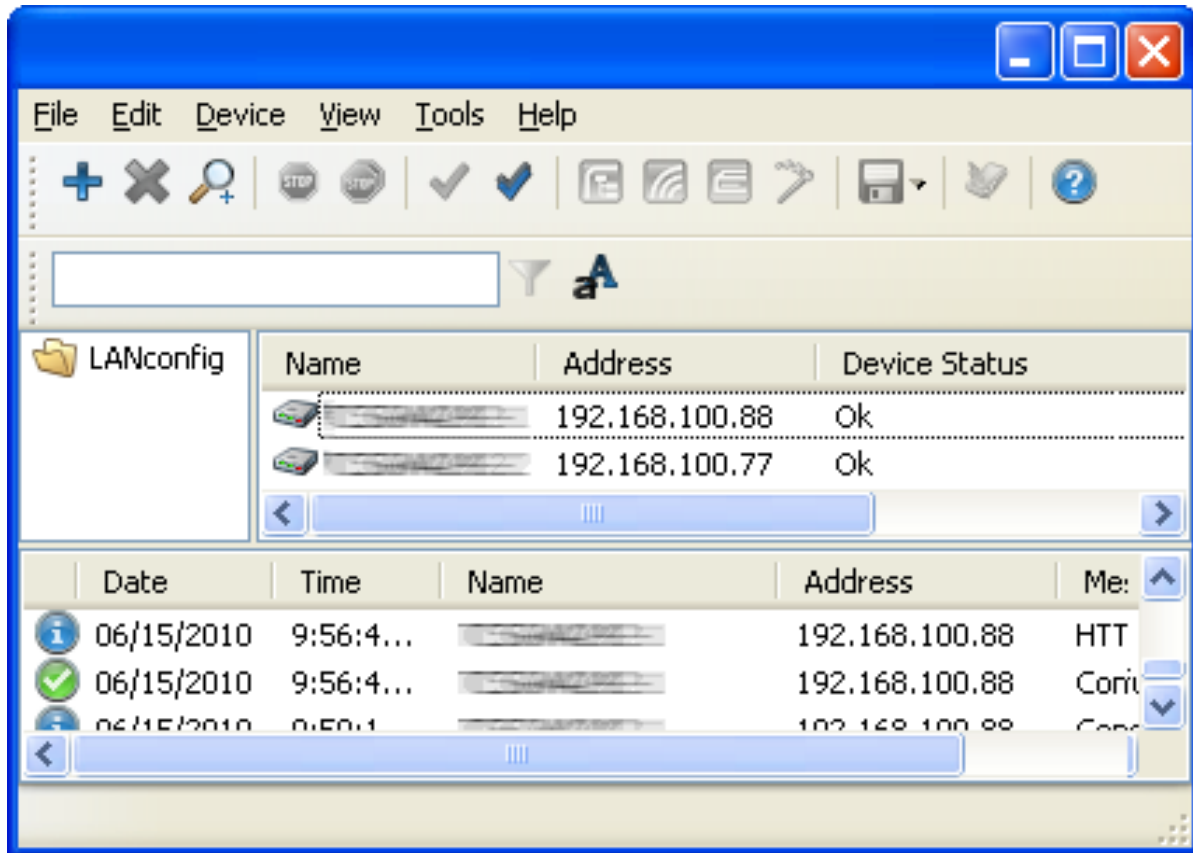
- Select **File** : **F**ind **D**eVICES. The 'Find Devices' dialog opens:



- Use the 'Find Devices' dialog to specify the scope of the search, including:
  - ▶ the networks to be searched: local, remote, or both
  - ▶ how long each network search should last
  - ▶ whether the search should include all serial ports

Selecting the 'Search the local network' option is usually sufficient. Click 'OK' and the search begins.

After LANconfig finishes the search, it displays a list of all the devices it has found, including each device name, IP address, and device status:



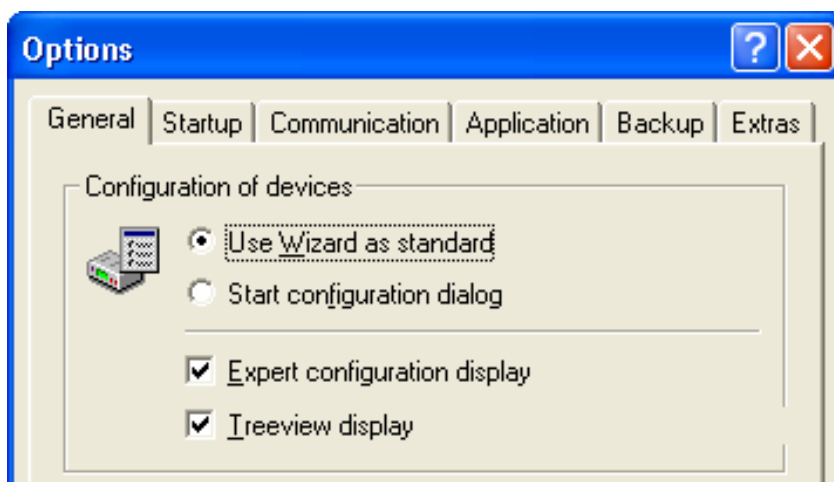
## 1.1.2 Expanding the Functional Display

Two different display options can be selected for displaying device configurations using LANconfig:

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

To specify the functional display option for all devices:

- Select **Tools** : **Options** to open the 'Options' dialog, then select the 'General' tab:



- Select 'Expert configuration display' to operate LANconfig in 'Complete configuration display' mode. De-select this to operate in 'Simple configuration display' mode.

### **1.1.3 Using the Integrated Help Function**

To assist you in using LANconfig, an integrated help feature is provided. Click on the 'Help' button located at the top right in any dialog, or right-click on a setting to call up context-sensitive help for the selected parameter.



---

## 1.2 LANconfig Behavior at Windows Startup

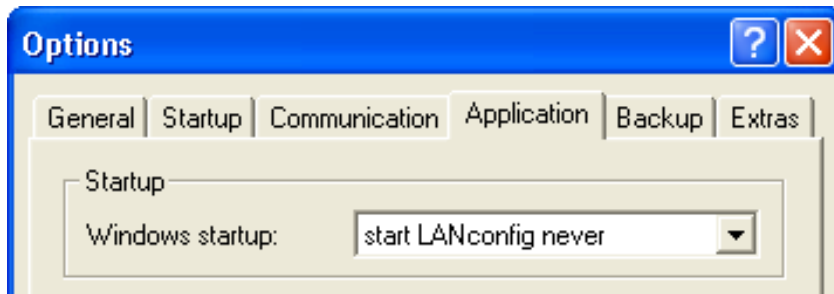
LANconfig can be configured to run automatically when the Windows operating system starts up. Options include:

- ▶ Start LANconfig never: LANconfig does not start during the Windows startup. If required, start LANconfig manually. This is the default setting.
- ▶ Start LANconfig always: LANconfig starts automatically after a successful Windows startup.
- ▶ Start LANconfig like before: LANconfig startup behavior depends on its run state before the last Windows shutdown. If LANconfig had been running, it will start automatically after the Windows startup; otherwise, LANconfig will not start automatically.

**Note:** When you change from 'never' to either of the other selections, LANconfig writes or deletes an entry in the autostart section of the system registry. Firewalls on the configuration computer or the operating system itself may interpret these changes as an attack and may alert you or even block the access. Because you make these changes in the Windows startup intentionally, you can ignore these alerts and confirm the new startup behavior.

To configure LANconfig behavior at Windows startup:

- Select **Tools** : options to open the 'Options' dialog, then select the 'Application' tab:

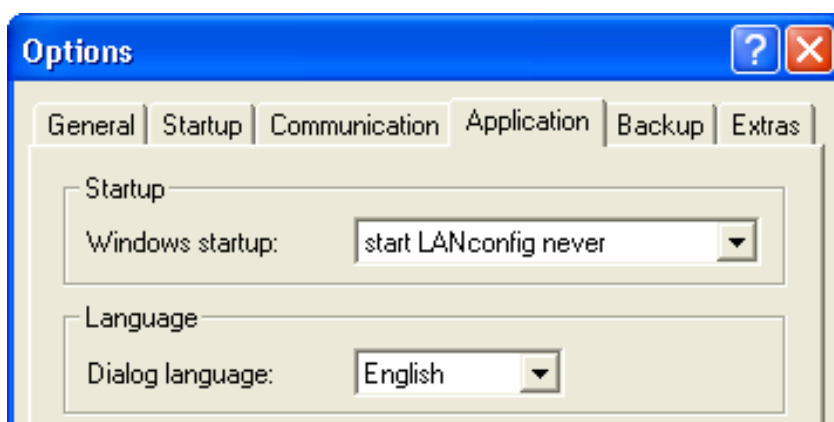


- Select a 'Windows startup' option, as described above.

## 1.3 Setting the GUI Language

The graphical user interface (GUI) language for LANconfig, LANmonitor or WLANmonitor can be set to either German or English. To change the GUI for LANconfig:

- Select `Tools : Options` to open the 'Options' dialog, then select the 'Application' tab:



- Select a 'Dialog language' option: German or English.

**Note:** In both LANmonitor and WLANmonitor, the language setting can be found in the `Tools : Options : General` dialog.

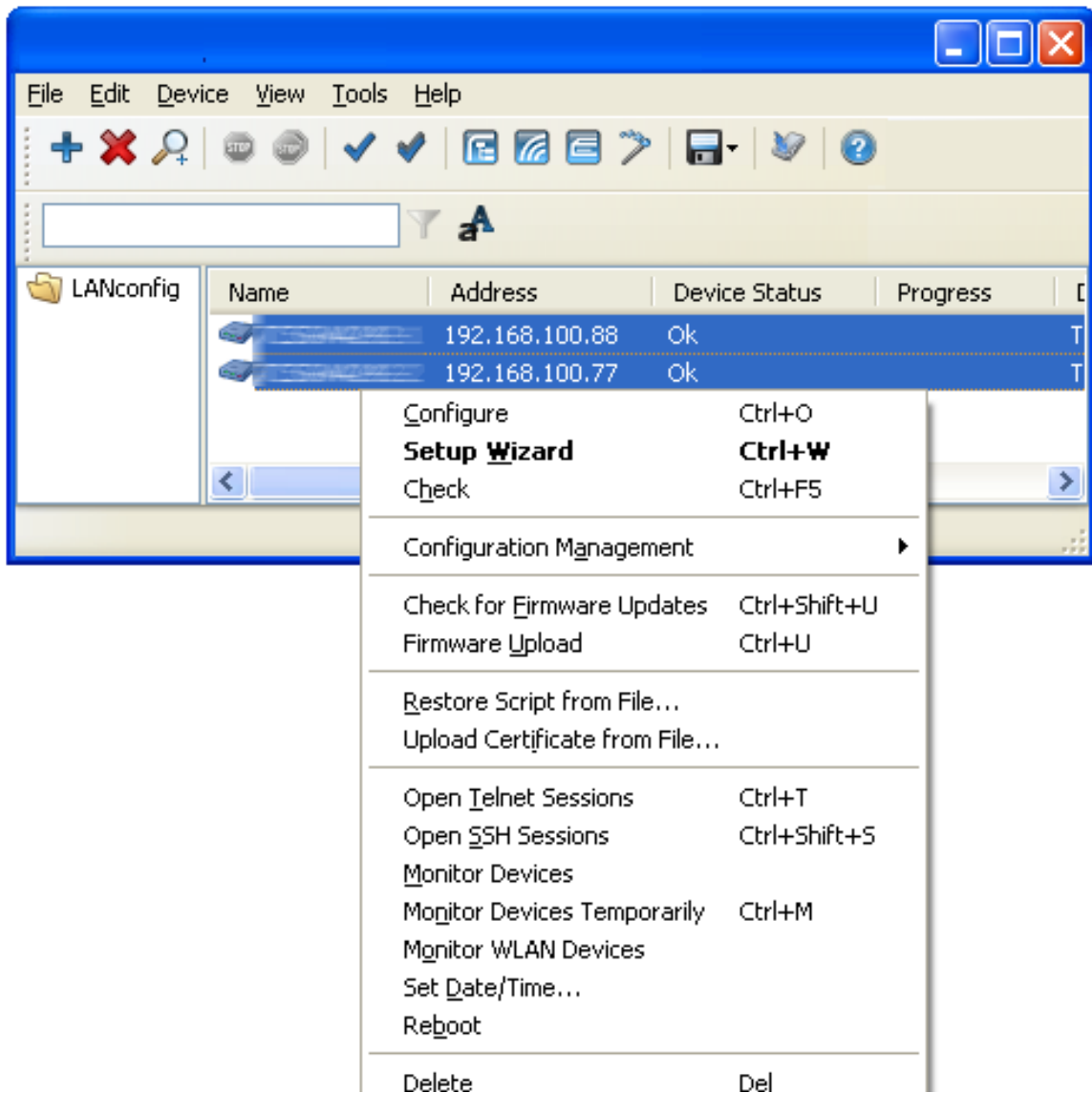
## 1.4 Managing Multiple Devices

LANconfig supports the remote management of multiple devices. Simply select two or more devices, and LANconfig performs all actions in sequence for each selected device. You can execute commands on multiple devices of the same type. You configure devices of different types individually.

To view the devices you are managing, activate the folder tree by selecting `View : Folder Tree`. To easily manage multiple devices, drag and drop the devices to be collectively managed into a common folder.

**Note:** LANconfig displays only those parameters that are common to multiple devices when you select more than one device.

With multiple devices selected, click the right mouse button to display the functions that can be executed for these devices.



For more information about group configurations, refer to the topic 'Group Configurations with LANconfig' in the 'Switch Configuration and Administration Guide'.

## 1.5 User-Specific Settings for LANconfig

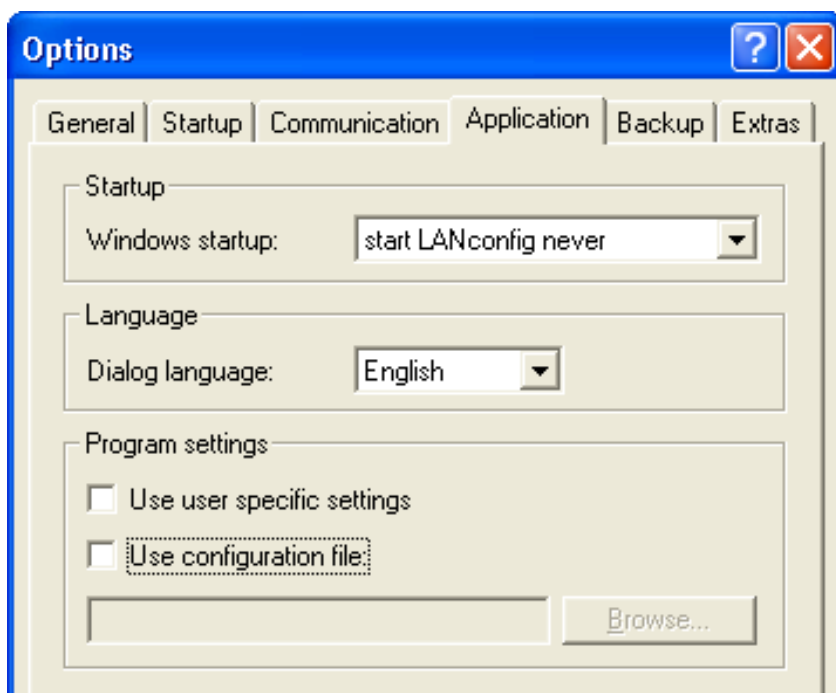
When LANconfig shuts down, program settings are saved to the file “lanconf.ini” located in the program directory. This includes the displayed devices, directory structure, selected language, etc. When LANconfig starts-up, it reads this ini file and restores the previous status of the software.

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

- ▶ By selecting the user directory, users can save their personal settings even if they exclusively have read 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.

To configure user-specific LANconfig settings:

- Select `Tools : Options`, then click the ‘Applications’ tab to open that dialog.



The following parameters can be set in this dialog:

- ▶ **Use user-specific settings:**  
Activates the use of the lanconf.ini file in the current user's directory: ...\\User\\Application Files\\Switch\\LANconfig. When you activate this option, changes to the program settings are saved to this ini file. When you activate this option in parallel with the "Use configuration file" option, LANconfig uses the file selected here when it starts, and it stores the changes in this file. In the default setting, this option is deactivated.
- ▶ **Use configuration file:**  
This activates the usage of the lanconf.ini from the given directory. With this option activated, changes to the program settings are saved to the selected ini file. De-selected by default.

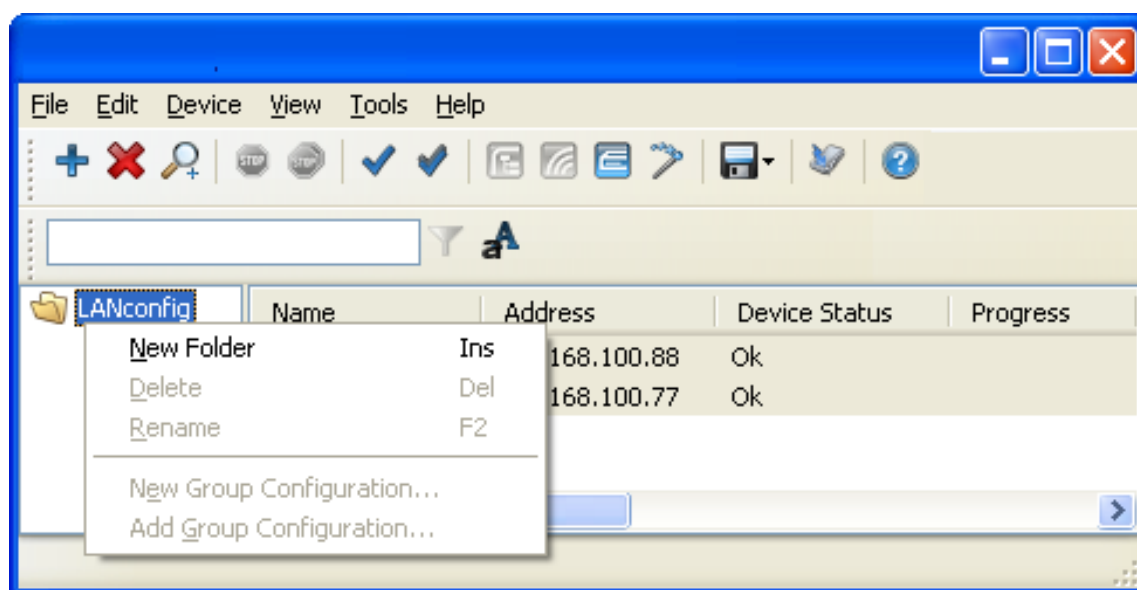
**Note:** The file you select needs to be a valid LANconfig settings file.

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

## 1.6 Directory Structure

LANconfig uses a directory structure to provide an overview when managing multiple devices. The arrangement of devices in folders effects the display of the devices within LANconfig. The organization of the folders has no influence on the actual configuration of the devices. Folders dedicated to projects or customers can be set up to organize the relevant devices:

- ▶ Create a new folder by right-clicking on the parent directory and selecting “New Folder” from the context menu.



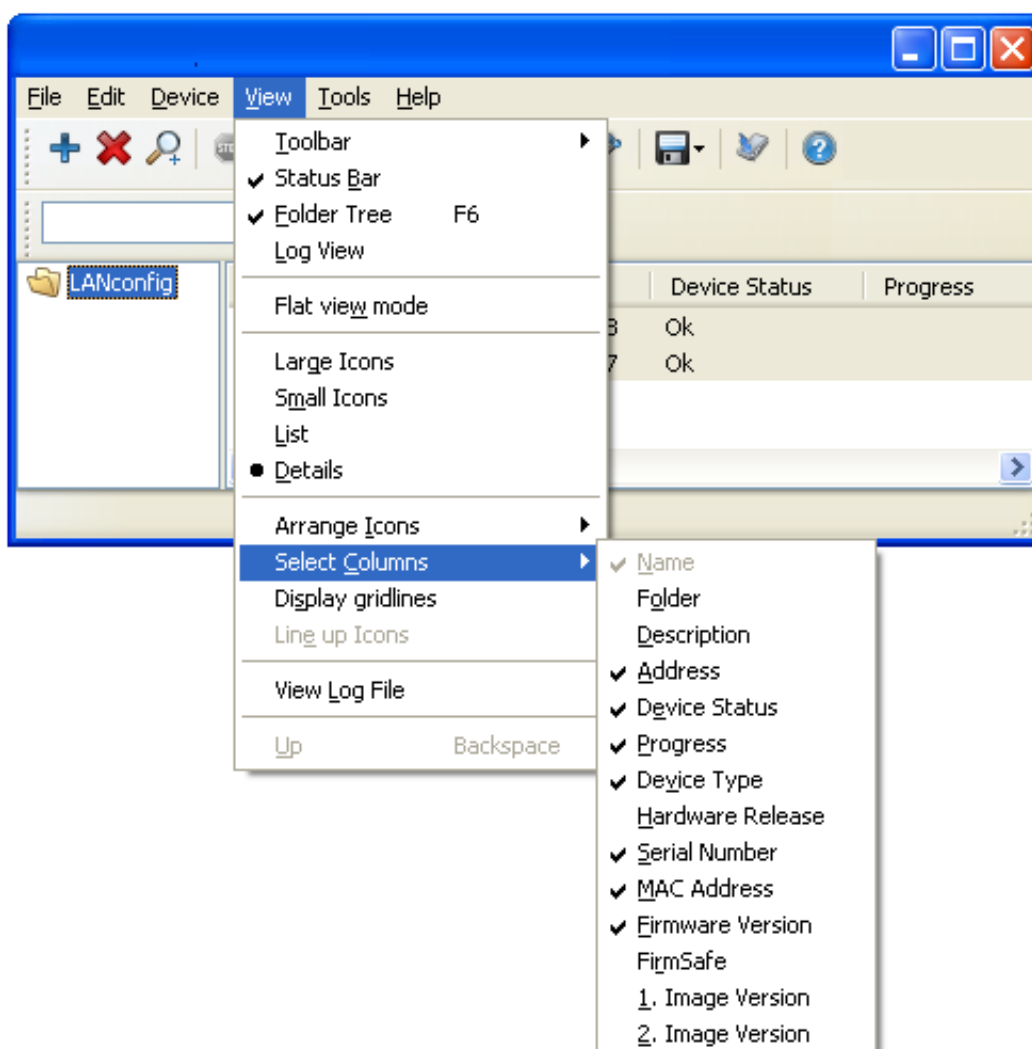
- ▶ Use the mouse to drag and drop the devices into the appropriate folder. Devices can also be moved from one folder to another using this method.

The directory structure in the left side of the LANconfig window can be switched on and off using either the F6 function key or the command View : Folder Tree.



## 1.7 Increasing the Number of Columns in LANconfig

You can attain a better overview and quicker orientation of your project in LANconfig by adding to or subtracting from the columns that describe the project's devices. To edit the specific parameters included as column headers for all devices, select **View : Select Columns**, then choose the parameters to be displayed as columns.



Use the menu item 'Select Columns' command to display the device properties you wish to view. The following properties can be displayed:

- ▶ Name
- ▶ Folder
- ▶ Description
- ▶ Address
- ▶ Device status
- ▶ Progress
- ▶ Device type
- ▶ Hardware release
- ▶ Serial number
- ▶ MAC address
- ▶ Firmware version
- ▶ FirmSafe
- ▶ 1. Image version
- ▶ 2. Image version

## 1.8 Searching with QuickFinder

The configuration dialogs in LANconfig, LANmonitor and WLANmonitor are comprised of numerous areas, parameters and their values, and tables. The QuickFinder helps you search for the desired value. In the main view of LANconfig, you will find QuickFinder in the tool bar. Enter a search term in the search window to reduce the number of devices displayed. LANconfig searches through all the values available in the columns of the device list – including the columns currently hidden. Click the symbol beside the magnifying glass to make the search case-sensitive.

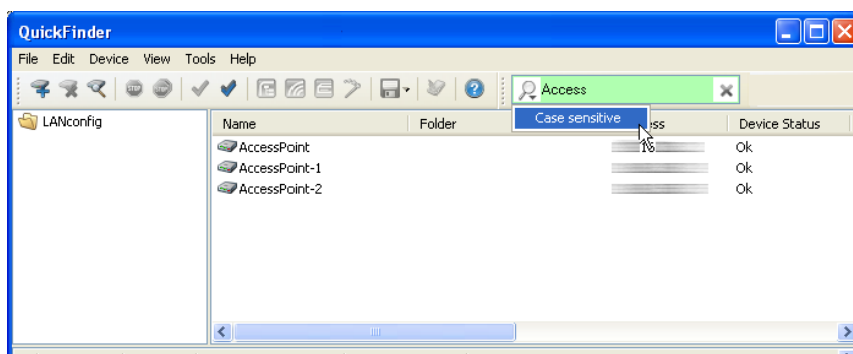


Figure 1: QuickFinder in the main view of LANconfig

When you search for a specific value or term in LANconfig or the configuration, the QuickFinder quickly shows you in the configuration dialogs of LANconfig all the places that contain the character string you are searching for.

- Start LANconfig.
- Open the configuration of the device you want to search in.
- Enter the desired term in the search field, e.g. 'wlan'. The search is not case-sensitive. You can enter parts or words or numbers, as well as complete search terms. Spaces in the search terms search for character strings that contain corresponding spaces. However, the search function does not support wildcards.

The configuration tree in the left area of LANconfig is now reduced to all the areas that contain the search term:

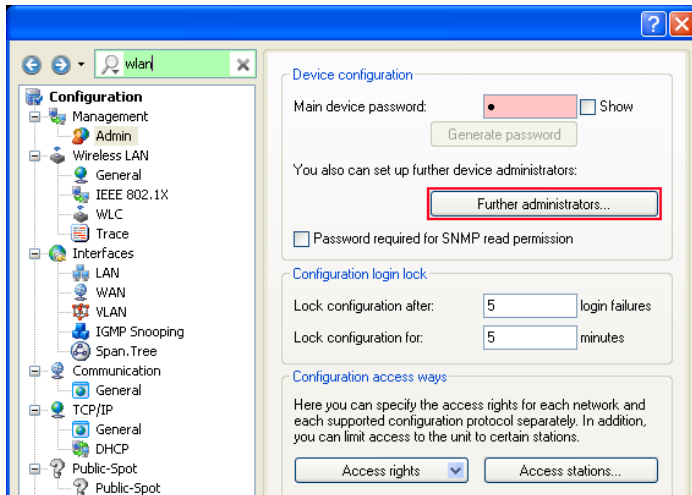


Figure 2: Searching in the configuration dialog of LANconfig using the QuickFinder

Select one of the areas in the configuration tree (e.g. 'WLAN/General') to display the corresponding search results framed in color in the configuration dialog:

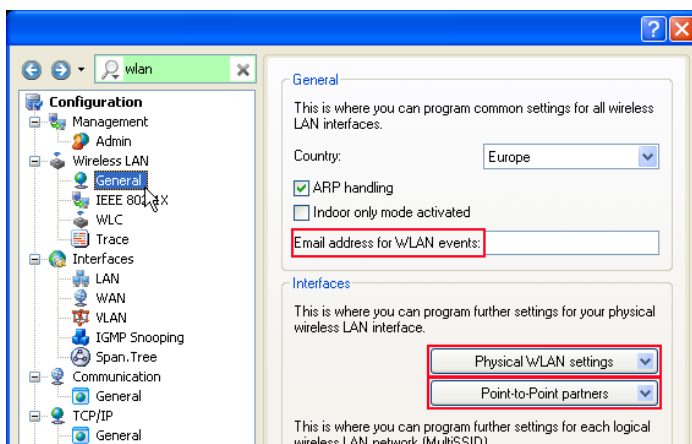


Figure 3: Selection of search results in QuickFinder

**Note:** LANconfig does not display the search hits in the firewall area in color in version 8.50.

Use the 'Forward' and 'Back' navigating buttons to the left of the search field to scroll to the dialogs you visited last:

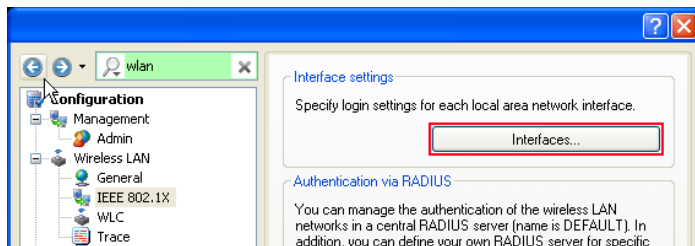


Figure 4: Navigating in the search results of the QuickFinder

To get faster access to the last 10 dialogs you visited, click on the arrow to the right of the 'Forward' button:

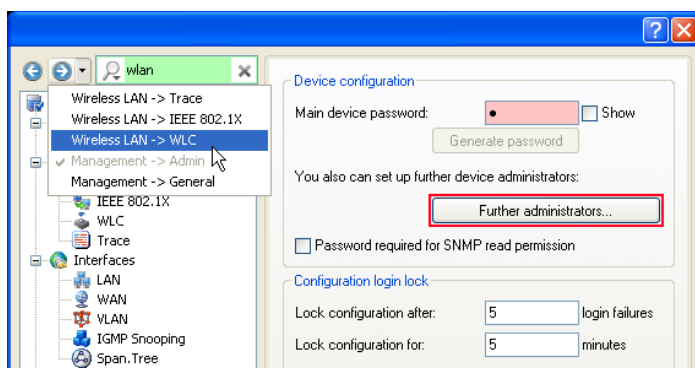


Figure 5: Fast access to the search results of the QuickFinder

Click the X to the right of the search field to delete the search and display all the entries in the configuration tree again. To optionally reduce the search results, select areas that you want LANconfig to include in the search. To do this, click the magnifying glass to the left of the search field and activate or deactivate the desired areas. Here you also specify whether the search highlights the hits in color or only reduces the configuration tree to the dialogs found:

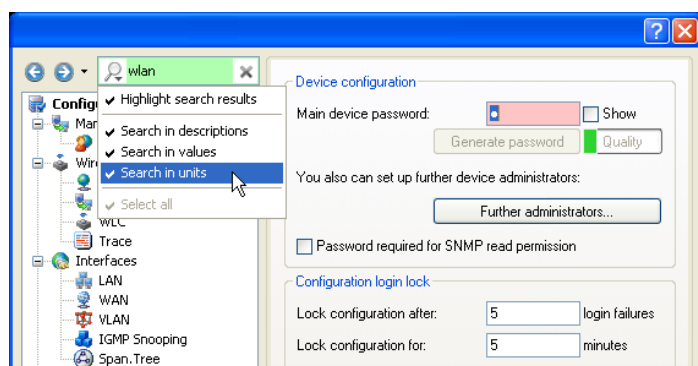


Figure 6: Selecting the search areas for QuickFinder

**Note:** When the configuration is closed, LANconfig deletes the setting for the search areas and the list of the last dialogs visited.

## 1.8.1 QuickFinder in the LANmonitor

Depending on the application, the LANmonitor shows multiple devices that could contain the search term. After the search is started, LANmonitor initially highlights the first find. Go to the next find using either the arrow buttons at the right side of the search window or with the key combination Ctrl+F3, or use the key combination Ctrl+Shift+F3 to go back to the previous find.

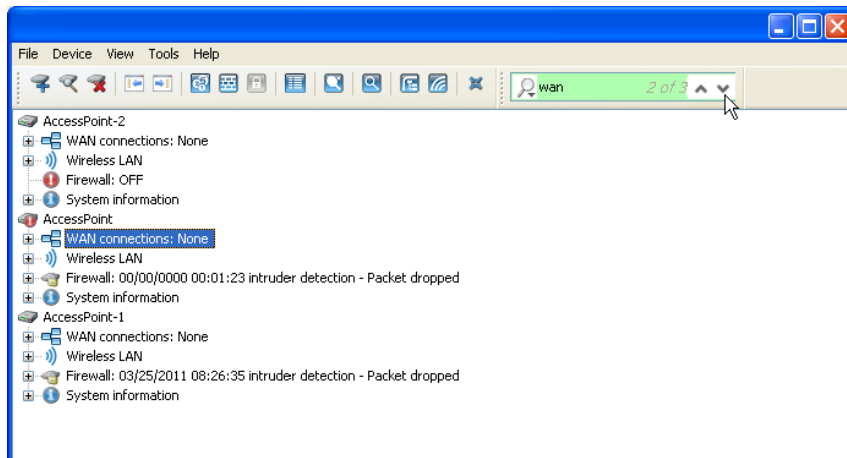


Figure 7: QuickFinder in the LANmonitor

## 1.8.2 QuickFinder in the WLANmonitor

The WLANmonitor includes both access points and WLAN clients. When you click on the magnifying glass on the left side of the search window, you open a context menu for selecting the scope of the search. Depending on the application, you select only the access points, only the clients, or all entries.

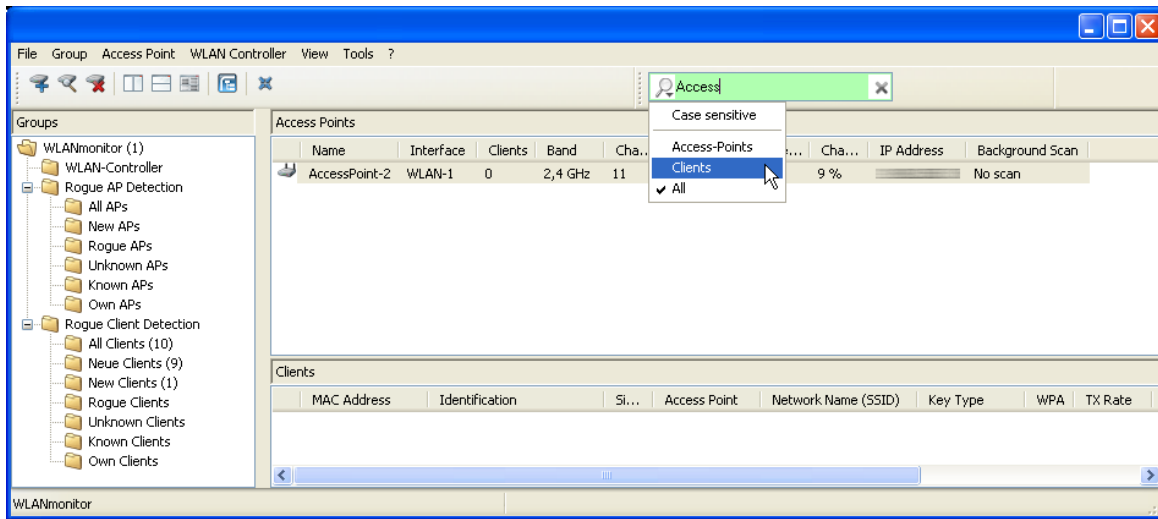


Figure 8: QuickFinder in the WLANmonitor

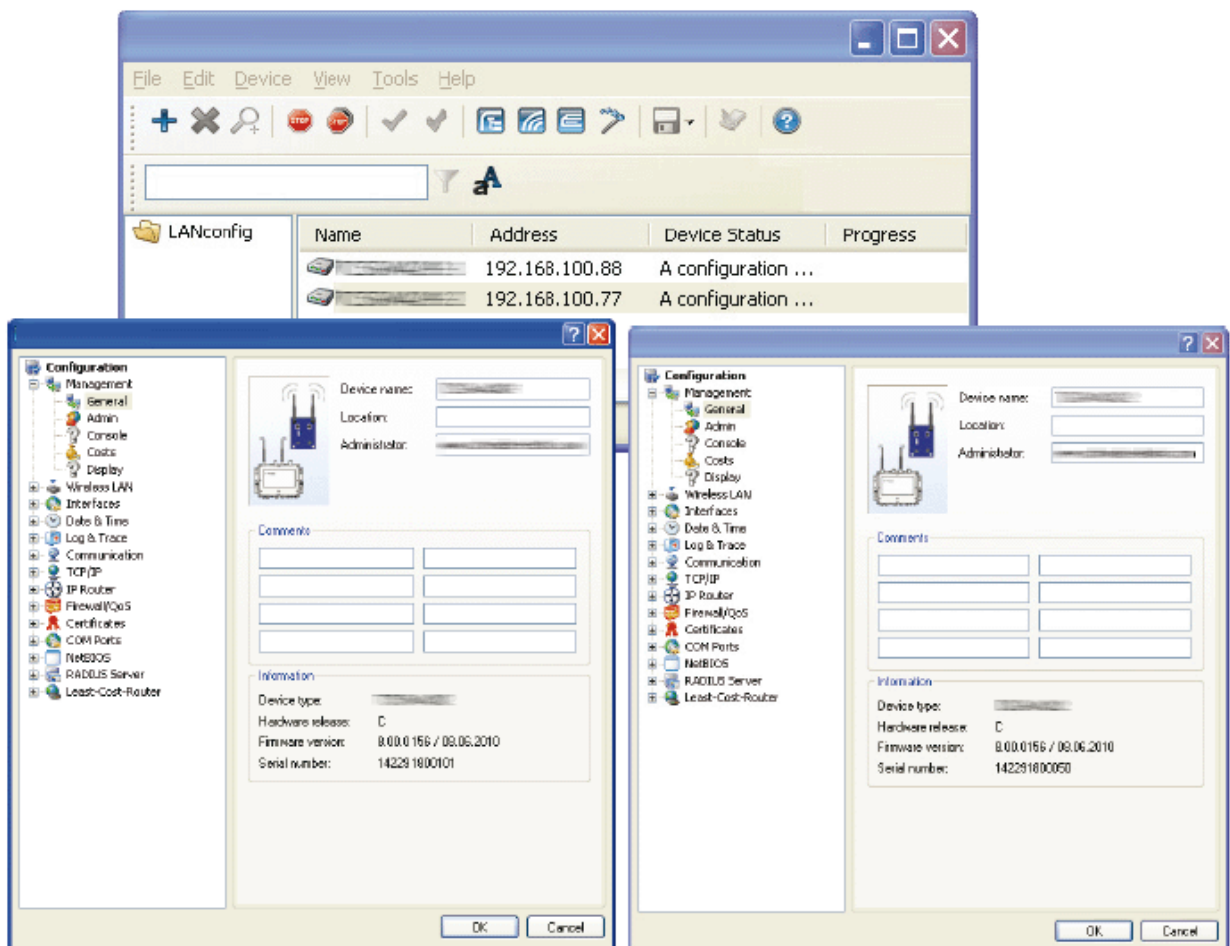
For example, if you have entered specific settings for your Internet provider in the configuration, by simply entering the name you can find all the positions in the configuration that relate to this provider. Specifically, the search includes the following areas:

- ▶ Entries in the configuration tree
- ▶ Designations for the areas (sections) in the individual configuration dialogs.
- ▶ Parameters
- ▶ Values of the parameters
- ▶ Explanatory texts in the dialogs
- ▶ Names of the tables
- ▶ Names of the table columns



## 1.9 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 additional configurations from the device list in LANconfig. All of the configurations can be processed in parallel.



