



**HIRSCHMANN**

A **BELDEN** BRAND

# Reference Manual

**GUI Graphical User Interface  
Industrial Ethernet Firewall  
EAGLE One**

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.

© 2013 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/DVD 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.hirschmann.com](http://www.hirschmann.com)).

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

# Contents

	<b>About this Manual</b>	<b>7</b>
	<b>Key</b>	<b>9</b>
	<b>Graphical User Interface</b>	<b>11</b>
<b>1</b>	<b>Basic Settings</b>	<b>15</b>
1.1	System	16
1.2	Network	20
	1.2.1 Global	21
	1.2.2 Transparent Mode	22
	1.2.3 Router Mode	24
	1.2.4 PPPoE Mode	27
	1.2.5 Routes	30
1.3	Software	31
1.4	Port Configuration	33
1.5	Serial Port	35
	1.5.1 Configuration as a Terminal/CLI interface	36
	1.5.2 Configuration as a Modem interface	37
1.6	Load/Save	39
	1.6.1 Status display	40
	1.6.2 Configuration in the non-volatile memory (NVM)	41
	1.6.3 Configuration on the AutoConfiguration Adapter (ACA)	42
	1.6.4 Saving and Loading a Configuration	43
	1.6.5 Cancelling a configuration change	44
1.7	Restart	45
<b>2</b>	<b>Security</b>	<b>47</b>
2.1	Password	48
2.2	SNMP Access	50
2.3	SNMPv1/v2	54
2.4	Web Access	56
2.5	SSH Access	60

2.6	External Authentication	64
2.6.1	User Firewall Accounts	64
2.6.2	Authentication Lists	66
2.6.3	RADIUS Server	69
2.7	Login Banner	71
<b>3</b>	<b>Time</b>	<b>73</b>
3.1	Basic Settings	74
3.2	SNTP configuration	77
3.3	NTP Configuration	80
<b>4</b>	<b>Network Security</b>	<b>83</b>
4.1	Packet Filter	84
4.1.1	Address Templates	86
4.1.2	Firewall Learning Mode (FLM)	87
4.1.3	Incoming and outgoing IP packets	105
4.1.4	Incoming and outgoing MAC packets	112
4.1.5	Incoming PPP packets	114
4.2	NAT – Network Address Translation	119
4.2.1	General NAT settings	119
4.2.2	IP Masquerading	120
4.2.3	1:1 NAT	120
4.2.4	Port forwarding	124
4.3	Helping protect against Denial of Service (DoS)	127
4.4	User Firewall	128
<b>5</b>	<b>VPN – Virtual Private Network</b>	<b>133</b>
5.1	Device connection	134
<b>6</b>	<b>Redundancy</b>	<b>151</b>
6.1	Transparent Redundancy	152
6.2	Router Redundancy	155
<b>7</b>	<b>Diagnostics</b>	<b>159</b>
7.1	Events	160
7.1.1	Event Log	160
7.1.2	Syslog Server	162
7.1.3	Event Settings	163

7.1.4	Advanced Settings	166
7.2	Ports	168
7.2.1	Network Load	168
7.2.2	Statistics table	169
7.2.3	ARP	170
7.3	Topology Discovery	172
7.4	Device Status	174
7.5	Signal contact	176
7.5.1	Function Monitoring	176
7.5.2	Manual Setting	177
7.5.3	Device Status	178
7.5.4	Configuring Traps	178
7.6	Alarms (Traps)	180
7.7	Report	183
7.7.1	System Information	183
7.8	MAC Firewall List	185
7.9	IP Firewall List	187
7.10	Configuration Check	189
7.11	Reachability Test (Ping)	192
<b>8</b>	<b>Advanced</b>	<b>195</b>
8.1	DNS	196
8.1.1	DNS Server	196
8.1.2	DynDNS	198
8.2	Packet Forwarding	200
8.3	DHCP Relay Agent	202
8.4	DHCP Server	205
8.4.1	Pool	206
8.4.2	Lease Table	211
<b>9</b>	<b>Logout</b>	<b>215</b>
<b>A</b>	<b>General Information</b>	<b>217</b>
A.1	List of RFCs	218
A.2	Underlying IEEE Standards	220
A.3	Technical Data	221

A.4	Maintenance	222
A.4.1	Service-Shell	222
A.5	Copyright of Integrated Software	223
A.5.1	Bouncy Castle Crypto APIs (Java)	223
A.5.2	Network Time Protocol Version 4 Distribution	224
<b>B</b>	<b>Readers' Comments</b>	<b>227</b>
<b>C</b>	<b>Index</b>	<b>229</b>
<b>D</b>	<b>Further Support</b>	<b>231</b>

## About this Manual

The “GUI Graphical User Interface” reference manual contains detailed information on using the graphical user interface to operate the individual functions of the device.

The “Command Line Interface” reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

The “Configuration” user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The Industrial HiVision Network Management Software provides you with additional options for smooth configuration and monitoring:

- ▶ Simultaneous configuration of multiple devices
- ▶ Graphical user interface with network layout
- ▶ Auto-topology discovery
- ▶ Event log
- ▶ Event handling
- ▶ Client/server structure
- ▶ Browser interface
- ▶ ActiveX control for SCADA integration
- ▶ SNMP/OPC gateway.








# Key

The designations used in this manual have the following meanings:







---

	List
	Work step
	Subheading
<a href="#">Link</a>	Cross-reference with link
<b>Note:</b>	A note emphasizes an important fact or draws your attention to a dependency.
<code>Courier</code>	ASCII representation in the graphical user interface

---

Symbols used:

---

	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch
	Bridge

---

# Key

---



Hub



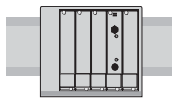
A random computer



Configuration Computer



Server



PLC -  
Programmable logic  
controller



I/O -  
Robot

# Graphical User Interface

## ■ **System requirements**

Use HiView to open the graphical user interface. This application offers you the possibility to use the graphical user interface without other applications such as a Web browser or an installed Java Runtime Environment (JRE).

Alternatively you have the option to open the graphical user interface in a Web browser, e.g. in Mozilla Firefox version 3.5 or higher or Microsoft Internet Explorer version 6 or higher. You need to install the Java Runtime Environment (JRE) in the most recently released version. You can find installation packages for your operating system at <http://java.com>.

## ■ **Starting the graphical user interface**

The prerequisite for starting the graphical user interface, first configure the IP parameters of the device correctly. The “Basic Configuration” user manual contains detailed information that you need to define the IP parameters.

Start the graphical user interface in HiView:

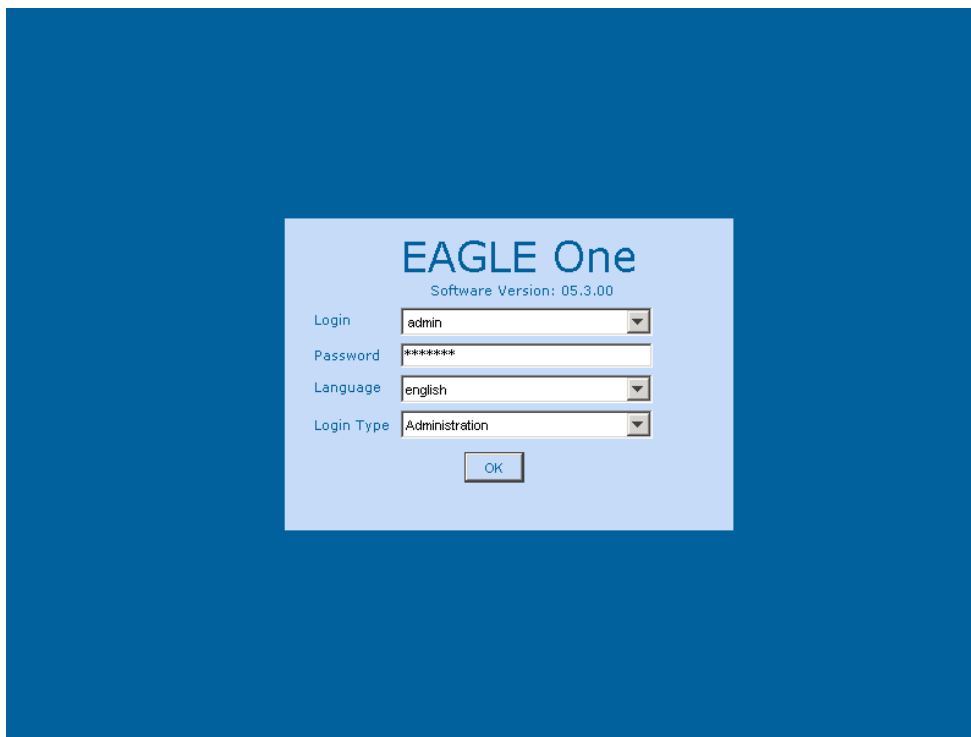
- Start HiView.
- In the URL field of the start window, enter the IP address of your device.
- Click "Open".

HiView sets up the connection to the device and shows the login window

Start the graphical user interface in the Web browser:

- This requires that Java is enabled in the security settings of your Web browser.
- Start your Web browser.
- Write the IP address of the device in the address field of the Web browser. Use the following form: `https://xxx.xxx.xxx.xxx`

The Web browser sets up the connection to the device and shows the login window.



*Figure 1: Login window*

- Select the desired language.
- In the `Login` drop-down menu, select
  - `user` to have read access to the device
  - `admin` to have read/write access to the device.

- The password “public”, with which you have read access, appears in the password field. If you wish to have write access to the device, then highlight the contents of the password field and overwrite it with the password “private” (default setting).
- In the Login Type drop-down menu, select
  - Administration if you want to manage the device, or
  - User Firewall if you want to login for the user firewall function (prerequisite: the user selected in the Login drop-down menu has already been created in the user firewall).
- Click "OK".

The screen shows the graphical user interface of the device.

**Note:** The changes you make in the dialogs will be copied to the volatile memory of the device (RAM) when you click “Set”. Click “Reload” to update the display.

To save any changes made so that they will be retained after a power cycle or reboot of the device use the save option on the "Load/Save" dialog (see on page 41 “Configuration in the non-volatile memory (NVM)”).

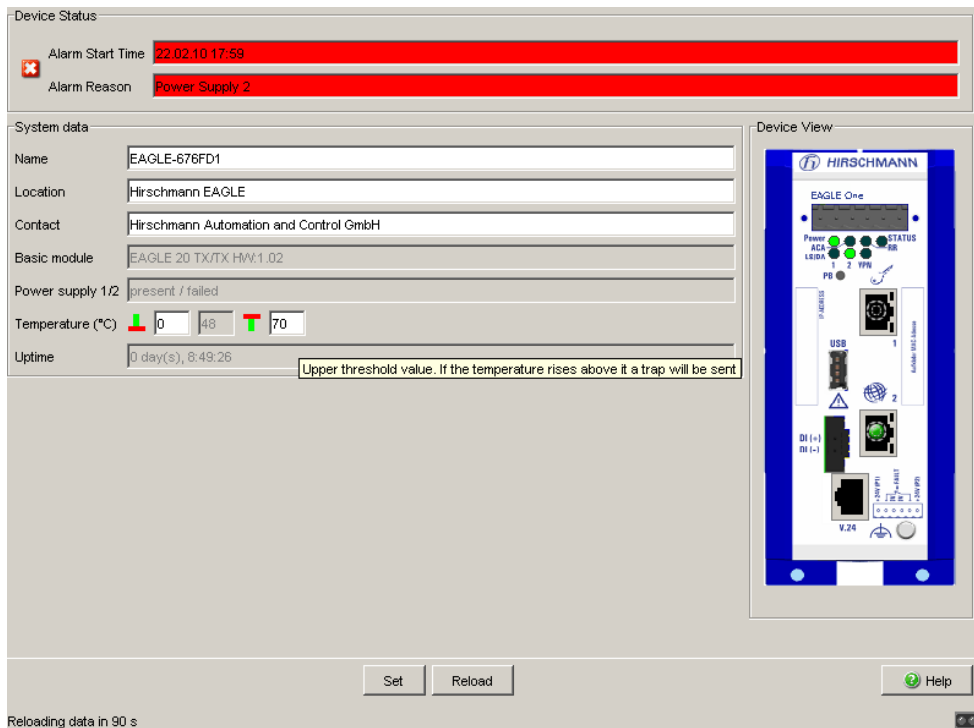
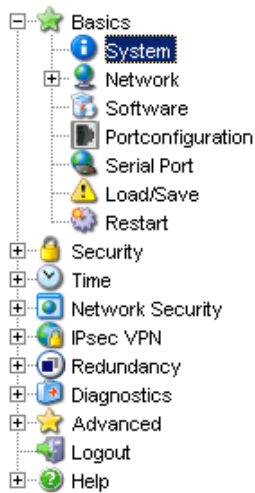


Figure 2: Graphical user interface of the device

## ■ Menu bar

The menu section displays the menu items. By placing the mouse pointer in the menu section and clicking the right mouse button you can use “Back” to return to a menu item you have already selected, or “Forward” to jump to a menu item you have already selected.



# 1 Basic Settings

The Basic Settings menu contains the dialogs, displays and tables for the basic configuration:

- ▶ System
- ▶ Network
- ▶ Software
- ▶ Port Configuration
- ▶ Serial Port
- ▶ Load/Save
- ▶ Restart

# 1.1 System

The “System” submenu in the basic settings menu is structured as follows:

- ▶ Device Status
- ▶ System Data
- ▶ Device View
- ▶ Reloading

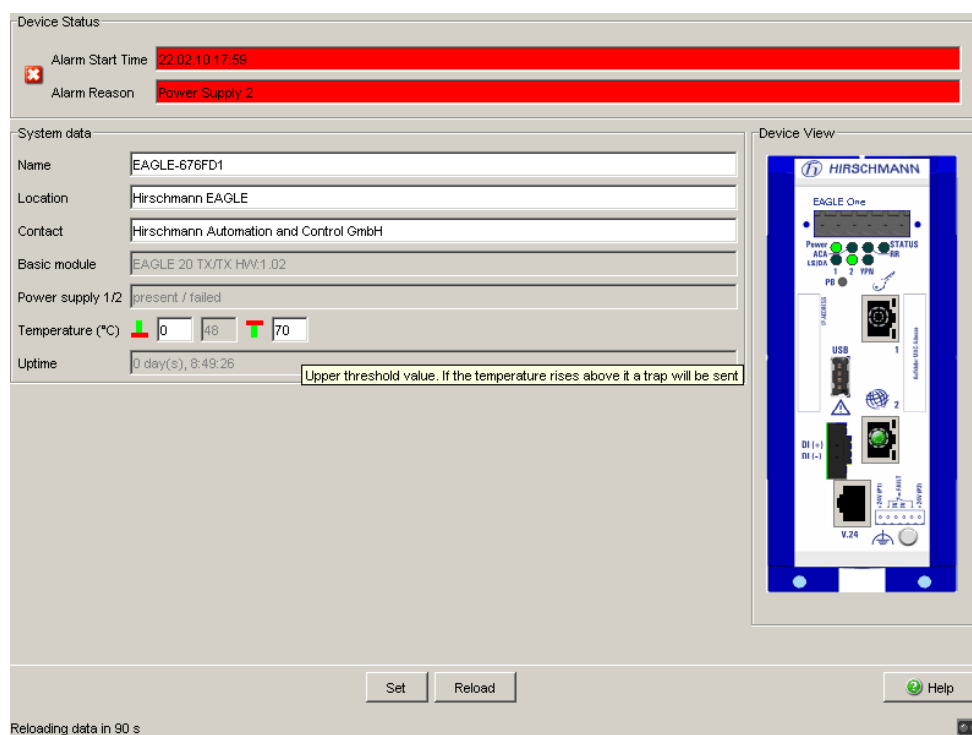
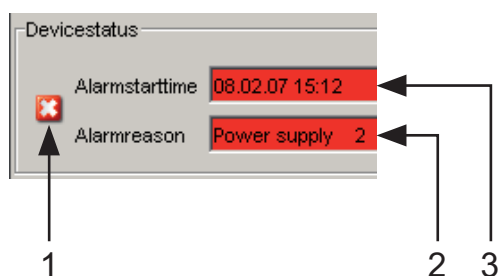


Figure 3: “System” submenu

## ■ Device Status

This section of the graphical user interface provides information on the device status and the alarm states the device has detected.





**Figure 4: Device status and alarm display**  
 1 - The symbol displays the device status  
 2 - Cause of the oldest existing alarm  
 3 - Start of the oldest existing alarm

## ■ System Data

The fields in this frame show operating data and information on the location of the device.

- the system name,
- the location description,
- the name of the contact person for this device,
- the temperature threshold values.

Name	Meaning
Name	System name of this device
Location	Location of this device
Contact	The contact for this device
Basic module	Hardware version of the device
Power Supply 1/2	Status of power units (P1/P2)
Temperature	Temperature of the device. Lower/upper temperature threshold values. If the temperature goes outside this range, the device generates an alarm.
Uptime	Time that has elapsed since this device was last restarted.

*Table 1: System Data*

## ■ Device View

The device view shows the device. Symbols on the ports represent the status of the individual ports.

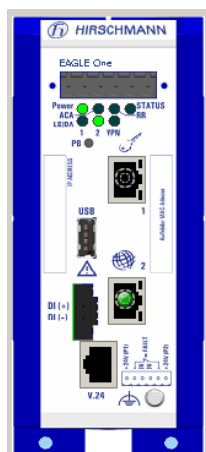







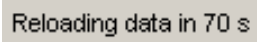
Figure 5: Device View

Meaning of the symbols:

-  The port (10, 100 Mbit/s) is enabled and the link has been established.
-  The port is disabled by the management and it has a link.
-  The port is disabled by the management and it has no link.
-  The port is in autonegotiation mode.
-  The port is in HDX mode.

## ■ Reloading

This area of the user interface (Web-based Interface) at the bottom left displays the countdown time until the applet requests the current data of this dialog again. Clicking the “Reload” button calls up the current dialog data immediately. The applet automatically calls up the current data of the device every 100 seconds.



Reloading data in 70 s

*Figure 6: Time to next Reload*

## 1.2 Network

The “Network” submenu in the Basic Settings menu allows you to configure and select the network mode, and to create static routes:

- ▶ Global
- ▶ Transparent Mode
- ▶ Router Mode
- ▶ PPPoE Mode
- ▶ Routes

## 1.2.1 Global

With this dialog you can select the network mode and enter settings for forwarding packets.

Name	Meaning
Mode	<p>Select the mode in which you want to operate the device:</p> <ul style="list-style-type: none"> <li>▶ <code>transparent</code> for transparent mode</li> <li>▶ <code>router</code> for router mode, or</li> <li>▶ <code>pppoe</code> for PPPoE mode</li> </ul> <p>Default setting: <code>transparent</code>.</p> <p><b>Note:</b> You configure the details for the respective network modes in the “Transparent Mode”, “Router Mode” and “PPPoE Mode” dialogs.</p>
Forward IP fragments	Sets whether the device forwards IP fragments. Default setting: <code>on</code> .
Forward net-directed Broadcasts	Sets whether the device forwards net-directed Broadcasts. Default setting: <code>off</code> .
Send ICMP redirects	Specifies whether the device additionally sends an ICMP redirect packet when the device routes a received packet back into the same subnetwork at the receiving interface. Default setting: <code>on</code> .

*Table 2: Global network configuration, mode and forwarding settings*

**Note:**

- ▶ The setting for:
  - “Forward IP fragments”
 is applied by the device in the Transparent, Router and PPPoE modes.
- ▶ The settings for:
  - “Forward net-directed Broadcasts” and
  - “Send ICMP redirects”
 are only applied by the device in the Router and PPPoE modes.

---

**Note:** Before switching to another mode, verify that the device can still be accessed with the configuration of the other mode.

## 1.2.2 Transparent Mode

This dialog allows you to configure the transparent mode. In transparent mode, the device behaves like a switch and transmits on layer 2 of the ISO/OSI layer model.

Name	Meaning
Protocol	Activate/deactivate the DHCP protocol. Activate the DHCP protocol if the device is to get its IP parameters from a DHCP server on the basis of the MAC address or the name of the device. <b>Note:</b> An EAGLE One device only supports standard DHCP. Therefore, if you are using a Hirschmann DHCP server, deactivate the “Hirschmann Device” setting for the EAGLE One device in its pool entry.

Table 3: Network: Protocol in transparent mode

Name	Meaning
IP Address	Enter the IP address via which you can access the device.
MAC Address	Display the MAC address.
Gateway Address	Enter the gateway address.
Netmask	Enter the netmask.
Use VLAN Tag	By selecting this you specify that the device evaluates the VLAN tag of the data packets that are addressed to the device (management). Thus the management of the device can only be accessed from the VLAN with the management VLAN ID.
VLAN ID	Define the VLAN ID (1-4.094) of the VLAN. <b>Note:</b> The device uses the VLAN ID entered in this field if "Use VLAN Tag" is marked exclusively.

*Table 4: Network: Locally in transparent mode*

Name	Meaning
Function	Activate/deactivate the HiDiscovery protocol.  The HiDiscovery protocol allows you to allocate an IP address to the device on the basis of its MAC address. Activate the HiDiscovery protocol if you want to allocate an IP address to the device from your PC with the supplied HiDiscovery software (default setting: "Operation" <sub>on</sub> , "Access" <sub>read-write</sub> ).
Access	read-write: read and allocate IP addresses read-only: read IP addresses

*Table 5: Network: HiDiscovery-Protocol in transparent mode*

Name	Meaning
Relay	By selecting this you specify that the device forwards the HiDiscovery protocol (setting on delivery: deactivated).

*Table 6: Network: HiDiscovery-Relay in transparent mode*

**Note:** The device displays the currently active network mode in the Network submenu **"Global"** .

---

**Note:** The `Advanced:Packet Forwarding` ([see on page 200](#)) dialog allows you to activate and deactivate the forwarding of RSTP, GMRP and DHCP data packets. Default setting: no forwarding of these packets.

**Note:** The device offers the configuration with HiDiscovery exclusively in and for transparent mode. The transparent mode is activated in the as-delivered condition.

### 1.2.3 Router Mode

This dialog allows you to configure the router mode. In the router mode, the device behaves like a router and transmits on layer 3 of the ISO/OSI layer model.

#### ■ Internal Interface (Port 1)

Name	Meaning
Protocol	Activate/deactivate the DHCP protocol. Activate the DHCP protocol if the device is to get its IP parameters from a DHCP server on the basis of the MAC address or the name of the device. <b>Note:</b> An EAGLE One device only supports standard DHCP. Therefore, if you are using a Hirschmann DHCP server, deactivate the “Hirschmann Device” setting for the EAGLE One device in its pool entry.

Table 7: Network: Protocol in router mode at internal interface



Name	Meaning
IP Address	Enter the IP address via which you can access the device.
Netmask	Enter the netmask.
Use VLAN Tag	When the function is switched on, the device accepts data packets with the VLAN ID entered in the field VLAN ID exclusively. The NAT functions are disabled.
VLAN ID	Define the VLAN ID (1-4.094) of the VLAN. <b>Note:</b> The device uses the VLAN ID entered in this field if "Use VLAN Tag" is marked exclusively.

Table 8: Network: Locally in router mode at internal interface

## ■ External Interface (Port 2)

Name	Meaning
Protocol	Activate/deactivate the DHCP protocol. Activate the DHCP protocol if the device is to get its IP parameters from a DHCP server on the basis of the MAC address or the name of the device. <b>Note:</b> An EAGLE One device only supports standard DHCP. Therefore, if you are using a Hirschmann DHCP server, deactivate the "Hirschmann Device" setting for the EAGLE One device in its pool entry.

Table 9: Network: Protocol in router mode at external interface

Name	Meaning
IP Address	Enter the IP address via which you can access the device.
Netmask	Enter the netmask.
Use VLAN Tag	When the function is switched on, the device accepts data packets with the VLAN ID entered in the field VLAN ID exclusively. The NAT functions are disabled.
VLAN ID	Define the VLAN ID (1-4.094) of the VLAN. <b>Note:</b> The device uses the VLAN ID entered in this field if "Use VLAN Tag" is marked exclusively.
Default Gateway	Define the standard gateway. If the subnetwork in which the gateway is integrated is assigned to the internal or external interface is of no concern. The purpose of a gateway is to reach nodes outside of subnetworks, which are assigned directly to an interface. To this gateway, the device sends packets whose destination address is outside of the subnetworks assigned to the interfaces. The IP address of the gateway needs to be in one of the subnetworks which are assigned to an interface.

Table 10: Network: Locally in router mode at external interface

## ■ Secondary IP Interfaces

This part of the dialog allows you to connect several subnetworks to a router interface (multinetting) and to create VLAN interfaces on a router interface. This allows you to route between VLANs.

- Click on “New...” to open a window for entering a new row in the table. Select “Internal Interface” or “External Interface”.  
After entering
  - the IP address,
  - the netmask,
  - Use VLAN Tag and
  - the VLAN ID,
 you click on “Set” to transfer the entry into the table.
- Click on “Back” to return to the table.
- If additional entries in the table are required, you create these by clicking on “Create...”.

In the “Active” column, you can activate/deactivate the individual entries in the table.

You can change the entries directly in the table.

To delete a row, select the row and click on “Delete Entry”.

Name	Meaning
IP Address	Enter the IP address
Netmask	Enter the netmask
Use VLAN Tag	When the function is switched on, the device accepts data packets with the VLAN ID entered in the field VLAN ID exclusively. The NAT functions are disabled.
VLAN ID	Define the VLAN ID (1-4.094) of the VLAN. <b>Note:</b> The device uses the VLAN ID entered in this field if "Use VLAN Tag" is marked exclusively.

Table 11: Network: Table for secondary IP address entries

**Note:** The device displays the currently active network mode in the Network submenu “Global” .

## 1.2.4 PPPoE Mode

This dialog enables you to configure PPPoE (Point to Point Protocol over Ethernet) mode.

In PPPoE network mode, the device creates a point-to-point connection to a dial-in node.

**Note:** In the PPPoE Mode, use the NAT function if you are using private IP addresses in the internal network and want to communicate with the public network. In the state on delivery, the device transmits from the internal network to the external network, even if NAT is deactivated. You can help prevent this by creating a packet filter.