**Note:** 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.

# 1.10 Password Protection for SNMP Read-Only Access

You can use a password to protect the read-only access to a Switch device via SNMP - e.g. with LANmonitor. This function uses the same user data that you use for the configuration access to the Switch device with LANconfig. When you have activated this function, enter the required user data before you access the device via SNMP.

## 1.10.1 Requiring a Password for SNMP Read-only Access

You can activate the password requirement for SNMP read-only access in the device configuration in LANconfig for that device. Do this in the dialog: Configuration Management Admin.

Device configuration

Main device password:   Show

Repeat:

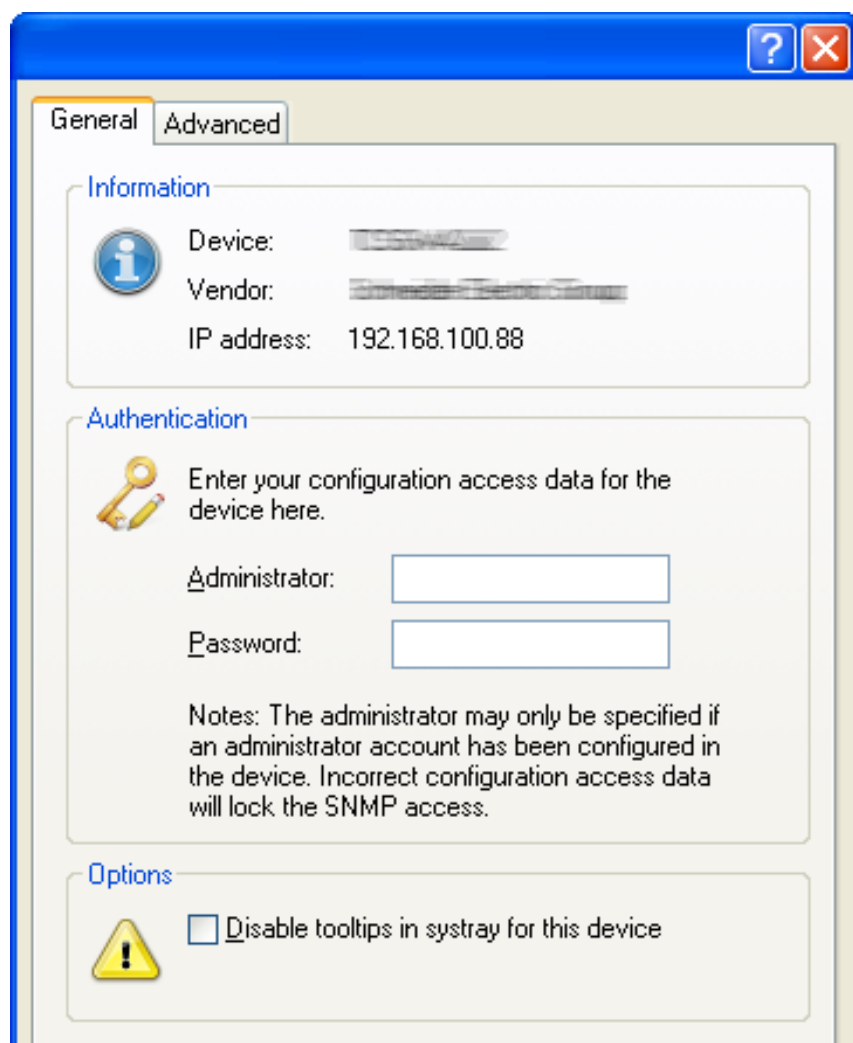
You also can set up further device administrators:

Password required for SNMP read permission

## 1.10.2 Configuring User Information for SNMP Access

Create the user data in LANmonitor separately for each device. Carry out the following steps:

- In LANmonitor, generate a list of found devices using the `File : Find Devices` command.
- Highlight a device, click the right mouse button, and select 'Options...' from the pop-up menu.
- In the 'Options' dialog, click the 'General' tab to display that dialog:



- Enter values for the 'Administrator' and 'Password' parameters.

The access rights available to the defined administrator depend upon the rights granted to that administrator in LANconfig or WEBconfig for the specific device. You can create an administrator profile, including password and function rights at the following location:

Configuration : Management : Admin :  
Further administrators...

# 1.11 Device-Specific Settings for Communication Protocols

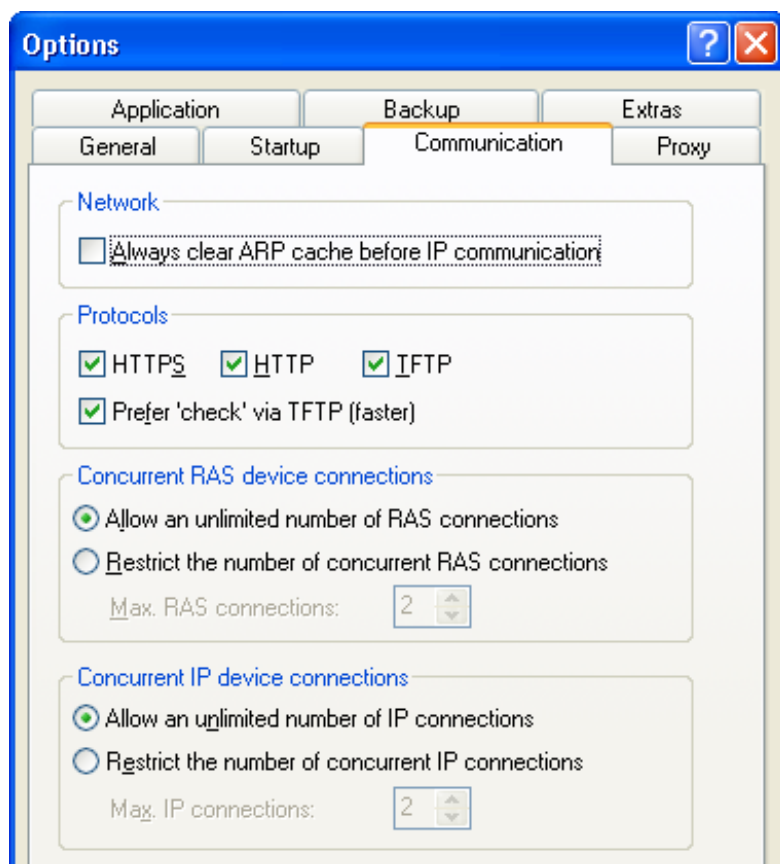
With LANconfig, device actions are typically conducted using the tftp protocol. Because this protocol has disadvantages compared to other protocols when transmitting large volumes of data, the protocols https and http can be used as alternatives.

The use of protocols can be set either globally for all devices managed by a LANconfig or specifically for each individual device. The global settings overwrite the local settings—thus when device-specific settings are selected, those settings take effect exclusively if they are also selected globally.

## 1.11.1 Global Settings for Communication Protocols

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

To access and configure global communication settings, open the following dialog: `Tools : Options : Communications:`



The following global communication settings can be configured:

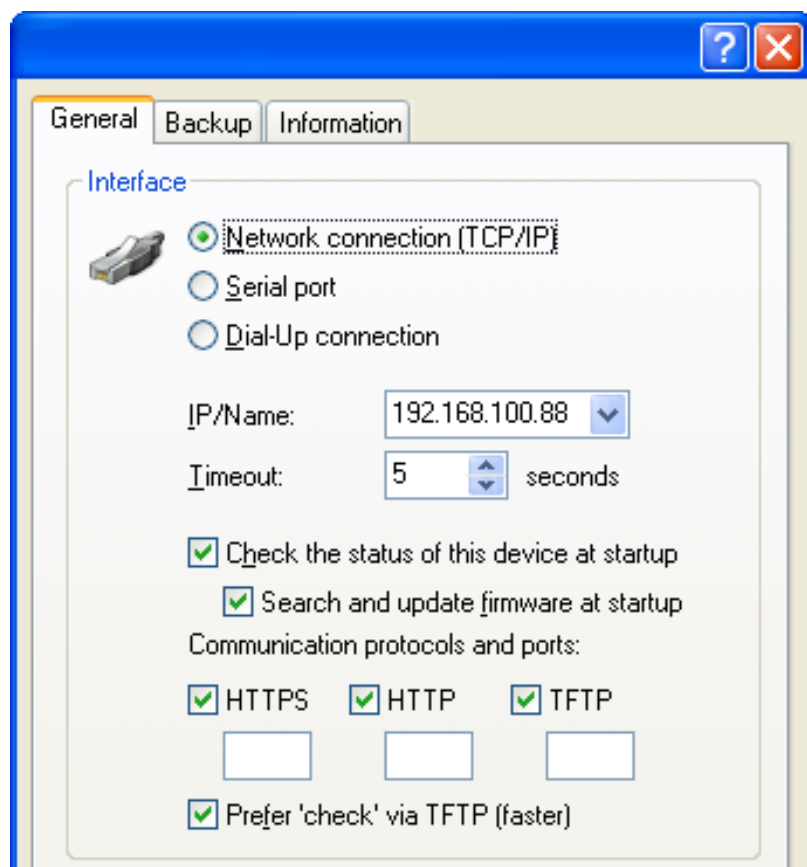
- ▶ **https, http, tftp:**  
When this is selected, the individual protocols are enabled for the operations firmware upload, configuration up/download, and script up/download. During these operations, LANconfig attempts to use these protocols in the order https, http and tftp. If the transfer cannot be performed using a selected protocol, then the next protocol is automatically attempted.
- ▶ **Prefer checks via tftp:**  
When checking the devices, 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 cannot be performed, then the protocols https, http and tftp are attempted in that order.

## 1.11.2 Device-Specific Settings for Communication Protocols

The device-specific settings are subordinate to the global communications settings. This lets you restrict a protocol centrally for the entire project. When multiple protocols are selected, LANconfig attempts to establish communications using protocols in the following sequence: https, http and tftp.

To access and configure device-specific communication settings for a selected device in LANconfig, follow these steps:

- In LANconfig, select a device in the list, click the right mouse button, and select 'Properties'.
- Open the 'General' tab of the 'Options' dialog:





The following device-specific communication settings can be configured:

- ▶ **https, http, tftp:**  
Select the communications protocols as described in the global settings. In the fields under the protocols, you can specify the port to be used for that protocol. The following default port settings are used if these fields are left blank, or if a value of '0' is entered:
  - https: port 443
  - http: port 80
  - tftp: port 69
- ▶ **Prefer checks via tftp:**  
Preferred checking via tftp as described in the global settings.

**Note:** For all specific communications settings, the global settings take priority. A protocol can therefore exclusively be used for operating a device when it is also activated in the global settings.



## **2 Connecting to the Device**

Before you can operate and manage the Switch device, set up a connection to the device. To do this, you have to identify the IP address of the device, among other things.

---

## 2.1 Identifying the specified IP address

The IP address initially assigned to the Switch device depends on where the device is connected when it is first switched on. Example:

- ▶ When the Switch device is physically connected with a private network of class C (e.g. 192.168.100.0/255.255.255.0), there are two possible scenarios:
  - The network contains an active DHCP (Dynamic Host Configuration Protocol) server. Then the Switch device behaves like a DHCP client and gets its IP address from the DHCP server.
  - The network does not contain a DHCP server, and none of the existing data network devices is a DHCP client. In this case, the IP addresses are assigned statically. The Switch device then takes over the general network address of the static devices (e.g. 192.168.100.x) and adds the value 254 as the fourth object. In this example, the Switch device would have the IP address “192.168.100.254”.

**Note:** In the above scenario, the Switch device is connected to a single configuration PC that has a static IP address. The device takes over the network address of the configuration PC and adds “254” as the fourth byte.

- ▶ When the Switch device in a network without a DHCP server is connected with other devices that are all acting as DHCP clients, the Switch device activates its own DHCP server and assigns IP addresses to all the devices, including itself. In this case, the Switch device assigns the general network address 172.23.56.x to all the devices, and the fourth byte 254 to itself. Then its IP address would be “172.23.56.254”.

**Note:** The above scenario also applies to devices that are connected with a single configuration PC that is configured as a DHCP client.

To simplify the first connection setup to the Switch device, connect the device to the configuration PC only.

---

## 2.2 Making the Initial Connection

The following section tells you how to set up the first connection to the Switch device. For this you require a configuration PC, the Switch device, a voltage source for the Switch device and an Ethernet cable.

Before you start, familiarize yourself with the following requirements:

- ▶ The configuration PC is connected to the Switch device by means of the Ethernet cable only. Do not set up any other data network connections to these devices.
- ▶ Carry out this procedure on one Switch device, not on multiple devices at the same time.
- ▶ The configuration PC is configured in such a way that it gets an IP address from the DHCP server.
- ▶ The factory settings of the Switch device are the standard parameters. To set up this basic configuration, press the reset button on the Switch before you start setting up the connection.

### 2.2.1 Connection Procedure

This is how you set up a connection between the configuration PC and the Switch device:

- Make sure that both devices are disconnected from the voltage source. Plug the Ethernet cable into the PC and the Switch device. Make sure that there are no other Ethernet connections to the devices.
- Connect the Switch device to the voltage source. Read section 2.11 “Connecting the Supply Voltage” in the “BAT Family Installation Guide”.

- When the Power LED and the LED to the right of it on the Switch device are flashing green or green/orange, hold down the reset button for five seconds with a pointed object (e.g. an opened paper clip or a small screwdriver) (see page 85). When the LEDs on the device are lit continuously in red, release the reset button.
- Once the LEDs on the Switch device are flashing green or green/orange again, switch on the PC. Within a few seconds, the BAT device assigns an IP address for networks of class C to the PC. The IP address begins with the bytes “172.23.56”.
- In order to see your computer’s IP address, open a command prompt window, type ‘ipconfig’, and push ‘Enter’. The window displays the IP address for the local area connection that you have just made, starting with 172.23.56. (Other IP addresses may be also displayed, but you are interested in just the one associated with this local area connection.)
- Open a web browser on your computer. In the address window of the browser, enter the first three octets of your computer’s IP address (172.23.56), and use 254 as the fourth octet (172.23.56.254).

**Note:**

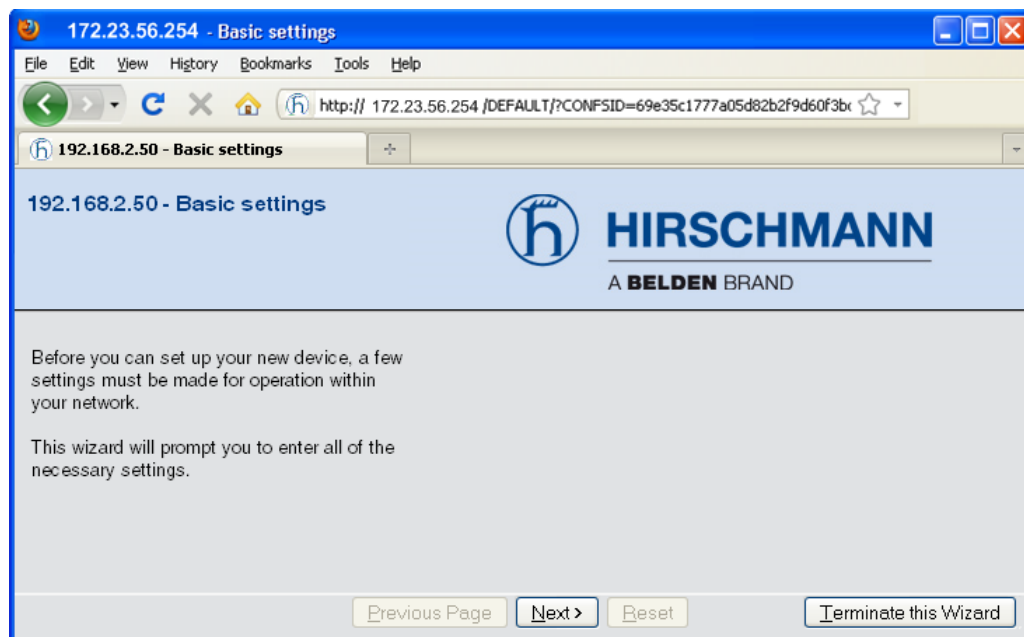
- ▶ The IP address that you use for the Switch device (172.23.56.254) is only used for the initialization of the device. During the device configuration, assign the BAT device either a new unique IP address, or configure the device so that when it is setting up a connection with the network, it gets an IP address from the server.
- ▶ If you configure multiple devices with the same IP address, it's possible that unforeseen functions will be triggered in the network.

 **WARNING****UNINTENDED EQUIPMENT OPERATION**

Establish and maintain a process for assigning unique IP addresses to all devices on the network.

**Failure to follow these instructions can result in death, serious injury, or equipment damage.**

The following page opens:



You are now connected with the first web page of the Switch device. You can configure the device as follows:

- ▶ using the device web pages, beginning with the first page of the setup wizard (above), or
- ▶ running the LANconfig software provided on the distribution CD.


**Note:** The IP address of the Switch device (with “254” as the last byte) is only used to initialize the device. During the device configuration, assign the Switch device either a new unique IP address, or configure the device so that when it is setting up a connection with the network, it gets an IP address from the server.






## 3 Upload Settings to the Device

As soon as a connection is set up to the new Switch device ([see page 43](#)), you have the option of loading pre-configured settings onto the device. These pre-configured settings can be found in the following form:

- ▶ as a configuration file (suffix “.lcf”):  
You either create this file yourself using LANconfig, or you transfer the existing settings from a Switch device using one of the following procedures:
  - ▶ with the LANconfig program: Select a device, then choose the following options: `Device : Configuration`  
`Management : Save as a file`
  - ▶ with the WEBconfig program: Navigate to a device, then choose the following options:  
 `File Management : Save Configuration`

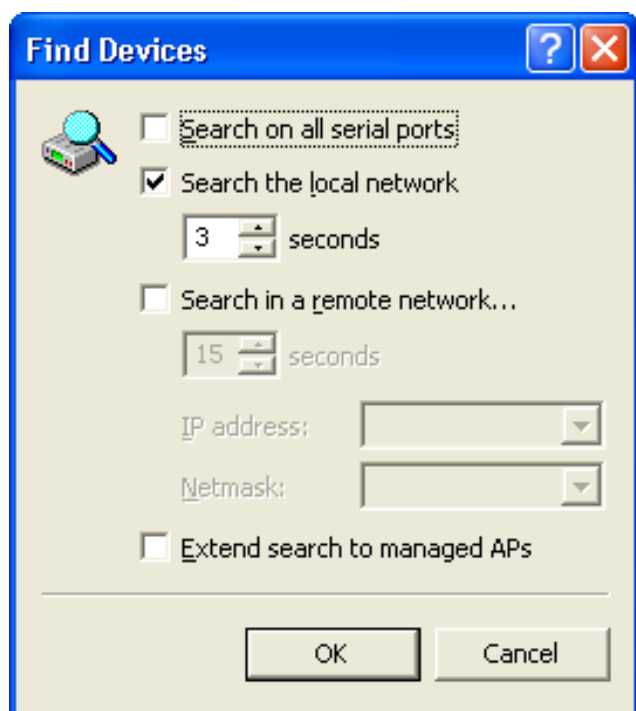
**Note:** You will find the instructions for creating, editing and saving configuration files in the BAT Configuration and Administration Guide.

- ▶ as a script file (suffix “.lcs”):  
You either create this file yourself using a text editor, or you load the existing settings from a Switch device using one of the following procedures:
  - ▶ with the LANconfig program: Select a device, then choose the following options: `Device : Configuration`  
`Management : Save as a script file`
  - ▶ with the WEBconfig program: Navigate to a device, then choose the following options:  
 `File Management : Save Configuration Script`

## 3.1 Uploading Settings in LANconfig

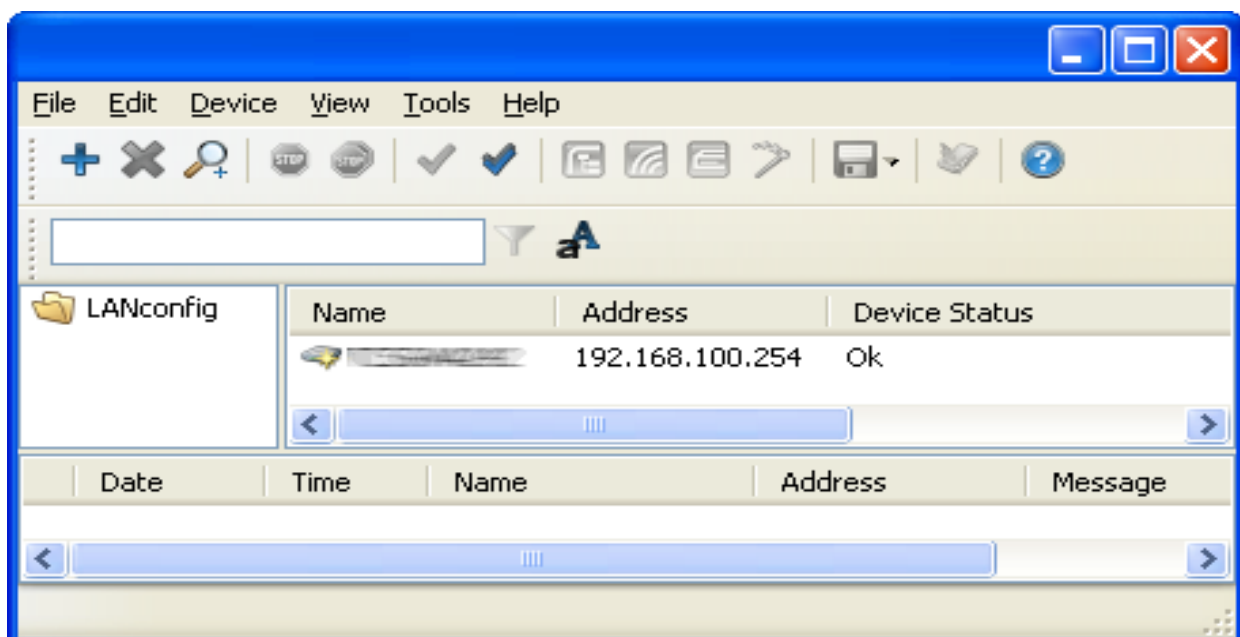
To upload a configuration or script file using the LANconfig software, follow these steps:

- Install and start-up the LANconfig software that is provided on the distribution CD.
- Find the Switch device using LANconfig. Select **File : Find Devices**. The “Find Devices” dialog opens:



- Click ‘OK’.

LANconfig searches for devices on the network, then displays the discovered device(s) in the LANconfig software:



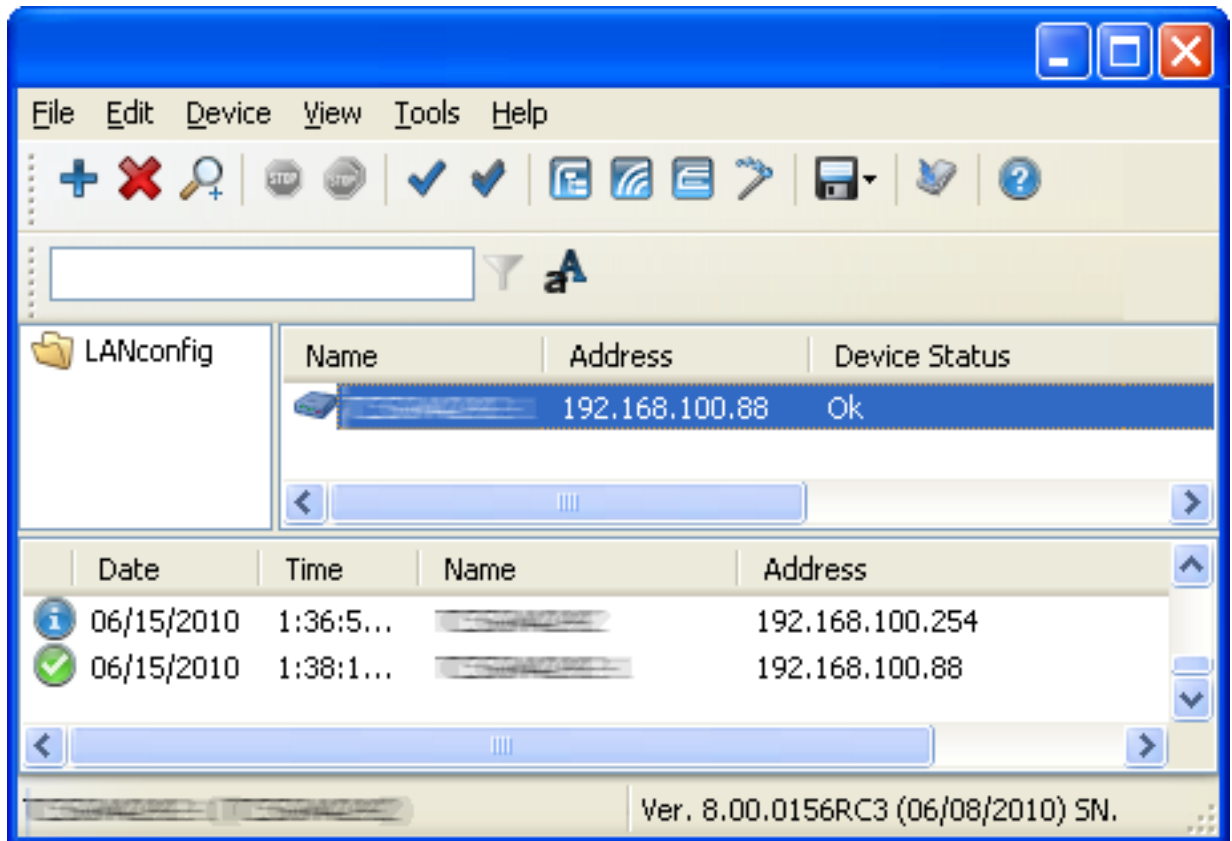
- If LANconfig starts the setup wizard, click 'Cancel' to end the wizard configuration process. If prompted, click 'Yes' to confirm the cancellation of the wizard and return to the LANconfig main window
  - In the list of devices found, select the device to which you want to transfer the settings.
  - With the target device selected, do one of the following:
    - ▶ To apply settings from a configuration file, select:  
Device : Configuration Management :  
Restore from File
    - ▶ To apply settings from a configuration script, select:  
Device : Configuration Management :  
Restore Script from File
- Note:** Select a configuration file or script that is pre-configured for the same device type and firmware version as the actual device you are configuring.
- If LANconfig asks for a password, input the password for the device.



**Note:** The default password is `private`. Do not enter a value in the 'Administrator' field.

- In the file selection dialog, navigate to and select the configuration file or script to apply to the selected device, then click 'Open'.

The LANconfig software applies the new settings and displays the following information when complete:



**Note:** The new settings include a different IP address. The device can no longer be reached using the original IP address.

## 3.2 Uploading Settings in WEBconfig

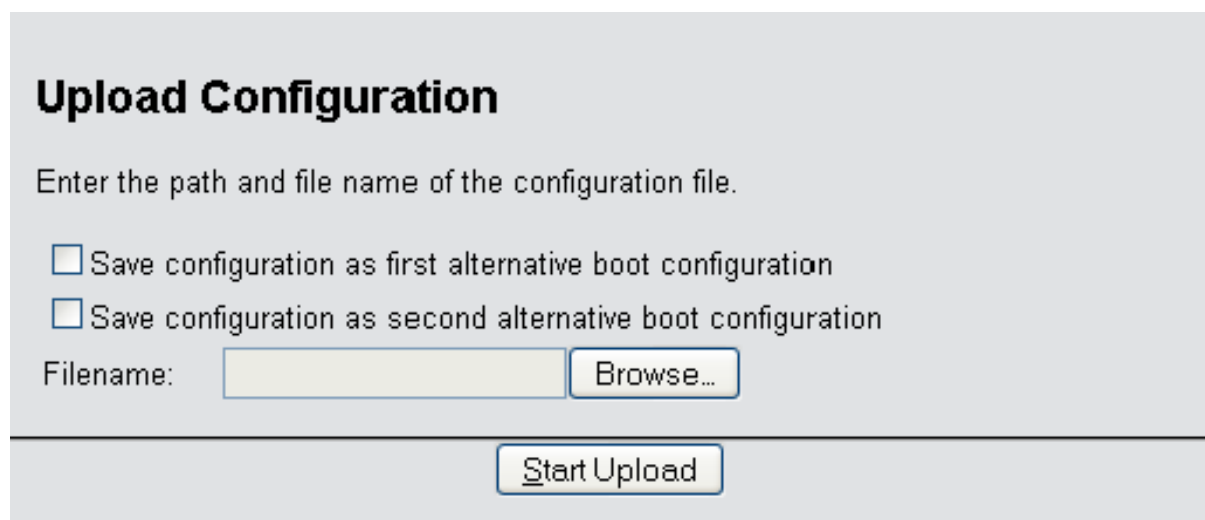
To upload a configuration or script file using WEBconfig, follow these steps:

Use WEBconfig to set up a first connection to the Switch device ([see page 45](#)).

▶ To upload a configuration file, select the following options:

File management : Upload Configuration

The following dialog opens:



**Upload Configuration**

Enter the path and file name of the configuration file.

Save configuration as first alternative boot configuration

Save configuration as second alternative boot configuration

Filename:

▶ To upload a script file, select:

File management : Execute Configuration Script

The following dialog opens:

---

Enter the path and file name of the script file.

Filename:

---

- Click the 'Browse' button, to open a 'File Upload' dialog.
- Navigate to and select the configuration or script file to execute, then click 'Open'.
- Click 'Start Upload'. When the upload successfully completes, WEBconfig displays the following dialog:

Upload successful.

---

**Note:** Remember that the new settings include a different IP address. The device can no longer be reached using the original IP address.





## **4 Working with Device Files**

## 4.1 Creating, Editing and Uploading Files

Both the LANconfig and the WEBconfig software let you work with configuration (.lcf) files and script (.lcs) files.

**Note:** You can upload a saved configuration file to a device that is the same type and with the same firmware version as defined in the configuration file.

### 4.1.1 Creating, Editing and Printing Files in LANconfig

LANconfig allows you to perform the following tasks:

- ▶ to create a new configuration file (.lcf) for the Switch device and save it on the configuration PC. For this you use the command `Edit : New Configuration File`
- ▶ to edit a saved configuration file on the PC. For this you use the command `Edit : Edit Configuration File`
- ▶ to open the setup wizard and edit a saved configuration file on the PC. For this you use the command `Edit : Wizard Configuration File`
- ▶ to print the selected file with the configuration settings. For this you use the command `Device : Configuration Management : Print`

## 4.1.2 Uploading and Downloading Device Files

Using either LANconfig or WEBconfig, you can:

- ▶ Download a device's configuration settings to an.lcf file on your configuration PC:  
Device : Configuration Management : Save as File  
■ File management : Save Configuration
- ▶ Upload a saved configuration (.lcf) file to a selected device:  
Device : Configuration Management : Restore from File  
■ File management : Save Configuration
- ▶ Download a device's settings to an script (.lcs) file on your configuration PC:  
Device : Configuration Management :  
Save Script as File  
■ File management : Save Configuration Script
- ▶ Upload a saved script (.lcs) file to a selected device:  
Device : Configuration Management :  
Restore Script from File  
■ File management : Execute Configuration Script
- ▶ Download a device certificate to a file on your configuration PC:  
Device : Configuration Management :  
Save Certificate as File  
■ File management : Download Certificate or File
- ▶ Upload a saved certificate file to a selected device:  
Device : Configuration Management :  
Upload Certificate from File  
■ File management : Upload Certificate or File

---

## 4.2 Automatic Backup of Files in LANconfig

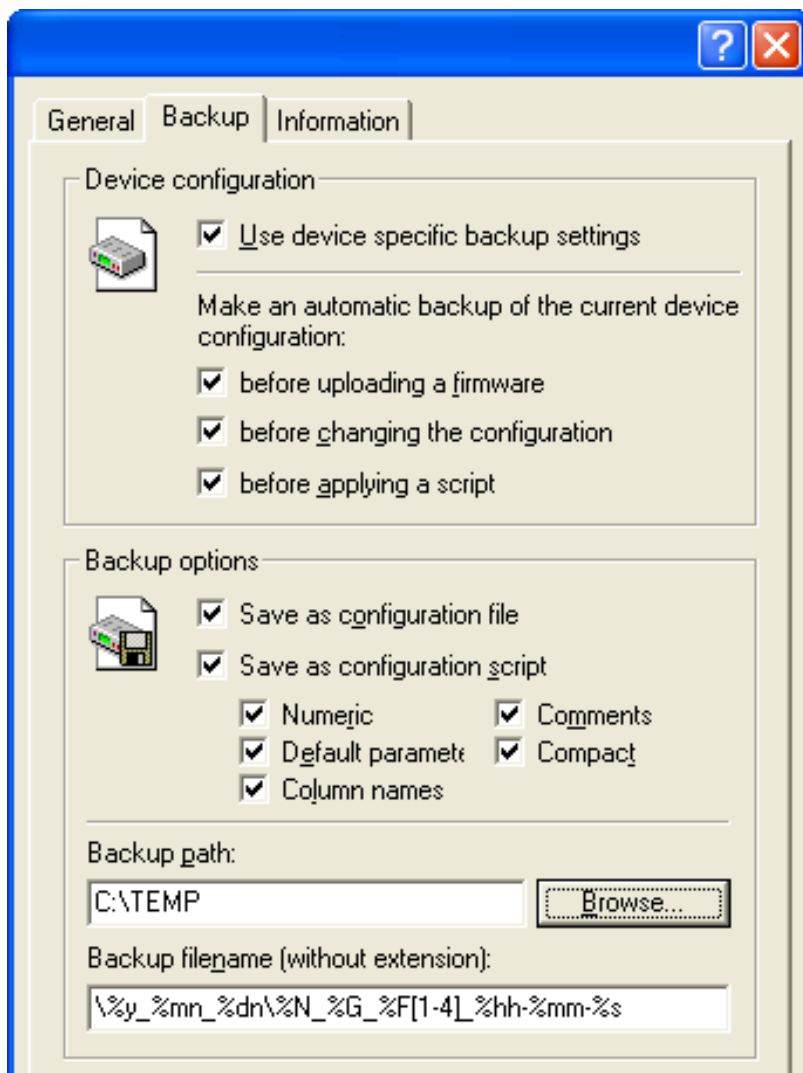
LANconfig can automatically save backups of the current configuration prior to changes in firmware or configuration. LANconfig can be configured to perform this task either globally for all devices, or for selected devices.

To configure global automatic configuration file backup for all devices:

- In LANconfig, select **Tools** : **Options**, then click the 'Backup' tab to open that dialog.

To configure automatic configuration file backup for a specific devices:

- In LANconfig, select the specific device to configure, and click the right mouse button.
- From the pop-up menu select **Properties**, then click the 'Backup' tab to open the following dialog:



Select the desired automatic file backup settings in these dialogs, including the following:

- ▶ Select 'Use device-specific backup settings' (in the device-specific dialog) and the automatic backup settings made in the device configuration will override the global settings.
- ▶ Select one or more events, prior to which the configuration is to be saved:
  - firmware upload
  - configuration change
  - script execution
- ▶ Select the formats in which the configuration is to be saved (configuration file, script - possibly with options).
  - configuration file
  - configuration script, specifying options

- ▶ Specify the backup path, i.e., the directory in which the configuration is to be saved.
- ▶ Indicate 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 for the 'Backup filename' parameter for further information on configuring this parameter.

## **5 Managing Device Configurations with an AutoConfiguration Adapter**

If you are using an AutoConfiguration Adapter (ACA), WEBconfig allows you to save the device configurations on this external storage medium. In the case of a reboot, you have the option of transferring the configuration settings in the ACA manually or automatically to unconfigured devices.

An ACA has the following advantages:

- ▶ If the device needs to be replaced, you have the option of assigning the previous configuration to the replacement device to have it ready for operation quickly.
- ▶ When you are setting up multiple devices of the same type, the ACA simplifies the first configuration.

You connect the ACA to the serial interface of the Switch device.

## 5.1 Manually Transferring Device Settings to the ACA

Before you can transfer a configuration from the ACA to a device, you need to save that configuration to the ACA. A configuration can be saved in either of two different file types:

- ▶ **Configuration:** A full configuration file in the format \*.lcf is transferred to the ACA. This configuration contains settings for a specific device—e.g. the name or site of the device.
- ▶ **Script:** A script file in the format \*.lcs is transferred to the ACA. A script can contain, in contrast to a configuration file, certain parts of a configuration. Information which depends on the device—e.g. name or site of the device—can be managed through variables.

To transfer device settings to a ACA, follow these steps:

- Connect the ACA to the serial interface of the Switch device.
- Use WEBconfig to login to the embedded web pages of the source device.
- Call up the following command in WEBconfig:

```
File management : Upload file to ACA
```

The following dialog opens:



File-Information

Filetype:	Configuration
Version:	0
Timestamp:	10/30/2009 11:34:15
File-Length (bytes):	8084
ACA-Filename:	Operations Device
Valid:	Yes

Here a configuration can be uploaded to the ACA.

Configuration file type:

Configuration  
 Script

ACA-Filename:

Local Filename:

Here the current device configuration can be saved to the ACA.