### ■ Internal Interface (Port 1)

Name	Meaning
Protocol	<p>Activate/deactivate the DHCP protocol.            Activate the DHCP protocol if the device is to get its IP parameters from a DHCP server on the basis of the MAC address or the name of the device.  <b>Note:</b> An EAGLE One device only supports standard DHCP. Therefore, if you are using a Hirschmann DHCP server, deactivate the "Hirschmann Device" setting for the EAGLE One device in its pool entry.</p>

Table 12: Network: Protocol in PPPoE mode at internal interface

Name	Meaning
IP Address	Enter the IP address via which you can access the device.
Netmask	Enter the netmask.
Use VLAN Tag	When the function is switched on, the device accepts data packets with the VLAN ID entered in the field VLAN ID exclusively. The NAT functions are disabled.
VLAN ID	<p>Define the VLAN ID (1-4.094) of the VLAN.  <b>Note:</b> The device uses the VLAN ID entered in this field if "Use VLAN Tag" is marked exclusively.</p>

Table 13: Network: Locally in PPPoE mode at internal interface

## ■ External Interface (Port 2)

Name	Meaning
User Name	Enter the user name allocated by the provider.
Password	Enter the password allocated by the provider.
Interface MTU	Enter the maximum packet size allocated by the provider for which the data packets are not fragmented yet (Maximum Transmission Unit). Permitted values: 60-1,500 bytes, default setting: 1,492 bytes.

*Table 14: Network: User identification and MTU in PPPoE mode at external interface*

Name	Meaning
Switch on automatic interruption	By selecting this you specify that the device automatically interrupts the PPPoE connection at the specified time every day. Before activating this function, check whether the system time of your EAGLE One device is set correctly.
Time (hours) until interruption	Set the time (hour) at which the device automatically interrupts the PPPoE connection every day. Value range: 0 to 23.

*Table 15: Network: the PPPoE connection is interrupted automatically*

Name	Meaning
IP Address	Display the IP address allocated by the provider
Netmask	Display the netmask allocated by the provider
Gateway	Display the gateway allocated by the provider
Status	Display the connection status

*Table 16: Network: Local parameters in PPPoE mode at external interface*

### ■ Creating secondary IP addresses

Entries for secondary IP addresses allow you to connect multiple subnetworks to one router interface (multinetting).

- Click on “Create...” to open a window for entering a new row in the table.

After entering

- the IP address,
- the netmask,
- Use VLAN Tag and
- the VLAN ID

you click on “Set” to transfer the entry into the table.

- Click on “Back” to return to the table.
- If additional entries in the table are required, you create these by clicking on “Create...”.

In the “Active” column, you can activate/deactivate the individual entries in the table.

You can change the entries directly in the table.

To delete a row, select the row and click on “Delete Entry”.

Name	Meaning
IP Address	Enter the IP address
Netmask	Enter the netmask
Use VLAN Tag	When the function is switched on, the device accepts data packets with the VLAN ID entered in the field VLAN ID exclusively. The NAT functions are disabled.
VLAN ID	Define the VLAN ID (1-4.094) of the VLAN. <b>Note:</b> The device uses the VLAN ID entered in this field if "Use VLAN Tag" is marked exclusively.

Table 17: Network: Table for secondary IP address entries

**Note:** The device displays the currently active network mode in the Network submenu “Global” .

## 1.2.5 Routes

The route table allows you to enter static routes.

### ■ Creating a route entry in the table

- Click on “New...” to open a window for entering a new row in the table. Select “Internal Interface” or “External Interface”.  
After entering
  - the destination network,
  - the destination netmask and
  - the next hop’s IP address,
 you click on “Set” to transfer the entry into the table.
- Click on “Back” to return to the table.
- If additional entries in the table are required, you create these by clicking on “Create...”.

In the “Active” column, you can activate/deactivate the individual entries in the table.

You can change the entries directly in the table.

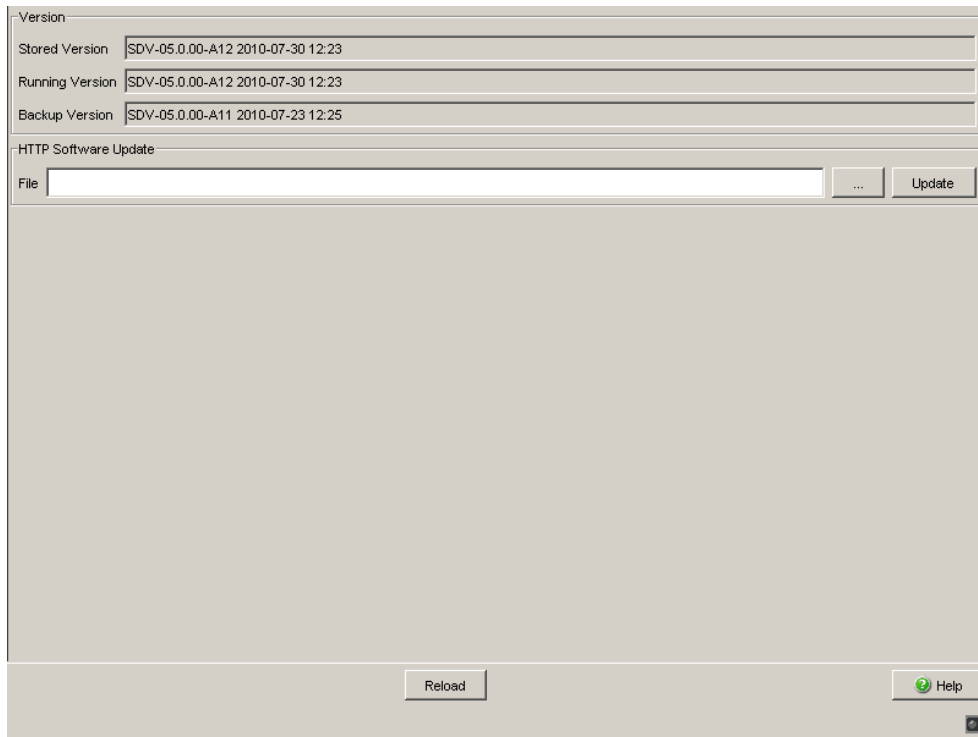
To delete a row, select the row and click on “Delete Entry”.

Name	Meaning
Destination Network	First IP address of the destination subnetwork
Destination Mask	Netmask of the destination subnetwork
Next Hop	The next hop’s gateway IP address

Table 18: Table for Routes

## 1.3 Software

The software dialog enables you display the software versions in the device and to carry out a software update of the device via file selection.



*Figure 7: Software Dialog*

For a HTTPS software update (via the file selection window), the device software has to reside on a drive that you can access from your PC.

Name	Meaning
<b>Frame „Version“</b>	
Stored Version	Show the version of the software stored in the flash memory.
Running Version	Show the version of the software running on the device.
Backup Version	Show the version of the backup software stored in the flash memory.
<b>Frame „https-Software-Update“</b>	
“File” input row	Show the device software selected (*.bin).
“...” button	Open a file selection window
“Update” button	Transfer the selected device software to the device.

*Table 19: Software Version Display and Update*

The end of the update is indicated by one of the following messages:

- ▶ Update completed successfully.
- ▶ Update failed. Reason: refer text string of the message.
- After successfully loading it, you activate the new software:  
Select the `Basic Settings:Restart` dialog and perform a cold start. On a cold start, the device reloads the software from the non-volatile memory, restarts, and performs a self-test.
- In your browser, click on “Reload” so that you can access the device again after it is booted.



## 1.4 Port Configuration

This configuration table allows you to configure every port of the device.

Variable	Meaning	Possible Values	State on Delivery
Port	Port designation (int: 1, ext: 2)	–	–
Name	Enter a name of your choice for each port.	ASCII characters, max. 64 characters	–
Port on	Activate the port by checkmarking it.		
Propagate Connection Error	When you checkmark this, you specify that when a connection error has been detected at this port this is propagated to the device status and signal contact.	on/off	on
Automatic Configuration	Activate automatic selection of the operating mode of a port by checkmarking the corresponding field. After autonegotiation has been switched on, it takes a few seconds for the operating mode to be set.	on/off	on
Manual Configuration	Set the operating mode for this port	– 10 Mbit/s half-duplex (HDX) <sup>a</sup> – 10 Mbit/s full-duplex (FDX) <sup>a</sup> – 100 Mbit/s half-duplex (HDX) – 100 Mbit/s Full duplex (FDX)	100 Mbit/s full-duplex (FDX)
Link/Current settings	Display the current operating mode and thus display an existing connection.	<sup>a</sup> For TX ports only	

*Table 20: Setting options per port*

**Note:** The active automatic configuration takes precedence over the manual configuration.

Port	Name	Port on	Propagate Connection Error	Automatic Configuration	Manual Configuration	Link/ Current Settings	
internal (Port...		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	100 Mbit/s FDX	100 Mbit/s FDX	
external (Por...		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	100 Mbit/s FDX	100 Mbit/s FDX	

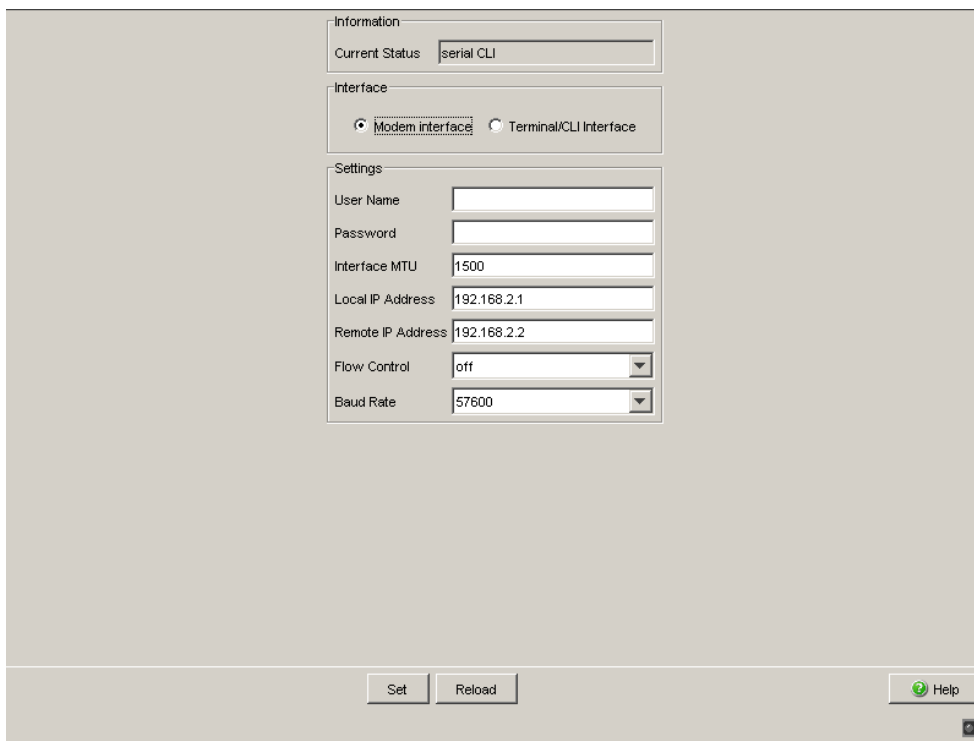
Set   Reload   Help

Figure 8: Port configuration table dialog

## 1.5 Serial Port

This dialog allows you to configure the serial port of the device

- ▶ as a Terminal/CLI interface (default setting) or
- ▶ as a Modem interface.



The screenshot shows a configuration dialog for the serial port. It is divided into three main sections: Information, Interface, and Settings. The Information section shows the current status as 'serial CLI'. The Interface section has two radio buttons: 'Modem interface' (which is selected) and 'Terminal/CLI Interface'. The Settings section includes fields for User Name, Password, Interface MTU (set to 1500), Local IP Address (192.168.2.1), Remote IP Address (192.168.2.2), Flow Control (set to off), and Baud Rate (set to 57600). At the bottom of the dialog, there are three buttons: 'Set', 'Reload', and 'Help'.

Figure 9: Serial Port dialog

## 1.5.1 Configuration as a Terminal/CLI interface

□ In the “Interface” frame, select Terminal/CLI interface.

In Terminal/CLI interface mode, the following parameters are fixed for the interface:

- ▶ 9,600 bits/s,
- ▶ 8 data bits,
- ▶ no parity,
- ▶ 1 stopbit,
- ▶ no flow control.

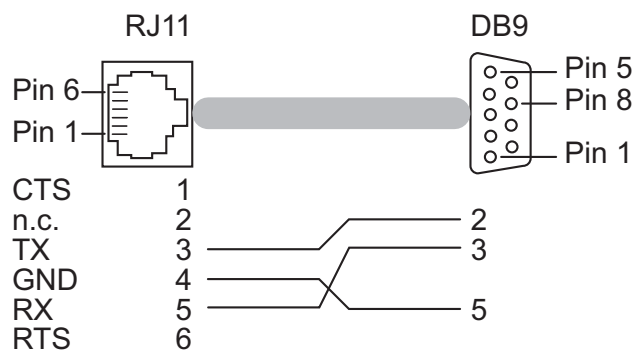
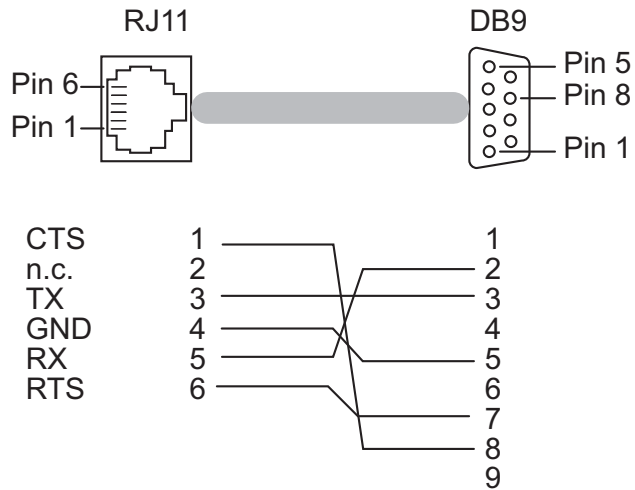


Figure 10: Terminal Cable Pin Assignment

## 1.5.2 Configuration as a Modem interface

In the “Interface” frame, select `Modem interface`.  
The device displays the “Settings” frame.



*Figure 11: Pin assignment of modem cable*

Name	Meaning
Username	Enter the PPP user name for accessing a remote device on the EAGLE One (PAP, CHAP).
Password	Enter the PPP password for accessing a remote device on the EAGLE One (PAP, CHAP).
Interface MTU	Enter the maximum packet size for the PPP connection (Maximum Transmission Unit). The device fragments data packets if they are larger than the value entered. Permitted values: 60-1,500 bytes. Default setting: 1,500 bytes. Select a smaller value if you know that your Internet service provider uses a smaller value or no connection can be made.
Local IP Address	Enter the IP address of the serial port. Select an IP address for the serial port that belongs to a different subnetwork than the IP addresses allocated under “Transparent Mode”, “Router Mode” and “PPPoE Mode”.
Remote IP Address	Enter the IP address of the remote device. Select an IP address for the serial port that belongs to a different subnetwork than the IP addresses allocated under “Transparent Mode”, “Router Mode” and “PPPoE Mode”.
Flow Control	Enable/Disable Flow Control.
Baud rate	Select the baud rate. Select the same baud rate (typically: 57,600 baud) on your modem and on the EAGLE One’s serial port.
Status	Status of the serial interface in modem mode. Possible messages: “not connected” or “peer connected”. In terminal/CLI mode, the message is “serial CLI mode”

*Table 21: Settings for Modem Mode*

**Note:** When you select the mode “Terminal/CLI Interface”, the device reduces the adjustable parameters to those for the Terminal/CLI Interface.

**Note:** Configure the filter rules in the “Incoming PPP packets” dialog in the `Network Security:Packet Filter` menu so that the Firewall enables data traffic between the remote and local IP addresses.

# 1.6 Load/Save

With this dialog you can:

- ▶ load a configuration,
- ▶ save a configuration,
- ▶ display a configuration,
- ▶ delete a configuration,
- ▶ activate a configuration,
- ▶ create a configuration,
- ▶ use the ACA for configuring,
- ▶ cancel a configuration change.

Status des nicht-flüchtigen Speichers (NVM) OK

Status des AutoConfig Adapters (ACA) Nicht vorhanden

Konfigurationsänderung widerrufen

Funktion  Watchdog IP-Adresse

Periode bis zum Widerruf bei Verbindungsunterbrechung [s]

---

Konfiguration im nicht-flüchtigen Speicher (NVM)

Name	Datum der letzten Änderung	Aktiv	
config	01.01.2009 09:15:18	<input checked="" type="checkbox"/>	<div style="display: flex; flex-direction: column; gap: 5px;"> <div style="border: 1px solid gray; padding: 2px;">Kopieren vom PC</div> <div style="border: 1px solid gray; padding: 2px;">Kopieren zum PC</div> <div style="border: 1px solid gray; padding: 2px;">Anzeigen</div> <div style="border: 1px solid gray; padding: 2px;">Löschen</div> <div style="border: 1px solid gray; padding: 2px;">Aktivieren</div> <div style="border: 1px solid gray; padding: 2px;">Erzeugen</div> </div>

---

Konfiguration auf dem AutoConfig Adapter (ACA)

Name	Datum der letzten Änderung	Aktiv	
			<div style="display: flex; flex-direction: column; gap: 5px;"> <div style="border: 1px solid gray; padding: 2px;">Kopieren vom PC</div> <div style="border: 1px solid gray; padding: 2px;">Kopieren zum PC</div> <div style="border: 1px solid gray; padding: 2px;">Anzeigen</div> <div style="border: 1px solid gray; padding: 2px;">Löschen</div> <div style="border: 1px solid gray; padding: 2px;">Kopieren nach NVM</div> </div>

Figure 12: Load/Save dialog

---

## 1.6.1 Status display

Name	Meaning
OK	The configuration data from the NVM and the device is consistent.
out-of-sync	The configuration data from the NVM and the device is not consistent.

*Table 22: Status of the non-volatile memory (NVM)*

Name	Meaning
OK	AutoConfiguration Adapter connected. The configuration data on the ACA and the device matches.
out-of-sync	The current configuration's data on the ACA and the NVM do not match.
Absent	No AutoConfiguration Adapter is connected.

*Table 23: Status of the AutoConfiguration Adapter (ACA)*



## 1.6.2 Configuration in the non-volatile memory (NVM)

The table lists the individual configuration files of the non-volatile memory.

Name	Meaning
Name	Name of the configuration file
Modification date	Date saved YYYY-MM-DD HH:MM:SS
Active	Display the active configuration

Table 24: Configuration in the Non-Volatile Memory (NVM)

**Note:** The device allows you to use up to 32 characters for the name of a configuration file. Allowed are alphanumeric characters ("A" to "Z", "a" to "z", "0" to "9") as well as the underline "\_" and the hyphen "-".

Name	Meaning
Copy from PC	Load a configuration file from a PC to the device. The configuration file appears in a new table entry.
Copy to PC	Save a configuration file from the device to a PC.
Show	Display a configuration file.
Delete	Delete a configuration file.
Activate	Activate a configuration file. In the "Active" column, the device shows you the active configuration.
New	Save the current configuration in a configuration file on the device (and the ACA).

Table 25: Editing the Table Entries

If you change the current configuration (for example, by switching a port off), the graphical user interface changes the "load/save" symbol in the navigation tree from a disk symbol to a yellow triangle. After saving the configuration, the graphical user interface displays the "load/save" symbol as a disk again.

**Note:** You can reset to the state on delivery with `Restart:Reset to Factory` (see page 45). Note that the device deletes all tables, settings and files on the device and on a connected ACA.

### 1.6.3 Configuration on the AutoConfiguration Adapter (ACA)

An ACA is a means for saving the configuration data of a device. In the case of a detected failure, an ACA enables the configuration data to be transferred easily by means of a substitute device of the same type.

The table lists the individual configuration files of an AutoConfiguration Adapter (ACA).

Name	Meaning
Name	Name of the configuration file
Modification date	Date saved YYYY-MM-DD HH:MM:SS
Active	Display the active configuration

*Table 26: Configuration on the AutoConfiguration Adapter (ACA)*

Name	Meaning
Copy from PC	Load a configuration file from a PC to the ACA. The configuration file appears in a new table entry.
Copy to PC	Save a configuration file from the ACA to a PC.
Show	Display a configuration file.
Delete	Delete a configuration file.
Copy to NVM	Save a configuration file from the ACA to the device.

*Table 27: Editing the Table Entries*

---

If you change the current configuration (for example, by switching a port off), the graphical user interface changes the “load/save” symbol in the navigation tree from a disk symbol to a yellow triangle. After saving the configuration, the graphical user interface displays the “load/save” symbol as a disk again.

**Note:** You can reset to the state on delivery with `Restart:Reset to Factory` (see page 45). Note that the device deletes all tables, settings and files on the device and on a connected ACA.

## 1.6.4 Saving and Loading a Configuration

Name	Meaning
Set	Write the setting for which configuration is marked as active to the non-volatile memory and to the ACA.
Reload	Update the table display in case this has been changed by another SNMP access.
Save to NVM + ACA	Replace the active configuration with the current configuration in the non-volatile memory and on the ACA
Restore from NVM	Reload the active configuration from the local non-volatile memory.

*Table 28: Saving and loading*

## 1.6.5 Cancelling a configuration change

### ■ Operation

If the function is activated and the connection to the device is interrupted for longer than the time specified in the field “Period to undo while connection is lost [s]”, the device then loads the last configuration saved.

- Activate the function before you configure the device so that you will then be reconnected if an incorrect configuration interrupts your connection to the device.
- Enter the “Period to undo while the connection is lost [s]” in seconds.  
Possible values: 10-600 seconds.  
Default setting: 600 seconds.

**Note:** Deactivate the function after you have successfully saved the configuration. In this way you help prevent the device from reloading the configuration after you close the web interface.

**Note:** When accessing the device via SSH, also note the TCP connection timeouts for the cancellation of the configuration.

### ■ Watchdog IP address

“Watchdog IP address” shows you the IP address of the PC from which you have activated the (watchdog) function. The device monitors the link to the PC with this IP address, checking for interruptions.

## 1.7 Restart

With this dialog you can:

- ▶ coldstart the device,
- ▶ reset the MAC address table,
- ▶ reset the ARP table,
- ▶ reset the firewall and NAT connections,
- ▶ reset the port counters,
- ▶ delete the log file,
- ▶ reset the device to the state on delivery.

Name	Meaning
Coldstart ...	The device reloads the software from the non-volatile memory, restarts, and performs a self-test.
Reset MAC Address table	The device resets the entries with the status “learned” in the filter table.
Reset ARP table	The device empties the ARP table.
Reset firewall and NAT connections	The device resets the state tables ( <a href="#">see on page 83 “Network Security”</a> ).
Reset port counter	The device resets the port counter.
Delete logfile	The device deletes the internal log file. The persistent files remain.
Reset to factory	The device resets all tables, settings and files on the device (and on a connected ACA) to the state on delivery.

*Table 29: Restart*

**Note:** During the restart, the device temporarily does not transfer any data, and it cannot be accessed via the graphical user interface or other management systems such as Industrial HiVision.

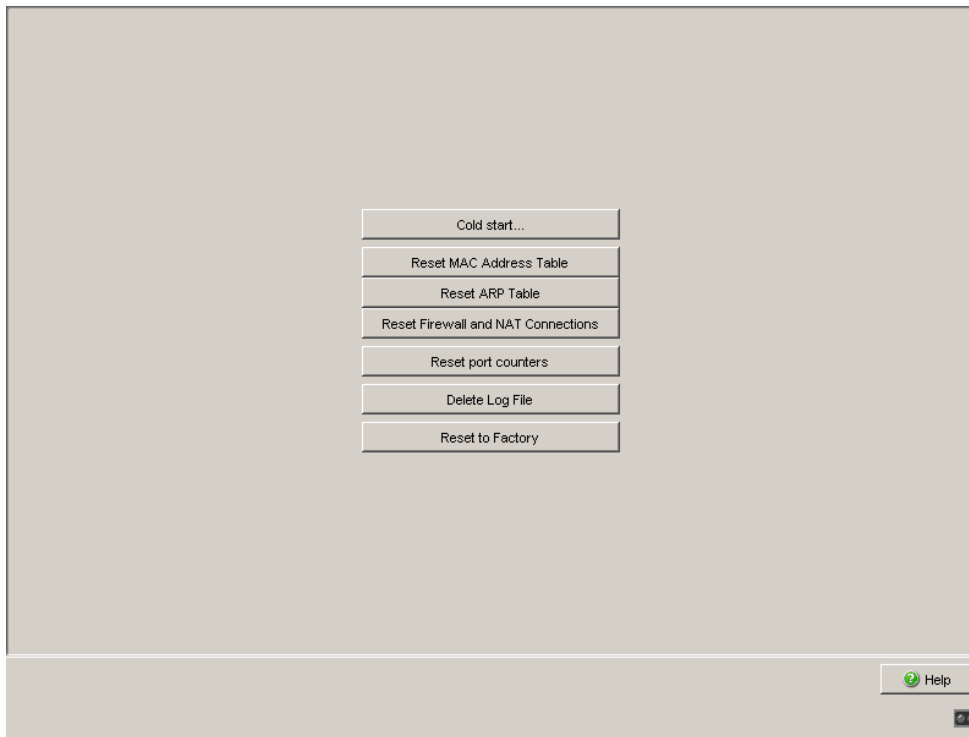


Figure 13: Restart Dialog

## 2 Security

The security menu contains the dialogs, displays and tables for configuring the security settings:

- ▶ Password
- ▶ SNMP Access
- ▶ Web Access
- ▶ SSH Access
- ▶ External Authentication
- ▶ Login Banner

## 2.1 Password

This dialog gives you the option of changing the read and read/write passwords for access to the device via the graphical user interface (GUI), via the CLI, and via SNMPv3 (SNMP version 3).

Set different passwords for the read password and the read/write password so that a user that only has read access (user name “user”) does not know, or cannot guess, the password for read/write access (user name “admin”).

The graphical user interface (GUI) communicates via SNMPv3, and the user interface (CLI) via SSH.

**Note:** Passwords are case-sensitive.

**Note:** For security reasons, change the factory setting password. You thus help prevent the device from being accessed with this password. If the password is the factory setting password, the device displays the message “Default Password” in every dialog’s header line.