Configuration file type:

Configuration  
 Script

ACA-Filename:

- ▶ If you want to transfer a configuration file or a script from an external storage medium to the ACA:
  - Select a file type: configuration or script
  - Enter a meaningful 'ACA Filename'
  - Click 'Browse' and navigate to and select a configuration file.

- Click 'Start Upload' to copy the selected file to the ACA.
- ▶ If you want to transfer the current configuration of the device to the ACA:
  - Select a file type: configuration or script
  - Enter a meaningful 'ACA Filename'
  - Click 'Browse' and navigate to and select a configuration file.
  - Click 'Save current configuration' to copy the device's present configuration settings to the ACA.

**Note:** During the reading process, the Power LED flashes yellow.

## 5.2 Automatically Uploading Settings from the ACA to the Device

This is how you automatically upload the configuration settings from the ACA to the Switch device:

- Connect the ACA to the serial interface of the Switch device.
- Depending on the configuration status of the device, execute one of the following steps:
  - If the device has never been configured before, switch on the device.
  - If the device has already been configured, switch on the device and set up the factory settings.

During a reboot, an unconfigured device detects the connected ACA and automatically takes over the configuration settings from the ACA. During the reading process, the Power LED flashes yellow.

**Note:** If an incorrect or unsuitable configuration is stored on the ACA (e.g. if the configuration on the ACA belongs to another device type or another firmware), it is no longer possible to access the device via a LAN or WLAN interface. In this case, you transfer the correct configuration to the device via the serial interface.

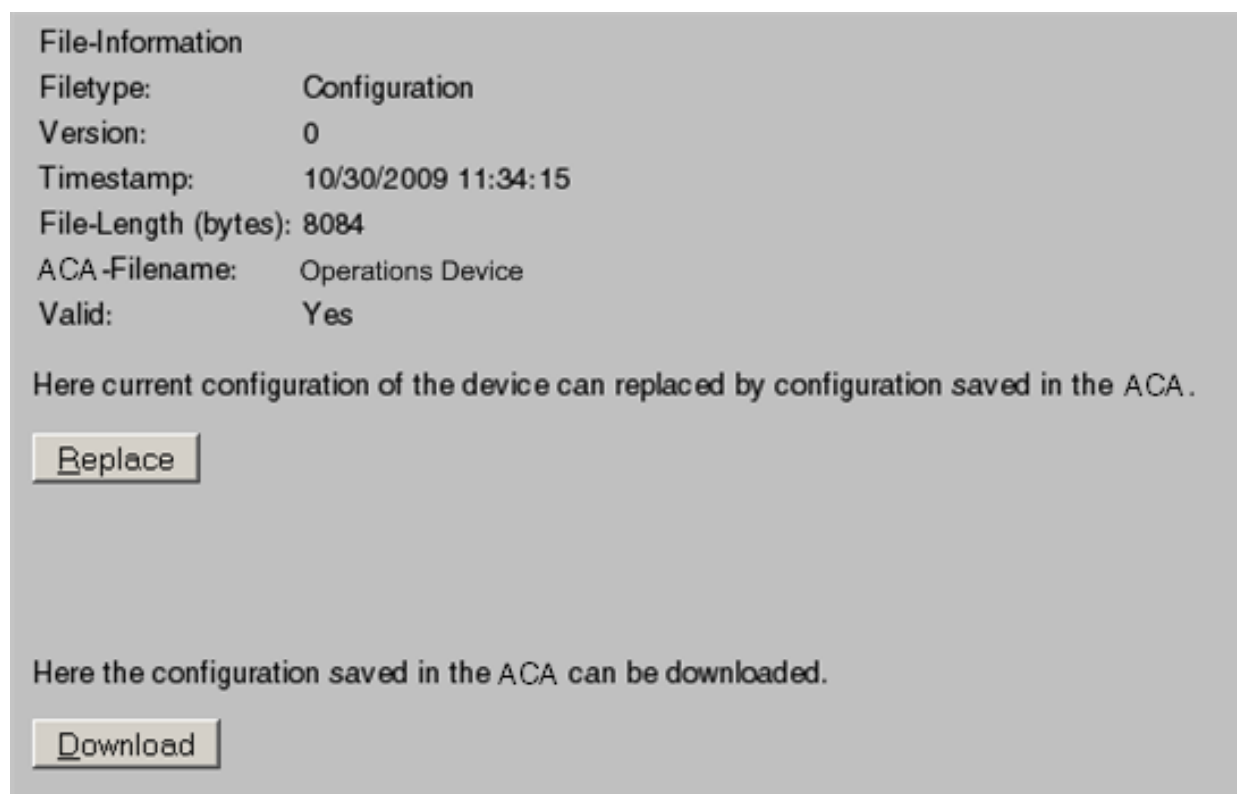
## 5.3 Manually Upload Settings from an ACA to the Device

To manually transfer device settings from a ACA to a device, follow these steps:

- Connect the ACA to the serial interface of the target Switch device.
- Use WEBconfig to login to the embedded web pages of the target device.
- Call up the following command in WEBconfig:

```
File management : Download a file from ACA
```

The following dialog opens:



- Indicate if the current configuration from ACA should be transferred to the device or should be saved to an external storage medium:
  - If the current configuration of the device should be replaced with the configuration in the ACA, click 'Replace'.
  - If a configuration or script from the ACA should be transferred to an external storage medium choose 'Download'.

**Note:** After the transmission of the configuration from ACA to the device, the new configuration is immediately active. In case of an incorrect or inappropriate configuration on the ACA, the device may no longer be accessible over a LAN or WLAN interface. In this case, either:

- use the serial interface to apply an appropriate configuration, or
- perform a system reset and restart the configuration process.



## 6 Rollout Wizard

In complex scenarios with multiple Switch devices at various locations, it is possible that there is no qualified technician at the location where the Switch device is being used who can perform the installation and the configuration. You can already carry out a significant part of the configuration in advance. Then the employees on site only have to set a few location-specific parameters.

The rollout wizard enables the on-site employees to perform these final steps with a browser. After the rollout wizard has been run, the device is either ready for operation or it can automatically get the missing configuration data from a central data storage. You will find the parameters for the configuration in WEBconfig at the following path:

 Hirschmann Menu Tree : Setup : HTTP : Rollout Wizard

## 6.1 Settings for the Rollout Wizard

- ▶ **Operating:**  
Switches the rollout wizard on or off. After you have switched it on, you will find the wizard on the start page of WEBconfig.
  - Possible values: Yes / No
  - Default: No
- ▶ **Title:**  
Name for the rollout wizard that is displayed on the start page of WEBconfig.
  - Possible values: Maximum 64 alphanumeric characters
  - Default: Rollout
- ▶ **Display Connection Status for:**  
This setting allows you to display the connection status of a DSL connection.



---

## 6.2 Variables

A maximum of ten variables can be defined with Index, Indent, Title, Type, Min. Value, Max. Value and Default Value.

- ▶ **Index:**  
Index for the variable. The Rollout Wizard displays the variables in ascending order.
  - Possible values: 1 to 4294967295
  - Default: 0
- ▶ **Indent:**  
Unique identifier of variables that are referenced during the execution of actions. Identifiers are not required for fields that are not used by users to enter their data (e.g. label).
  - Possible values: Maximum 64 alphanumerical characters
  - Default: blank
- ▶ **Title:**  
Name of the variable as displayed by the Rollout Wizard in WEBconfig.
  - Possible values: Maximum 64 alphanumerical characters
  - Default: blank
- ▶ **Type:**  
Name of the variable as displayed by the Rollout Wizard in WEBconfig. Possible values include the following:
  - **Label:** Text that is displayed to provide explanations of the other variables. Min. Value and Max. Value are not significant for these entries.
  - **Integer:** Allows the entry of a positive integer number between 0 and 4294967295. By entering the Min. Value and Max. Value, the range of entries can be limited. Also, a default value can be defined. This default value must be between the Min. and Max. Values.
  - **String:** Enables text to be entered. By entering the Min. Value and Max. Value, the length of the string can be limited. Also, a default value can be defined. If this default text is longer than the maximum length, it will be truncated.
  - **Password:** displayed while being entered. Repeat entering the password. The Rollout Wizard will execute no actions if the passwords are different.

- Checkmark: Simple option that can be switched on or off. Checkmarks are activated as standard if the default value is other than empty and the action executed accordingly.
- Default: Label
- ▶ Min. Value:  
Minimum value for the current variable (if type = integer) or minimum number of characters (if type = String or Password).
  - Possible values: 0 to 4294967295
  - Default: 0
- ▶ Max. Value:  
Maximum value for the current variable (if type = integer) or maximum number of characters (if type = String or Password).
  - Possible values: 0 to 4294967295
  - Default: 0
- ▶ Default value:  
Default value of the current variable.
  - Possible values: Maximum 64 alphanumerical characters
  - Default: blank

## 6.3 Actions Executed by the Rollout Wizard

A maximum of 19 definitions (with index and action) can be executed by the Rollout Wizard once the user data has been entered.

- ▶ **Index:**  
Index for the action. The Rollout Wizard executes the actions in ascending order.
  - Possible values: 1 to 4294967295
  - Default: 0
- ▶ **Action:**  
Action to be executed by the Rollout Wizard once the user data has been entered.
  - Possible values: Similar to Cron commands, actions are entered with the syntax [Protocol:]Argument. If no protocol is entered, 'exec.' is applied.
  - exec: Executes any command in the same way it is used in Telnet to configure a Switch. The following example sets the name of the device to “MyWLANDevice”:  

```
exec: set /setup/name MyWLANDevice
```
  - mailto: Enables an e-mail to be sent upon entry of the address, subject and body text, for example:  

```
mailto:admin@mywlandevice.de?subject=Rollout?body=WLANDevice setup completed
```

To make use of the mail function, set up an simple mail transfer protocol (SMTP) account in the device.
  - https and http: Enables a Web site to be accessed, for example to carry out an action:  
(`<https:|http:>//[user[:pass]@]hostname[:port]/...`)
  - Variables in the actions: When actions are executed, the values as defined with the Rollout Wizard can be referenced. The variable's identifier is used for the action with a leading percent character. Enclose the identifier in curly brackets if other alphanumeric characters are included in the action. The following example sets the name of the device to the format “Site (branch)”, if the location of the device is being queried as a variable with the identifier “Location”:

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

For variables of the type Integer or String, the value as entered by the user is used. In the case of variables of the type Checkmark, “1” (switched on) or “0” (switched off) is used. If the expression for the action contains spaces, enclose the expression in quotation marks.

- Default: blank

---

## 6.4 Actions for Managing the Rollout Wizard

- ▶ **Renumber variables / Renumber actions:**  
As explained above, variables and actions are displayed or processed in the order of their index. Occasionally, variables or actions with neighboring index numbers require a new entry to be entered between them. The indices can then be automatically renumbered with a specified interval between them.

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



# **7 Configuring a Device without an IP Connection**

## 7.1 Introducing the LANCOM Layer 2 Management Protocol

An IP connection between the configuration PC and the Switch device is the prerequisite for configuring the Switch device via LANconfig, WEBconfig or Telnet. If the TCP/IP or VLAN settings of the device are configured unclearly or are damaged, it may be that it is no longer possible to set up an IP connection, and that the device cannot be configured in this way.

In this case you can either access the device via the serial configuration interface or reset the device to the factory settings. For both of these approaches, you must physically access the device. However, this is not always possible via remote connections or for integrated systems, and it can mean a considerable amount of work for larger systems.

With the LANCOM Layer 2 Management Protocol (LL2M), you can configure a device without an IP connection. For a configuration with this protocol, you require a Layer 2 connection either directly via Ethernet or indirectly via Layer 2 switches. LL2M connections are possible via LAN or WLAN, but not via the WAN. LL2M connections are secured by means of a password and are protected from replay attacks.

LL2M sets up a client-server structure for this purpose: The LL2M client (a Switch) sends requests or commands to the LL2M server, which replies to the requests or executes the commands. The LL2M client is executed via the command line. The LL2M server is usually only activated for a short time after the device is switched on. In this time frame, the administrator has the option of using the LL2M client to make changes to the configuration of the device with the LL2M server.



## 7.2 Configuring the LL2M Server

The LL2M server can be configured using WEBconfig at:

 Hirschmann Menu Tree : Setup : Config : LL2M

The following parameters can be configured for the server:

- ▶ **Operating:**  
Enables/disables the LL2M server. An LL2M client can contact an enabled LL2M server for the duration of the time limit following device boot/power-on. Values include: Yes (default), No.
- ▶ **Time Limit:**  
Defines the period in seconds during which an enabled LL2M server can be contacted by an LL2M client after device boot/power-on. The LL2M server is disabled automatically after expiration of the time limit. Values include 0 to 4294967295. Default = 0 seconds.

**Note:** The value 0 disables the time limit. The LL2M server stays permanently enabled in this state.

## 7.3 LL2M Client Commands

For every LL2M command an encrypted tunnel is set up that helps secure the login information transferred during the transmission. To use the integrated LL2M client, start a Telnet session on a Switch device that has local access to the LL2M server via the available physical medium (LAN, WLAN). In this console session you can use the following commands to contact the LL2M server.

**Note:** You need root rights on the LL2M server to execute the commands on the LL2M client.

► **LL2Mdetect:**

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

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

**Note:** If you do not specify a restriction for MAC addresses, the detect command is sent as a Multicast (or optionally as a Broadcast) to all LL2M-compatible devices. To contact groups of MAC addresses, you can insert \* or x as a placeholder for individual MAC address positions, e.g. “00-a0-57-xx-xx-xx” for all Switch MAC addresses.

- `-t <device type>`: Restricts the command to only those devices of the corresponding hardware type.
- `-r <hardware release>`: Restricts the command to only those devices with the corresponding hardware release.
- `-f <version>`: Restricts the command to only those devices with the corresponding firmware version.
- `-s <serial number>`: Restricts the command to only those devices with the corresponding serial number.

- `-b`: Sends the LL2Mdetect request as a Broadcast and not as a Multicast.
- `-v <VLAN ID>`: Sends the LL2Mdetect request only in the specified VLAN. If no VLAN ID is specified, the VLAN ID of the first defined IP network is used.

Example:

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

The response from the LL2M server contains the following information:

- Name of the device
- Device type
- Serial number
- MAC address
- Hardware release
- Firmware version with date

► **LL2Mexec:**

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

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

The following parameter allows you to restrict the LL2Mexec command:

- `-v <VLAN ID>`: Sends the LL2Mexec command only in the specified VLAN. If no VLAN ID is specified, the VLAN ID of the first defined IP network is used.

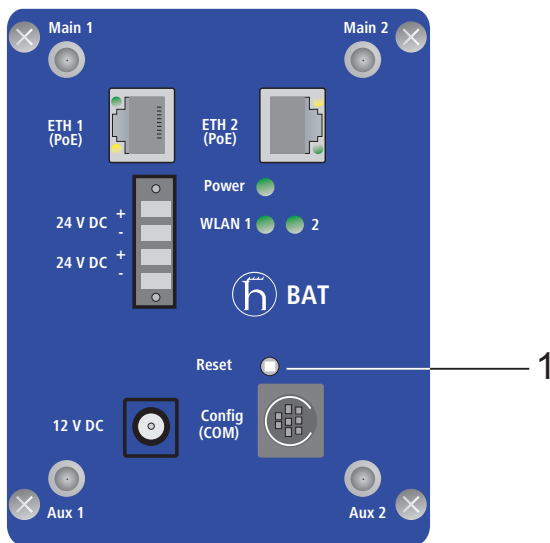
Example:

- `ll2mexec root@00a057010203 set name MyDevice`: This command logs the LL2M client on as the “root” on the LL2M server with the MAC address “00a057010203”. The user enters the password in the console session. Then the LL2M client sets the name of the remote device to the value “MyDevice”.



## 8 Resetting and Re-Starting the Device

The Switch device has a reset button.



---

1: Reset button

---

---

## 8.1 Default Reset Behavior

The reset button offers two basic functions, which are activated by holding down the Reset button for different lengths of time:

- ▶ **Restart:** Restarts the device and loads the current configuration settings. To restart the device, press the reset button only briefly.
- ▶ **Reset:** Resets the device to the factory settings. Press the reset button for around 5 seconds, or until the LEDs light up red. When you release the button, the device activates the factory settings (state on delivery).

**Note:** Create and store a copy of the current device configuration before pressing the reset button. After the button is pressed and held down for about 5 seconds, the existing configuration settings will be discarded and replaced by the factory default settings.



### **WARNING**

#### **LOSS OF CONFIGURATION DATA**

Never press the reset button when the access point is operating.

**Failure to follow these instructions can result in death, serious injury, or equipment damage.**

**Note:** Save the current configuration of the device before the reset. After a hard reset, the device re-starts in the non-configured state, and all settings are lost.

## 8.2 Disabling the Reset Button

In some applications, you may want to disable—or limit the effect of pressing—the Reset button. This can be accomplished by modifying the behavior of this button in the WEBconfig software at the following location:

```
Hirschmann Menu Tree : Setup : Config : Reset-  
button
```

The settings for this button include:

- ▶ **ignore:**  
Disables the Reset button on the device.
- ▶ **boot-only:**  
Pressing the Reset button causes the device to re-start, but does not reset the device configuration to its default settings.
- ▶ **reset-or-boot:**  
Pressing the Reset button causes the device to re-start and resets the device configuration to its default settings. This is the default setting.

### Note:

- ▶ The settings 'ignore' and 'boot-only' disable the ability of the Reset button to restore the factory default device settings. If the device password is lost, you will be unable to access and reset the device configuration over the LAN or WLAN interfaces. In this case, use the serial communication interface to upload a new firmware version to the device, and thereby reset the device to its factory settings.
- ▶ The WLAN encryption settings of the device will be lost in case of a reset and the standard WAP key comes into effect again. The wireless configuration of a device with WLAN interface will succeed exclusively after a reset, if the standard WAP key is programmed into the WLAN adapter.





## 9 Updating Firmware

Always use the latest firmware version for your Switch device. Visit the Hirschmann website regularly ([www.beldensolutions.com](http://www.beldensolutions.com)) to check the availability of firmware updates and download the latest firmware versions.

**Note:** Save all the versions of the device firmware in the same folder, which serves as your firmware archive.

The Switch device allows you to update the firmware while also saving the previous firmware version on the device. If necessary, you can reinstall the previous firmware version. If the new firmware has not been installed successfully, the device automatically activates the previous version.

This chapter shows you how to install the new firmware successfully using the following tools and procedures:

- ▶ LANconfig
- ▶ WEBconfig (embedded web pages)
- ▶ Terminal program (e.g. command line interface)
- ▶ tftp

---

## 9.1 How FirmSafe Works

With FirmSafe, firmware is overwritten and saved in the device as a backup, limiting the effects of a power blackout or disconnection while installing the firmware.

Of the two firmware versions saved in the device, one can be active. The current firmware version is retained when you load a new firmware version. You can decide which firmware will be activated after the upload:

- ▶ 'Immediate': Loads the new firmware and activates it immediately. The following situations can result:
  - The new firmware is loaded successfully and works as desired.
  - The device no longer responds after loading the new firmware. If the upload process cannot be completed, the device automatically reactivates the previous firmware version and reboots the device.
- ▶ Login: The firmware is uploaded and immediately booted.
  - In contrast to the 'Immediate' option, the device waits for the adjusted FirmSafe timeout, which can be set as follows:
    - using WEBconfig at:  
Hirschmann menu tree : Firmware : Timeout-firmsafe
    - using Telnet with 'Firmware/Timeout-firmsafe'When this login attempt is successful, the new firmware is activated.
  - If the device no longer responds or it is impossible to log in, it automatically loads the previous firmware version and reboots the device.
- ▶ 'Manual': With this 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. Activate the new firmware as follows:
  - using LANconfig, Device : Firmware Management : Activate Firmware running in Test Mode,
  - using Telnet at '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  
Hirschmann menu tree : ;Firmware.

The method for the firmware upload can be adjusted as follows:

- using WEBconfig at Hirschmann menu tree : Firmware Mode  
firmsafe
- using Telnet under 'firmware/timeout firmsafe'
- using LANconfig, select the method when selecting the new firmware file.

**Note:** You can upload a second firmware version if the device has enough memory for two versions. Current firmware versions may use more than half of the available memory.

## 9.2 How to Load New Firmware

There are four methods to perform a firmware upload:

- ▶ LANconfig
- ▶ WEBconfig
- ▶ Terminal program
- ▶ tftp

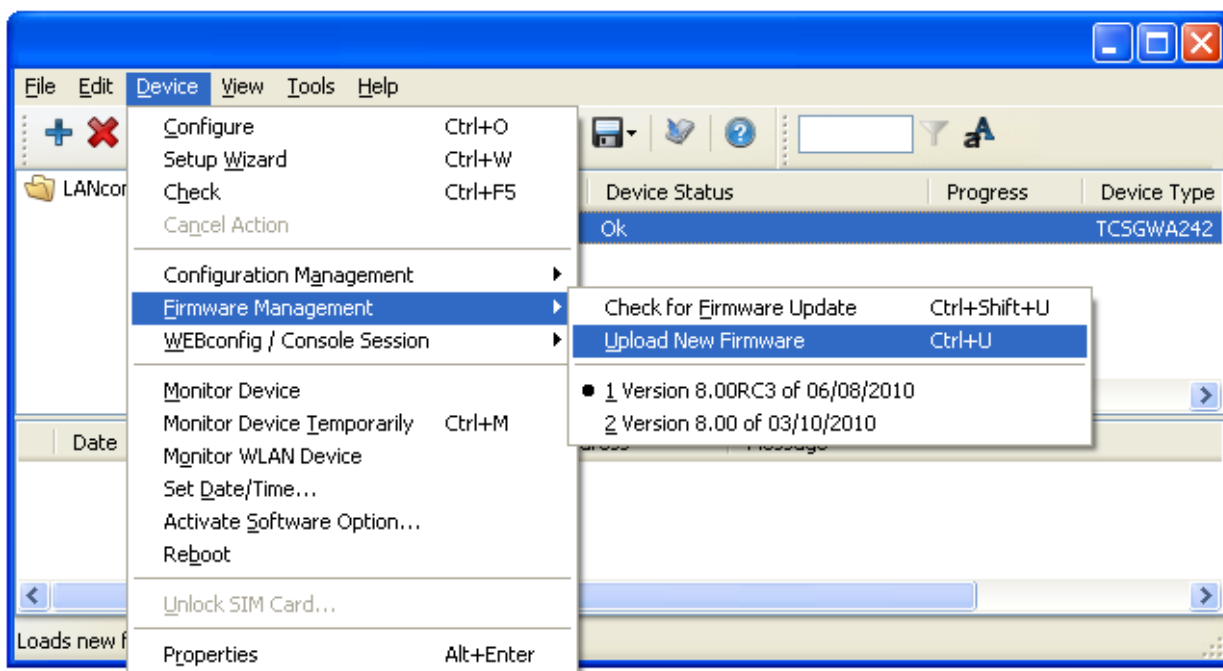
Before uploading, save the configuration and a version of the current firmware.

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.

### 9.2.1 LANconfig

To upload new firmware using LANconfig, follow these steps:

- Highlight the desired device in the selection list, then select:  
Device : Firmware Management : Upload New Firmware.



A file selection dialog opens.

- In the file selection dialog, select the new firmware file.
  - ▶ Optionally, you can select 'After upload, start the new firmware in test mode', and specify a time, in minutes, for the duration of test mode.
- Click **Open** to apply the selected firmware.

## 9.2.2 WEBconfig

Start WEBconfig in your web browser and follow the path starting at:

■ Perform a Firmware Upload

In the next window you can browse the folder system to find the firmware file. Click the following command to begin the installation:

■ Start Upload

### 9.2.3 Terminal Program

Examples of terminal programs include Telix or Hyperterminal in Windows. When using a terminal program, use the “set mode firmsafe” command in the “Firmware” menu to initially select the mode in which you want to load the new firmware (immediately, on login or manually). If desired, you can also set the duration of the firmware test using “set timeout firmsafe”.

Select the “do firmware upload” command to prepare the router to receive the upload, then start the upload procedure from your terminal program:

- ▶ If you are using Telix, click the `Upload` button. Specify “XModem” as the transfer protocol and select the desired file for the upload.
- ▶ If you are using Hyperterminal, click `Transfer : Send File`. Select the file, specify “XModem” as the protocol and start the transfer with `OK`.

**Note:** To use a terminal program for the firmware upload, you require a serial configuration interface.

### 9.2.4 TFTP

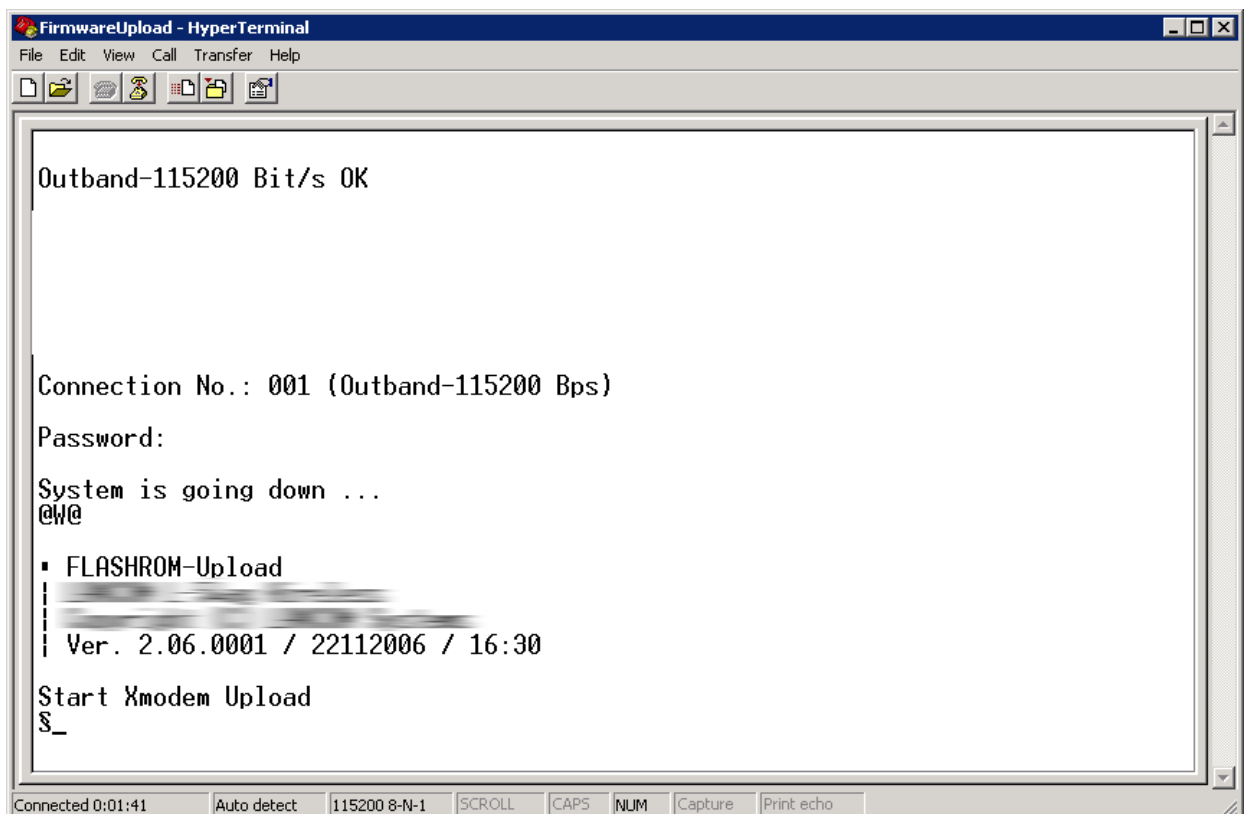
You can use `tftp` to install the new firmware on the Switch device. You use the “writeflash” command for this. Example: To transfer a new firmware to a Switch device with the IP address 10.0.0.1, enter the following command in Windows 2000 or Windows NT:

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

### 9.2.5 Loading the Firmware via the Serial Interface with a 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 factory settings. This lets you re-open the device if the configuration password is lost and the reset button has been set to 'Ignore' or 'Boot only'.

- Use the serial configuration cable to connect the device to a computer.
- Start a terminal program such as Hyperterminal.
- Open a connection with the settings 115200 bps, 8n1, hardware handshake (RTS/CTS).
- In the terminal program's welcome screen, press the Return key until the request to enter the password appears.
- Enter the serial number that is displayed under the firmware version and press Return again.



- The device now expects the firmware upload. If you are using Hyperterminal, click `Transfer : Send File` to start the upload. Select “XModem” as the transfer protocol.

**Note:** Uploading the firmware in this way overwrites the configuration with the default factory settings. Consequently, this option should only be used if the configuration password is no longer available.



## 9.3 Searching for New Firmware

After you have obtained new firmware for your devices, you can simplify the firmware update for the Switch devices by saving the new firmware files in a central firmware archive. Over time, this firmware archive can accumulate many firmware versions. Either search this archive manually for new firmware versions or have the search executed automatically every time LANconfig is started.

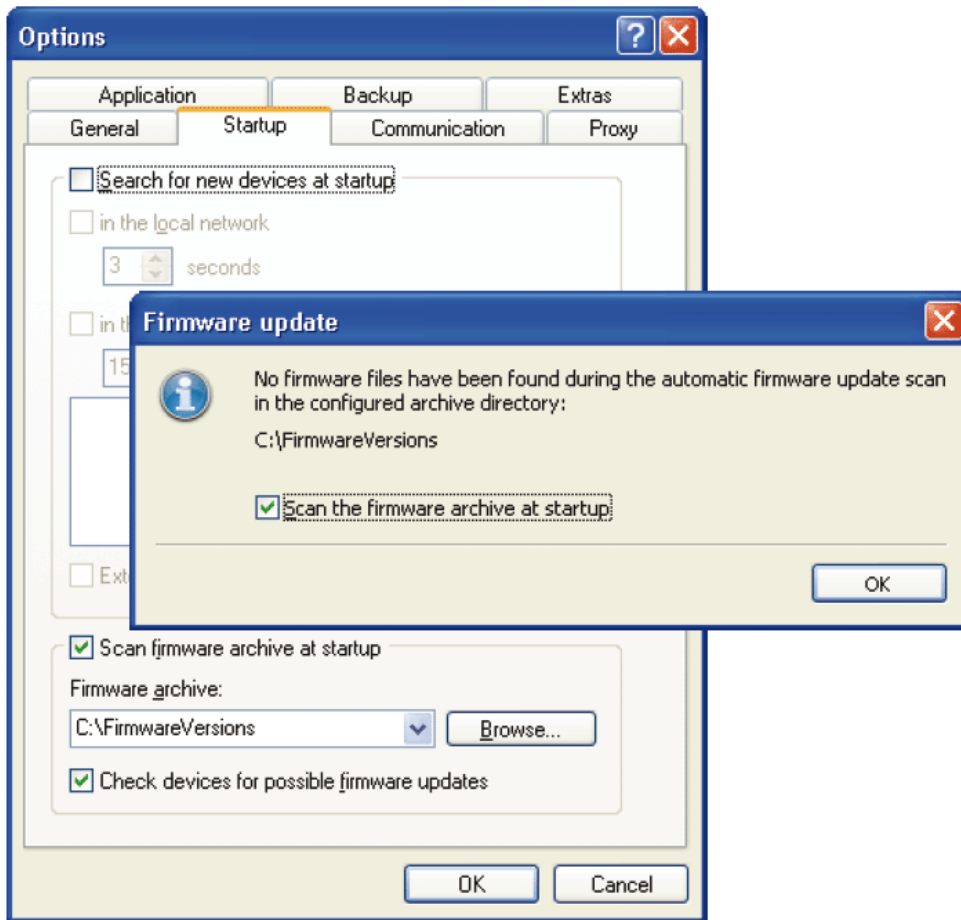
### 9.3.1 Automatic Search for Firmware Updates

If your firmware archive contains many version files, you may want to let LANconfig identify the specific files that apply to your devices. You can configure LANconfig to automatically perform the following tasks on startup:

- ▶ scan the central firmware archive to identify its contents, then
- ▶ identify those networked devices to which a firmware update applies

To do this, take the following steps:

- In LANconfig, open the `Tools : Options : Startup` dialog.



- Select 'Scan firmware archive at startup' to enable this function.
- To identify the 'Firmware archive', click 'Browse...' then navigate to and select the central firmware archive.

**Note:** The central firmware archive is where you should keep all device firmware files.

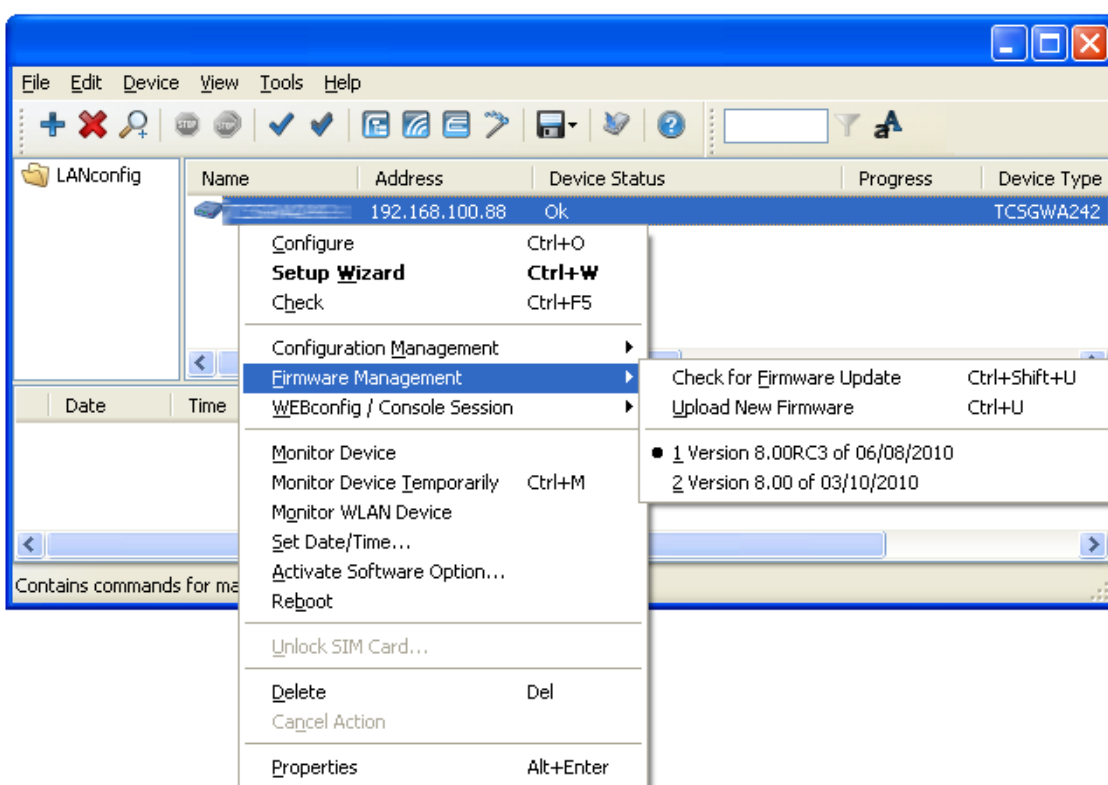
- Select 'Check devices for possible firmware updates'.

Each time LANconfig starts up, it automatically identifies the devices for which firmware updates are available in the specified firmware archive.

## 9.3.2 Manually Search for Firmware Updates

You can also manually manage the firmware update process. To do so, follow these steps:

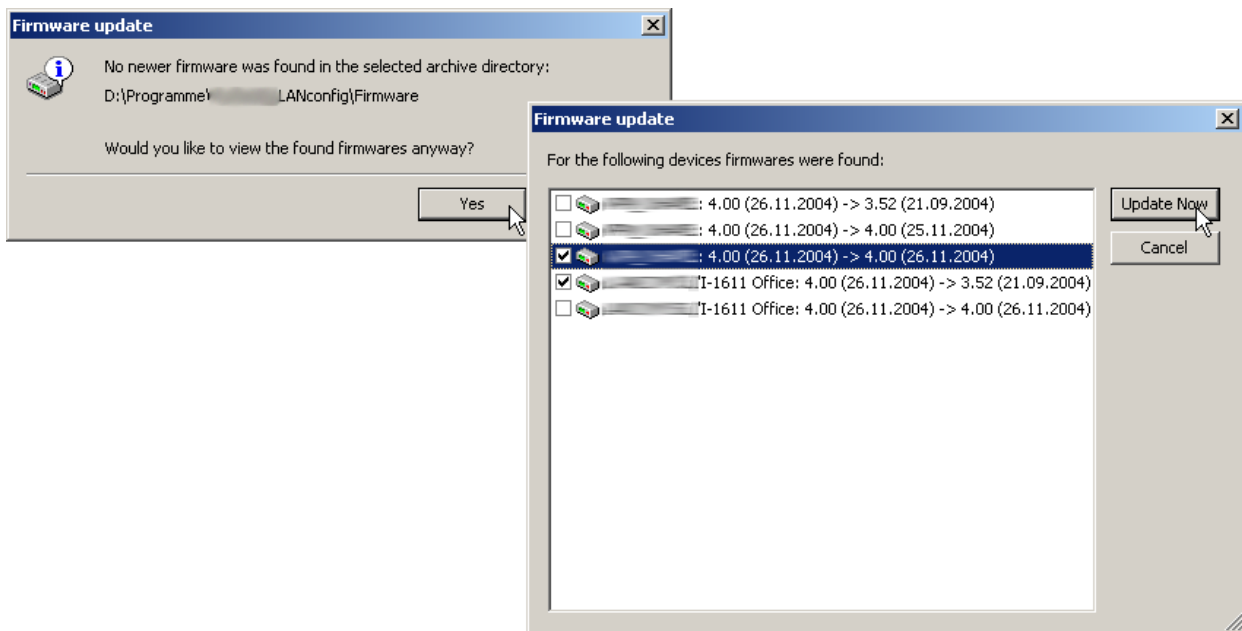
- In LANconfig, right-click on one or more devices in the list, then in the pop-up menu, select:  
Firmware management : Check for firmware update(s).



LANconfig checks the 'Firmware archive' folder to see if it contains firmware updates for any of the selected devices.

### 9.3.3 Viewing All Device Firmware Versions

If your search in the archive does not reveal a new firmware version, you can view a full list of all of the firmware files and, for example, switch back to an older version. LANconfig displays all versions found for the selected devices, including the version currently active in each device. For each device, you can select one firmware version, which will then be uploaded to the device.



## **10 Load Files from a TFTP or HTTP Server to the Device**

Certain functions cannot be run, or run satisfactorily, via Telnet. These functions include those where entire files are transferred, such as the upload of firmware, and saving or restoring configuration data. Use tftp or http(s) in these cases.

## 10.1 TFTP

In Windows operating systems, tftp enables the 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]
```

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

If the device is password-protected, include the user name and password 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) and with the command as a suffix. A command sent by tftp therefore resembles one of the following:

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

The rights to use tftp can be restricted for administrators.

## 10.2 Loading Firmware, Device Configuration or Script via HTTP(S)

Switch devices can also use http and https to download firmware, device configurations or scripts for automatic processes (e.g. to obtain files from the Internet themselves). In practice, it is easier to provide a central https server with a unique Internet address (URL) than a comparable tftp server. You can modify an existing Web server for this function.

An optional certificate for the https server can be uploaded by WEBconfig to the device as the SSL root CA certificate at the following location:

File management : Upload Certificate or File

### Upload Certificate or File

Select which file you want to upload, and its name/location, then click on 'Start Upload'.  
In case of PKCS12 files, a passphrase may be necessary.

File Type:

File Name/Location:

Passphrase (if required):

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

## 10.3 Loading Firmware, Device Configuration or Script via HTTP(S) or TFTP

In addition to 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 updates and/or configuration changes. HTTP(S) and tftp can also be used to load scripts (e.g. with partial configurations) into devices.

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 it 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>
- ▶ By using 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, the 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

### 10.3.1 Examples

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

```
LoadFirmware -s 192.168.2.200 -f Hirschmann/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 the 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
```

-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 commands `LoadConfig` and `LoadFirmware` can be used to load the relevant files.

# 11 Scripting

In installations with multiple Switch devices, you might want to execute specific configuration tasks automatically. The scripting functions in the Switch device allow you to save entire sets of commands for configuring the devices in one file (a script) and to transfer them to one or more devices in a single step.

---

# 11.1 Applications

Scripting provides users with a powerful tool for centrally configuring the Switch devices, with a wide range of potential applications:

- ▶ Reading out the device configuration in a form that is easy to read and save:  
The configuration files created by LANconfig are not intended to be processed directly with other tools. Only by printing the configuration file will you get an overview of the complete configuration. The scripting functions allow you to output the configuration as an ASCII text and then save it as a simple text file.
- ▶ Editing the configuration with a simple text editor:  
If offline configuration with LANconfig is not possible or is not desired, you have the option of using a text editor to edit a configuration file created by scripting, then load it to the device again.
- ▶ Editing parts of a configuration:  
Instead of a complete configuration, you can also read specific parts of the configuration from a device (e.g. only the firewall settings). Just like with complete configurations, parts of configurations can be edited and then transferred to one or more devices. This gives you the option of loading specific settings in a device to other models or devices with a different firmware version.
- ▶ Automated configuration updates:  
The centralized storage of configuration scripts in combination with scheduled commands (cron jobs) can be used to update important parts of the configuration (e.g. the encryption settings for a WLAN) automatically in multiple devices at the same time.
- ▶ Convenient rollout in larger installations:  
If multiple devices are installed at different locations, it is very easy to control the configuration centrally. Employees without administrator rights can then set up the devices using a single command.
- ▶ Saving the configuration in volatile memory only:  
Scripting commands allow you to save the changes to the configuration in RAM only. Saving it to non-volatile memory is then not allowed. As a result, the configuration is only available until the next system booting.

- ▶ Changing the configuration in the test mode:  
The same mechanism allows you to change the configuration very easily in the test mode. You use a script to trigger a time-delayed system boot, and until the boot is activated you can change and test the configuration of the device. The device automatically reboots after the time delay and is reset to its previous configuration.  
Like the FirmSafe function, this variant also provides you with a kind of “ConfSafe”. If you make changes to the configuration after a firmware update, sometimes the configuration may no longer be editable after a subsequent downgrade to the old firmware version. However, if you only change the configuration in test mode after the firmware upgrade, you can very easily restore the original firmware and configuration status of the devices by downgrading and then rebooting.

---

## 11.2 Scripting Function

With scripting you transfer a series of configuration commands collectively to a Switch – just as you would enter the commands in the Telnet console of the device, for example. There are two variants for this collective transfer of configuration commands:

- ▶ You put the device in console mode by entering the “beginscript” command in the script mode. In this mode the program does not execute the transferred commands individually, but initially writes them to the intermediate memory of the Switch. Only when you enter the “exit” command does the program execute these commands.
- ▶ Alternatively, you can write the configuration commands offline to a script file (text file) and then upload them to the device as a complete script.

The configuration commands executed using the script file initially effect only the configuration that is stored in the RAM of the device. The flash mode then determines whether the configuration is also changed in the flash memory.

- ▶ In Flash Yes mode (standard), the configuration commands are directly written to the flash memory of the device, and are thus boot resistant. Since the flash mode is always ON with the other methods of configuration (console without script, LANconfig or WEBconfig), the configuration changes are written first to the RAM memory and then immediately to the flash memory
- ▶ In Flash No mode the data is written only to RAM and is thus available only until the next boot.
  - During the boot process, the device reads the configuration data from the flash memory.
  - At any time, you can transfer the configuration from the RAM to the flash memory using the command “Flash Yes”. When actively operating, the Switch devices use the information stored in the RAM configuration. The script commands stored in the intermediate memory are, like the configuration in flash memory, not relevant to the real-time operations of a Switch device.

## 11.3 Generate Script Files

A script for a Switch configuration is a conventional text file. This includes any necessary comments and all of the commands used to set the configuration, for example when using a Telnet console. There are two ways to generate a script file:

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

### 11.3.1 Reading Out the Configuration via the Console

To read the configuration out of the console, follow these steps:

- Log on to the console with write access rights.
- Switch to the branch of the configuration tree that you wish to read out.
- At the command prompt, execute the command `readscript`. Observe the optional command extensions (Scripting commands).
- Using the Clipboard, copy and paste the required text section into a text editor and adapt the script to your requirements.

### 11.3.2 Reading the Configuration via TFTP from the CLI

The configuration commands can be read out directly from the command line interface (DOS command line interface) via tftp. Note that device passwords will be clearly visible as plain text while entering this command. Follow these steps:

- Open a DOS screen.
- Enter the following command at the prompt:

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

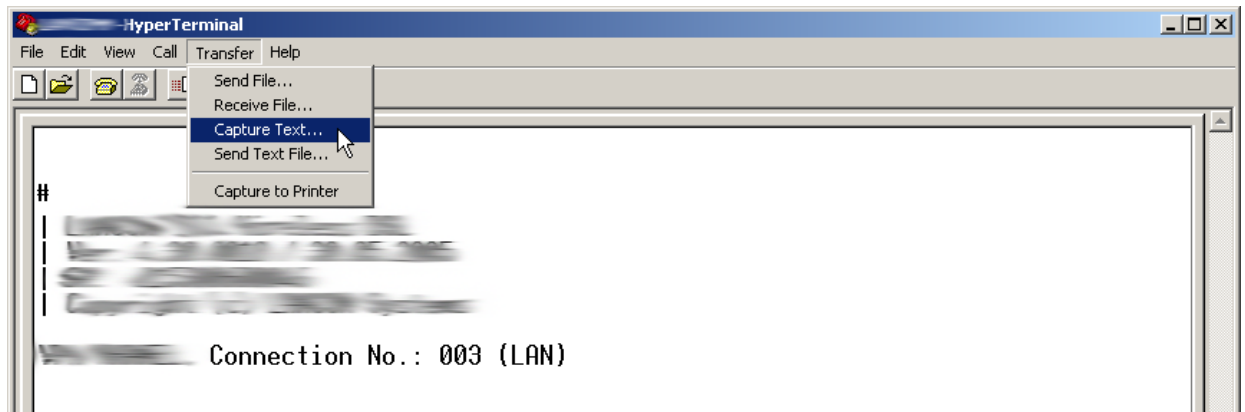
- IP address is the address of the device containing the configuration commands you wish to read out.
  - PASSWORD is the appropriate password for the device.
  - Path defines the branch of the configuration menu tree that is to be read out. If no path is entered then the entire configuration will be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

### 11.3.3 Reading the Configuration with Hyperterminal

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

- Set up a connection to the device with Hyperterminal.
- Select the menu item **Transfer : Capture Text** and select the desired storage location and file name for the script.





- At the command prompt, execute the command `readscript`. Observe the optional command extensions.
- After you have called up all required sections of the configuration, stop the recording with the following menu item:  
`Transfer : Capture Text : Stop.`

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

### 11.3.4 Download Script from the Device

In installations with multiple Switch devices, you might want to execute specific configuration tasks automatically. The scripting functions in the Switch device allow you to save entire sets of commands for configuring the devices in one file (a script) and to transfer them to one or more devices in a single step.

In addition to manually creating a script and reading via the console, you can also use LANconfig to read script files from a device. To do this, right-click on the corresponding entry in the device list, and in the context menu select `Configuration Management : Save script to file`. Select the following options:

- ▶ **Numeric section**  
Enable this option if you do not want the configuration sections in the script to be displayed numerically (e.g. /2/2/5), rather than in clear text (/setup/wlan/ppp).
- ▶ **Default values**  
Unless defined otherwise, the parameters saved in a script are always only those that deviate from the default values. Enable this option if you also want the default values to be entered in the script.
- ▶ **Column names**  
Unless defined otherwise, the fields in a table are initially entered as column names in the scripts, after which the respective values are inserted into the rows. Enable this option if you want every value in the table to be explicitly given the name of the column in which it is stored.
- ▶ **Comments**  
Enable this option if you want to include additional comments in the script file.
- ▶ **Compact formatting**  
Enable this option to suppress spaces and tabs.
- ▶ **Download only selected sections**  
Unless defined otherwise, the program always saves the entire device configuration in a script. By defining specific script sections, you can also save parts of configurations. In this field you enter the sections that you want transferred to the script (e.g. /setup/wlan).

## 11.4 Uploading Configuration Commands and Script Files

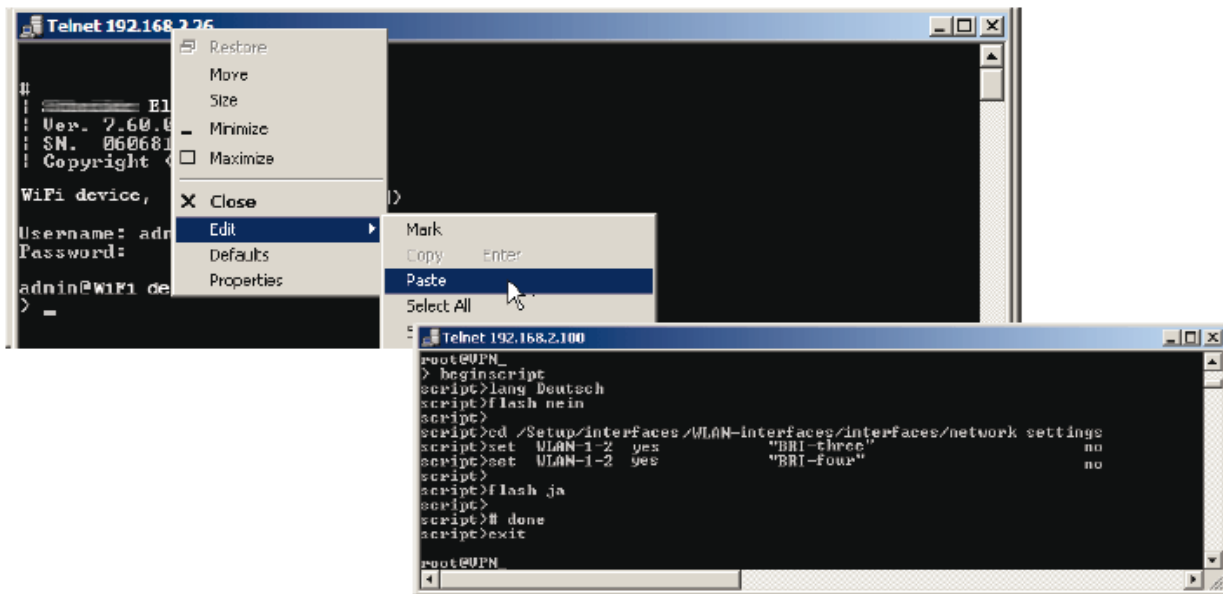
You have 2 different methods for loading the script commands to the intermediate memory of the Switch device:

- ▶ You enter the commands manually at a console in script mode with the command “beginscript”. You thus write the commands directly from the console to the intermediate memory. When you have completed all the commands, enter the command “exit” to transfer them to the RAM.
- ▶ You save the desired command sequence in a text file. This text file is then transferred to the intermediate memory using the corresponding tool (LANconfig, terminal program, TFTP). If the file contains the required commands, the program automatically begins transferring the configuration to the RAM.

### 11.4.1 Entering Commands in a Console Session (Telnet, SSH)

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

- Open your script with any text editor and transfer the configuration commands to the Clipboard.
- Log on to the console with Supervisor rights.
- Start the script mode with the command `beginscript`.



- Paste the commands from the Clipboard after the script prompt (script>). In Telnet, for example, right-click on the upper frame of the window.
- Entering the command `exit` executes the configuration commands.

**Note:** If the command `exit` is already included in the pasted commands, execution of the configuration will be carried out automatically.

## 11.4.2 Upload Script with TFTP Client

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

- Log on to the console with Supervisor rights.
- Enter the following command at the prompt:  

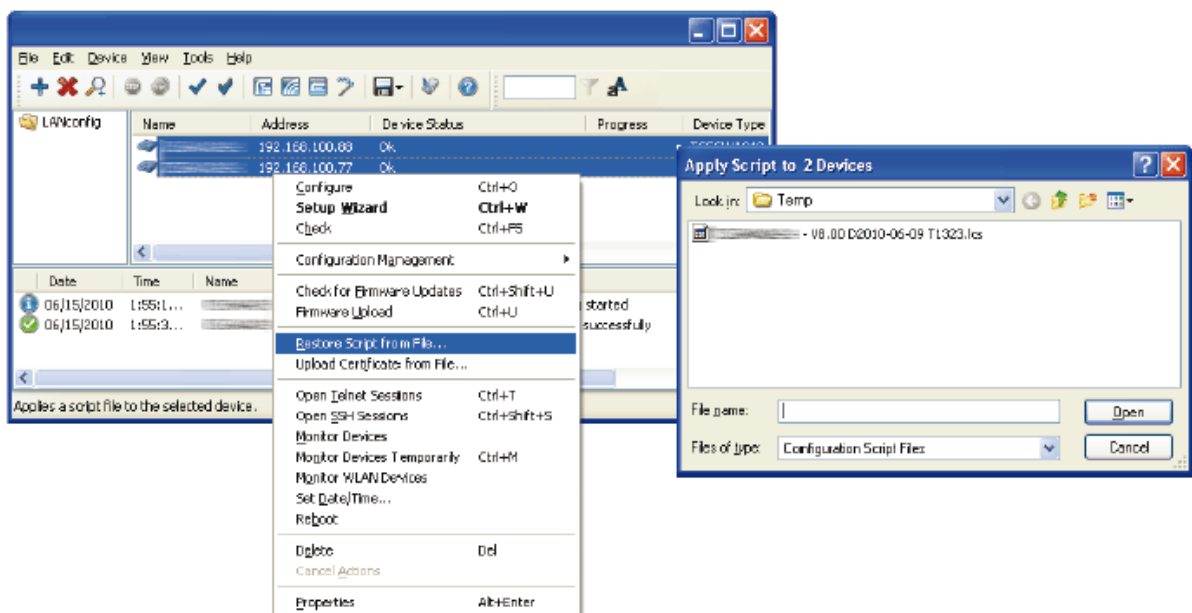
```
loadscript -s IP address -f script.lcs
```
- IP address is the address of the TFTP server where the script file is stored.

- `script.lcs` is the name of the script file on the tftp server.

### 11.4.3 Upload Script with LANconfig

LANconfig has the option to upload a script either to a single device or to multiple devices simultaneously, as follows:

- Right-click on a device and use the context menu to select the entry `Configuration Management : Restore Script from File`. If multiple devices are marked, the entry `Restore Script from File` appears directly in the context menu.
- In the following dialog, select the required script file (\*.lcs) for upload.

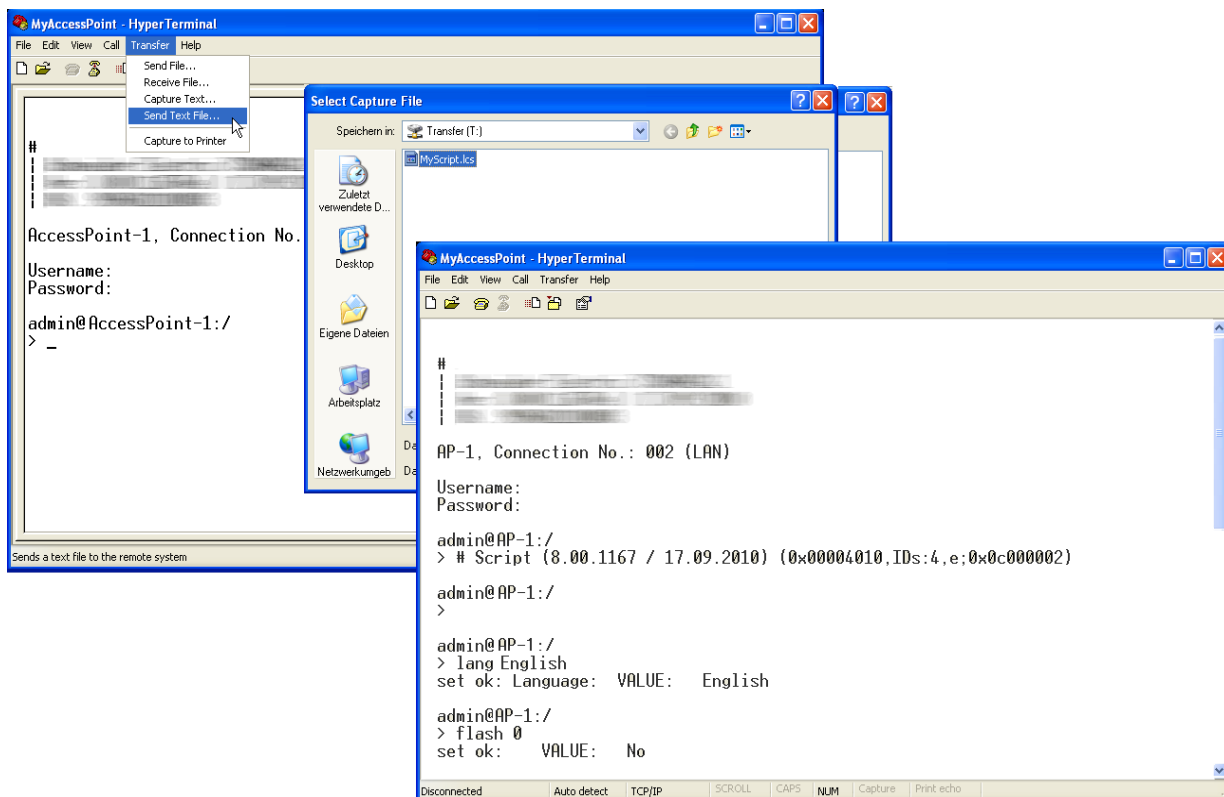


**Note:** The upload of the script starts automatically. Status and event messages are either displayed directly by LANconfig or can be viewed in a console session with the command `show script`.

## 11.4.4 Upload Script with Hyperterminal

Another way to upload scripts to a Switch device is to use terminal programs such as Hyperterminal, which is supplied with Windows.

- Set up a connection to the device with Hyperterminal.
- Select the menu item **Transfer : Send Text File**.
- Select a script file and start the transfer.



After successful completion of the transfer, the script starts automatically.

## 11.4.5 Multiple Parallel Script Sessions

The Switch device can manage multiple parallel script sessions. Just as multiple console sessions can be run simultaneously on a single device, different scripts can also access the Switch device in parallel. Parallel script sessions are useful in the following scenarios:

- ▶ Script 1 initiates a reboot of the device after a time delay of 30 minutes. Script 2 is active while the device is running and changes the configuration for test purposes. The flash mode remains deactivated for this. If the changes script 2 made to the configuration make the device unreachable, script 1 reboots the device after 30 minutes and thus rejects the changes to the configuration.
- ▶ When different scripts are being used for partial configurations, it is possible for multiple scripts to be started automatically at the same time, e.g. via cron jobs. You have the option of starting a task while other tasks are still running.

## 11.4.6 Scripting Commands

- ▶ `readscript`  
In a console session, the “readscript” command creates a text output of all the commands and parameters required for the configuration of the Switch device in its current state. In the simplest case, the Switch only lists commands that are relevant to parameters that deviate from the factory settings.

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

**Note:** Log on to the console with write access rights to execute this command.

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

```

Telnet 192.168.2.101
Connection No.: 002 <LAN>
root@:/
> readscript
# Head
lang English
flash No

cd /Setup/WAN/Dialup-Remote-Peers
del *
add "DEFAULT" "" 20 20 ""
add "ARCOR" "0192070" 90 90 "ARCOR"
cd /Setup/WAN/Layer
del *
add "DEFAULT" TRANS PPP TRANS bnd+cmpr HDLC64K
add "T-ISDN" TRANS PPP TRANS none HDLC64K
add "MLPPP" TRANS PPP TRANS bnd+cmpr HDLC64K
add "PPPHDLC" TRANS PPP TRANS none HDLC64K
add "RAWHDLC" TRANS TRANS TRANS none HDLC64K
add "T-DSL" TRANS PPP PPPoE none ETH
add "PPPOE" TRANS PPP PPPoE none ETH
add "IPOE" ETHER TRANS TRANS none ETH
add "DHCPoE" ETHER DHCP TRANS none ETH
add "U_24_DEF" TRANS APPP TRANS none SERIAL
add "ARCOR" TRANS PPP TRANS none HDLC64K
cd /Setup/WAN/PPP
del *
add "DEFAULT" PAP "" "arcor" 0 5 ""
add "ARCOR" none "arcor" 0 5 "arcor"
set /Setup/LAN/Connector 32
set /Setup/TCP-IP/Intranet-Address 192.168.2.101
cd /Setup/IP-Router/IP-Routing-Table
del *
add 192.168.0.0 255.255.0.0 0 "0.0.0.0" 0 No
add 172.16.0.0 255.240.0.0 0 "0.0.0.0" 0 No
add 10.0.0.0 255.0.0.0 0 "0.0.0.0" 0 No
add 224.0.0.0 224.0.0.0 0 "0.0.0.0" 0 No
add 255.255.255.255 0.0.0.0 0 "ARCOR" 0 on
set /Setup/DHCP/Operating No
cd /Setup/Config/Access-Table
set LAN Yes Yes Yes Yes Yes Yes Yes
set WAN No No No No No No No
set /Setup/Mail/SMTP-Port 0
set /Setup/Mail/POP3-Port 0
set /Setup/Mail/Send-Again-(min.) 0
set /Setup/Mail/Hold-Time-(hrs.) 0
set /Setup/Mail/Buffers 0
flash Yes

# done
exit

```

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

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

**Note:** For table lines or strings containing passwords, the passwords are displayed in clear text, as this is the format required by the Telnet interface. With the generated script you can configure a Switch device exactly like the original device. As these scripts can be very long in some cases, you can also generate scripts for specific parts of the configuration. To do this, you first switch to the directory containing the configuration that you want to record (e.g. `cd set/ip router/`



`firewall` for the firewall settings). Then execute the command “`readscript`”. Alternatively, enter the path directly with the command “`readscript`” as a `PATH` parameter (e.g. `readscript set/ip router/firewall`). In both cases, only the firewall settings that have been changed will be recorded in the script.

The following options can be used with the `readscript` command:

- `-d` (default): The commands for modifying parameters that are set to the factory settings will also be listed. These long scripts are useful for transferring configurations between different types of devices, or between devices with different firmware versions, as the factory settings can vary.
- `-n` (numeric): This suffix causes the paths to be output in the numeric form of the SNMP description, instead of in plain text. This also facilitates the transfer of scripts between devices with different firmware versions, as the path names may change but the SNMP tree generally remains unchanged.
- `-c` (comment): In combination with `-d` and `-n`, this parameter generates additional comments that make the script easier to read. For the parameter `-d`, every command combination that sets a default value is marked with `# default value`. With `-n`, each numeric path is supplemented with its plain text equivalent.
- `-m` (minimize): This parameter removes any gaps in the script, making it more compact.

▶ `#`

The `#` character followed by a space at the start of a line comprise the first characters of a comment. Any subsequent characters to the end of the line will be ignored.

**Note:** Insert a space after the `#` symbol.

▶ `del *`

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

Syntax: `del [PATH]*`

▶ `default`

This command resets individual parameters, tables or entire menu trees to their factory settings.

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

This command resets the parameters addressed with PATH to their factory settings. If PATH refers to a branch of the menu tree, enter the option “-r” (recursive).

Login to the console with write permission to execute this command.

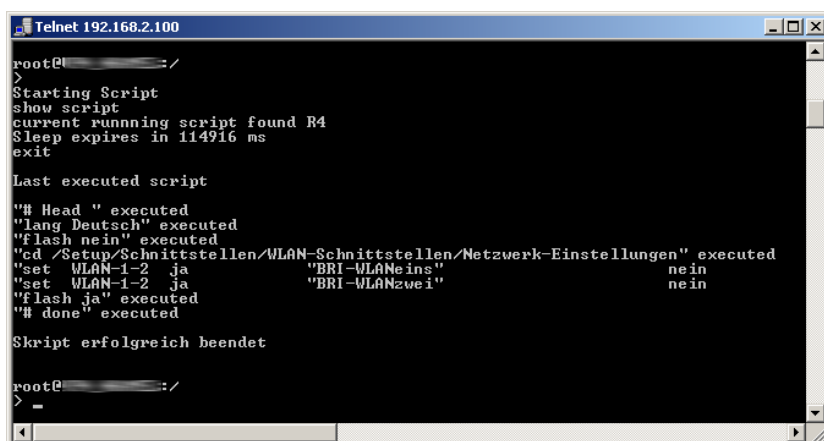
#### ► `beginscript`

The `beginscript` command sets a console session to the script mode. In this state, commands entered are not transferred directly to the configuration RAM of the Switch device, but initially to the script memory of the device. The “exit” command is required to transfer the commands exclusively via a script session to the configuration RAM and execute them there.

**Note:** Login to the console with write permission to execute this command.

#### ► `show script`

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



```

Telnet 192.168.2.100
root@:~#
>
Starting Script
show script
current running script found R4
Sleep expires in 114916 ms
exit
Last executed script
"# Head " executed
"lang Deutsch" executed
"flash nein" executed
"cd /Setup/Schnittstellen/WLAN-Schnittstellen/Netzwerk-Einstellungen" executed
"set WLAN-1-2 ja "BRI-WLANeins" nein
"set WLAN-1-2 ja "BRI-WLANzwei" nein
"flash ja" executed
"# done" executed
Skript erfolgreich beendet
root@:~#
> -

```

**Note:** Log on to the console with write access rights to execute this command.

- ▶ `killscript`  
The command `killscript` deletes the content of a script session that has not yet been executed. The script session is selected by its name.
  
- ▶ `flash Yes/No`  
When configuring a device with scripts, any `add-`, `set-` or `del-` command can lead to an unintentional update of the configuration in flash. To combat this, the update to flash function can be deactivated. After concluding the configuration, this function can be activated again with `flash Yes`. Changes in the RAM configuration are then written to flash. The status `flash Yes/No` is stored globally.

**Note:** Log on to the console with write access rights to execute this command.

- ▶ `sleep`  
The `sleep` command allows the processing of configuration commands to be delayed for a certain time period, or to be scheduled for a certain time. Syntax: `sleep [-u] value[suffix]`

Permissible suffixes are `s`, `m`, or `h` for seconds, minutes, or hours; if no suffix is defined, the units are milliseconds. With the option switch `-u`, the `sleep` command accepts times in the formats:

`MM/DD/YYYY hh:mm:ss` (English)

`TT.MM.JJJJ hh:mm:ss` (German)

**Note:** Times will be accepted if the system time has been set.

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



## 12 Managing Rights for Administrators

You can configure each Switch device for a maximum of 16 administrators, all with different access rights.

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

As soon as you have set up a password for the “root” administrator in the configuration of the device, the “Login” button appears when you call up WEBconfig. When you click this, the login window opens. After you have entered the correct user name and password, the main menu of WEBconfig opens. This menu only displays the options that are available to the administrator who is currently logged in.

If at least one more administrator is set up in the admin table, the main menu also contains the “Change administrator” button, which allows you to switch to a different user ID (with different rights, if applicable).

## 12.1 Administrator Rights

An administrator's rights are determined by assignments from two different groups:

- ▶ Each administrator belongs to a specific administrator group with globally defined group-based access rights.
- ▶ Each administrator also is assigned specific function rights that determine the administrator's ability to perform specific tasks.

### 12.1.1 Access Rights

Each administrator is a member of one of the following administrator groups:

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

- ▶ Supervisor:  
Has full access to the configuration.

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

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

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

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

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

## 12.1.2 Function Rights

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

- ▶ Basic wizard
- ▶ Internet wizard
- ▶ RAS wizard
- ▶ WLAN linktest
- ▶ Rollout wizard
- ▶ Adjustment of date and time
- ▶ Search of further devices in LAN
- ▶ SSH client
- ▶ Security wizard
- ▶ Provider selection
- ▶ LAN-LAN wizard
- ▶ WLAN wizard
- ▶ Content filter wizard



## 12.2 Administrators' Access via TFTP and SNMP

In addition to using LANconfig, WEBconfig, Telnet, terminal programs or secure shell (SSH) access, administrators can also access a Switch via tftp or SNMP.

### 12.2.1 TFTP Access

In tftp, the administrator name and password are coded in the source (tftp read request) or target file names (tftp write request). The file name is made up of either the master password and the command to be executed, or the combination of administrator name and password (separated by a colon), with the command as a suffix. Therefore, a command sent via tftp looks like this:

```
<Master password><Command>
```

or...

```
<User name>:<Password>@<Command>
```

In the following examples, the Switch device has the configuration:

- ▶ Address = "mydevice.intern"
- ▶ Master password = "RootPwd"
- ▶ Administrator name = "LocalAdmin"
- ▶ Administrator password = "Admin"

Read the configuration from the device (supervisor):

```
tftp mydevice.intern GET  
RootPwdreadconfig mydevice.lcf
```

Write the configuration to the device (supervisor):