- Select “Modify Read-Only Password (User)” to enter the read password.
- Enter the new read password in the “New Password” line and repeat your entry in the “Please retype” line.
- Select “Modify Read-Write Password (Admin)” to enter the read/write password.
- Enter the read/write password and repeat your entry.



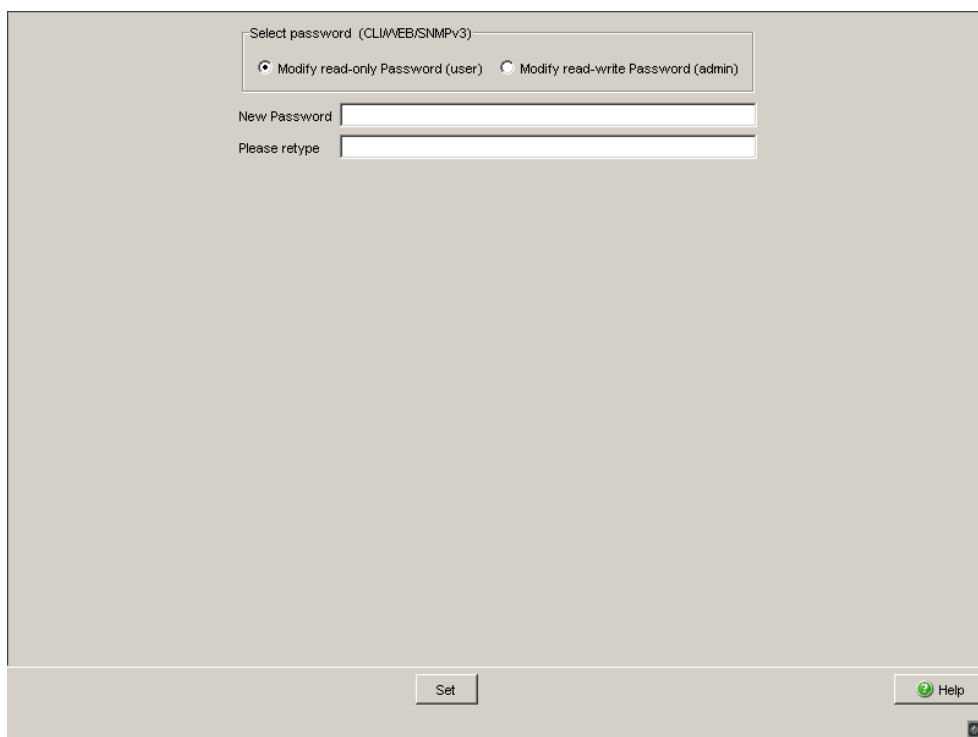


Figure 14: Password Dialog

**Note:** If you do not know a password with “read/write” access, you will have no write access to the device.

**Note:** For security reasons, the dialog shows the passwords as asterisks. Make a note of every change. You cannot access the device without a valid password.

**Note:** In SNMP version 3, use between 5 and 32 characters for the password, because many applications do not accept shorter passwords.

Access via a Web browser can be disabled in a separate dialog ([see on page 56 “Web Access”](#)).

## 2.2 SNMP Access

With this dialog you can

- ▶ enter an SNMP port. The factory setting for the port is 161.  
Enter a different UDP port number if, for administration or security reasons, you want to use a different port number. The graphical user interface will automatically use the new port number after a restart.
- ▶ manage, create and delete entries for accessing the device via SNMP.  
Click on “↑” oder “↓” to move a selected entry up or down.
- ▶ tunnel the SNMP access of the graphical user interface to the device via HTTPS. Thus only HTTPS connections to the device are necessary. With this function you can also perform a RADIUS authentication for SNMP users.  
The factory setting for the function SNMP over HTTPS (Tunnel) is inactive.

**Note:** A change to the setting SNMP over HTTPS (Tunnel) only takes effect after reloading the graphical user interface. Access via SNMP is still possible.

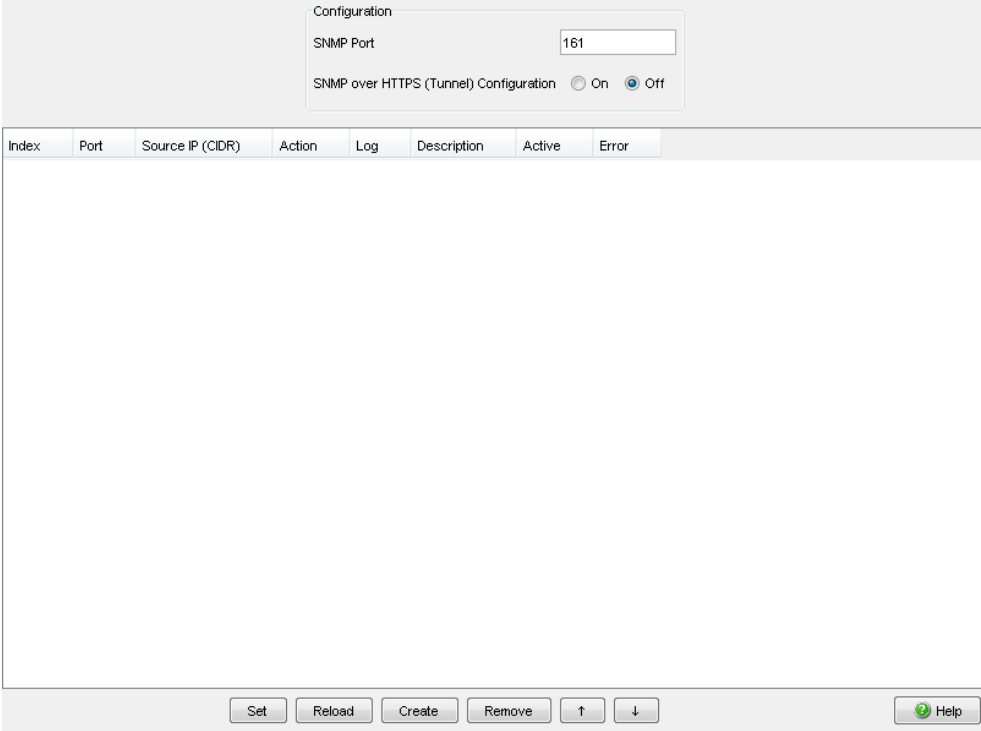


Figure 15: SNMP Access dialog

Parameter	Meaning	Possible Values
Index	Sequential number to which the access restriction refers	(Automatically generated)
Port	Select port.	int - settings refer to the internal port ext - settings refer to the external port ppp - settings refer to the V.24 port configured as a modem.
Source IP (CIDR)	Enter an IP address or a group of IP addresses in mask form that can access the device, or “any”. When you enter an IP address without a mask, the device changes the form of the IP address to the mask form with a 32-bit long network mask (x.x.x.x in x.x.x.x/32).	Any IP address in mask form. This may be the IP address or the group of IP addresses which the device can access. any - Access to this device is permitted for computers with any IP address.
Action	Select the action for the device if (one of) the IP addresses entered under “Source Address (CIDR)” accesses the device.	accept - access allowed drop - access not allowed, no message to sender reject - access not allowed, message to sender
Log	When the rules of a table entry have been used by the device, the device writes this as an event in the event log ( <a href="#">see on page 160 “Event Log”</a> ).  <b>Note:</b> The <code>logAndTrap</code> setting can generate large quantities of trap data traffic. This is especially the case when sending the trap triggers a match in the Firewall rule again (e.g. if the trap host cannot be reached and a router responds with an ICMP message).	enable, disable, logAndTrap
Description	Enter a description of your choice for this entry, e.g. the name or location of the PC that has the IP address entered.	Maximum 128 characters
Active	Activate/deactivate table entry	on/off
Error	Shows the last detected error for an attempt to activate the table entry (usually a detected syntax error).	-

Table 30: SNMP access table

- ▶ The “Create” button enables you to create a new row in the table.
- ▶ With “Remove” you delete the selected rows in the table.

**Note:** If no row is selected,

- there are no access restrictions at the internal port
- there is no access option to the external port via SNMP.

**Note:** In the state on delivery, the firewall allows the outgoing IP traffic and the management access (SNMP, HTTPS and SSH) to the device at the internal port. If you want to deactivate the management access, you have the following options:

- ▶ Define explicit `drop` rules for the management access.
- ▶ Change the corresponding firewall rules for the outgoing IP traffic.

**Note:** The Firewall supports up to 1024 IP rules.

In the dialog `Diagnostics:IP Firewall List`, you find the summary of the active rules.

---

## 2.3 SNMPv1/v2

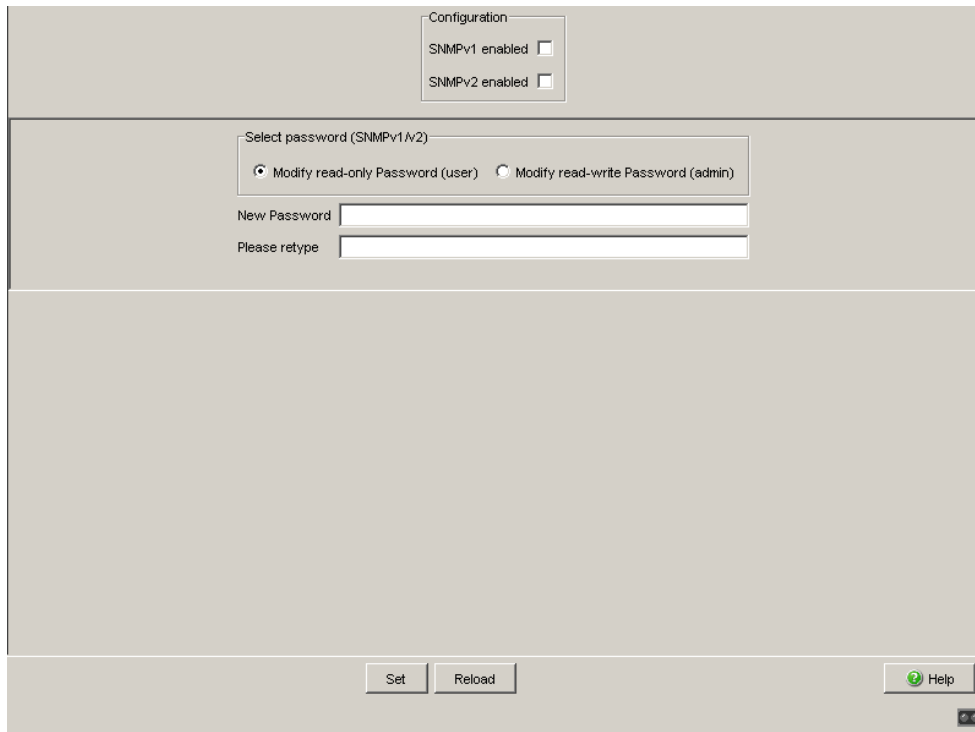
With this dialog you can:

- ▶ select the access via SNMPv1 or SNMPv2. In the state on delivery, both protocols are deactivated, so SNMP access is only possible via SNMPv3, for security reasons.
- ▶ change the read and read/write passwords for access to the device via SNMPv1/v2. The passwords are case-sensitive. For security reasons, create unique passwords for read and read/write access.

**Note:** In the state on delivery, SNMPv1 and SNMPv2 access is deactivated. As SNMPv1 and SNMPv2 transfer data unencrypted, using SNMPv1 and SNMPv2 creates a potential security risk. Only allow SNMPv1 or SNMPv2 access if you want to use an application that requires this.

**Note:** For security reasons, change the factory setting password. You thus help prevent the device from being accessed with this password. If the password is the factory setting password, the device displays the message “Default Password” in every dialog’s header line.

- Select “Modify Read-Only Password (User)” to enter the read password.
- Enter the new read password in the “New Password” line and repeat your entry in the “Please retype” line.
- Select “Modify Read-Write Password (Admin)” to enter the read/write password.
- Enter the read/write password and repeat your entry.



The image shows a web-based configuration dialog for SNMPv1/v2. At the top, there is a 'Configuration' section with two checkboxes: 'SNMPv1 enabled' and 'SNMPv2 enabled', both of which are currently unchecked. Below this is a section titled 'Select password (SNMPv1/v2)' containing two radio buttons: 'Modify read-only Password (user)' (which is selected) and 'Modify read-write Password (admin)'. Underneath the radio buttons are two text input fields: 'New Password' and 'Please retype'. At the bottom of the dialog, there are three buttons: 'Set', 'Reload', and 'Help' (which has a question mark icon).

Figure 16: SNMPv1/v2 dialog

**Note:** For security reasons, the dialog shows the passwords as asterisks. Make a note of every change. You cannot access the device without a valid password.

Access via a Web browser can be disabled in a separate dialog ([see on page 56 “Web Access”](#)).

## 2.4 Web Access

With this dialog you can:

- ▶ activate/deactivate the Web server on the device. In the delivery state, the Web server on the internal port is activated.

The Web server of the device allows you to configure the device by using the graphical user interface. Deactivating the Web server helps prevent Web access to the device.

- ▶ enter an HTTPS port (TCP port number that uses the device for the Web server).

Possible values: 1 - 65,535. Default setting: Well Known Port for HTTPS (443). This port change becomes effective when the device is restarted. When changing the port for access to the device, add the port number to the URL, e.g. <https://192.168.1.1:444>.

- ▶ manage, create and delete entries for accessing the device via the graphical user interface.
- ▶ upload certificates to the device.  
In its delivery state, the device includes a certificate.

After the Web server has been switched off, it is no longer possible to log in via a Web browser. The login in the open browser window remains active.

**Note:** The graphical user interface communicates with the device via SNMP. If you want to access the graphical user interface via the external port and the function SNMP over HTTPS (Tunnel) is inactive, you create an SNMP access rule ([see on page 50 “SNMP Access”](#)).



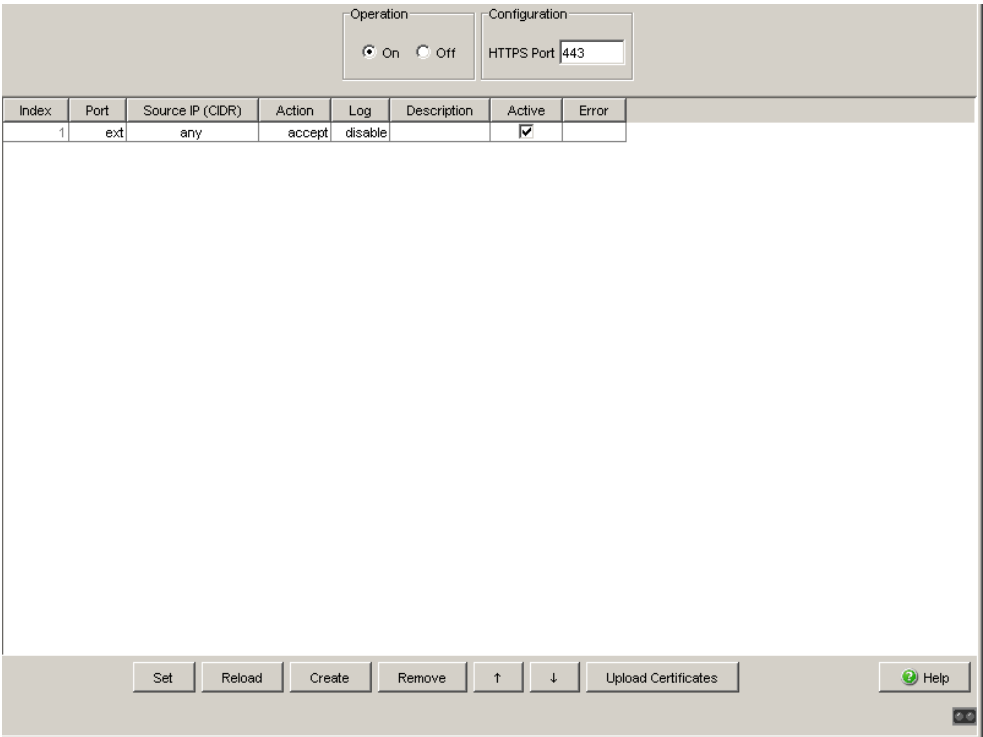


Figure 17: Web Access dialog

Parameter	Meaning	Possible Values
Index	Sequential number to which the access restriction refers	(Automatically generated)
Port	Select port.	int - settings refer to the internal port ext - settings refer to the external port ppp - settings refer to the V.24 port configured as a modem.
Source IP (CIDR)	Enter an IP address or a group of IP addresses in mask form that can access the device, or "any". When you enter an IP address without a mask, the device changes the form of the IP address to the mask form with a 32-bit long network mask (x.x.x.x in x.x.x.x/32).	Any IP address in mask form. This may be the IP address or the group of IP addresses which the device can access. any - Access to this device is permitted for computers with any IP address.
Action	Select the action for the device if (one of) the IP addresses entered under "Source Address (CIDR)" accesses the device.	accept - access allowed drop - access not allowed, no message to sender reject - access not allowed, message to sender
Log	When the rules of a table entry have been used by the device, the device writes this as an event in the event log ( <a href="#">see on page 160 "Event Log"</a> ).  <b>Note:</b> The <code>logAndTrap</code> setting can generate large quantities of trap data traffic. This is especially the case when sending the trap triggers a match in the Firewall rule again (e.g. if the trap host cannot be reached and a router responds with an ICMP message).	enable, disable, logAndTrap
Description	Enter a description of your choice for this entry, e.g. the name or location of the PC that has the IP address entered.	Maximum 128 characters
Active	Activate/deactivate table entry	on/off
Error	Shows the last detected error for an attempt to activate the table entry (usually a detected syntax error).	-

Table 31: Web access table

- ▶ The "Create Entry" button enables you to create a new row in the table. The device displays a dialog to remind you to create an additional SNMP rule where necessary if you want to use the graphical user interface.
- ▶ With "Delete Entry" you delete the selected rows in the table.
- ▶ With "↑" oder "↓" you move a selected entry up or down.

To upload a certificate, the file has to reside on a drive that you can access from your PC.

- Click on “Certificates”.
- In the file selection frame, click on “...”.
- In the file selection window, select the certificate file (e.g. certificate.p12) and click on “Open”.
- Click on “Copy from PC” to transfer the file to the device.

The end of the upload is indicated by one of the following messages:

- ▶ Update completed successfully.
- ▶ Update failed. Reason: file copy failed.

**Note:** In the state on delivery, the firewall allows the outgoing IP traffic and the management access (SNMP, HTTPS and SSH) to the device at the internal port. If you want to deactivate the management access, you have the following options:

- ▶ Define explicit `drop` rules for the management access.
- ▶ Change the corresponding firewall rules for the outgoing IP traffic.

**Note:** The device accepts HTTPS server certificates with a key length of between 512 and 2048 bits (RSA key in PEM format with non-encrypted private key).

Encryption algorithms supported by the server:

- ▶ SSLv3: AES128-SHA
- ▶ TLSv1: AES256-SHA AES128-SHA DES-CBC3-SHA

**Note:** The Firewall supports up to 1024 IP rules.

In the dialog `Diagnostics:IP Firewall List`, you find the summary of the active rules.

## 2.5 SSH Access

With this dialog you can:

- ▶ activate/deactivate the SSH server on the device. In the state on delivery, the SSH server is activated on the internal port.  
The SSH server of the device allows you to configure the device using the Command Line Interface (in-band). Deactivating the SSH server helps prevent SSH access to the device.
- ▶ enter an SSH port. Possible values are 1 - 65,535. The state on delivery is 22.
- ▶ view the DSA and RSA fingerprints. The fingerprints are used to identify the key used to login.
- ▶ manage, create and delete entries for accessing the device via SSH.

After the SSH server has been deactivated, you will no longer be able to access the device via a new SSH connection. If a SSH connection already exists, it is maintained.

**Note:** The Command Line Interface (out-of-band) and the `Security:Web Access` dialog in the graphical user interface (or another SNMP administration tool) allow you to reactivate the SSH server.

**Note:** The device allows you to use SFTP to access device files such as configuration files or the ACA, or to load a firmware update or VPN certificates onto the device. To do this, use an SFTP client, such as WinSCP. For the SFTP access, you must have SSH access to the device.

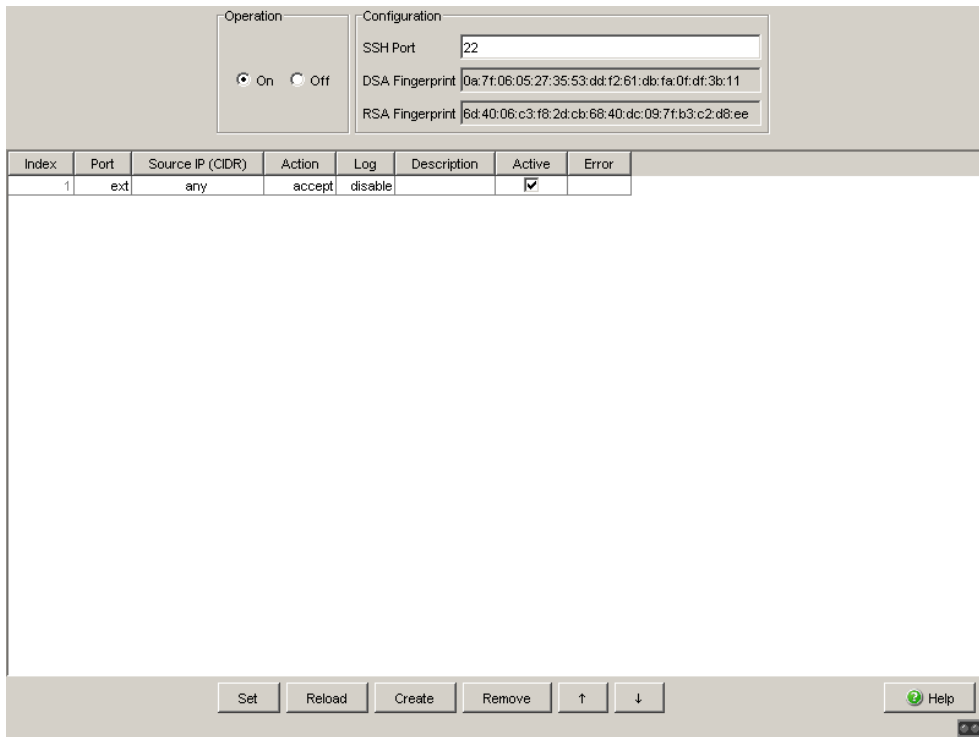


Figure 18: SSH Access dialog

Parameter	Meaning	Possible Values
Index	Sequential number to which the access restriction refers	(Automatically generated)
Port	Select port.	int - settings refer to the internal port ext - settings refer to the external port ppp - settings refer to the V.24 port configured as a modem.
Source IP (CIDR)	Enter an IP address or a group of IP addresses in mask form that can access the device, or “any”. When you enter an IP address without a mask, the device changes the form of the IP address to the mask form with a 32-bit long network mask (x.x.x.x in x.x.x.x/32).	Any IP address in mask form. This may be the IP address or the group of IP addresses which the device can access. any - Access to this device is permitted for computers with any IP address.
Action	Select the action for the device if (one of) the IP addresses entered under “Source Address (CIDR)” accesses the device.	accept - access allowed drop - access not allowed, no message to sender reject - access not allowed, message to sender
Log	When the rules of a table entry have been used by the device, the device writes this as an event in the event log ( <a href="#">see on page 160 “Event Log”</a> ).  <b>Note:</b> The <code>logAndTrap</code> setting can generate large quantities of trap data traffic. This is especially the case when sending the trap triggers a match in the Firewall rule again (e.g. if the trap host cannot be reached and a router responds with an ICMP message).	enable, disable, logAndTrap
Description	Enter a description of your choice for this entry, e.g. the name or location of the PC that has the IP address entered.	Maximum 128 characters
Active	Activate/deactivate table entry	on/off
Error	Shows the last detected error for an attempt to activate the table entry (usually a detected syntax error).	-

Table 32: SSH Access Table

- ▶ The “Create” button enables you to create a new row in the table.
- ▶ With “Remove” you delete the selected rows in the table.

**Note:** In the state on delivery, the firewall allows the outgoing IP traffic and the management access (SNMP, HTTPS and SSH) to the device at the internal port. If you want to deactivate the management access, you have the following options:

- ▶ Define explicit `drop` rules for the management access.
- ▶ Change the corresponding firewall rules for the outgoing IP traffic.

**Note:** Deactivating an entry helps prevent logging in again via SSH. However, an existing SSH connection to which the deactivation criteria apply remains in place until it is logged out.

**Note:** The Firewall supports up to 1024 IP rules. In the dialog `Diagnostics:IP Firewall List`, you find the summary of the active rules.

## 2.6 External Authentication

This dialog allows you to create up to 5 firewall user accounts. With the account name and the corresponding password, a user can log into the device on the login screen using the “user firewall” login type ([see on page 11 “Graphical User Interface”](#)). For each user firewall account, an authentication list is stored on the basis of which the device authenticates the account during the login.

You must have a user firewall account to be able to create an entry in the dialog `Network Security:User Firewall Entries` ([see page 128](#)).

### 2.6.1 User Firewall Accounts

This dialog allows you to create, configure and delete users that can login to the device under the “user firewall” login type ([see page 11](#)).