```
tftp mydevice.intern PUT  
mydevice.lcf RootPwddwriteconfig
```

Read the device MIB from the device (for local administrator):

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

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

## 12.2.2 SNMP Access

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

Under SNMP, administrator name and password are coded as part of the 'community'. Permissible selections include:

- ▶ the 'public' community name
- ▶ the master password
- ▶ a combination of user name and password divided by a colon

**Note:** The 'public' community setting corresponds with the rights of a local administrator with read-only access, as long as the SNMP read access without password is enabled. If this access is prohibited, then the 'public' community setting denies access to all menus.

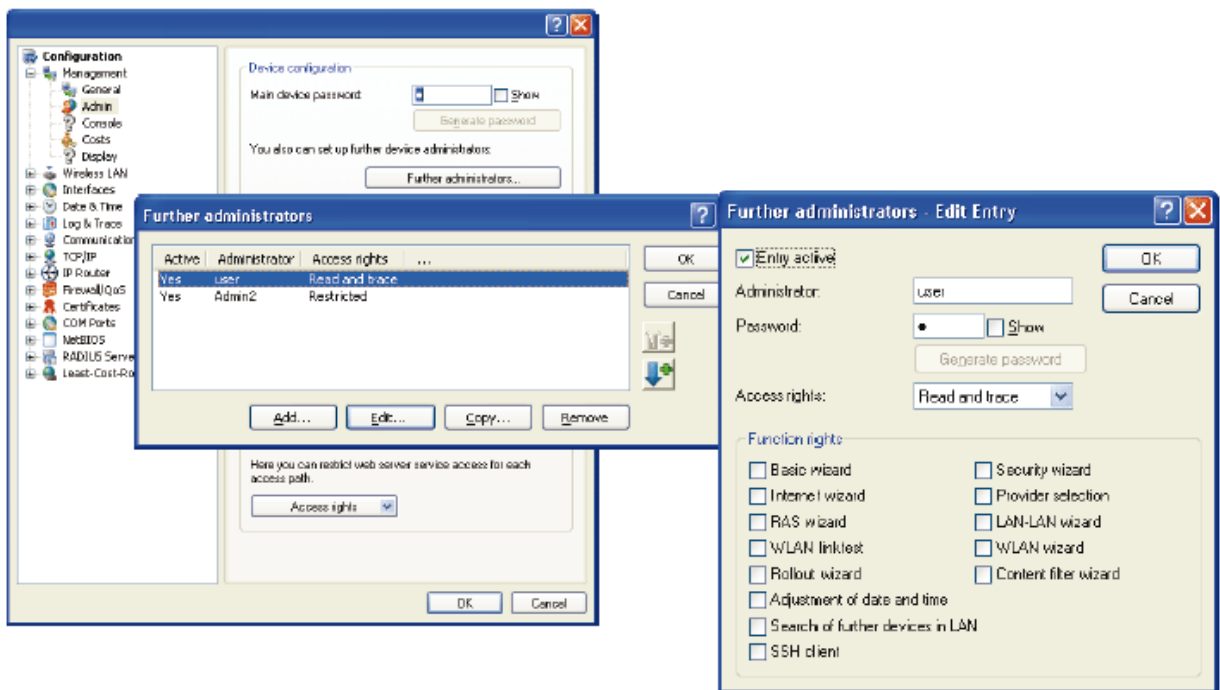
Otherwise, the same limitations on rights apply for the menus as with Telnet.

## 12.2.3 Configuring User Rights

### ■ LANconfig and WEBconfig

To access a list of administrators, where you can edit the rights of a selected administrator account in LANconfig, follow these steps:

- Open the configuration file for a device in LANconfig by highlighting the device, then selecting **Device : Configure**.
- Open the **Configuration : Management Admin** dialog, and click 'Further administrators...' to open that window.
- In the 'Further administrators' window, either click 'Add...' to create a new administrator account, or select an existing entry and click 'Edit...' to open the 'Edit Entry' dialog:



To access the administrator accounts in WEBconfig, the path is virtually the same as in LANconfig:

■ **Configuration : Management : Admin**

In both LANconfig and WEBconfig, you can edit the name, password, access rights, and function rights for each administrator account. You can also enable and disable the account. By disabling the account, you can save the administrator account configuration for future use.

### ■ Telnet or Terminal Program

In Telnet or a terminal program, you will find the administrator accounts in the same location as for WEBconfig:

**Configuration : Management : Admin**

Administrator group access rights are described above ([see page 126](#)). Function rights are represented by the following hexadecimal values:

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

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

Third Column	Second Column	First Column
WLAN linktest = 1	RAS Wizard = 1 Change Time = 4	Security Wizard = 2 Internet Provider = 8
Total = 1	Total =5	Total = a

In the above example, the function rights value equals '0x0000015a'.

Examples:

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

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

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

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

## 12.2.4 TCP Port Tunnel

In some cases it can be useful to enable temporary remote access to a Switch device in a LAN via http (TCP port 80) or TELNET (TCP port 23). For example, if a question arises regarding the performance of a device, technical support personnel can provide better assistance if they can directly access the device in the customer's LAN.

However, the standard method for accessing LAN devices via inverse masquerading (port forwarding) sometimes requires a special configuration of the firewall. As an alternative to port forwarding, you can set up temporary access for remote maintenance that automatically closes again after a specific period of inactivity. To enable this access, the support staff member requiring access to a device in the network creates a "TCP/http tunnel" via TCP port 80.

**Note:** This access is only valid for the IP address from which the tunnel was created. This type of access to devices in the network is not transferable.

## ■ Configuring the Device for TCP/HTTP Tunnels

To configure the Switch device for a TCP/http tunnel, call up the following dialog in WEBconfig:

Hirschmann Menu Tree : Setup : HTTP

Configure the following properties:

- ▶ **Max. tunnel connections:**  
Maximum number of simultaneously active TCP/http tunnels.
- ▶ **Tunnel idle timeout:**  
Life span of a tunnel without activity. After this time expires, the tunnel closes automatically unless it is being used to transfer data.

## ■ Creating a TCP/HTTP Tunnel

To create a TCP/http tunnel, navigate to the following dialog in WEBconfig:

Extras : Create TCP/HTTP Tunnel

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

Host Name/IP address	<input type="text"/>
TCP Port	<input type="text" value="80"/>
Routing Tag	<input type="text" value="0"/>

Configure the following properties:

- ▶ **Host name/IP address:**  
Enter the name or IP address of the device that is to be temporarily available via http
- ▶ **TCP Port:**  
Select a port for the http tunnel.
- ▶ **Routing Tag:**  
If necessary, select a routing tag.

**Note:** In addition to http or https-based access, remote maintenance can also be based on any other TCP service such as telnet connections (TCP port 23) or SSH (TCP port 22).

The newly created HTTP tunnel is deleted automatically if the tunnel remains inactive for the duration of the tunnel idle timeout. To delete the tunnel earlier, access the list of active tunnels and delete the one you no longer require at the following WEBconfig location:

Hirschmann-Menu Tree : Status : TCP-IP : HTTP :  
Active Tunnels

**Note:** While active TCP connections in this tunnel will continue to exist for a short time, new connections cannot be established.



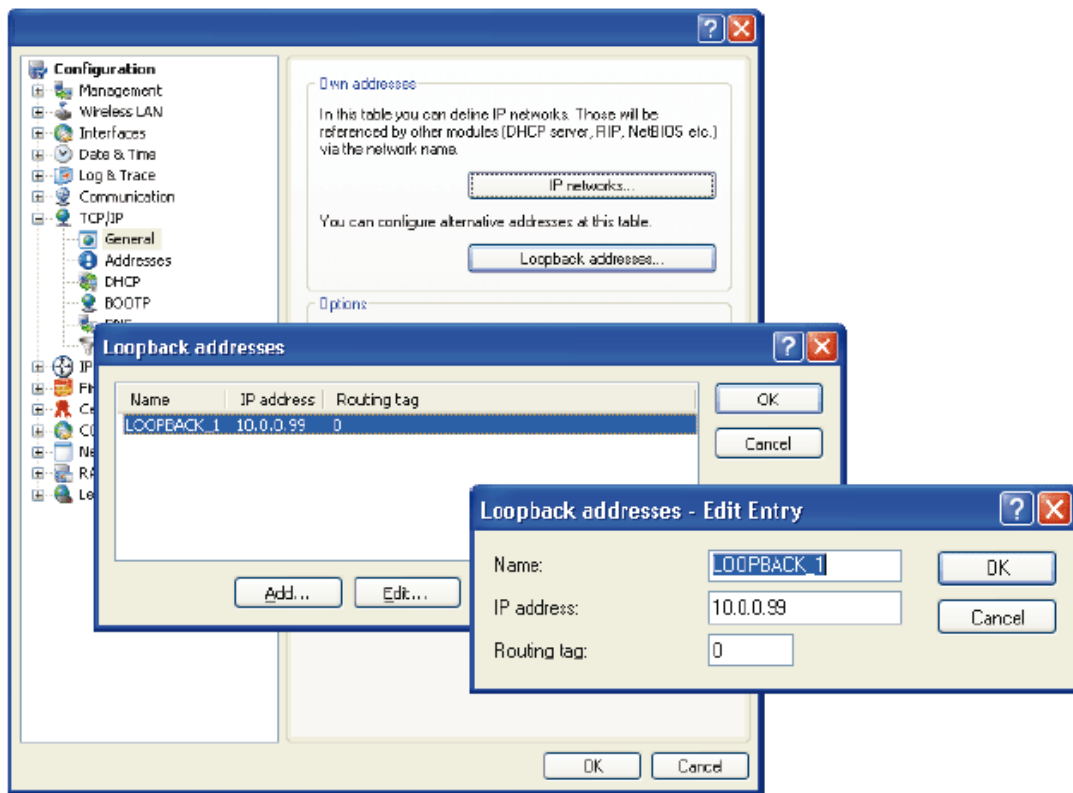


## 13 Managing Networks with Loopback Addresses

You have the option of configuring up to 16 loopback addresses in a Switch device, by means of which the device can be addressed. This can be an advantage when managing larger network structures. To use the loopback addresses for certain networks (e.g. in connection with advanced routing and forwarding), routing tags can be assigned to these addresses. To make them easier to identify in other configuration units, the loopback addresses are also given a freely definable name.

To manage loopback addresses for a Switch device:

- Open the LANconfig device configuration file to the following dialog:  
Configuration : TCP/IP : General, and click  
'Loopback addresses...'
- In the 'Loopback addresses' window, click 'Add...' to create a new loopback address, or select an existing entry and click 'Edit...' to modify an existing loopback address.



Configure the following properties for each loopback address:

- ▶ **Name:**  
A freely definable name for the loopback address, up to 16 characters.
- ▶ **Loopback address:**  
The IP address used for this loopback address for the device.
- ▶ **Routing tag:**  
Routing tag of the loopback address. Loopback addresses with the routing tag '0' (untagged) are visible to all networks. Loopback addresses with a different routing tag are only visible to networks with the same routing tag.

## 13.1 Loopback Addresses with ICMP Polling

Similarly to LCP monitoring, with ICMP polling the device regularly sends requests to a remote site. The device sends ping commands and monitors the responses. In contrast to LCP monitoring, you have the option of freely defining the remote site for the ICMP pings. With one ping to a router in a remote network it is possible to monitor the entire connection, not just the section to the Internet provider.

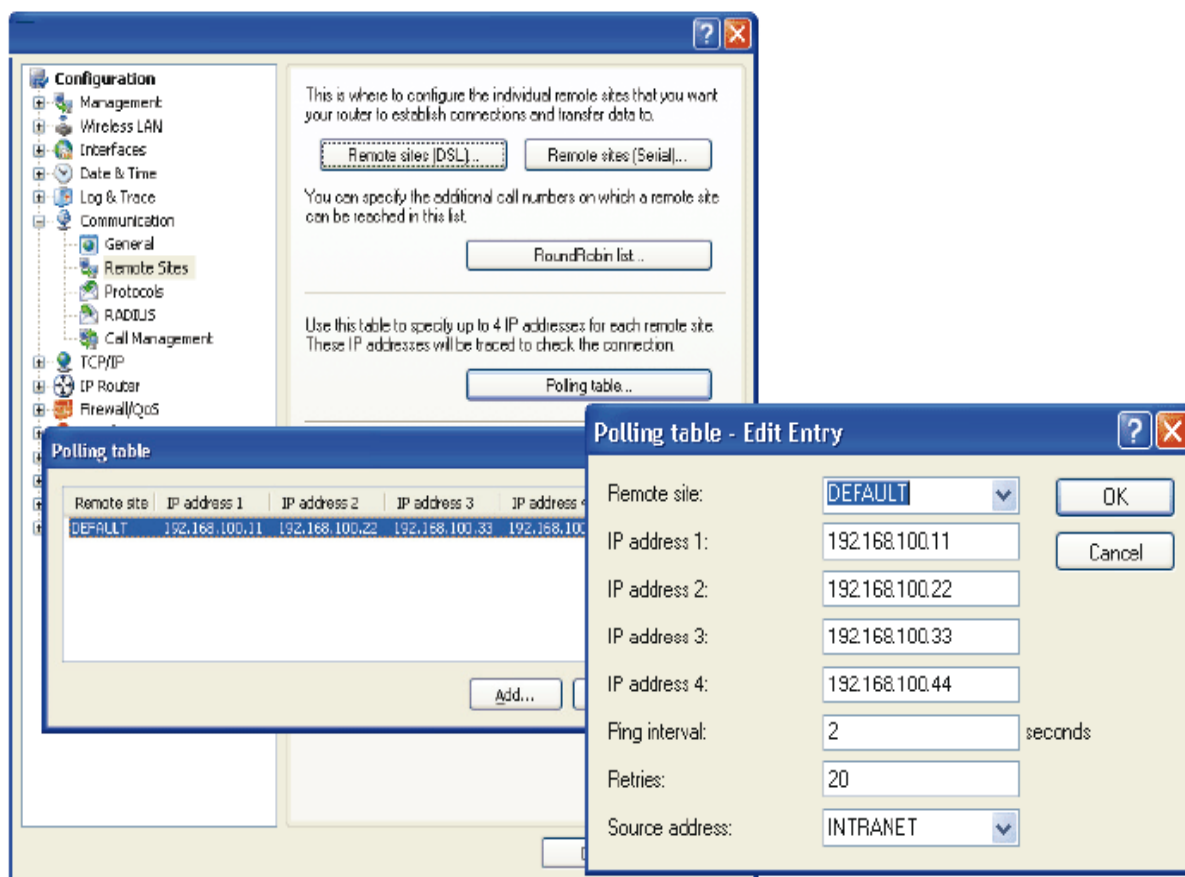
A ping interval is defined for the remote site in the polling table. Also defined, in the event that replies are missed, is the number of retries before the transmission of a new LCP request. If the transmitter does not receive any reply to the retries, the target for the ping requests is classified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

Up to four different IP addresses can be entered for each remote site that will be checked in the remote network in parallel. Only if all of the IP addresses are unavailable is the connection considered to be no longer active.

**Note:** ICMP polling enables you to monitor an entire connection from end to end.

To configure the polling entries with loopback addresses for a Switch device:

- Open the LANconfig device configuration file to the following dialog:  
Configuration : Communication : Remote Sites, and click 'Polling table...'
- In the 'Polling table' window, click 'Add...' to create a new polling entry, or select an existing entry and click 'Edit...' to modify an existing polling entry:



Configure the following properties for each ICMP polling entry:

- ▶ Peer:  
Name of the remote station which is to be checked with this entry.
- ▶ IP address 1 - 4:  
IP addresses for targeting with ICMP requests to check the remote site.

**Note:** If no IP address that can be checked with a ping is entered for a remote site, then the IP address of the domain name service (DNS) server that was determined during the point to point protocol (PPP) negotiation will be checked.

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

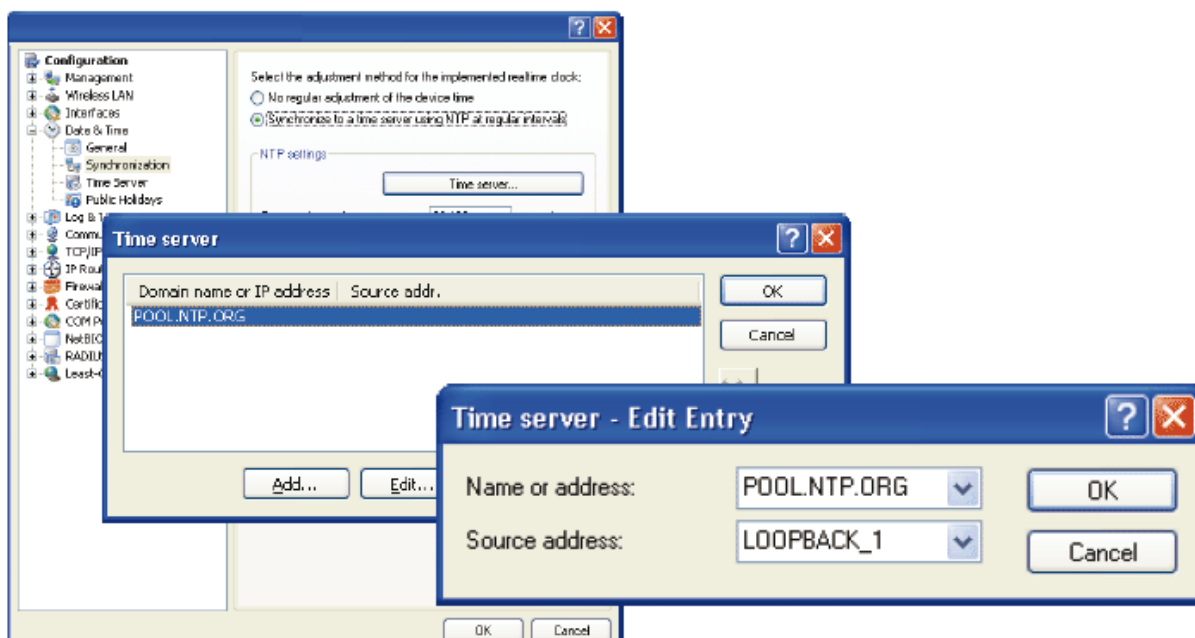
- ▶ **Retries:**  
If no reply to a ping is received, the remote site is checked in shorter intervals of once a second. The number of retries defines how many times these attempts are repeated. If the value "0" is entered, then the standard value of 5 retries applies.
- ▶ **Loopback address:**  
Sender address sent with the ping; this is also the destination for the answering ping.

# 13.2 Loopback Addresses for Time Servers

Switches can retrieve time information from public time servers via the Internet (NTP server). When defining the time server, the name or IP address of the NTP server being queried by the Switch can be entered, as well as loopback addresses.

To configure time servers with loopback addresses for a Switch device:

- Open the LANconfig device configuration file to the following dialog: Configuration : Date & Time : Synchronization, and click 'Time server...'
- In the 'Time server' window, click 'Add...' to create a new entry, or select an existing entry and click 'Edit...'



Configure the following properties for each ICMP polling entry:

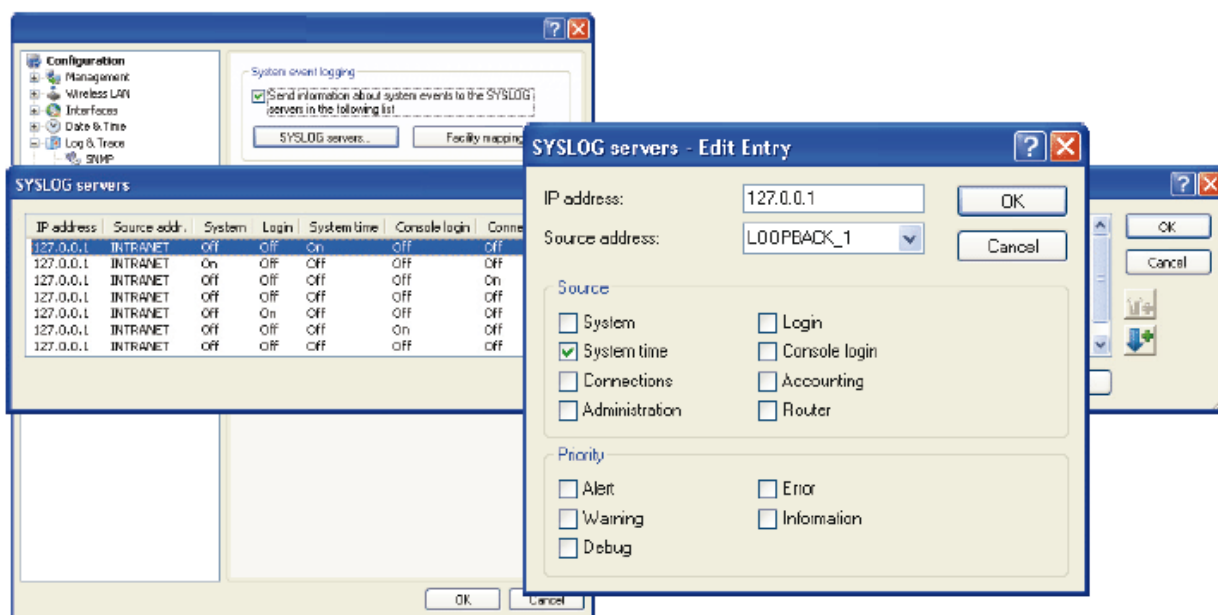
- ▶ **Name**  
Name or IP address of the NTP server. The Switch router attempts to reach the servers in the order in which they are entered.
- ▶ **Loopback address**  
Sender address sent with the NTP request; this is also the destination for the NTP answer.

## 13.3 Loopback Addresses for SYSLOG Servers

You can configure SYSLOG servers to receive SYSLOG messages from the Switch device. SYSLOG servers are configured to receive SYSLOG messages. The messages can be sent via loopback addresses in the Switch device.

To configure a Switch device to send SYSLOG messages to a remote SYSLOG server:

- Open the LANconfig device configuration file to the following dialog: Configuration : Log & Trace : SYSLOG, and click 'SYSLOG servers...'
- In the 'SYSLOG servers' window, click 'Add...' to create a new entry, or select an existing entry and click 'Edit...' to modify it:





Configure the following properties for each SYSLOG entry:

- ▶ IP address:  
IP address of the SYSLOG client
- ▶ Loopback address:  
Sender address entered into the SYSLOG message. No answer is expected to a SYSLOG message.
- ▶ Source: Select one or more of the following:
  - System: System messages (boot events, timer system, etc.)
  - Logins: Messages concerning the user's login or logout during the PPP negotiation, and any errors detected during login or logout.
  - System time: Messages about changes to the system time.
  - Console logins: Messages about console logins (Telnet, Outband, etc.), logouts and any errors detected during login.
  - Connections: Messages about establishment and termination of connections and any errors detected (e.g., display trace).
  - Accounting: Accounting information stored after termination of a connection (user, online time, transfer volumes).
  - Administration: Messages on changes to the configuration, remotely executed commands, etc.
  - Router: Regular statistics about the most frequently used services (breakdown per port number) and messages about filtered packets, routing errors, etc.
- ▶ Priority: Select one or more of the following:
  - Alert: This is a collection of messages of interest to the administrator (general SYSLOG priority: PANIC, ALERT, CRIT).
  - Error: All event messages which can occur under normal conditions are communicated, e.g. connection errors detected (e.g., general SYSLOG priority: ERROR). No specific action is required by the administrator.
  - Warning: Messages that do not compromise normal operating conditions (general SYSLOG priority: WARNING) are communicated.
  - Information: Messages that are of a purely informational character (general SYSLOG priority: NOTICE, INFORM) are communicated.

- Debug: Communication of all debug messages. Debug messages generate large data volumes and can compromise the device's operation. For this reason they should be disabled for normal operations and only used for troubleshooting (general SYSLOG priority: DEBUG).

## 14 Monitoring the LAN

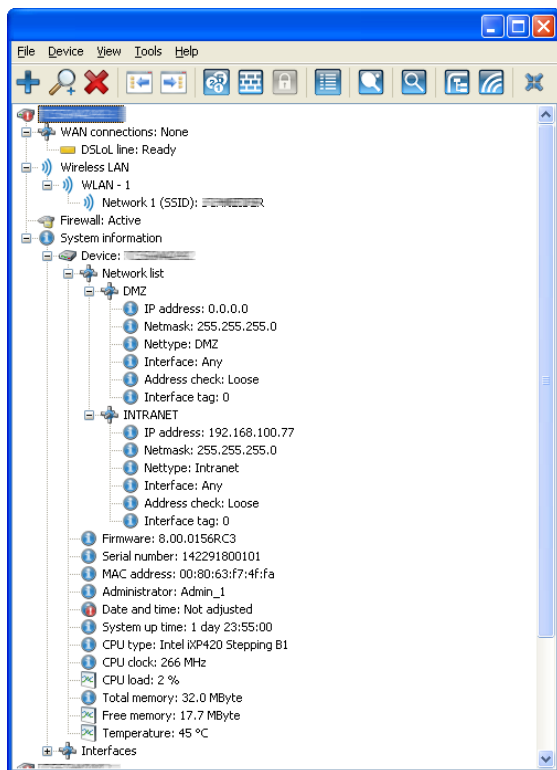
You use the LANmonitor software tool for the following tasks:

- ▶ To display the status of the individual Switch devices in the network
- ▶ To monitor traffic at the various interfaces of the Switch device
- ▶ To gather information about configurable device settings that are used to optimize the data traffic

**Note:** Monitoring with LANmonitor is only possible for devices that are connected via their IP address. LANmonitor is unable to access devices that are connected via their serial interface.

# 14.1 Display Functions in LANmonitor

LANmonitor supports the administration of the Switch applications by offering a range of functions that simplify the surveillance of devices at widely dispersed locations. The overview of devices monitored by LANmonitor displays information about the status of the devices:



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

Right-clicking on a device in LANmonitor opens a context menu with additional 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:

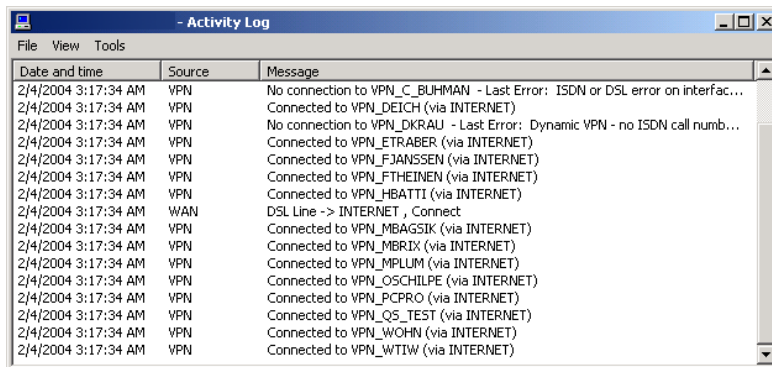
- Name or IP address of the station
- Remote station used to establish the connection
- Type of connection, e.g. digital subscriber line (DSL)
- Number of connections
- Data volume transmitted and received
- total online time

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
	VPN_WOHN	VPN connection	0	3,904 KB	113,534 KB	17 days and 21 hours
	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
	VPN_ETRABER	VPN connection	0	17,761 KB	12,425 KB	14 days and 8 hours
	VPN_TNIO	VPN connection	0	189 KB	386 KB	13 days and 14 hours
	VPN_MPLUM	VPN connection	0	3,758 KB	40,226 KB	11 days and 22 hours
	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
	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
	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

► Activity log

The activity log is a detailed list of the connections via WAN, WLAN, and a list of firewall activities. The detailed information recorded includes:

- Date and time
- Source
- Message

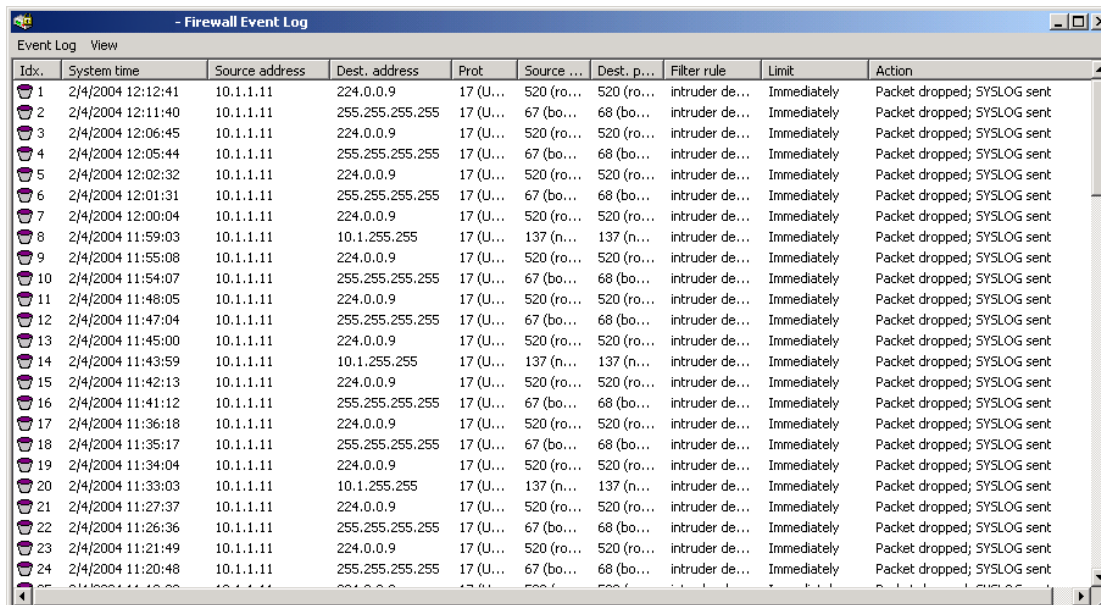


Date and time	Source	Message
2/4/2004 3:17:34 AM	VPN	No connection to VPN_C_BUHMANN - Last Error: ISDN or DSL error on interfac...
2/4/2004 3:17:34 AM	VPN	Connected to VPN_DEICH (via INTERNET)
2/4/2004 3:17:34 AM	VPN	No connection to VPN_DKRAU - Last Error: Dynamic VPN - no ISDN call numb...
2/4/2004 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)

### ► Firewall actions log

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

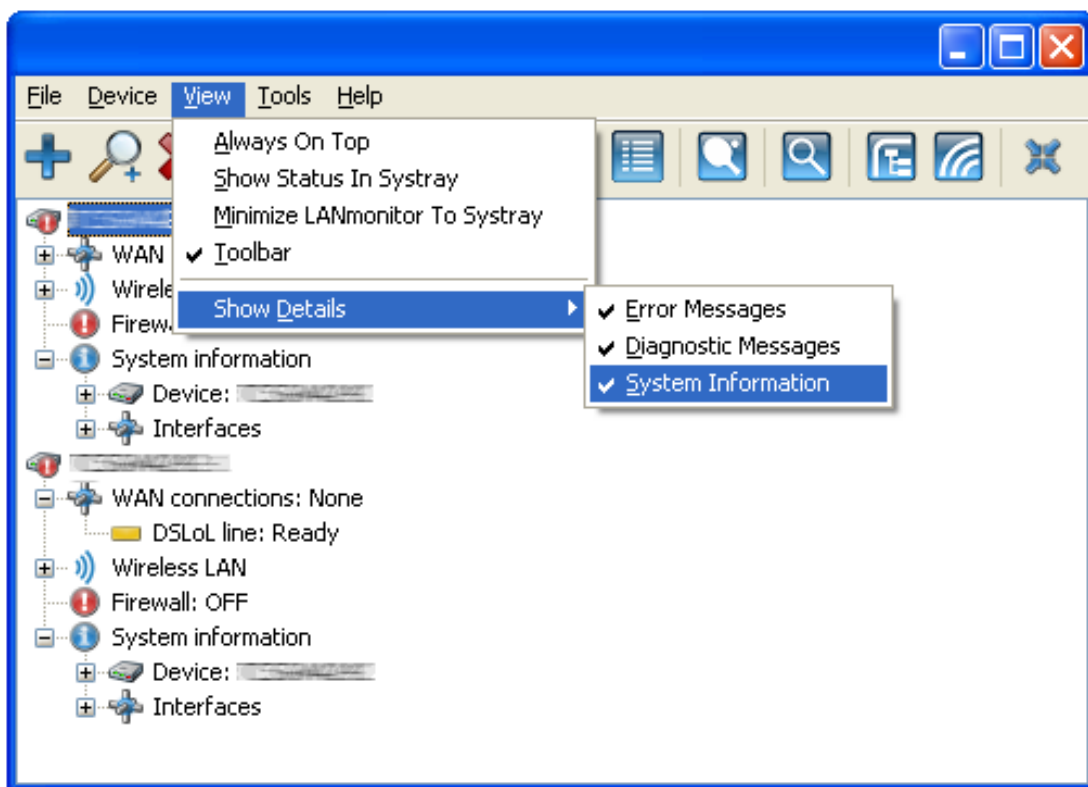
- Time
- Source and destination address
- Protocol with source and destination port
- Activated filter rule and exceeded limit
- Action carried out



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
16	2/4/2004 11:41:12	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
17	2/4/2004 11:36:18	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
18	2/4/2004 11:35:17	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
19	2/4/2004 11:34:04	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
20	2/4/2004 11:33:03	10.1.1.11	10.1.255.255	17 (U...	137 (n...	137 (n...	intruder de...	Immediately	Packet dropped; SYSLOG sent
21	2/4/2004 11:27:37	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
22	2/4/2004 11:26:36	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
23	2/4/2004 11:21:49	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
24	2/4/2004 11:20:48	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent

## 14.2 Expanded Display Options

You can expand the display of monitoring information presented in LANmonitor, by clicking **View : Show Details**, then activating the individual expanded display options:



The additional display options include:

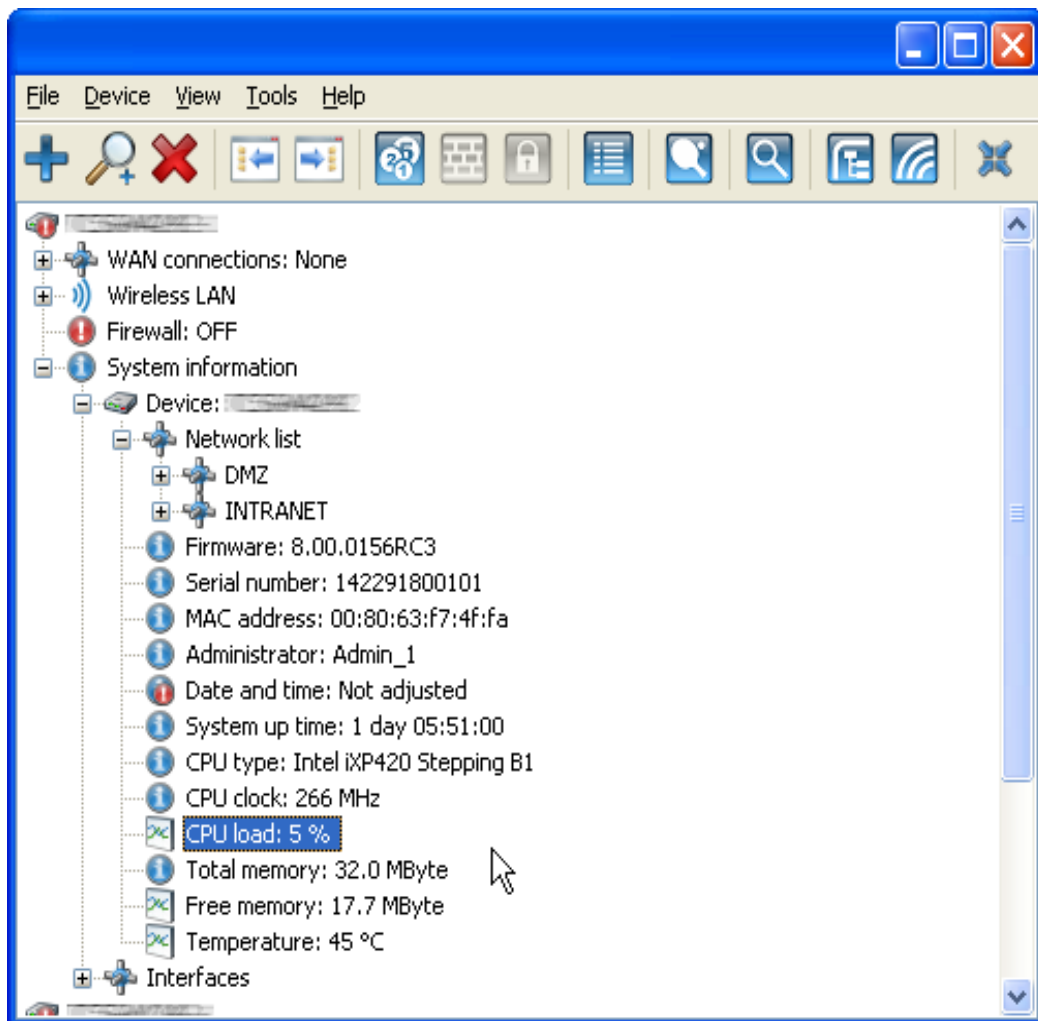
- ▶ Error messages
- ▶ Diagnostic messages
- ▶ System information

**Note:** Many important details about the status of the Switch device are only displayed when the system information display is activated. This includes, for example, the ports and the call charge management.



## 14.3 Querying CPU and Memory Utilization via SNMP

You can query the CPU and memory utilization of the Switch device via SNMP or display it in LANmonitor.



## 14.4 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 test the parameters and display the results in LANmonitor, open the 'Ping' dialog, either by:

- ▶ Selecting **Tools** : **Ping**, or
- ▶ Selecting a device in the LANmonitor list, then selecting **Device** : **Ping...**

Description	Total run time	Period
Test run time:		
Transmitted:		
Last ping (ms):		
Received until timeout:		
Minimum (ms):		
Maximum (ms):		
Average (ms):		
Standard deviation (ms):		
Received after timeout:		
Late (%):		
Minimum (ms):		
Maximum (ms):		
Average (ms):		
Lost:		
Lost (%):		
Last error:		

## 14.4.1 Ping Configuring

Configure the ping using the following parameters. The following information can be entered for each different network device (servers, clients, routers, printers, etc.) which can be reached via LAN, WAN or WLAN:

- ▶ Host name or IP address  
The remote station which is to be queried is entered here.

- ▶ Ping interval  
The time interval, in ms, between two consecutive pings.

**Note:** 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 wait interval for the response to a ping to arrive [ms]. If this time expires and no response is 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.

**Note:** 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.

## 14.4.2 Ping 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.

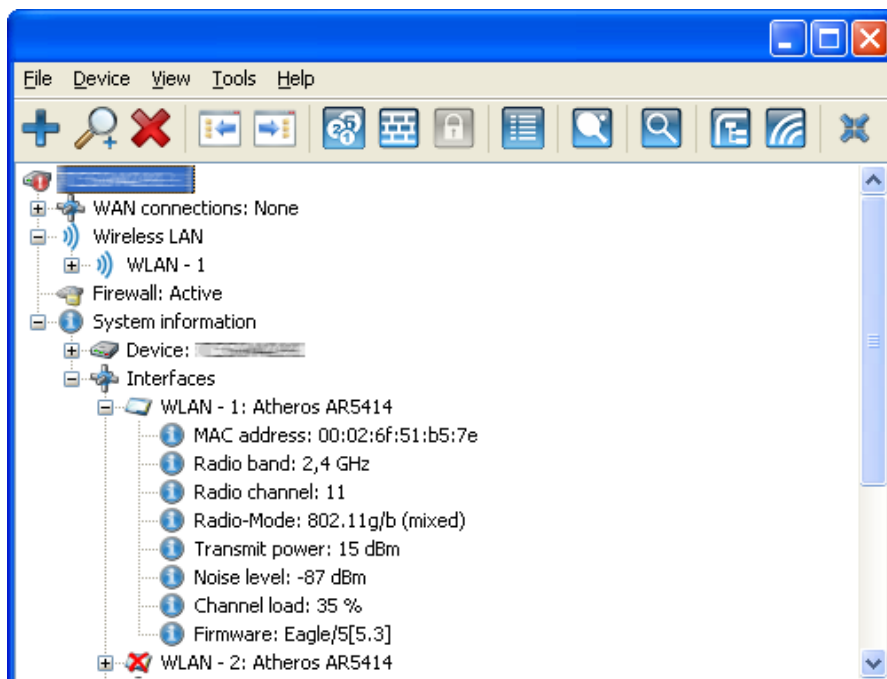
The following information is displayed for evaluation:

- ▶ 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
- ▶ Last error
  - The last error detected by the tool while attempting to ping the host (e.g. 'Time Limit Exceeded' when the host is not reachable).

# 14.5 Monitoring Internet Connections

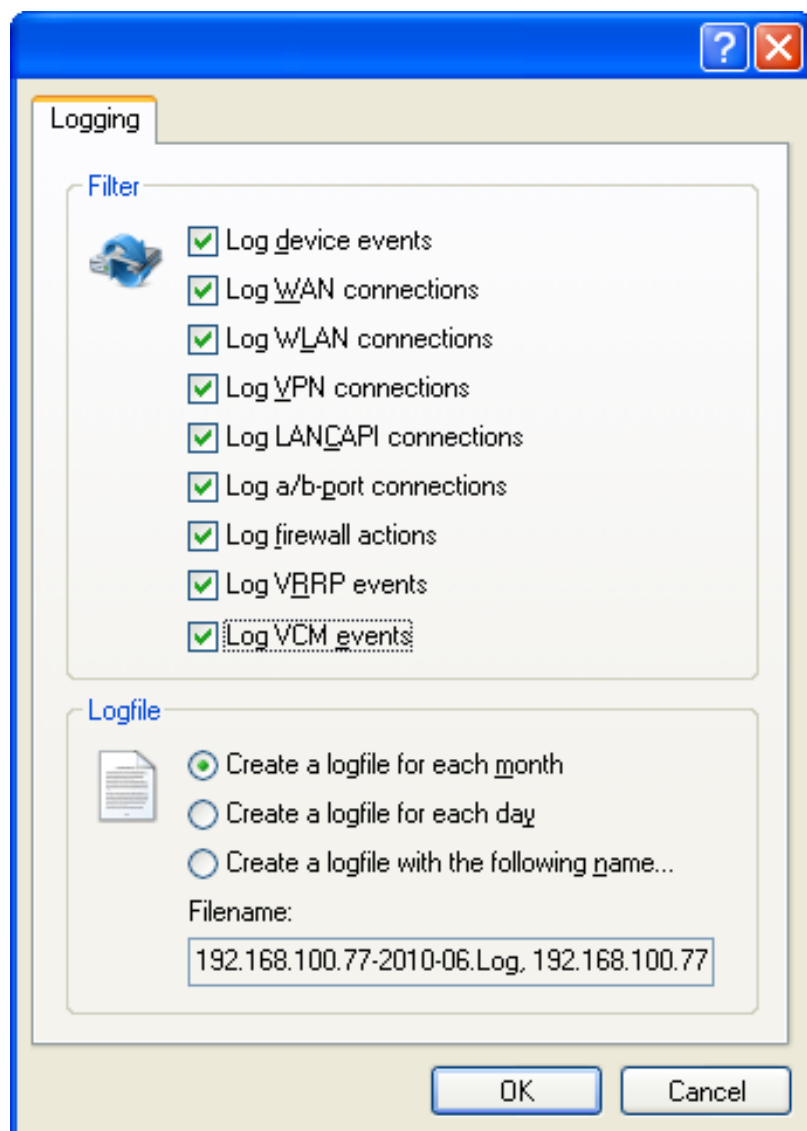
LANmonitor can display information about connections to your Internet provider.

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 the desired web page. LANmonitor shows a connection being established on one channel and the name of the remote site being called. Once the connection is established, a plus sign on the communication channel entry indicates that further information about 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:



The PPP protocol information lets you determine 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.

- ▶ To break the connection manually, right-click on the active channel. You may be required to enter a configuration password.
- ▶ If you would like a log of the LANmonitor output in file form, select `Device : Device Activities Logging` and select the 'Logging' tab:



In the above dialog, you can specify the activities to be logged, and how frequently LANmonitor should create a log file: daily, monthly, or on an ongoing basis.

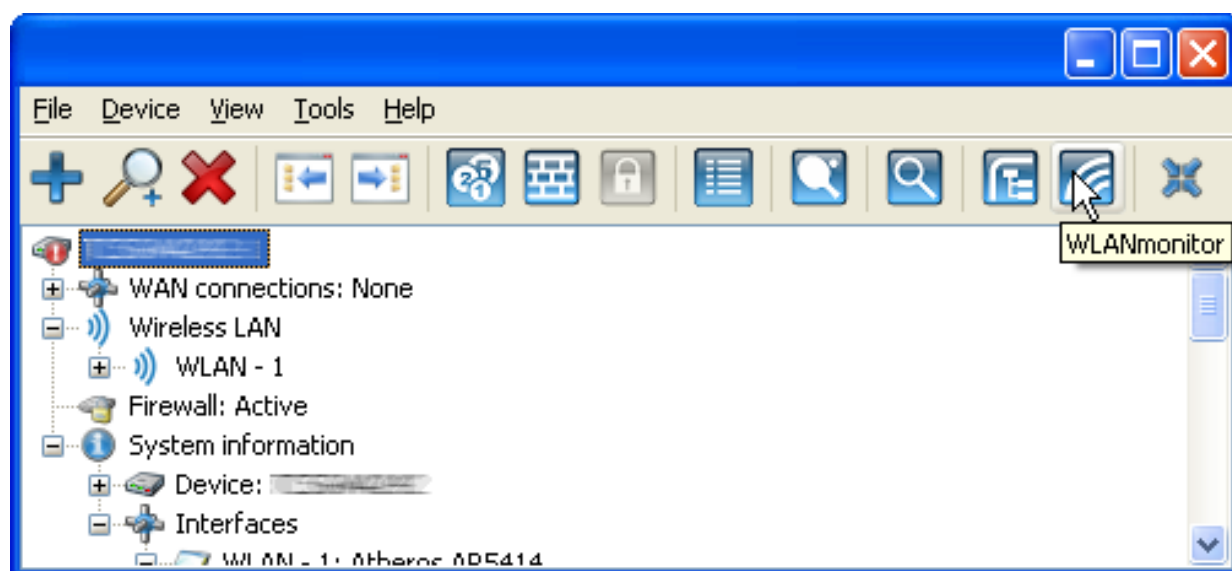
## **15 Monitoring WLANs with WLANmonitor**

WLANmonitor is a component of LANmonitor. You can use WLANmonitor to collect access points into groups. These groups may consist of access points located in buildings, departments, or at individual locations. This helps give you an overview of the entire network for large WLAN infrastructures.

## 15.1 Starting WLANmonitor

You can open WLANmonitor several ways:

- ▶ from LANmonitor using the command `Tools : WLANmonitor`
- ▶ from LANmonitor using the WLANmonitor menu button
- ▶ from the Windows `start` button, navigating to the location where you installed the LANmonitor and WLANmonitor programs.





## 15.2 Searching for Access Points

After starting WLANmonitor, you can search for available access points using the `Access Point : Find Access Points` command.

Access Points list:

WLANmonitor lists the access points it discovers in the center of the dialog, along with the following information each access point interface:

- ▶ Access point name
- ▶ WLAN interface name
- ▶ Number of the connected clients
- ▶ Frequency band
- ▶ Channel
- ▶ Transmit power
- ▶ Noise level
- ▶ Channel load
- ▶ IP address of the access point
- ▶ Background scan

Clients list:

The right side of the dialog lists the clients that are logged on to each access point, along with the following information for each client:

- ▶ Connection Quality: A bar-chart icon indicating signal strength
- ▶ MAC address: Hardware address of the WLAN client
- ▶ Identification: The name of the logged-in client as entered into the access list or a RADIUS server.

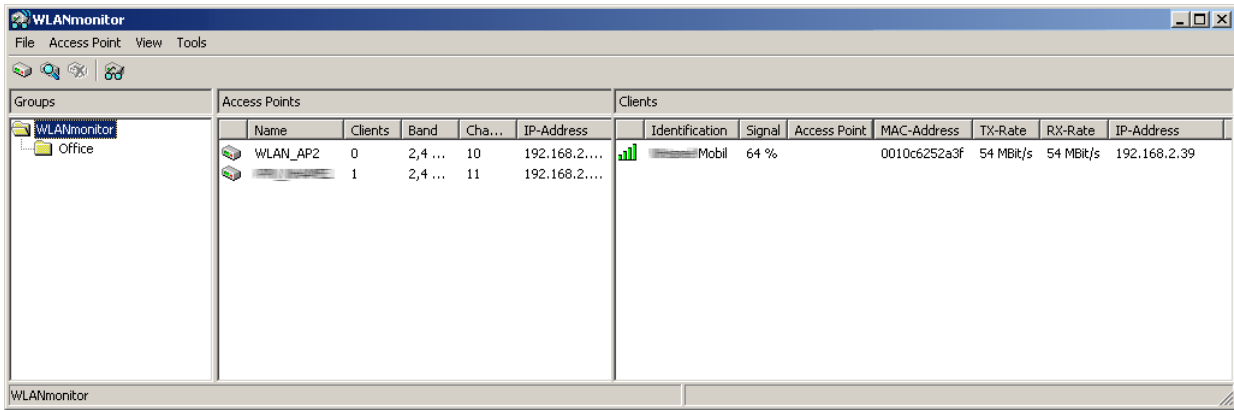
LANconfig: `WLAN Security : Stations : Stations`

Telnet: `Setup/WLAN/Access-List`

WEBconfig: `Hirschmann`

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
- ▶ Key type: The type of encryption used for the wireless connection
- ▶ WPA version: WPA-1 or WPA-2
- ▶ TX rate: Transmission data rate
- ▶ RX rate: Reception data rate
- ▶ Last error
- ▶ IP address of the WLAN client



The screenshot shows the WLANmonitor application window. On the left, a tree view under 'Groups' shows 'WLANmonitor' and 'Office'. The main area is divided into two tables: 'Access Points' and 'Clients'.

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

Identification	Signal	Access Point	MAC-Address	TX-Rate	RX-Rate	IP-Address
Mobil	64 %		0010c6252a3f	54 MBit/s	54 MBit/s	192.168.2.39

## 15.3 Adding Access Points

If an access point was not recognized automatically, you can manually add it to the list. **Access Point : Add Access Point.**

- In WLANmonitor, select **Access Point : Add Access Point.**

**New Device**

**Address**

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

IP

**Authentication**

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

Administrator:

Password:

Notes: The administrator may only be specified if an administrator account has been configured in the device. Incorrect configuration access data will lock the SNMP access.

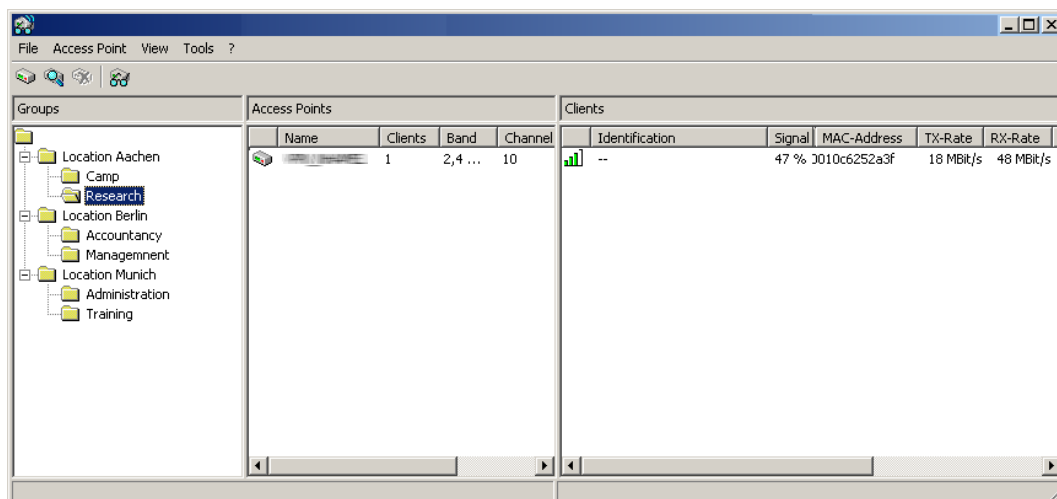
OK Cancel

Use this dialog to enter the IP address or the name of the access point, the administrator name, and the corresponding password.

## 15.4 Organize Access Points

Use WLANmonitor to organize all available access points independent of their physical location. This helps to maintain an overview of the network and is particularly useful when troubleshooting. Further, WLAN information can be called up according to the groups. You can group your access points according to their departments, locations or applications.

The groups are shown in the left column in WLANmonitor. Starting from the top group “WLANmonitor,” use the command `Group : Add Group` to create new sub-groups and build a structure. Access points found during a search are assigned to the currently selected group in the group tree. Access points that have already been recognized can be dragged and dropped to another group.



To aid the allocation of access points and clients, you can mark a device by selecting it with the mouse. Any associated devices are also be marked in the list, as follows:

- ▶ If an access point is selected in the access point list, all of the clients logged in to this device is also selected in the client list.
- ▶ If a client is selected in the client list, the access point that it is associated with it is also selected in the access point list.

## **15.5 Detecting Rogue Access Points and Clients with WLANmonitor**

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

Rogue clients:

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.

Rogue Access Points:

An example of a rogue access point is one that a company's employees use to connect to the network without the knowledge or permission of the system administrators. This practice renders a network vulnerable to potential attackers via unsecured WLAN access. Another example is an access point that belongs to third-party networks, but which are within the range of the local WLAN. If such devices use the same service set identity (SSID) and channel as a local access point (for example, by application of default settings), local clients could unintentionally log on to external networks.

Unidentified access points within the range of the local network are not desired. These devices need to be identified to be able to determine 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 Switch wireless router. Once activated, background scanning identifies any 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" and "rogue."

## 15.5.1 Rogue Access Point Detection

WLANmonitor sorts all of the access points it detects into predefined subgroups, under the folder 'Rogue AP Detection'. Activate background scanning in the wireless router in order to use rogue access point detection.

**Note:** Rogue access point detection is active exclusively when background scanning is enabled in the Switch configuration. To enable background scanning, use LANconfig to enter a positive integer value into the 'Background scan' property for a WLAN interface in the following location:

```
Configuration : Wireless LAN : General :  
Physical WLAN settings : <WLAN interface> : Radio.
```

WLANmonitor displays the following under Rogue AP Detection

- ▶ Time of first and last detection
- ▶ BSSID: The MAC address of the access point for this WLAN network
- ▶ Network name
- ▶ Type of encryption
- ▶ Frequency band
- ▶ Radio channel
- ▶ Use of 108 Mbps mode

The WLANmonitor uses the following groups for sorting access points:

- ▶ All APs: List of all scanned WLAN networks (access points are colored according to their group)
- ▶ New APs: New unknown and unconfigured WLAN networks are automatically grouped here (access points are displayed in yellow)
- ▶ Rogue APs: WLAN networks identified as rogue and in need of urgent observation (access points are displayed in red)
- ▶ Unknown APs: WLAN networks which need to be further analyzed (access points are displayed in gray)
- ▶ Known APs: WLAN networks which are not a threat (access points are displayed in gray)
- ▶ Own APs: New affiliated WLAN networks from access points monitored by WLANmonitor are automatically grouped here (access points are 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 (with the exception of the group “All APs”) using the context menu. If a parameter, such as the security settings, is changed on an access point, then it is displayed again as a newly discovered access point.

The screenshot shows the WLANmonitor application window. On the left, a tree view displays the following groups:

- WLANmonitor (12)
  - Rogue AP Detection
    - All APs (111)
    - New APs
    - Rogue APs
    - Unknown APs
    - Known APs
    - Own APs
  - Rogue Client Detection
    - All Clients (2)
    - New Clients (1)
    - Rogue Clients
    - Unknown Clients
    - Known Clients
    - Own Clients

The main window displays the 'Rogue AP Detection' table with the following columns: Last Seen, Identification, Network Name (S...), Band, Cha..., Encry..., 108..., and First Seen. The table contains 30 rows of data. A tooltip is visible over the table, showing details for IP addresses 10.1.1.31, 10.1.10.193, 10.1.10.192, 10.1.10.189, and 10.1.10.188, including interface information and signal strength.

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 11:46:02
18.08.2006 15:45:49	Client02	Network01	2,4 GHz	11	None	No	29.06.2006 11:46:02
03.07.2006 16:39:05	Client03	Network01	5 GHz	100	AES	No	03.07.2006 15:29:43
03.07.2006 16:39:05	Client04	Network01	5 GHz	100	AES	No	03.07.2006 15:29:43
04.07.2006 18:16:46	Client01	Network02	2,4 GHz	11	None	No	03.07.2006 15:29:47
09.08.2006 15:39:52	Client02	Network02	2,4 GHz	11	None	No	09.08.2006 14:49:27
18.08.2006 15:45:44	Client03	Network02	2,4 GHz	11	None	No	10.08.2006 18:58:49
11.08.2006 09:15:06	Client04	10.1.1.31: Interface: WLAN-1, Signal: 50 %	2,4 GHz	11	None	No	10.08.2006 18:58:50
11.08.2006 12:27:58	Client01	10.1.10.193: Interface: WLAN-1, Signal: 10 %	2,4 GHz	11	None	No	11.08.2006 10:06:49
18.08.2006 15:46:03	Client02	10.1.10.192: Interface: WLAN-1, Signal: 31 %	2,4 GHz	11	None	No	11.08.2006 10:06:49
18.08.2006 15:46:03	Client03	10.1.10.189: Interface: WLAN-1, Signal: 45 %	2,4 GHz	11	None	No	18.08.2006 12:40:46
18.08.2006 15:46:03	Client03	10.1.10.188: Interface: WLAN-1, Signal: 18 %	2,4 GHz	11	None	No	18.08.2006 12:40:46
18.08.2006 15:45:20	Client04	Network04	2,4 GHz	11	None	No	18.08.2006 12:40:50
18.08.2006 15:45:20	Client01	Network04	2,4 GHz	11	None	No	18.08.2006 14:54:08
18.08.2006 15:45:44	Client02	Network04	2,4 GHz	5	WEP	No	29.06.2006 11:46:02
18.08.2006 15:45:49	Client03	Network04	2,4 GHz	7	WEP	No	29.06.2006 11:46:02
18.08.2006 15:45:49	Client04	Network04	2,4 GHz	7	WEP	No	29.06.2006 11:46:02
11.08.2006 12:28:44	Client01	Network04	2,4 GHz	11	WEP	No	29.06.2006 11:46:02
18.08.2006 15:45:49	Client02	Network04	2,4 GHz	3	WEP	No	03.07.2006 15:29:44
13.07.2006 09:11:34	Client03	Network04	2,4 GHz	1	WEP	No	12.07.2006 23:10:24
18.08.2006 15:45:44	Client04	Network04	2,4 GHz	11	WEP	No	18.08.2006 15:44:35
15.07.2006 11:33:43	Client01	Network04	2,4 GHz	6	WEP	No	29.06.2006 11:46:02
04.07.2006 18:16:53	Client02	Network04	2,4 GHz	11	WEP	No	29.06.2006 11:46:02
04.07.2006 18:16:53	Client03	Network04	2,4 GHz	11	WEP	No	29.06.2006 11:46:02
15.07.2006 11:33:43	Client04	Network04	2,4 GHz	11	AES	No	12.07.2006 23:10:21
11.08.2006 09:15:06	Client01	Network04	5 GHz	140	AES+TKIP	No	09.08.2006 14:49:19
18.08.2006 15:45:44	Client02	Network04	2,4 GHz	6	WEP	No	09.08.2006 14:49:21
18.08.2006 15:45:44	Client03	Network04	2,4 GHz	11	WEP	No	18.08.2006 12:40:34
18.08.2006 15:45:49	Client04	Network04	5 GHz	100	AES	No	29.06.2006 11:45:56
18.08.2006 15:45:44	Client01	Network04	2,4 GHz	1	AES+TKIP	No	29.06.2006 11:46:02
18.08.2006 15:45:44	Client02	Network04	2,4 GHz	1	AES	No	29.06.2006 11:46:02
18.08.2006 15:45:44	Client03	Network04	2,4 GHz	1	AES	No	29.06.2006 11:46:02

## 15.5.2 Rogue Client Detection

WLANmonitor sorts all the clients found into pre-defined subgroups in the “Rogue Client Detection” folder. It is not necessary to configure the Switch device to activate the Rogue Client Detection.

The following information is displayed under Rogue Client Detection:

- ▶ Time of first and last detection
- ▶ MAC address of the client
- ▶ Network name (SSID)

The WLANmonitor uses the following groups for sorting clients:

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

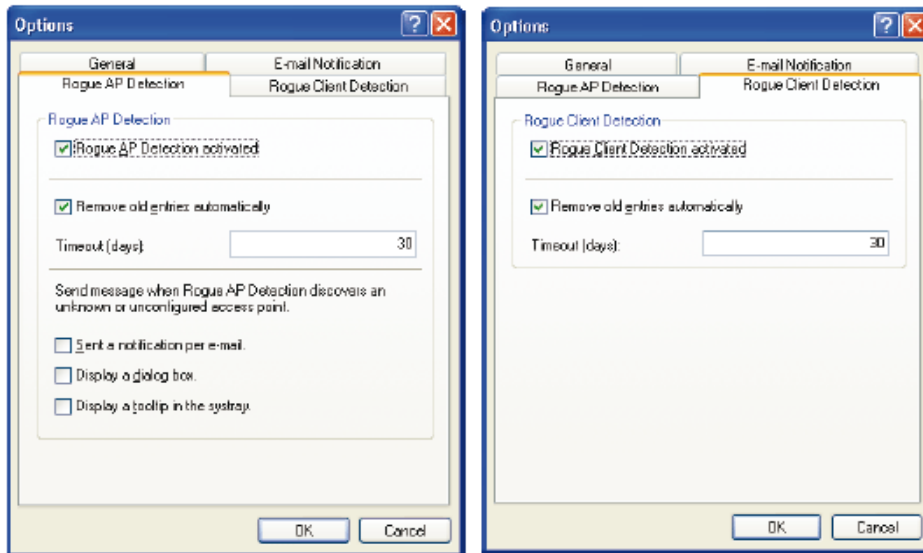
Clients can be placed into a corresponding group depending on their status. You can set up your own network groups within the individual groups (except for the group “All clients”) using the context menu.

### **15.5.3 Activating Rogue Access Point and Client Detection**

You can activate automatic detection of rogue devices in WLANmonitor:

- ▶ For rogue access points:  
Tools : Options : Rogue AP Detection
- ▶ For rogue clients:  
Tools : Options : Rogue Client Detection

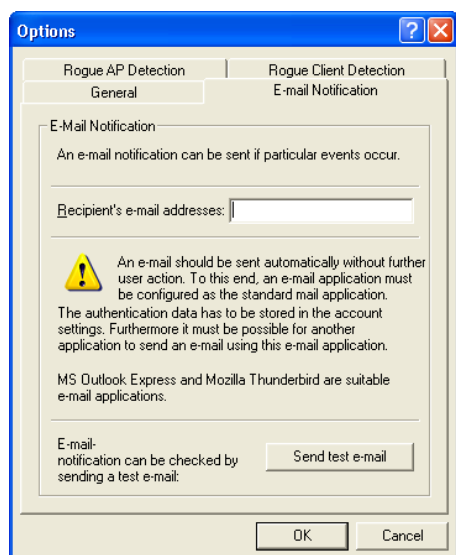




### 15.5.4 Configuring the Alert Function with WLANmonitor

WLANmonitor can inform the administrator automatically via e-mail whenever an unknown or unconfigured access point is discovered. In order to send e-mail alerts, start and configure an e-mail client that supports automatic e-mail transmission on the computer on which WLANmonitor is running.

Enable the e-mail notification function by entering a recipient e-mail address in the `Tools : Options : E-mail Notification` dialog:



The following features apply to the e-mail function:

- ▶ **Recipient e-mail addresses**  
Enter the e-mail address(es) of the administrators who should be informed in the event of rogue access point detection. Separate multiple e-mail addresses by commas.
- ▶ **Send a test e-mail**  
Some mail clients require a confirmation from the user before sending via third-party applications. Select this option to test your system.

## 16 Device Diagnostics

Trace outputs may be used to monitor the internal processes in the router during or after configuration. One such trace can be used to display the individual steps involved in negotiating the PPP. Experienced users may interpret these outputs to trace any errors occurring in the establishment of a connection. This helps you determine if a detected event arises from the configuration of your own router or the remote site.

**Note:** The trace outputs are slightly delayed after the actual event, but are always in the correct sequence. This should be taken into consideration if making precise analyses.

## 16.1 Starting a Trace in Telnet

Trace output can be started in a Telnet session. Set up a Telnet connection to your device. The command to call up a trace follows this syntax:

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

The trace command, the code, the parameters and the combination commands are all separated from each other by spaces.

### 16.1.1 Code Key Overview

The following keys can be used in trace code:

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

### 16.1.2 Trace Parameters

The trace parameters available depend on the specific Switch device. To call up the list of device parameters available, enter the `trace` command without arguments in the command line.

This parameter...	...opens the following trace display...
ADSL	ADSL connections status
ARP	Address Resolution Protocol
ATM-cell	spoofing at the ATM packet level

<b>This parameter...</b>	<b>...opens the following trace display...</b>
ATM-error	ATM errors
Bridge	Information concerning WLAN bridge
Connect	Messages from the activity protocol
Cron	cron table
DFS	Trace for Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service Protocol
EAP	Trace for EAP
Error	error messages for the connection
Ethernet	Status of Ethernet interface
Firewall	Firewall activities
IAPP	Trace for Inter Access Point Protocol: information concerning WLAN roaming
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP masquerading	processes in the masquerading module
IPX-RIP	IPX Routing Information Protocol
IPX-router	IPX routing
IPX-watchdog	IPX watchdog spoofing
LANAUTH	LAN authentication
LCR	Least-Cost Router
Load-Balancer	Load balancing information
Mail-Client	E-mail processing of the integrated mail client
NetBIOS	NetBIOS management
NTP	Timeserver Trace
Packet dump	display of the first 64 bytes of a package in hexadecimal form
PPP	PPP protocol negotiation
RADIUS	RADIUS trace
RIP	IP Routing Information Protocol
SAP	IPX Service Advertising Protocol
Script	script processing
Serial	Status of serial interface
SMTP-Client	E-mail processing of the integrated mail client
SNTP	Simple Network Time Protocol information
Spgtree	Information concerning Spanning Tree Protocol
SPX-watchdog	SPX watchdog spoofing
Status	status messages for the connection
USB	Status of USB interface
VLAN	Information concerning virtual networks
VRRP	Information concerning Virtual Router Redundancy Protocol
WLAN	Information concerning wireless networks

### 16.1.3 Combination Commands

The following commands can be used to display multiple results:

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

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

### 16.1.4 Trace Filters

Some traces, such as the IP router trace, produce a large quantity of output data. In many instances, the output can become unmanageable. Using trace filters lets you sift out important information. Activate a trace filter by adding the parameter "@" that induces the following filter description. Trace filters use the following operators:

Operator	Description
(space)	OR: The filter applies if one of the operator occurs in the trace output.
+	AND: The filter applies if the operator occurs in the trace output.
-	NOT: The filter applies if the operator does not occur in the trace output.
"	The output must match the search string exactly.

An operator can be entered as any string of characters, such as the name of a remote station, protocols or ports. The trace filter then processes the output according to the operator rules, much like an Internet search engine.

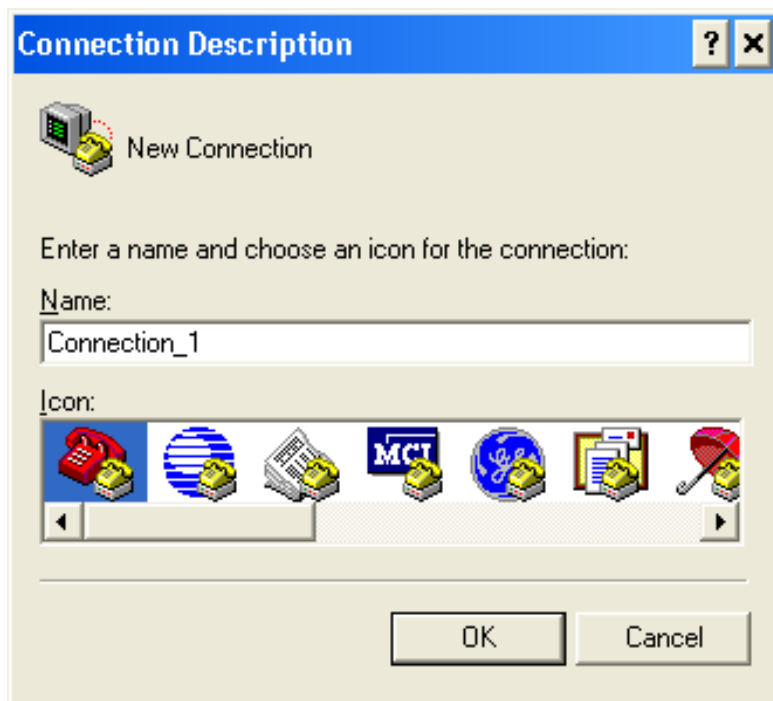
## 16.1.5 Trace Examples

<b>This code...</b>	<b>...causes the following:</b>
trace	Displays all protocols that can generate outputs during the configuration, and the status of each output (ON or OFF).
trace + all	Switches on all trace outputs.
trace - all	Switches off all trace outputs.
trace + protocol display	Switches on the output for all connection protocols together with the status and error messages.
trace + all - icmp	Switches on all trace outputs with the exception of the ICMP protocol.
trace ppp	Displays the status of the PPP.
trace # ipx-rt display	Toggles between the trace outputs for the IPX router and the display outputs.
trace + ip-router @ REMOTE SITE-A REMOTE SITE-B	Switches on all trace outputs for IP routers related to remote site A or B.
trace + ip-router @ REMOTE SITE-A REMOTE SITE-B -icmp	Switches on all trace outputs for IP routers related to remote site A or B that do not use ICMP.
trace + ip-router @ REMOTE SITE-A REMOTE SITE-B +ICMP	Switches on all trace outputs for IP routers related to remote site A or B that use ICMP.
trace + ip-router @+TCP +"port: 80"	Switches on all trace outputs from the IP router with TCP/IP and port 80. ("port: 80" is in quotes so that the space is recognised as a part of the string.)

## 16.2 Recording Traces with HyperTerminal

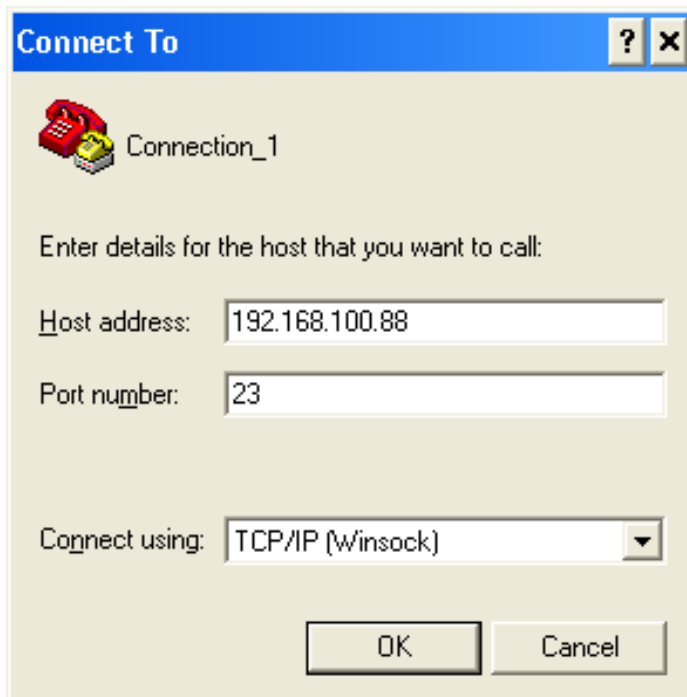
Traces can be conveniently recorded under Windows (e.g. as an aid to support), and we recommend you do this as follows:

- On your PC, start the program HyperTerminal by selecting:  
Start : Programs : Accessories : Communications :  
Hyper Terminal.

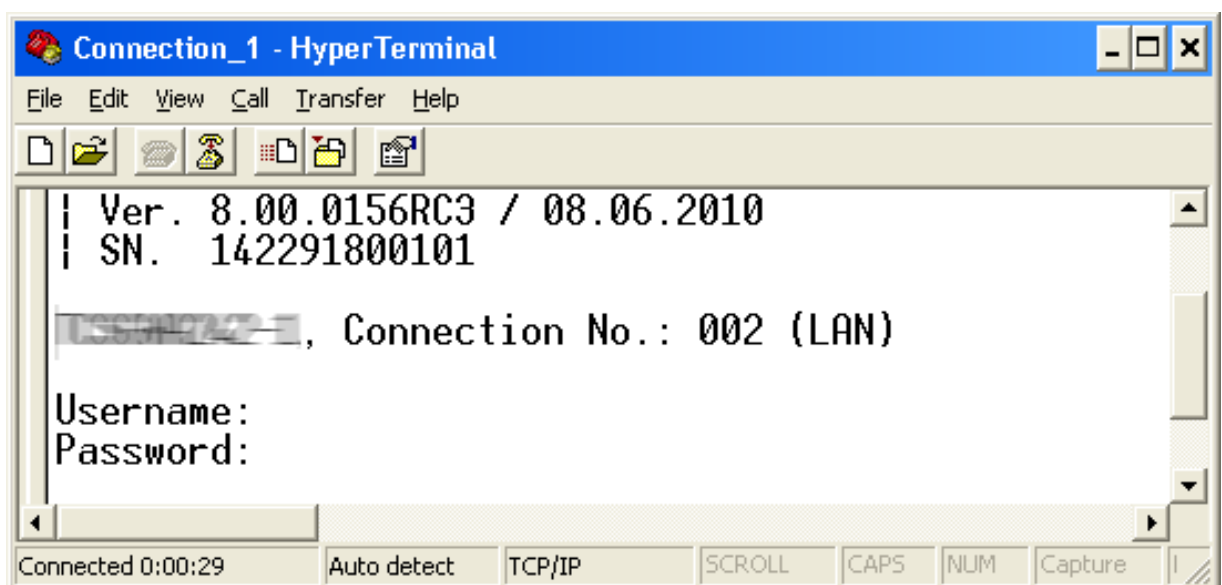


- Enter a 'Name', select an icon, and click 'OK'. The 'Connect To' dialog opens:





- In the 'Connect To' dialog, enter values for the following fields:
    - ▶ Connect using: TCP/IP (Winsock)
    - ▶ Host address: The local/official IP address or the device FQDN.
    - ▶ Port number: Use the default, port '23'.
- Click 'OK'. HyperTerminal displays a request to log in.



- Enter the 'Username' (if any) and click 'Enter', then enter the 'Password' and again click 'Enter'.
- To record a trace, select `Transfer : Capture Text...`, enter the path to the directory where the text file is to be saved, and click 'Start'. Now change back to the dialog window and enter the required trace command.
- In the Hyper Terminal dialog, enter the required trace command at the command line.
- To end the trace, select `Transfer : Capture Text : Stop`.

## 16.3 Tracing with LANmonitor

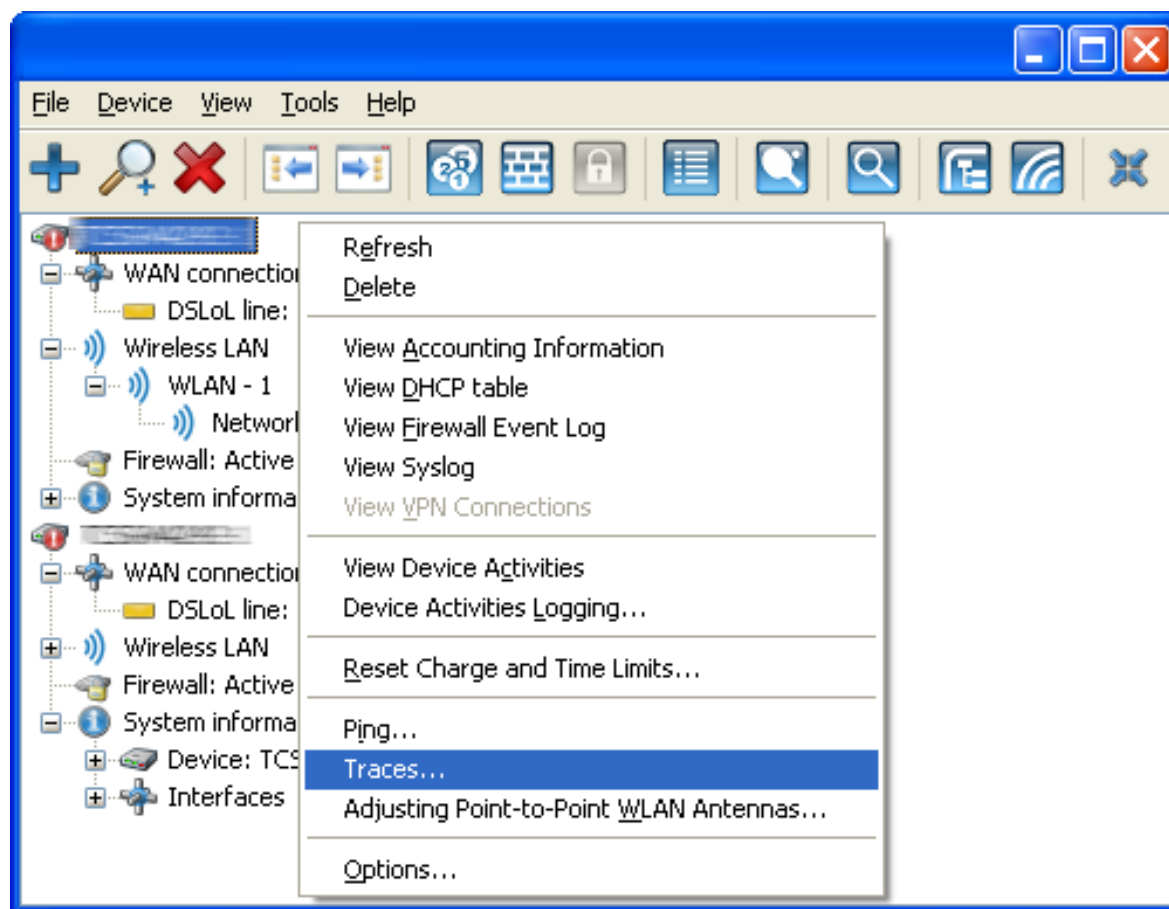
The trace function in LANmonitor is more robust than the standard trace functions available via Telnet, and offers greater convenience in the generation and analysis of traces.

For example, a trace configuration that triggers desired trace commands can be stored to a configuration file. An experienced service technician can program a trace configuration and deliver it to a less experienced operator who then can execute specialized trace requests for a device. Trace results can be stored in a file and returned to the technician for analysis.

Telnet-access to the device must be enabled to carry out trace requests with LANmonitor. When starting the trace dialog, LANmonitor first attempts to establish an SSL-encrypted Telnet connection to the device. If the device does not support SSL connections, LANmonitor automatically switches to unencrypted Telnet.

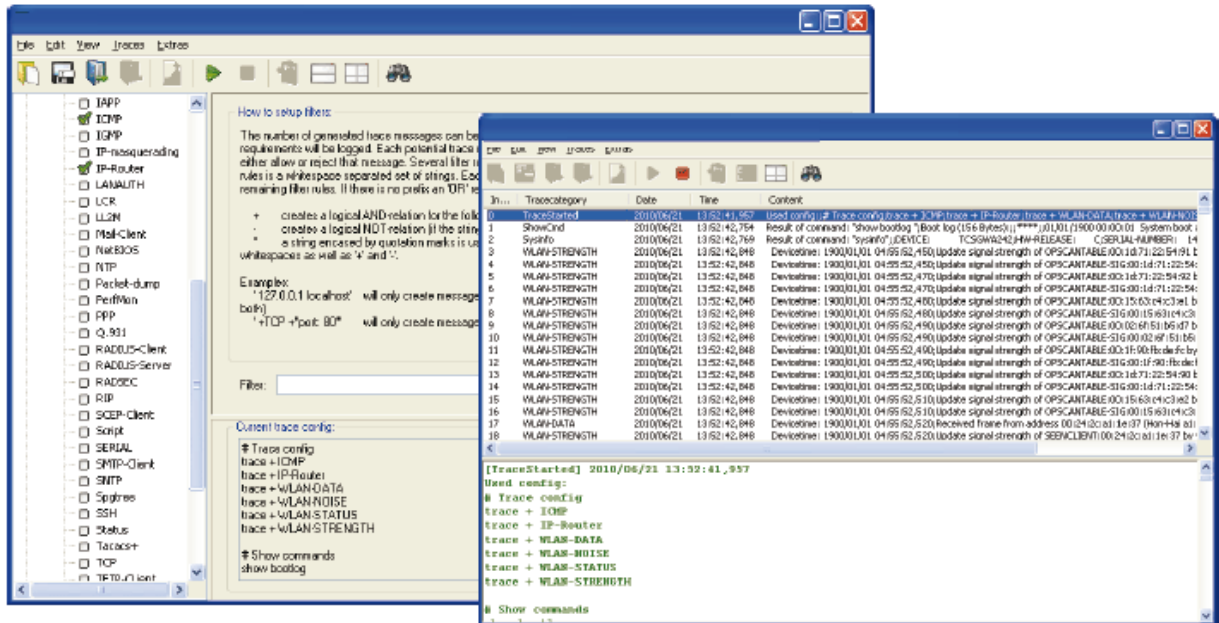
To open the “Traces” dialog for a specific Switch device:

- Right-click the device entry in LANmonitor and select “Traces” in the context menu:



- ▶ If SNMP access to the device is password-protected, enter the access data—name and password—for an administrator with trace rights in order to proceed with the trace.




The 'Traces' dialog presents two different appearances: configuration mode (left, below) and output display mode (right, below):



The LANmonitor 'Traces' dialog presents the following command buttons for operating traces:

Icon	Description
	Opens a pre-defined configuration for the trace command.
	Saves the current trace configuration.
	Opens a file with trace results for viewing in the 'Traces' dialog.
	Saves the current trace results to a file.
	Clears the current display or trace results.
	Starts outputting the trace results as produced by the current configuration and automatically switches the 'Traces' dialog interface to trace output display mode.

---

Icon	Description
	Stops the output of trace results.
	Switches the 'Traces' dialog interface to configuration mode.
	Switches the 'Traces' dialog interface to trace output display mode.

---

### 16.3.1 Creating Traces with the Trace Configuration Wizard

The trace settings can be configured very easily using the Trace Configuration Wizard. To use the wizard, follow these steps:

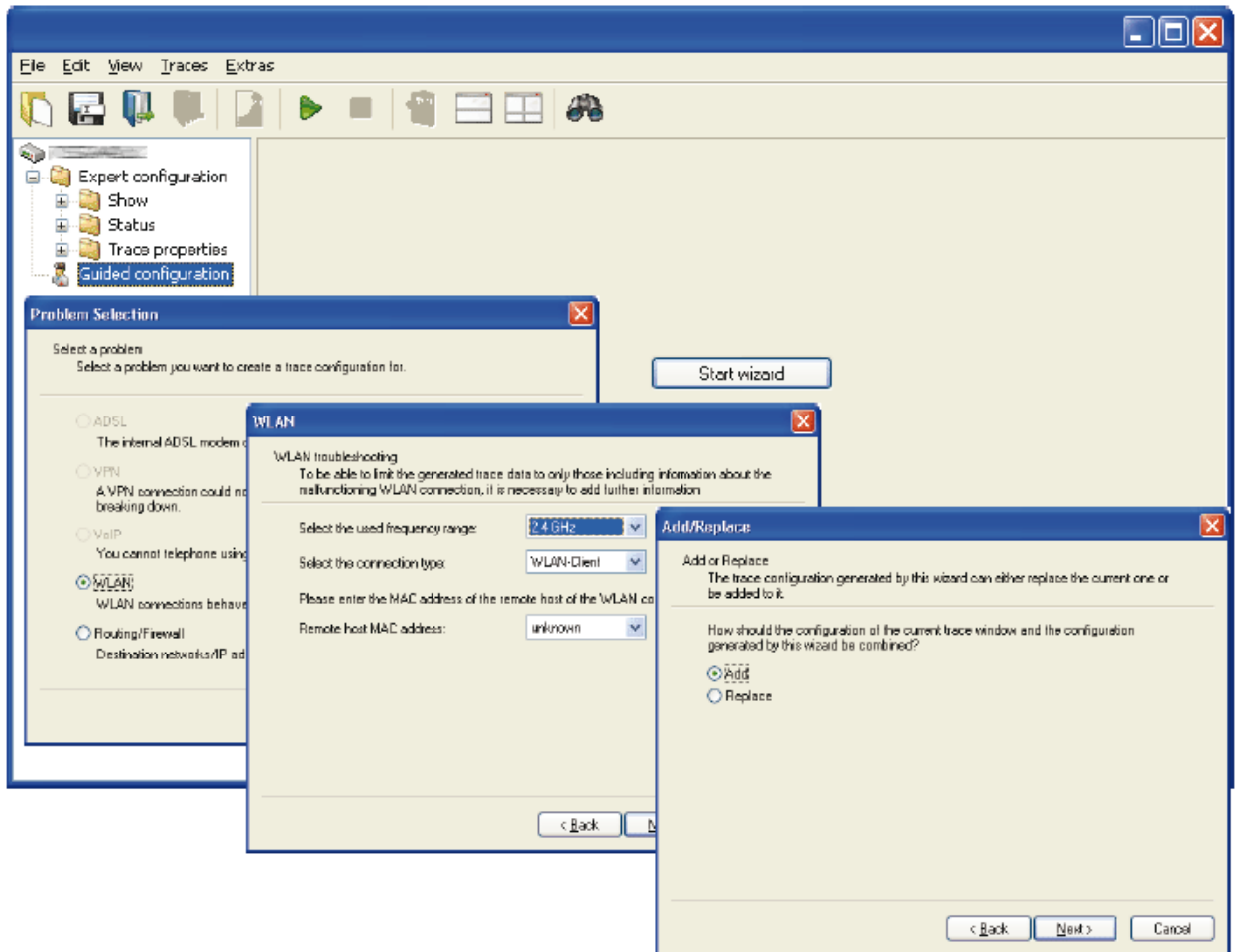
- With the 'Traces' dialog open for a selected device, select:  
<Device Name> : Guided configuration.
- Click the 'Start wizard' button to open the wizard, then follow the steps presented in the wizard.

Trace functions (e.g. WLAN) can be selected in the wizard dialogs, and the trace can be restricted as needed (for example, to a particular remote host).

The last step in the wizard is to indicate how the new trace configuration, created by the wizard, should be saved. Select either:

- ▶ Add, to combine the new configuration with the current trace configuration displayed in the 'Traces' dialog.
- ▶ Replace, to save only the new configuration created by the wizard, and deleting the previous trace configuration.

**Note:** Except for the bootleg trace (which is included automatically), all previous trace settings are deleted when the trace configuration is replaced. Save the previous trace configuration for later use before running the trace configuration wizard.



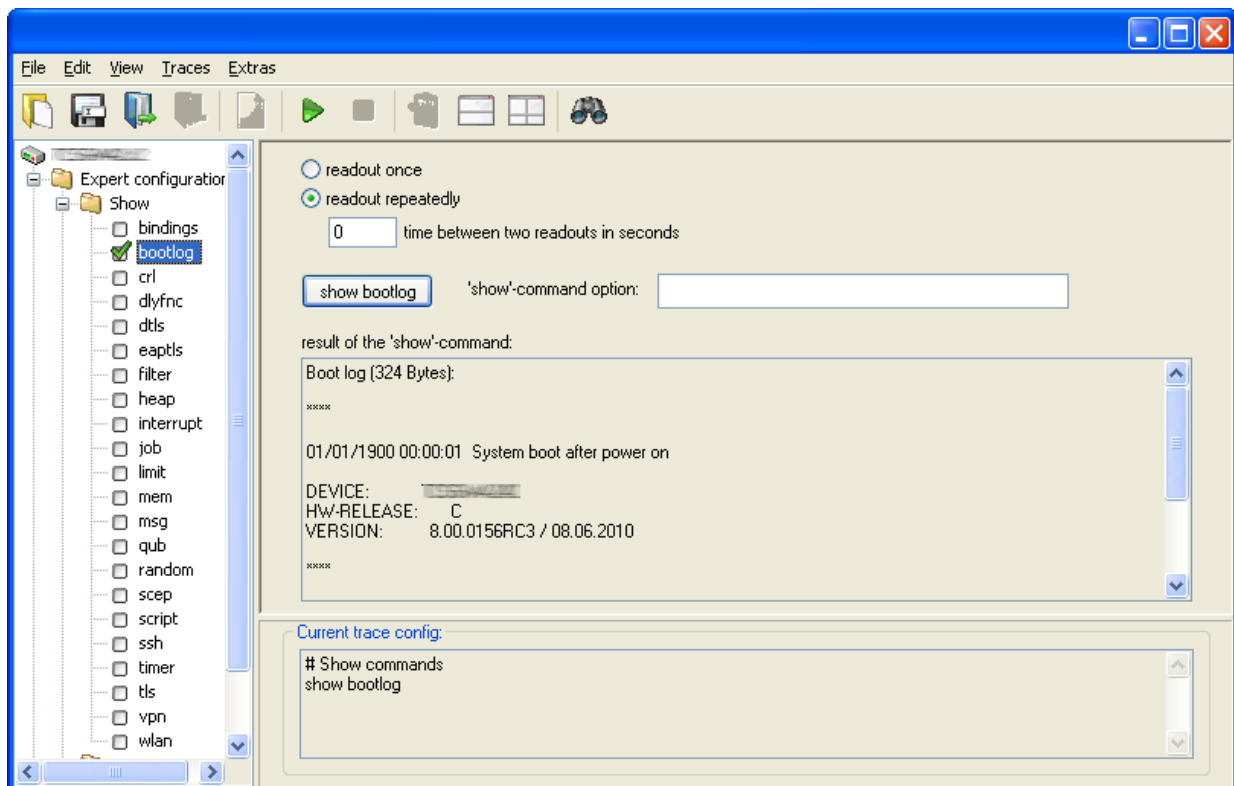
## 16.3.2 Manually Creating Trace Configurations

In addition to creating trace configurations with the wizard, you can also manually create trace configurations in the 'Traces' dialog, as follows:

- With the 'Traces' dialog open for a selected device, select:  
<Device Name> : Expert configuration.
- Enter trace settings in the Show, Status, and Trace properties folders. These folders and their contents are described, below.

### ■ Show folder settings

Use the contents of the 'Show' folder to retrieve device data that would ordinarily be obtained using the Show command from a command line interface (e.g. Telnet). You can either manually execute the Show command and immediately display selected device data, or you can add a Show command to the Trace configuration that will later be executed and generate the Trace dump.



- ▶ Immediately display selected data:  
You can manually display current values for selected device data. To do this, follow these steps:
  - Open the 'Show' folder and highlight one of the available data selections for the device. The 'show' button displays the data selection.

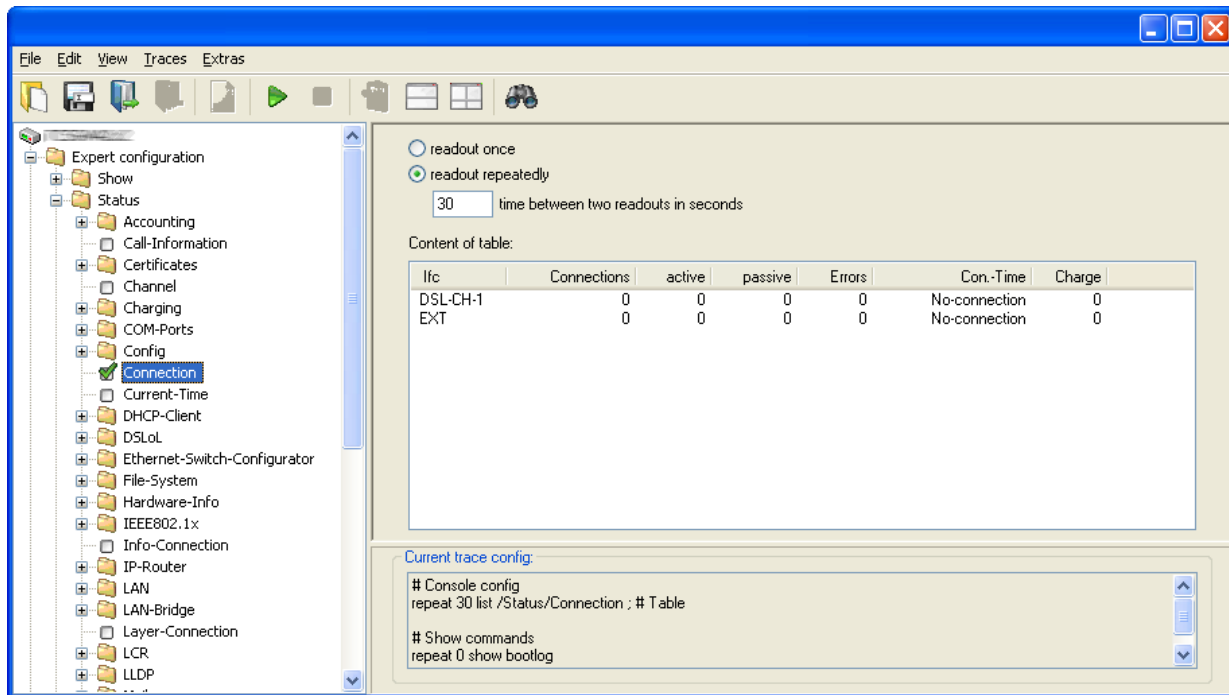


- Depending upon the selection, you may elect to—or may be required to—enter additional parameters in the input box labeled: ‘show-command option’.
- Click the ‘show’ button. Device data of the selected type is displayed in the ‘result’ area.
- ▶ Add a ‘Show’ command to the Trace dump:  
To add a command to the Trace dump, follow these steps:
  - Open the ‘Show’ folder and place a check mark in the check-box to the left one of the available data selections for the device. This enables the ‘readout’ selections for the entry.
  - Specify the readout frequency, i.e., how often the selected data will be read as part of the Trace dump:
    - readout once
    - readout repeatedly (and type in the time between readouts)

The selected entry is added to the Trace configuration, and appears as a line added to the ‘Current trace config’ area.

### ■ **Status folder settings**

You can access comprehensive status information and statistics for a device in the ‘Status’ folder of the ‘Traces’ dialog. Depending on your selection, the information accessed will be in the form of either a discrete value, or a table of values.