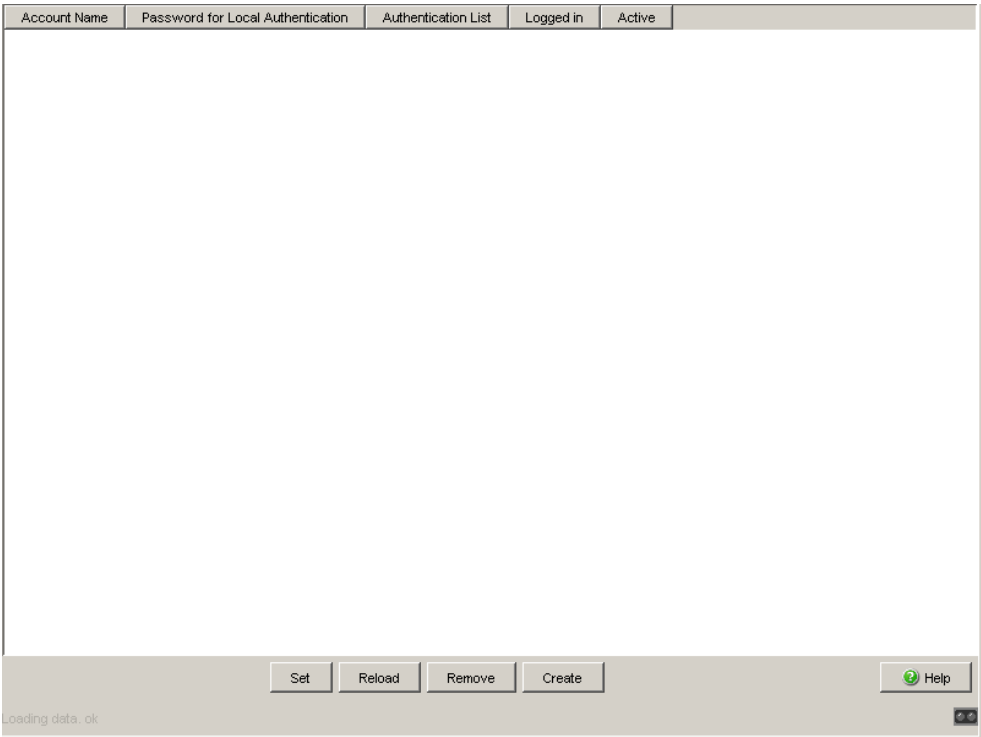


Figure 19: User Firewall Accounts Dialog

Parameter	Meaning	Possible Values
Account Name	Enter the name of a user (account name) that can login in the login window under the “user firewall” login type .	1-128 ASCII characters
Password for Local Authentication	Enter the password for this user.	Maximum 5-32 characters
Authentication list	Select an authentication list ( <a href="#">see on page 66 “Authentication Lists”</a> )	- userFirewallLoginDefaultList, - systemLoginDefaultList , - Lists that you created under Security:External Authentication:Authentification Lists ( <a href="#">see page 66</a> ).
Logged in	Show whether this user is logged into the user firewall. If this user is logged in, the administrator can log him off the user firewall by clicking on the checkmark, then on “Set”.	on/off
Active	Activate/deactivate table entry	on/off

Table 33: User Access table

- ▶ The “Create” button enables you to create a new row in the table.
- ▶ With “Remove” you delete the selected rows in the table.

## 2.6.2 Authentication Lists

This dialog allows you to create, configure and delete authentication lists. In an authentication list, you define

- ▶ which authentication methods the device uses when a user allocated to this authentication list logs in,
- ▶ in which sequence the device uses these authentication methods.

In the delivery state, this dialog already offers you the authentication lists “userFirewallLoginDefaultList” and “systemLoginDefaultList” to simplify the configuration.

Name	First Method	Second Method	Third Method	Active
systemLoginDefaultList	local	none	none	<input checked="" type="checkbox"/>
userFirewallLoginDefaultList	local	none	none	<input checked="" type="checkbox"/>

*Figure 20: Authentication lists*

If required, in “Authentication List for unknown System Login Users”, you select one of the authentication lists that the device uses when an unknown user accesses it as administrator. If you do not make a selection, the result is that no unknown users can access the device as administrator.

If required, in “Authentication List for unknown Firewall Users”, you select one of the authentication lists that the device shall use when an unknown user accesses it. If you do not make a selection, no unknown users are able to access the device.

Parameter	Meaning	Possible Values
Name	Name of the authentication list. "userFirewallLoginDefaultList" and "systemLoginDefaultList" are already created in the state on delivery.	Any ASCII characters
First method	Define the authentication method that the device uses first.	<p>none - access to the device without authentication</p> <p>local - authentication of user and password by the device</p> <p>radius - authentication of user and password by the RADIUS server</p> <p>deny - reject authentication</p>
Second method	Define the authentication method that the device uses if the first authentication method was not successful.	<p>none - access to the device without authentication</p> <p>local - authentication of user and password by the device</p> <p>radius - authentication of user and password by the RADIUS server</p> <p>deny - reject authentication</p>
Third method	Define the authentication method that the device uses if the first and second authentication methods were not successful.	<p>none - access to the device without authentication</p> <p>local - authentication of user and password by the device</p> <p>radius - authentication of user and password by the RADIUS server</p> <p>deny - reject authentication</p>
Active	Activate/deactivate table entry	on/off

Table 34: Authentication lists

- ▶ The "Create" button enables you to create a new row in the table.
- ▶ With "Remove" you delete the selected rows in the table.

### 2.6.3 RADIUS Server

RADIUS (Remote Authentication Dial-In User Service) is a client server protocol for the central authentication of users and terminal devices (AAA system).

This dialog allows you to enter the data for 1 to 3 RADIUS servers. If “radius” is selected as the authentication method in `External Authentication:Authentication Lists`, the device contacts the RADIUS servers one after the other in the case of authentication queries.

Address	UDP Port	Shared Secret	Active
0.0.0.0	1812		<input type="checkbox"/>
0.0.0.0	1812		<input type="checkbox"/>
0.0.0.0	1812		<input type="checkbox"/>

Figure 21: RADIUS Server Dialog

Parameter	Meaning	Possible Values
Retries	Enter how often the device resubmits an unanswered request to the RADIUS server before the device sends the request to another RADIUS server.	1 - 15
Timeout	Enter how long (in seconds) the device waits for a response after a request to the RADIUS server before the device resubmits the request.	1 - 30
<b>Table</b>		
Address	Enter the IP address of a RADIUS server.	
UDP Port	Enter the UDP port of the RADIUS server.	0 - 65,535 (default setting 1,812)
Shared Secret	Enter the character string which you get as a key from the administrator of your RADIUS server.	Maximum 20 characters
Active	Activate/deactivate table entry	on/off

*Table 35: RADIUS Server*

## 2.7 Login Banner

This dialog allows you to enter a login banner.

The device displays the login banner when a user logs in to the user interface (graphical user interface or CLI).

The login banner is up to 255 characters long. The characters in the ASCII code range 0x20 (space character, “ ”) to ASCII code 0x7E (tilde “~”) are allowed with the exception of percent signs (% , 0x25).





## **3 Time**

## **3.1 Basic Settings**

With this dialog you can enter general time-related settings.

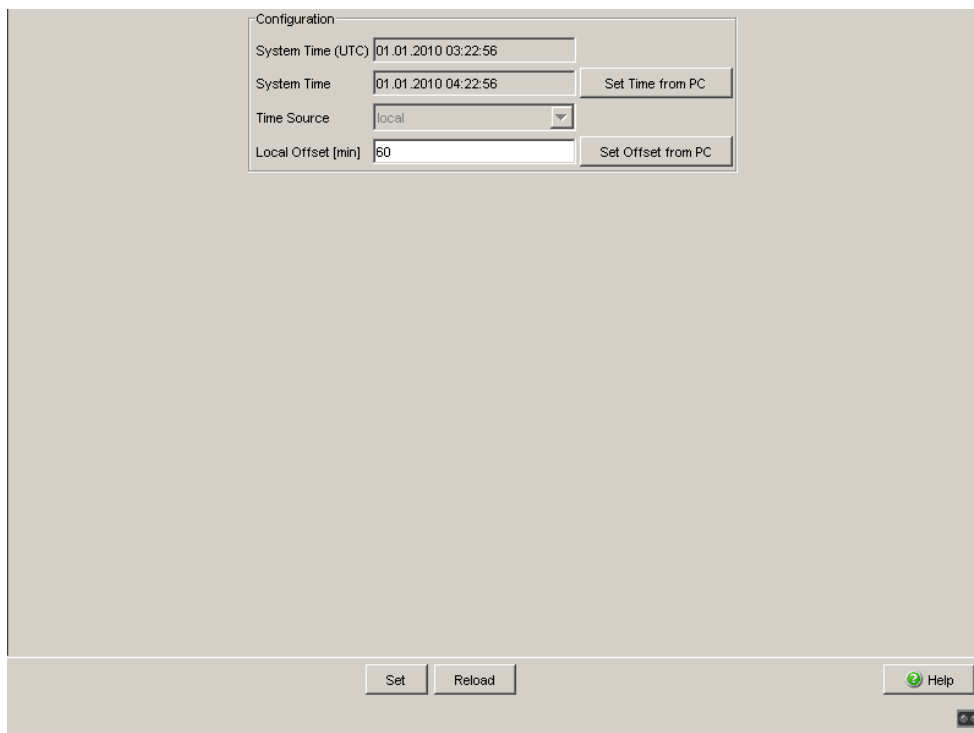


Figure 22: Time:Basic Settings dialog

- ▶ The “System time (UTC)” displays the time with reference to the coordinated world time scale UTC (Universal Time Coordinated). The display is the same worldwide. Local time differences are not taken into account.  
Possible sources of the system time (UTC) are: `local`, `sntp` and `ntp`, see “Time source”.
- ▶ The device calculates the “system time” from the “system time (UTC)” and the “local offset” (the local time difference from UTC).  
“System time” = “System time (UTC)” + “Local offset”.
- ▶ “Time Source” displays the source of the system time (UTC). The device automatically selects the available source based on accuracy.  
Possible sources are: `local`, `sntp` and `ntp`.
  - The source is initially `local`. This is the system clock of the device.
  - If you have activated the SNTP client and if the device receives a valid SNTP packet, the device sets its time source to `sntp`.
  - If you have activated the NTP client and if the client has synchronized itself, the device sets its time source to `ntp`.

- With the “Set Time from PC” button, the device takes the local time from the work station on which you are running the graphical user interface. It calculates the system time (UTC) using the local time difference.  
“System time (UTC)” = “System time” - “Local offset”
- ▶ The “Local Offset” is for displaying/entering the time difference between the local time and the “System time (UTC)”.
- With the “Set offset from PC” button, the device determines the time zone on your PC, uses it to calculate the local time difference, and takes this over.

**Note:** When setting the time in zones with summer and winter times, make an adjustment for the local offset, if applicable.

The SNTP client can also get the SNTP server IP address and the local offset from a DHCP server.

The NTP client gets its NTP server IP address exclusively from the configuration that you set.

## 3.2 SNTP configuration

The Simple Network Time Protocol (SNTP) enables you to synchronize the system time in your network.

The device supports the SNTP client and the SNTP server function.

The SNTP server makes the UTC (Universal Time Coordinated) available. UTC is the time relating to the coordinated world time measurement. The time displayed is the same worldwide. Local time differences are not taken into account.

SNTP uses the same packet format as NTP. In this way, an SNTP client can receive the time from an SNTP server as well as from an NTP server.

**Note:** For accurate system time distribution with cascaded SNTP servers and clients, use only network components (routers, switches, hubs) in the signal path between the SNTP server and the SNTP client which forward SNTP packets with a minimized delay.

► Operation

- In this frame you switch the SNTP function on/off globally.

**Note:** If you switch SNTP on when NTP is already active on the device, the device reports a detected error.

To switch SNTP on, first deactivate NTP.

On delivery, NTP is switched off.

► SNTP Status

- The “Status message” displays statuses of the SNTP client as one or more test messages, e.g. `Server 2 not responding`.

► Configuration SNTP Client

- In “External server address” you enter the IP address of the SNTP server from which the device periodically requests the system time.
- In “Redundant server address” you enter the IP address of an additional SNTP server. The device periodically requests from this server the system time if it does not receive a response from the server to a request from the “External server address” within 1 second.

**Note:** If you are receiving the system time from an external/redundant server address, you do not accept any SNTP Broadcast packets (see below). You thus help ensure that the device uses the time of the server entered.

- In “Server request interval” you specify the interval at which the device requests SNTP packets (valid entries: 1 s to 3,600 s, on delivery: 30 s).
- With “Accept SNTP Broadcasts” the device takes the system time from SNTP Broadcast/Multicast packets that it receives.

► Configuration SNTP Server

- In “Anycast destination address” you enter the IP address to which the SNTP server of the device sends its SNTP packets (see table 36).
- In “Anycast send interval” you specify the interval at which the device sends SNTP packets (valid entries: 1 s to 3,600 s, on delivery: 120 s).
- With “Disable Server at local time source” the device disables the SNTP server function if the source of the time is `local` (see `Time:Basic Settings` dialog).

IP destination address	Send SNTP packet to
0.0.0.0	Nobody
Unicast address (0.0.0.1 - 223.255.255.254)	Unicast address
Multicast address (224.0.0.0 - 239.255.255.254), especially 224.0.1.1 (NTP address)	Multicast address
255.255.255.255	Broadcast address

*Table 36: Destination address classes for SNTP and NTP packets*

The screenshot shows the SNTP configuration dialog box. It is organized into several sections:

- Operation:** Contains two radio buttons, 'On' and 'Off', with 'Off' selected.
- Configuration SNTP Client:** Contains four fields:
  - External Server Address: 0.0.0.0
  - Redundant Server Address: 0.0.0.0
  - Server Request Interval [s]: 30
  - Disable Server at local Time Source:
- SNTP Status:** Contains a single text input field.
- Configuration SNTP Server:** Contains three fields:
  - Anycast Destination Address: 0.0.0.0 (dropdown menu)
  - Anycast Send Interval [s]: 120
  - Accept SNTP Broadcasts:

At the bottom of the dialog, there are four buttons: 'Set', 'Reload', 'Ping', and 'Help'.

*Figure 23: SNTP Dialog*

---

## 3.3 NTP Configuration

The Network Time Protocol (NTP) enables you to synchronize the system time in your network. The device supports the NTP client and the NTP server function.