To display the current contents of the table or value, click the name of a status entry in the left-hand area of the trace dialogue. To accept the dump of the Status entry into the trace data, click the appropriate checkbox to the left of the entry name. For every Status entry enabled, a setting defines whether it is read out once only on starting the trace or whether it is read out at regular intervals (set in seconds).

- Open the 'Status' folder and select one of the available status entries for the device. The item value or the table values are displayed.
- To add the item as a Status entry in the Trace dump, place a check mark in the check-box next to the item. This enables the 'readout' selections for the Status entry.
- Specify the readout frequency, i.e., how often the selected status information will be read as part of the Trace dump:
  - readout once
  - readout repeatedly (and type in the time between readouts)

The selected entry is added to the Trace configuration, and appears as a line added to the 'Current trace config' area.

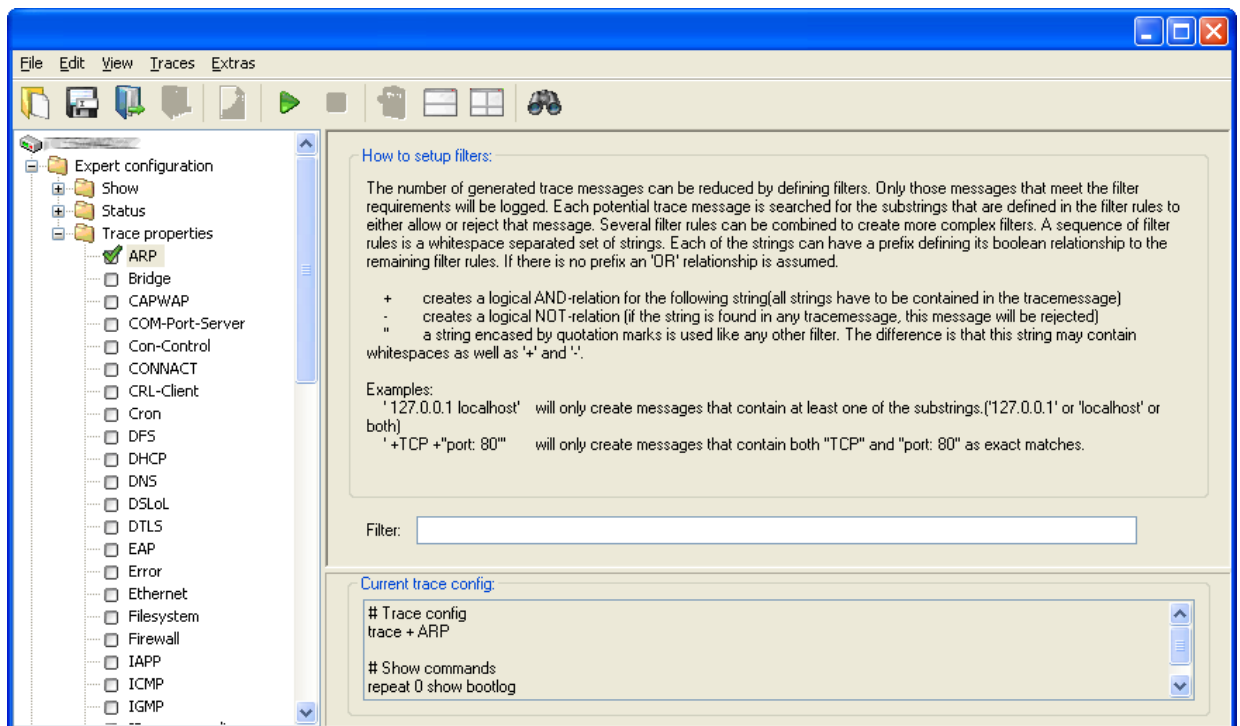
**Note:** This device Status information also can be accessed from the command line (Telnet) or via WEBconfig.

## ■ Trace properties folder settings

The traces to be dumped for the current device can be enabled in the trace settings area. To include the dump of the trace into the trace data:

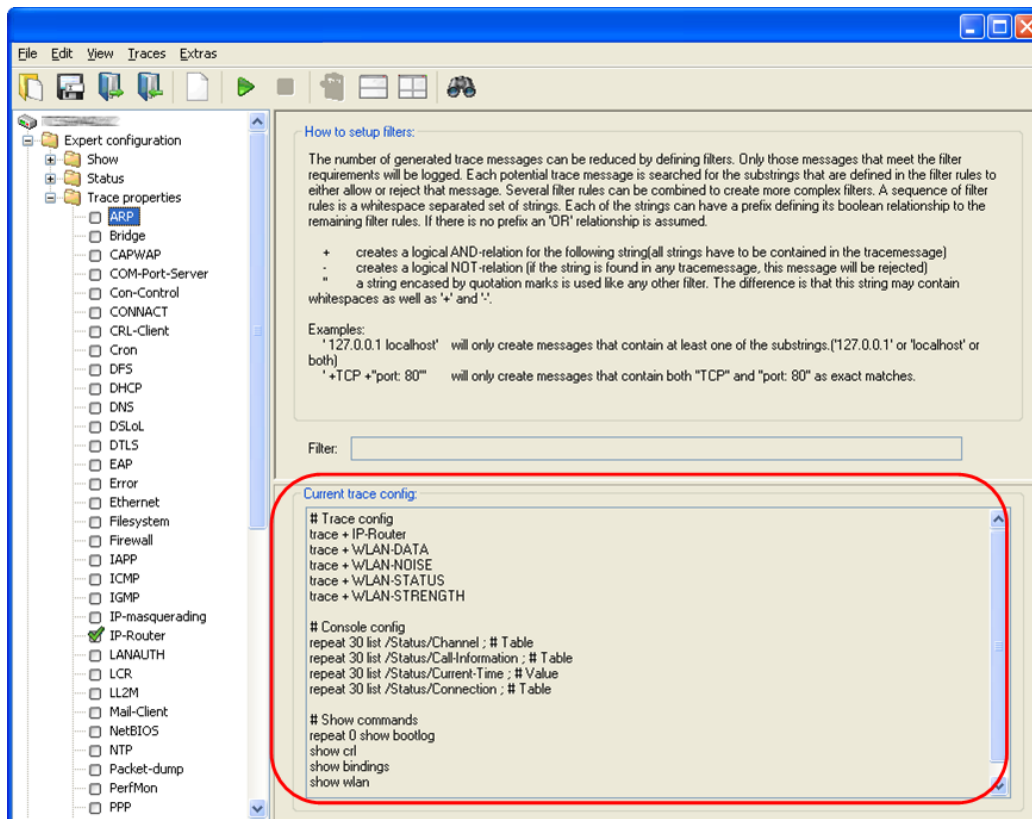
- Open the 'Status' folder and select one of the available trace entries for the device. The 'Filter' field for the entry is enabled.

A filter can be entered for every trace. For example, if you want to display only the IP traces of a particular workstation, enter the appropriate IP address as a filter of the IP router trace.



### 16.3.3 Displaying Trace Data

The entire trace configuration is shown in the lower area of the dialog where all active Trace properties, Status and Show entries are listed with the respective filters and parameters.



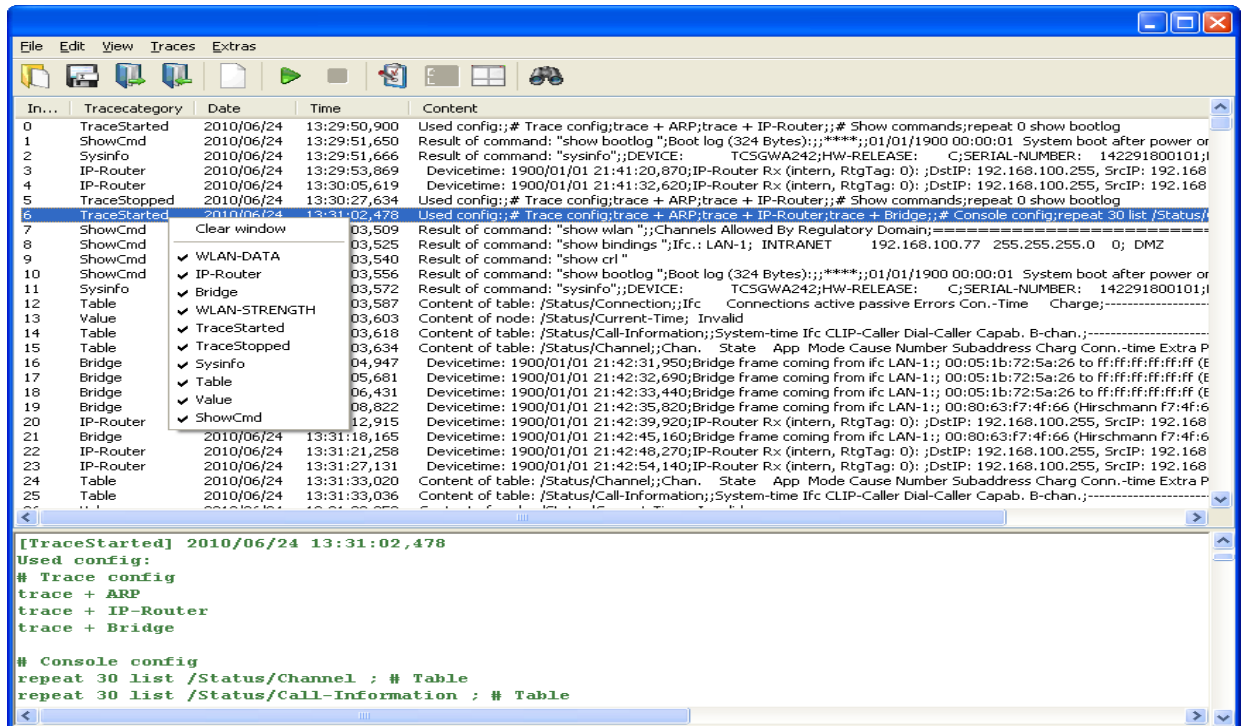
To start the dump of the trace data, use the `Traces : Start tracing` menu command, or click the 'Start tracing' button (with the green arrowhead). The 'Traces' dialog presents the trace output display:

- ▶ Trace events are displayed in the top part of the dialog.
- ▶ Results of a selected event are displayed in the bottom part of the dialog.

You have the option of editing the trace results displayed in the upper section of the dialog using the context menu. Carry out the following steps:

- Click the right mouse button in the top of the dialog, to open the context menu.

- Select/de-select the traces to be displayed, or select 'Clear window' to empty the list of trace events.



**Note:** Trace data is collected while the trace dump is enabled, and is periodically written to a back-up file. Refer to 'Back Up Settings for Traces' (see page 190).

## 16.3.4 Backing Up and Restoring Trace Configurations

The entire configuration of the trace dump can be written to a storage medium for later re-use or for transfer to another user.

To back up a trace configuration:

- In the 'Traces' dialog, select `File : Save trace config`, then navigate to the location where you want to save the trace configuration.

To restore a trace configuration:

- In the 'Traces' dialog, select `File : Load trace config`, then navigate to the location where the saved trace configuration is stored.

### **16.3.5 Saving and Restoring Trace Data**

For later editing, or for transfer to another user, the actual trace data can be written to a storage medium and later re-opened.

To back up trace data:

- In the 'Traces' dialog, select:  
`File : Save trace data/support configuration`, then navigate to the location where you want to save the trace data.

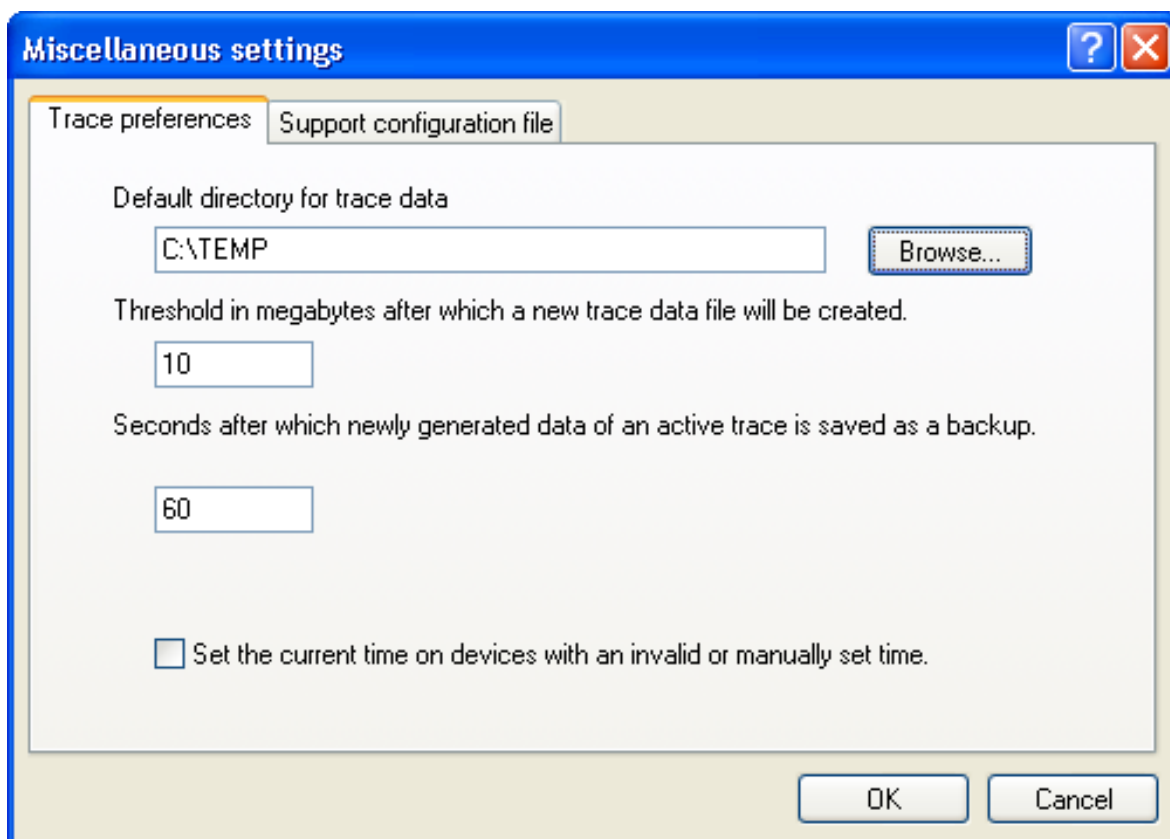
To restore trace data:

- In the 'Traces' dialog, select `File : Load trace data`, then navigate to the location where the saved trace data is stored.

### **16.3.6 Back-Up Settings for Traces**

When starting a trace in the 'Traces' dialog, a back-up file with the current trace data is automatically saved. The settings for the trace back-up can be configured at the following location:

`Extras : Miscellaneous settings : Trace preferences`.



The following settings can be configured for trace back-up:

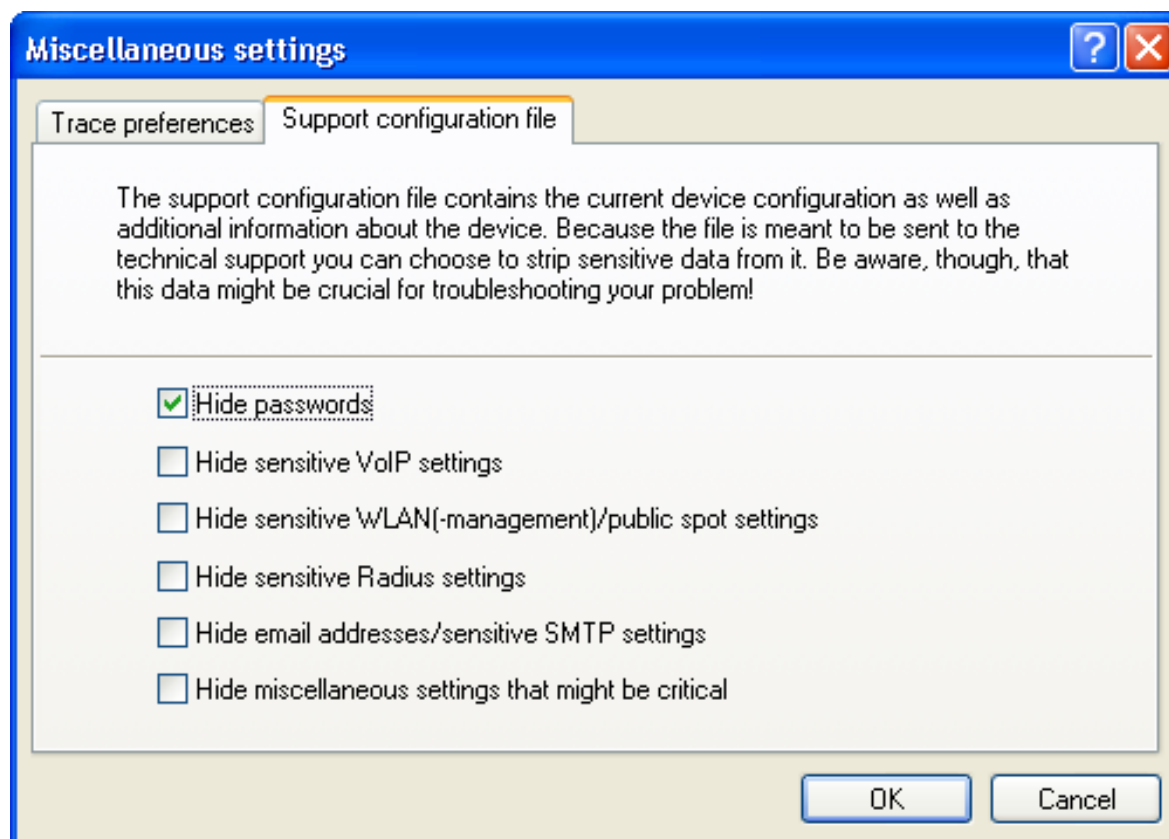
- ▶ Default directory for trace data
- ▶ Threshold in megabytes after which a new trace data file will be created: This sets the maximum size of the back-up file.
- ▶ Seconds after which newly generated data of an active trace is saved as back-up: This is the save interval for the back-up file.
- ▶ Set the current time on devices with an invalid or manually set time: Because some traced devices do not have valid time information, this setting applies workstation time as the device time.

## 16.3.7 Saving Support File

A support file enables all information pertaining to device support to be easily written to one file. This data can include:

- ▶ Trace data as configured in the current settings
- ▶ Current device configuration
- ▶ Bootlog
- ▶ Sysinfo

When saving the device configuration, you can hide security-related information of no relevance. This can be configured in the 'Traces' dialog at **Extras : Miscellaneous settings : Support configuration file**





## 16.4 Performance Monitoring with LANmonitor

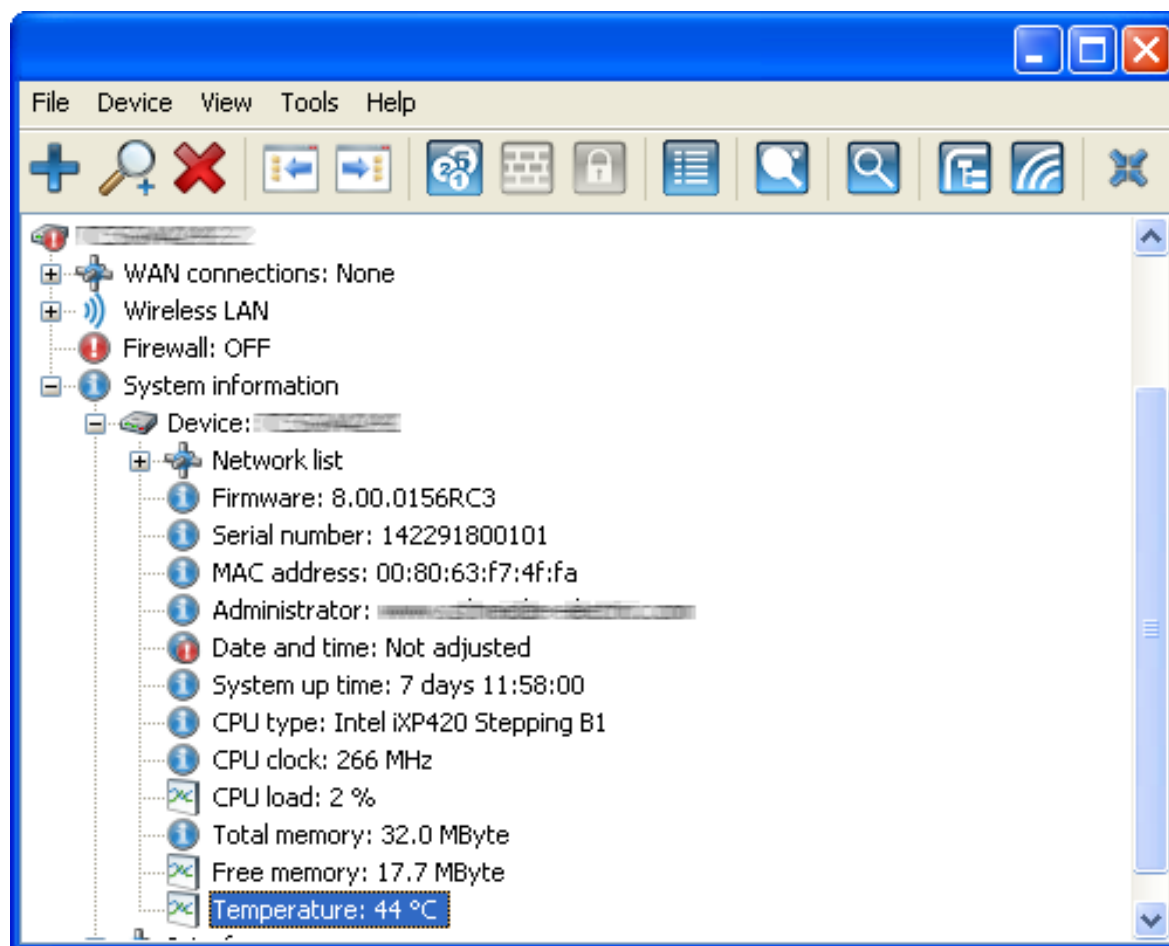
LANmonitor logs various parameters in the devices and displays these graphically:

- ▶ Transmit and receive rates for WAN connections
- ▶ Transmit and receive rates for point-to-point connections
- ▶ Signal reception strength for point-to-point connections
- ▶ Link signal strength for point-to-point connections
- ▶ Throughput for point-to-point connections
- ▶ CPU load
- ▶ Free memory
- ▶ Temperature (not available on all models)

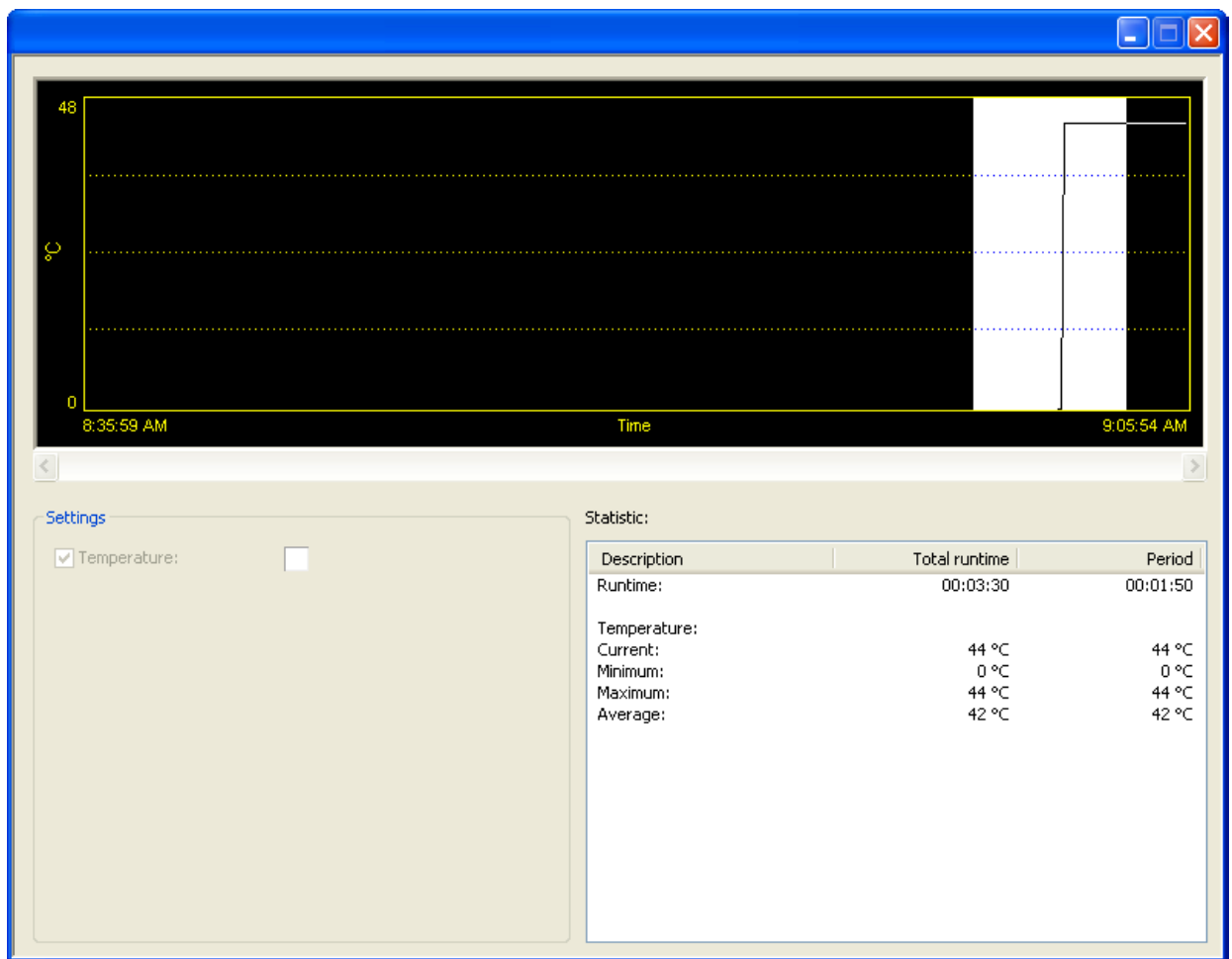
LANmonitor displays the current values directly in the corresponding groups.

To display a graphical log of monitored data:

- In LANmonitor, select a parameter that can be displayed graphically, and click the right mouse button.
- Select `Graph` in the context menu.



A new graph window opens that displays the selected parameter value over time:



You can hold down the left mouse key and drag it over a part of the graph to mark that time period. The statistical values associated with that time period are displayed separately.

**Note:** These graphically displayed values are deleted when the window is closed. For monitoring over a longer period, leave the window open.

## 16.5 SYSLOG

The SYSLOG protocol records the activities of a Switch device. You use this function to log the entire progress of all the activities in the device.

### 16.5.1 Accessing SYSLOG Data

The information captured in the SYSLOG log can be handled in different ways:

#### ■ Central Collection Point

You have the option of sending the SYSLOG messages to a central collection point, known as the SYSLOG client or daemon. This option is useful if, for example, you have to record messages from a large number of devices.

##### ▶ Logging under UNIX/Linux:

Under UNIX/Linux the logging is usually performed by the SYSLOG daemon, which is usually set up as standard. The daemon either reports directly via the console or writes the log in a corresponding SYSLOG file. The `/etc/syslog.conf` file specifies which facilities are to be written in which log file.

**Note:** In the configuration of the daemon, check whether it explicitly monitors network connections.

##### ▶ Logging under Windows:

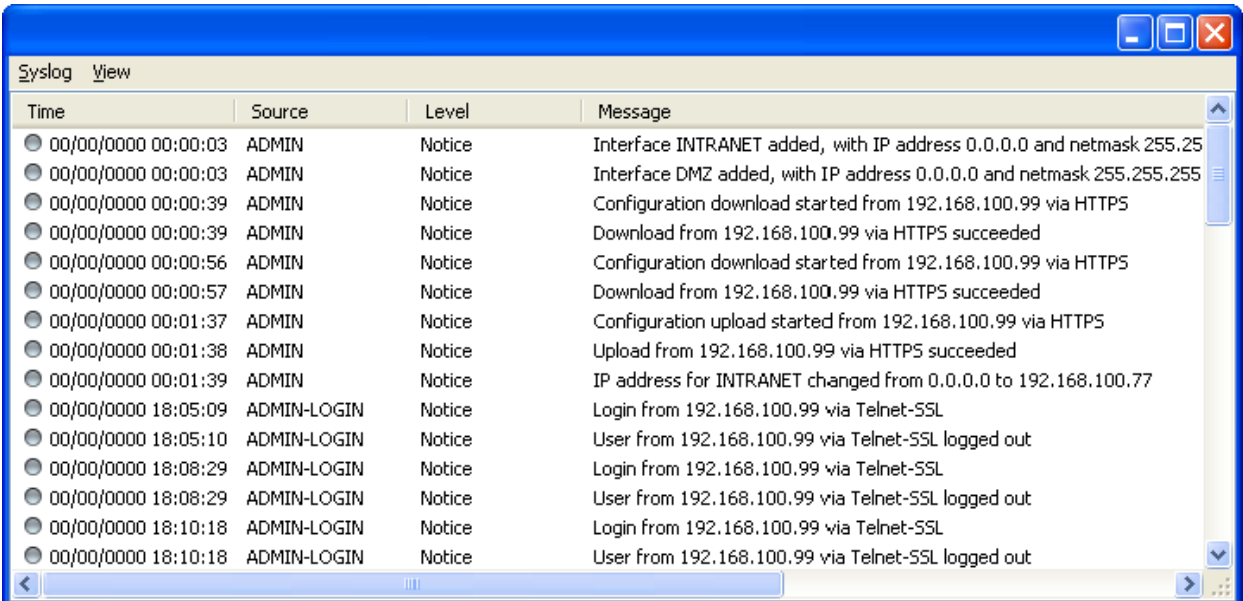
Windows does not provide a corresponding system function. You require special software that fulfills the function of a SYSLOG daemon.

- ▶ Logging in the device memory:  
You have the option of configuring every Switch device to manage a SYSLOG file in its memory.

## ■ Accessing SYSLOG in Device Memory

The most recent SYSLOG messages are stored in the device's RAM. Depending on the memory size, this can vary from 100 to 2048 SYSLOG messages. These internal SYSLOGs can be viewed using the following tools:

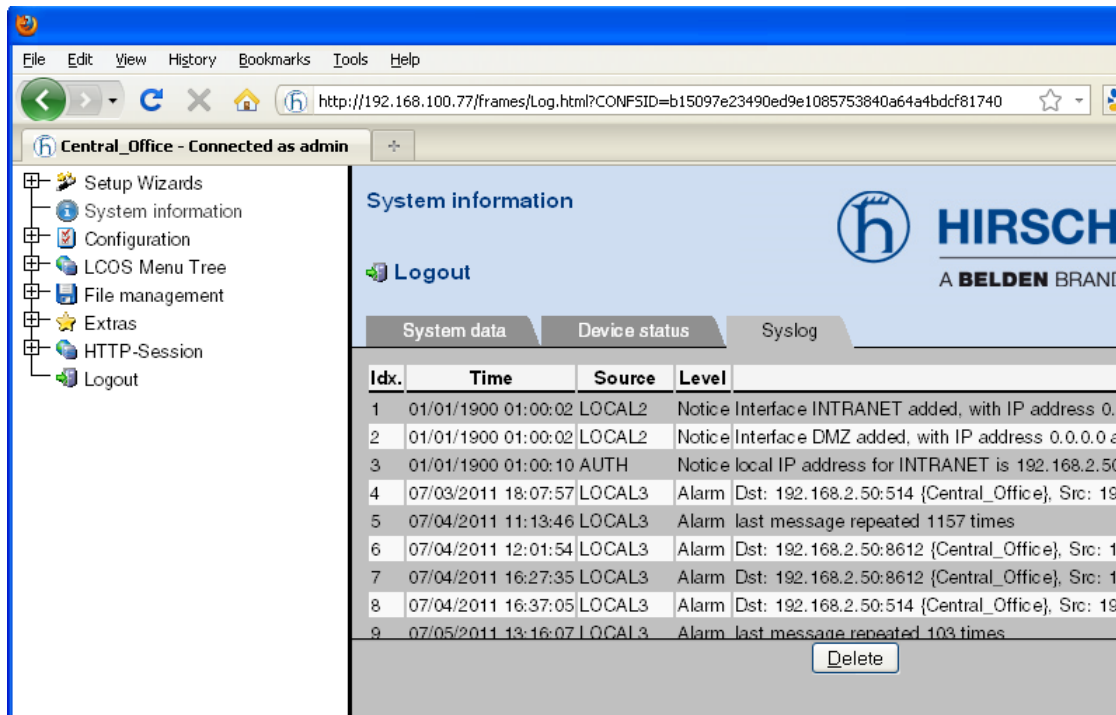
- ▶ Telnet, in the device statistics using the command line.
- ▶ LANmonitor:  
You can access a snapshot of the current SYSLOG file via LANmonitor: highlight a device, then select `Device : View Syslog`. With the SYSLOG window open, you can select the following commands in the `Syslog` menu:
  - `Refresh`: updates the current SYSLOG file and displays it in the Syslog window.
  - `Save Syslog...`: stores the current display to a file.
  - `Load Syslog...`: lets you open and view a saved SYSLOG file.



Time	Source	Level	Message
00/00/0000 00:00:03	ADMIN	Notice	Interface INTRANET added, with IP address 0.0.0.0 and netmask 255.255.255.255
00/00/0000 00:00:03	ADMIN	Notice	Interface DMZ added, with IP address 0.0.0.0 and netmask 255.255.255.255
00/00/0000 00:00:39	ADMIN	Notice	Configuration download started from 192.168.100.99 via HTTPS
00/00/0000 00:00:39	ADMIN	Notice	Download from 192.168.100.99 via HTTPS succeeded
00/00/0000 00:00:56	ADMIN	Notice	Configuration download started from 192.168.100.99 via HTTPS
00/00/0000 00:00:57	ADMIN	Notice	Download from 192.168.100.99 via HTTPS succeeded
00/00/0000 00:01:37	ADMIN	Notice	Configuration upload started from 192.168.100.99 via HTTPS
00/00/0000 00:01:38	ADMIN	Notice	Upload from 192.168.100.99 via HTTPS succeeded
00/00/0000 00:01:39	ADMIN	Notice	IP address for INTRANET changed from 0.0.0.0 to 192.168.100.77
00/00/0000 18:05:09	ADMIN-LOGIN	Notice	Login from 192.168.100.99 via Telnet-SSL
00/00/0000 18:05:10	ADMIN-LOGIN	Notice	User from 192.168.100.99 via Telnet-SSL logged out
00/00/0000 18:08:29	ADMIN-LOGIN	Notice	Login from 192.168.100.99 via Telnet-SSL
00/00/0000 18:08:29	ADMIN-LOGIN	Notice	User from 192.168.100.99 via Telnet-SSL logged out
00/00/0000 18:10:18	ADMIN-LOGIN	Notice	Login from 192.168.100.99 via Telnet-SSL
00/00/0000 18:10:18	ADMIN-LOGIN	Notice	User from 192.168.100.99 via Telnet-SSL logged out

- ▶ WEBconfig, at the following location:

System information : Syslog



**Note:** SYSLOG messages are written to the internal memory of the Switch device if the device is configured as a SYSLOG client with the loopback address 127.0.0.1. In the LANconfig configuration file, you set this via the following path:

Configuration : Log & Trace : SYSLOG, table SYSLOG Server.

## 16.5.2 Structure of SYSLOG Messages

SYSLOG messages consist of three parts:

- ▶ Priority
- ▶ Header
- ▶ Contents

## ■ Priority

The priority in a SYSLOG message contains information about the importance of the message and the facility (i.e. the service or component that triggered the message). The following table shows the correlation between priority level, meaning and SYSLOG priority.

Priority	Meaning	SYSLOG priority
Alarm	This category includes all the messages that the system administrator has to check.	PANIC, ALERT, CRIT
Error	This level indicates all the error messages that can also occur during normal operation without the administrator having to act (e.g. connection errors).	ERROR
Warning	This level comprises messages that do not prevent the device from operating correctly.	WARNING
Information	This level comprises all messages of a purely informative character (e.g. accounting data).	NOTICE, INFORM
Debug	All debug messages. Debug messages create large data quantities and may prevent the device from operating correctly. Therefore, they should be deactivated during normal operation and only be used for troubleshooting.	DEBUG

The following table provides an overview of the meaning of all the internal message sources that you can set up in the Switch device. The final column in the table also shows the standard assignment between the internal sources of the Switch device and the SYSLOG facilities. You can change this assignment if required.

Source	Meaning	Facility
System	System messages (boot procedures, timer system, etc.)	KERNEL
Logins	Messages about a user's logins and logouts during the PPP negotiation and any errors that occurred in the process	AUTH
System time	Messages about changes to the system time	CRON
Console logins	Messages about console logins (Telnet, Outband, etc.), logouts and any errors that occurred	AUTHPRIV
Connections	Messages about connections setups and terminations and any errors that occurred (e.g. display trace)	LOCAL0
Accounting	Accounting data after a connection is set up (users, online time, transfer volume)	LOCAL1
Management	Messages about configuration changes, remotely executed commands, etc.	LOCAL2
Router	Regular statistics about the most frequently used services (broken down by port number) and messages about filtered packets, routing errors, etc.	LOCAL3

## ■ Header

The header contains the name or the IP address of the device which sent the SYSLOG message. The chronological sequence is used to evaluate the messages. Time information is only added to the messages at the SYSLOG client in order not to disturb their chronological consistency due to different device times.

**Note:** The Switch needs a valid time stamp for the evaluation of the SYSLOG messages in internal memory.

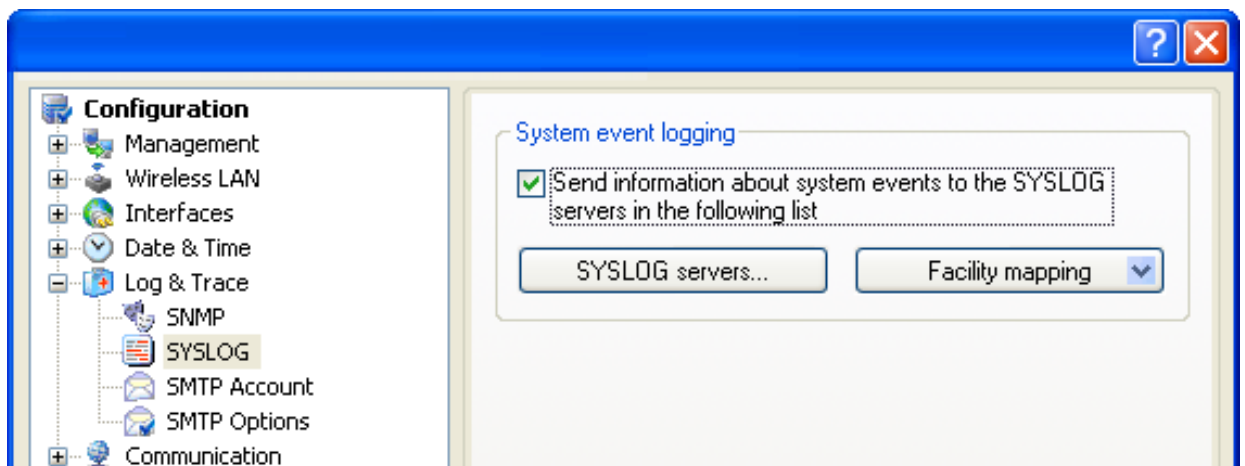
## ■ Contents

The actual contents of the SYSLOG messages describe the event, for example a login occurrence, the establishment of a WAN connection, or firewall activities.

### 16.5.3 Configuring SYSLOG with LANconfig

You can find the parameters to configure SYSLOG under LANconfig at  
Configuration : Log & Trace : SYSLOG:

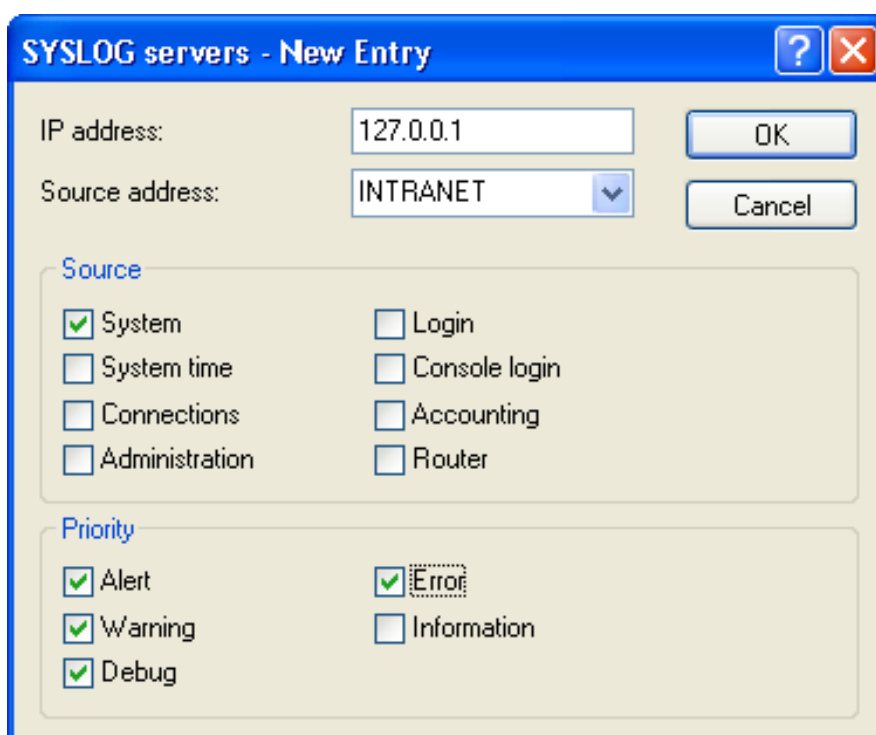




## ■ Identifying SYSLOG Servers

Working from the SYSLOG dialog, above, you can open a configuration dialog for the identification of SYSLOG servers with which the device will communicate in its role as SYSLOG client, as follows:

- Click on the `SYSLOG servers...` button.
- In the 'Syslog servers' window, click `Add...` to open the 'New Entry dialog':



When setting up a SYSLOG client, you can configure the following parameters:

- ▶ **IP address:**  
The IP address to which SYSLOG messages are to be sent.
- ▶ **Source address:**  
An optional, source address can be set here. This address is used instead of the IP address, above.
- ▶ **Source:**  
Select which of the internal Switch sources are to send messages to this SYSLOG client.
- ▶ **Priority:**  
You can further restrict the volume of messages by filtering on the basis of selected priorities.

The table of syslog servers (factory settings) is set up to display events that are relevant to diagnostics, and to save these to the internal syslog memory. The following screenshot shows these pre-defined SYSLOG servers in LANconfig:

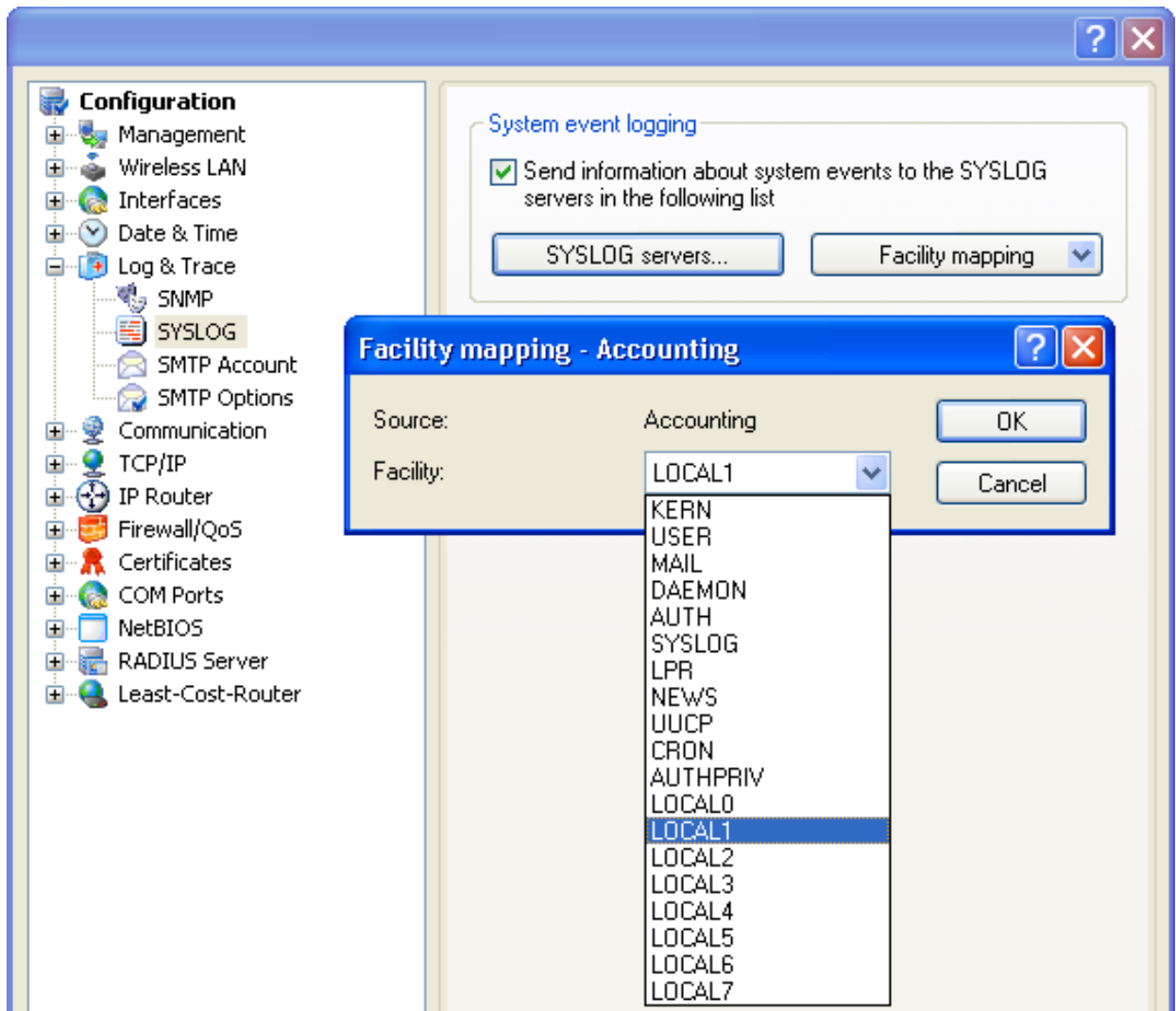
IP address	Source addr.	System	Login	System time	Console login	Connections	Accounting	Administration	Router	Alert	Error	Warning	Information	Debug
127.0.0.1	INTRANET	Off	Off	On	Off	Off	Off	Off	Off	On	On	On	Off	On
127.0.0.1	INTRANET	On	Off	Off	Off	On	Off	Off	Off	On	On	Off	Off	Off
127.0.0.1	INTRANET	Off	Off	Off	Off	Off	Off	On	Off	Off	Off	Off	On	Off
127.0.0.1	INTRANET	Off	On	Off	Off	Off	Off	Off	Off	On	On	Off	On	Off
127.0.0.1	INTRANET	Off	Off	Off	On	Off	Off	Off	Off	Off	Off	Off	On	Off
127.0.0.1	INTRANET	Off	Off	Off	Off	Off	On	Off	Off	Off	Off	Off	On	Off
127.0.0.1	INTRANET	Off	Off	Off	Off	Off	Off	Off	On	On	Off	Off	Off	Off

## ■ Assignment of Internal Device Sources for SYSLOG Facilities

The SYSLOG protocol uses certain designations for message sources, the so-called facilities. Each internal source in the Switch that can generate a SYSLOG message needs to be assigned to a SYSLOG facility. The standard mapping can be changed, if necessary. For example, all SYSLOG messages from a device can be sent with the same specified facility (e.g., Local7). It is therefore possible to collect all device messages in a common log file by appropriately configuring the SYSLOG client.


To map a specific internal source to a facility, beginning in the SYSLOG dialog:

- Click on the Facility mapping button, and select a device source from the drop-down list.
- In the 'Facility mapping' dialog, select a facility to associate with the source.



## 16.5.4 Configuring SYSLOG with Telnet or WEBconfig

You have the option of configuring the SYSLOG function for the Switch device under the following path with Telnet or WEBconfig:

 Hirschmann Menu Tree : Setup : SYSLOG

### ■ Parameters

The following parameters can be configured:

- ▶ Operating:  
Select 'Yes' to activate the dispatch of information about system events to the configured SYSLOG client.
- ▶ Port:  
The number of the port used for sending SYSLOG messages.
- ▶ Messages-Table-Order:  
Indicate how you want SYSLOG to be sorted in the table: oldest on top, or newest on top.

### ■ Facility Mapping

Select an item in the table to map each SYSLOG source to a facility.

### ■ Server table

Use the Server table to identify the servers with which the device will communicate in its role as SYSLOG client. Click on a device to edit it, or click Add to create a new SYSLOG server item. Parameters include:

- ▶ IP address:  
IP address of the SYSLOG client.
- ▶ Source:  
Source that caused the message to be sent. Enter the sum of the hexadecimal values for the selected sources:

Source name	Hex value	Source name	Hex value
System	1	Login	2
System time	4	Console login	8
Connections	10	Accounting	20
Administration	40	Router	80

- ▶ **Level:**  
SYSLOG level with which the message is sent. Enter the sum of the hexadecimal values for the selected levels:

Level name	Hex value
Alert	1
Error	2
Warning	4
Information	8
Debug	10

- ▶ **Loopback address:**  
An optional, source address can be set here. This address is used instead of the IP address, above.

All pre-defined SYSLOG clients transmit the messages to the IP address 127.0.0.1, i.e. to the Switch itself. The sender IP address is the IP address from the "INTRANET" network. Individual entries have the following functions:

Index	Source	Level	Meaning
0001	4	0	System time without a specified level
0002	1	17	System messages with the level alarm, error, alert or debug
0003	10	2	Connection messages with the level error
0004	40	8	Management messages with the level information
0005	2	a	Logins with the level error or information
0006	8	8	Console logins with the level information
0007	20	8	Accounting messages with the level information
0008	80	1	Router messages with the level alarm

## 16.6 The Ping Command

With the ping command in Telnet or in a terminal connection an 'ICMP Echo Request' is sent to the addressed host. As long as the recipient provides the protocol and the request is not filtered by the firewall, the addressed host answers with an 'ICMP Echo Reply'. If the host is not available, the last router before the host answers with a 'Network unreachable' or 'Host unreachable' response.

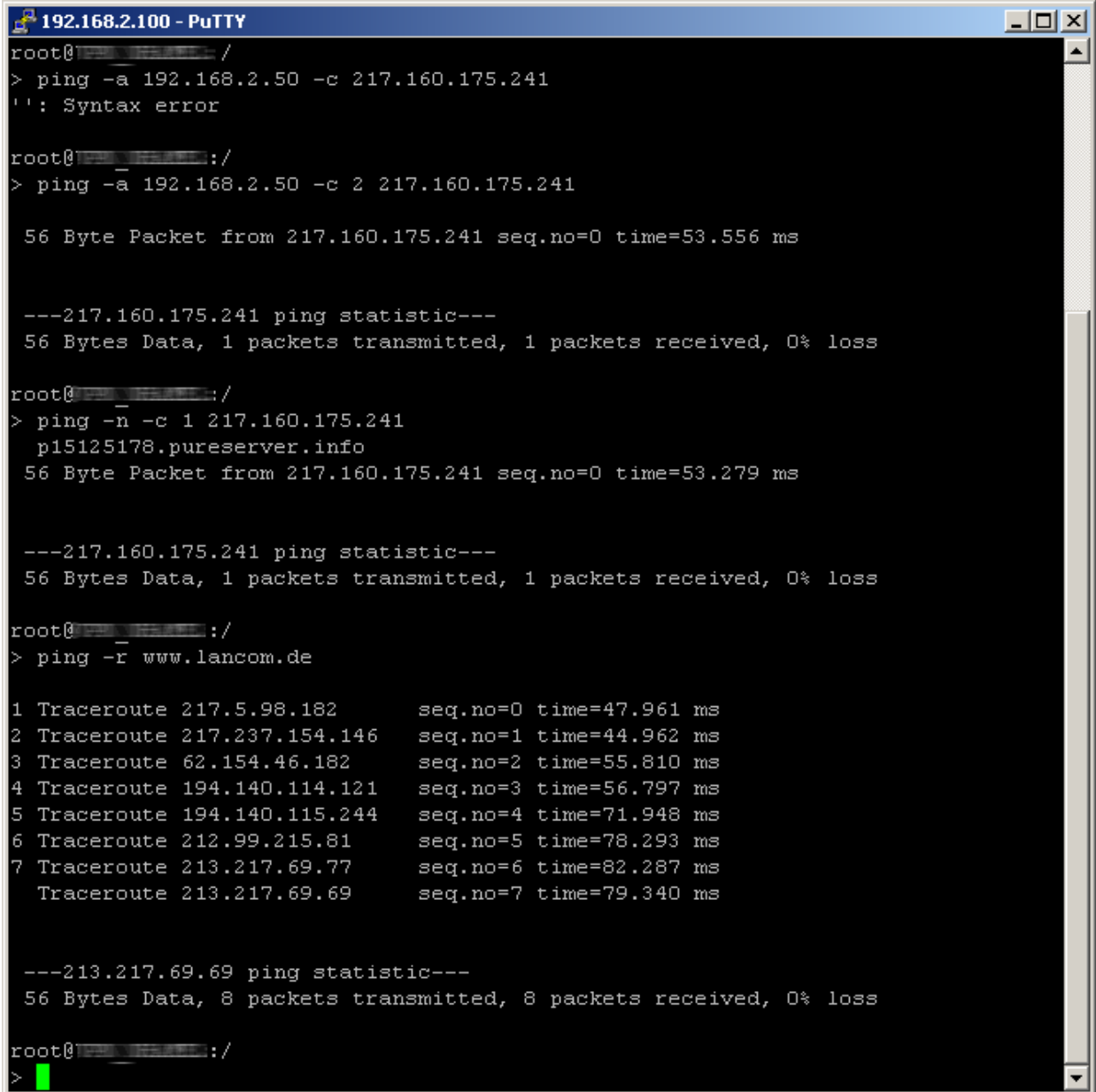
The syntax of the ping command is:

```
ping [-fnqr] [-s n] [-i n] [-c n] [-a a.b.c.d] hostaddress
```

The meaning of the optional parameters are listed in the following table:

Parameter	Meaning
-a a.b.c.d	Sets the sender address of the ping (standard: IP address of the router)
-a INT	Sets the intranet address of the router as sender address
-a DMZ	Sets the DMZ address of the router as sender address
- a LBx	Sets one of the 16 Loopback addresses as sender address. Valid for x are the hexadecimal values 0-f
-f	flood ping: Sends many ping signals in a small amount of time. Can be used e. g. to test the broadband of the network. Note: flood ping can easily be interpreted as a DoS attack
-n	Sends the computer name back to the given IP address
-q	Ping command does not give an output on the pane
-r	Change to traceroute mode: every interstation passed by the data package is listed
-s n	Sets the package size to n Byte (max. 1472)
-i n	Time between the packages in seconds
-c n	Send n ping signals
hostaddress	Address or hostname of the recipient
stop /<RETURN>	Entering "stop" or pressing the RETURN button terminates the ping command

The following is an example of a series of ping commands:



```
192.168.2.100 - PuTTY
root@:/
> ping -a 192.168.2.50 -c 217.160.175.241
': Syntax error

root@:/
> ping -a 192.168.2.50 -c 2 217.160.175.241

56 Byte Packet from 217.160.175.241 seq.no=0 time=53.556 ms

---217.160.175.241 ping statistic---
56 Bytes Data, 1 packets transmitted, 1 packets received, 0% loss

root@:/
> ping -n -c 1 217.160.175.241
p15125178.pureserver.info
56 Byte Packet from 217.160.175.241 seq.no=0 time=53.279 ms

---217.160.175.241 ping statistic---
56 Bytes Data, 1 packets transmitted, 1 packets received, 0% loss

root@:/
> ping -r www.lancom.de


1 Traceroute 217.5.98.182      seq.no=0 time=47.961 ms
2 Traceroute 217.237.154.146 seq.no=1 time=44.962 ms
3 Traceroute 62.154.46.182   seq.no=2 time=55.810 ms
4 Traceroute 194.140.114.121 seq.no=3 time=56.797 ms
5 Traceroute 194.140.115.244 seq.no=4 time=71.948 ms
6 Traceroute 212.99.215.81   seq.no=5 time=78.293 ms
7 Traceroute 213.217.69.77   seq.no=6 time=82.287 ms
  Traceroute 213.217.69.69   seq.no=7 time=79.340 ms

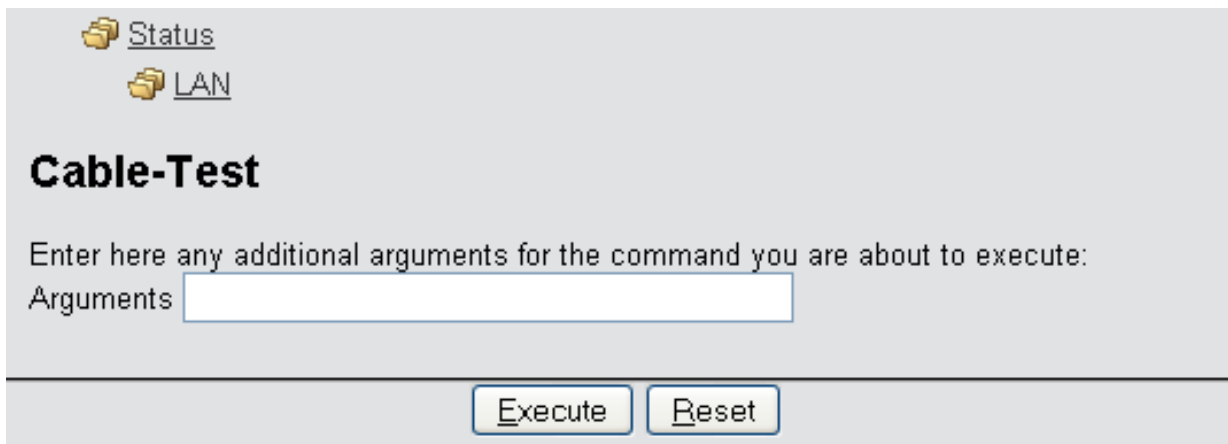
---213.217.69.69 ping statistic---
56 Bytes Data, 8 packets transmitted, 8 packets received, 0% loss


root@:/
>
```


## 16.7 Cable Testing

You can use the WEBconfig software to test the cable connecting the device to a LAN or WAN. WEBconfig can detect a non-functioning cable even in the absence of any detected events. You can perform a cable test, in WEBconfig at the following location:

 Hirschmann Menu Tree : Status : LAN : Cable Test



 [Status](#)

 [LAN](#)

### Cable-Test

Enter here any additional arguments for the command you are about to execute:

Arguments

To perform a cable test:

- In the 'Argument' field, input the name of the device interface that you want to test, then click 'Execute'.
- To see the results of the test, navigate to the following location:

 Hirschmann Menu  
Tree : Status : LAN : Cable Test Results

Possible test results include:

- ▶ OK:  
Cable plugged in correctly, line ok.
- ▶ open with distance '0m':  
No cable plugged in, or interruption within less than 10 meters distance.



- ▶ open with indication of distance:  
Cable is plugged in, but the cable ceases to operate at the indicated distance.
- ▶ Impedance error:  
The pair of cables is not terminated with the correct impedance at the other end.



# A Index

<b>A</b>		
Access point:adding	163	Loopback Addresses:SYSLOG Server 144
Access point:organizing multiple	164	Loopback Addresses:Time Server 142
Access point:searching for	161	Loopback addresses 137
Admin rights:TFTP access; Admin rights:SNMP access	129	<b>M</b>
Admin rights:access	126	Message URL http://
Administrator Rights:Management	125	www.beldensolutions.com 213, 213
AutoConfiguration Adapter (ACA)	63	Message URL
		http://www.hicomcenter.com 213, 213
<b>C</b>		Monitor:CPU Query; Monitor:
Cable testing	208	Memory Utilization via SNMP 153
Communication protocols	38	Monitor:Functions 148
Configuration file:automatic backup	60	Monitor:Internet Connections 157
Configuration file:create; Configuration file:edit; Configuration file:upload	57	Monitoring:WLANs; WLANmonitor 159
Connection setup	43	Monitoring:extended display options 151
Connection:diagnosing;		Monitoring; LANmonitor 147
LANmonitor:diagnosing connection	154	<b>P</b>
		Password 35
<b>D</b>		Performance monitoring 193
Devices:finding	13	Ping 155, 206
Diagnostics	171	<b>Q</b>
		QuickFinder 32
<b>F</b>		<b>R</b>
FAQ	213	Reset button:disabling 87
Files:loading via TFTP; Files:loading via HTTP	101	Reset; Device:Restart; Restart; Device:Restarting 85
FirmSafe	90, 90	Resetting device; Re-starting device 85
Firmware:Find	97	Rogue access point; Rogue client 165
Firmware:Update; Updating the firmware	89	Rogue device detection:activating 168
Firmware:load via LANconfig	92	Rollout wizard 71
Firmware:load via TFTP; TFTP	94	<b>S</b>
Firmware:load via WEBconfig	93	SNMP:access 36
Firmware:loading new	92	SYSLOG 196
Firmware:updating	89	SYSLOG:configuring via LANconfig 200
Firmware:viewing multiple versions	100	SYSLOG:configuring via WEBconfig;
		SYSLOG:configuring via Telnet 204
<b>I</b>		SYSLOG:message structure 198
IP address: specified	44	Script commands 119
		Script files:generating 111
<b>L</b>		Script sessions:multiple 119
LANconfig:help	16	Script:Upload file to device; Uploading script files 115
LANconfig:ini file	22	Script:download file from device;
LANconfig:language	19	Download script file 113
LANconfig:starting	12	Scripting 107
LCF file	49	Scripting:offline versus online 110
LCS file	49	
LL2M	79	
Loopback Addresses:ICMP Polling	139	

## Index

---

Search in: LANconfig	32
Search in: configuration	32
Support file:saving	192
Symbol	8

### T

TCP/HTTP tunnels	134
Technical questions	213
Trace Configuration Wizard	182
Trace:Manual Configuration	183
Trace:Start	172
Trace:backup and restore	189
Trace:display commands	174
Trace:displaying data	188
Trace:filters	174
Trace:function codes	172
Trace:parameters	172
Trace:via HyperTerminal	176
Trace:via LANmonitor	179
Training courses	213

### U

Upload configuration;Configuration: upload	49
Uploading:in LANconfig	50
Uploading:in WEBconfig	54
User rights:configuring	131

### W

WLANmonitor:enabling alerts	169
WLANmonitor:starting	160

## B Further Support

### ■ Technical Questions and Training Courses

In the event of technical queries, please contact your local Hirschmann distributor or Hirschmann office.

You can find the addresses of our distributors on the Internet:

[www.beldensolutions.com](http://www.beldensolutions.com).

Our support line is also at your disposal:

- ▶ Tel. +49 1805 14-1538
- ▶ Fax +49 7127 14-1551

Answers to Frequently Asked Questions can be found on the Hirschmann internet site ([www.beldensolutions.com](http://www.beldensolutions.com)) at the end of the product sites in the FAQ category.

The current training courses to technology and products can be found under <http://www.hicomcenter.com>.

### ■ Hirschmann Competence Center

In the long term, excellent products alone do not guarantee a successful customer relationship. Only comprehensive service makes a difference worldwide. In the current global competition scenario, the Hirschmann Competence Center is ahead of its competitors on three counts with its complete range of innovative services:

- ▶ Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- ▶ Training offers you an introduction to the basics, product briefing and user training with certification.
- ▶ Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.

Internet:

<http://www.hicomcenter.com>.



**HIRSCHMANN**

---

A **BELDEN** BRAND