With NTP, the device can determine the time more accurately than with SNTP. Thus, as an NTP server it can also provide a more accurate time.

The NTP and SNTP packet formats are identical.

In contrast to the SNTP client, the NTP client uses multiple NTP servers and a more complex algorithm for the synchronization. It can thus determine the time more accurately. Therefore, the synchronization of the NTP client can take longer than an SNTP client.

Only use NTP if you require this increased accuracy.

The NTP server makes the UTC (Universal Time Coordinated) available. UTC is the time relating to the coordinated world time measurement. The time displayed is the same worldwide. Local time differences are not taken into account.

The NTP client obtains the UTC from one or more external NTP servers.

**Note:** To obtain as accurate a system time distribution as possible, use multiple NTP servers for an NTP client.

### ► Operation

- In this frame you select the NTP operation mode globally. Possible values:

- `off`:

The NTP client and the NTP server are switched off (default setting)

- `symmetric-active`:

The NTP client and the NTP server are active, and the association mode is “Symmetric active” (mode 1)

- `symmetric-passive`:

The NTP client and the NTP server are active, and the association mode is “Symmetric passive” (mode 2)

- `client`:



Only the NTP client is active, and the association mode is “Client” (mode 3)

- `server:`

Only the NTP server is active, and the association mode is “Server” (mode 4).

- `client-server:`

The NTP client and the NTP server are active. The association mode of the client is “Client” (mode 3, sends request packets with mode 4). The association mode of the server is “Server” (mode 4, sends reply packets with mode 3).

- `broadcast-client:`

Only the NTP client is active and accepting NTP Broadcast packets (mode 5)

**Note:** If you switch NTP on (set any value other than `off`) when SNTP is already active on the device, the device reports a detected error. To switch NTP on, first deactivate SNTP. On delivery, SNTP is switched off.

► NTP status

- The “Status message” displays statuses of the NTP client as one or more text messages, e.g. `Server 1 not responding`.

► Configuration NTP Client

- In “External server address” you enter the IP address of the first NTP server from which the device obtains the system time.
- In “Redundant server address” you enter the IP address of an additional NTP server from which the device obtains the system time.
- In “Server request interval” you specify the interval at which the device requests NTP packets (valid entries: 1 s to 3,600 s, on delivery: 64 s).

► Configuration NTP Server

- In “Anycast destination address” you enter the IP address to which the NTP server of the device sends its NTP packets ([see table 36](#)).
- In “Anycast send interval” you specify the interval at which the device sends NTP packets (valid entries: 1 s to 3,600 s, on delivery: 128 s).

The screenshot shows a configuration window for NTP. It is organized into four main panels:

- Operation:** A dropdown menu for 'Operation Mode' is currently set to 'off'.
- NTP Status:** A text field for displaying the current status.
- Configuration NTP Client:** Contains three text input fields: 'External Server Address' (0.0.0.0), 'Redundant Server Address' (0.0.0.0), and 'Server Request Interval [s]' (30).
- Configuration NTP Server:** Contains two text input fields: 'Anycast Destination Address' (0.0.0.0) and 'Anycast Send Interval [s]' (120).

At the bottom of the window, there are four buttons: 'Set', 'Reload', 'Ping', and 'Help'.

Figure 24: NTP dialog

**Note:** If you change a parameter for NTP the NTP service will be restarted.

## 4 Network Security

To help you establish network security, the Firewall provides you with:

- ▶ Packet filters with address templates and Firewall learn mode
- ▶ NAT - Network Address Translation
- ▶ DoS - Helping protect against Denial of Service (DoS)
- ▶ User Firewall

The Firewall observes and monitors the data traffic. The Firewall takes the results of the observation and the monitoring and combines them with the rules for the network security to create so-called status tables. Based on these status tables, the Firewall decides whether to accept, drop or reject the data.

You can use address templates to create and modify IP packet filter entries quickly and more easily.

As a special feature, the Firewall has an innovative set-up assistant, the Firewall learn mode. It helps you analyze the traffic and create suitable rules for permitting the traffic you desire.

---

## 4.1 Packet Filter

In the Packet Filter submenu, you can create rules on the basis of which the Firewall handles received data packets. The Firewall can accept data packets, i.e. forward them, or it can drop or reject them.

Here you are able to

- ▶ create rules yourself
- ▶ define address templates and use them in your rules
- ▶ analyze the traffic through the Firewall using an innovative assistant for the Firewall learn mode (FLM), and accept the proposed rules and modify them if necessary.

The Firewall allows you to create rules for the following groups:

- ▶ Incoming IP packets (received at the external port)
- ▶ Outgoing IP packets (received at the internal port)
- ▶ Incoming MAC packets (received at the external port)
- ▶ Outgoing MAC packets (received at the internal port)
- ▶ Incoming PPP packets (received at the serial port)

The Firewall initially checks every data packet based on first rule in the table. If the conditions of this rule apply, the Firewall performs the corresponding action (accept, reject, drop). If the first rule does not apply, the Firewall checks the data packets on the basis of the second rule in the table, etc., down to the last rule in the table.

The last default rule of the device is “drop everything”. This rule is not visible in the tables and cannot be deleted.

With IP and PPP packets you have the option of creating a log entry if none of the rules applies.

You can create, delete and edit rules, and you can change their order. Select one or more sequential rows to be moved and move your selection with the “↑” and “↓” buttons. You can also duplicate (clone) a rule and then edit it.

Settings in the state on delivery:

- ▶ In the state on delivery, no address templates are defined.
- ▶ The assistant for the Firewall learn mode is switched off.
- ▶ The Firewall is asymmetrical. This means:
  - It transmits the data packets from the internal network to the external network.  
The table also contains a visible “accept all” rule for the internal interface.
  - The Firewall transmits data packets from the external network to the internal network only if a subscriber to the internal network requested these data packets.  
This behavior corresponds to the Stateful Packet Inspection (SPI), a dynamic packet filter technique that allocates every data packet to a certain active communication connection.  
The Firewall drops the other data packets.  
The table for the external interface also contains a “drop everything” rule.
- ▶ For IP or PPP packets, the Firewall does not create a log entry if no rule applies.

**Note:** Firewall rules can also apply to the CPU of the device. In this case, you can enter the IP target address of the device with the symbolic entry `me`. For the CPU of the device to be reachable in the state on delivery, it uses default rules that accept SSH, SNMP and HTTPS traffic. These rules are invisible in the tables and cannot be deleted.

## 4.1.1 Address Templates

This dialog allows you to create address templates, which you can then use to create and modify IP packet filter entries quickly and more easily. An address template consists of 1 or more address entries with the same name.

The device automatically creates the suitable packet filter entries from a packet filter entry with variables. If you change the address template for a variable, the device automatically modifies the packet filter entries created.

Parameter	Meaning	Value range	Default setting
Template Name	Name of an entry for an address template.  <b>Note:</b> The active entries with the same name make up an address template.	1-19 ASCII characters; recommendation: in the range 0x21 ("!") to 0x7e ("~").	
Index	Sequential line index.		
IP-Address (CIDR)	IP address range of the entry in CIDR notation. The device automatically adds the netmask /32 to an entry for a host address. To edit an existing address entry, click on the table row.	Valid IPv4 address range	
Active	Activates or deactivates a single entry of an address template.	On, Off	on
"Create" button	Open a subdialog with the input fields "List name" and "IP address (CIDR)" to create a new entry for an address template.  <b>Note:</b> If you want to add an address entry to an existing address template, select the existing name for the "List name" field in the subdialog.	-	-
"Remove" button	Deletes the selected entries for one or more address templates.	-	-

Table 37: Description of the Address Templates dialog

**Note:** After adding entries, re-sort the list on the basis of the “Template Name” column. You thus help ensure that the graphical user interface displays the entries that belong to one and the same address template underneath each other.

**Note:** The maximum number of active entries in the address templates is restricted by the maximum number of IP packet filter entries ([see on page 105 “Incoming and outgoing IP packets”](#)).

### 4.1.2 Firewall Learning Mode (FLM)

The Firewall learn mode is an innovative set-up assistant. It helps you analyze the traffic and create suitable rules for permitting the traffic you desire.

The assistant for the Firewall learn mode allows you to

- ▶ automatically determine in an easy way the traffic which your existing rules do not permit yet (actual learn mode)
- ▶ analyze this traffic based on various criteria
- ▶ automatically create new rule defaults from the desired traffic
- ▶ modify these rules if required and automatically visualize their traffic coverage, and
- ▶ test the new rules for the desired coverage.

**Note:** However, the assistant for the Firewall learn mode still requires specialized knowledge of data networks, as the user is responsible for the rules created.

---

The FLM only applies to packets that want to pass through the device (the Firewall). It does not apply to packets that are sent to the device itself, and those that the device itself creates.

Perform the following steps to create the rules supported by FLM:

- Implement the Firewall at the desired position in your network.
- Activate the FLM assistant on the desired interfaces of the Firewall (typically on both interfaces).
- Start the actual learn mode.
- Operate the devices in your network for a while, so that the Firewall learns the desired traffic.
- Start the learn mode.
- Display the learned traffic on the selected interface:
  - ▶ If the Firewall has learned too little traffic, continue with the learn mode in order to learn more traffic.
  - ▶ When the Firewall has learned enough traffic, inspect the captured data.
- Select desired entries from the captured data and add them to the temporary rule set.
- If necessary, modify the added rules.
- Ignore undesired entries in the captured data, i.e. do not create any rules for them. Thus, the Firewall blocks this traffic after the learn and test mode has ended.
- Release the desired rules for testing.
- Start the test mode:
  - ▶ If the devices in your network are working as desired, write the temporary rules to your rule base.
  - ▶ If the devices in your network are not working as desired, modify the rules released for testing. Alternatively, restart the learn mode in order to learn more traffic.
- End the assistant for the Firewall learn mode.
- Save the rules in the configuration.



**Note:** While learning, the Firewall observes and learns only the traffic that it has not permitted up to now based on the existing rules. The Firewall deactivates the packet filter entry “drop everything” on the external interface. As a result of this, it is possible that the Firewall also accepts undesired traffic when in the learn mode.

Therefore, during the learning period, only create desired traffic via the Firewall. If you still find undesired entries when evaluating the learned traffic, do not create any rules for this, and if necessary delete any rules already created.

After the learn and test phase is complete, if you accept the temporary rules derived from the learned data, the Firewall generally does not behave asymmetrically any more.

**Note:**

- ▶ Switching the device between the router and transparent modes during the learn phase can have unpredictable results.
- ▶ Manually adding, deleting or changing packet filter entries during the learn phase can reduce the efficiency of the rules that you derive from the learned data.

Parameter	Meaning	Value range	Default setting
<b>Frame „Operation“</b>	Switches the assistant for the Firewall learn mode on or off.	On, Off	Off
<b>Frame „Configuration“</b>			
Learning on interfaces	Select the interfaces of the Firewall on which you want the Firewall to learn traffic.	Both, Internal, External	Both
Adjustment of the “accept-any” rule	<p>► <b>Automatic:</b> The Firewall automatically deactivates the “accept-any” rules on the interfaces before the learn and test phases. If such a rule is active during the learning or the testing, it applies to the traffic for the relevant interface. This situation disables new traffic from being learned. The automatic deactivation of these rules during the learning and testing enables new traffic to be learned easily. During the traffic analysis and the rule creation, the Firewall activates these rules again or inserts such a rule. This helps make your productive environment secure. If you take over the newly created, temporary rules, the device deactivates the “accept-any” rules on the relevant interfaces.</p> <p>► <b>Manual:</b> Manually deactivate the “accept-any” rules on the relevant interfaces before the learn and test phases. During the traffic analysis and the rule creation, activate these rules again. If you take over the newly created, temporary rules, deactivate the “accept-any” rules on the relevant interfaces.</p>	Automatic, Manual	Automatic

*Table 38: Firewall Learning Mode, “FLM Control” tab page, Operation and Configuration frames*

Parameter	Meaning	Value range	Default setting
<b>Buttons</b>			
“Start learning mode”/ “Stop learning mode”/ “Continue learning mode” buttons	▶ Start learning mode: Starts the learning of traffic data when there is no data there yet.	Start learning mode, Stop learning mode,	Start learning mode
	▶ Stop learning mode: Interrupts the learning of traffic data.	learning mode,	(deactivated)
	▶ Continue learning mode: Continue the learning of traffic data when data is already there.	Continue learning mode	
“Start testing mode”/ “Stop testing mode” buttons	▶ Start testing mode: Temporarily enters the rules released for testing for the relevant interface in the set of rules.	Start testing mode, Stop testing mode	Start testing mode
	▶ Stop testing mode: Ends the test mode.	mode	(deactivated)
“Delete data” button	Interrupts the learning and deletes the learned traffic data. You have the option to restart the learning.		

Table 39: Firewall Learning Mode, “FLM control” tab page, buttons

**Note:** This dialog only provides you with the tab pages that you can use in the current status of the learn or test mode. If it is not possible to operate them, the “Internal interface” or “External interface” dialog tabs display your text as deactivated (grayed out).

The buttons in the dialog can display different names. They only provides the actions that you can perform in the current status of the FLM assistant. If no action is possible, the text on the button is displayed as deactivated (grayed out).

Parameter	Meaning	Value range	Default setting
<b>Frame „Information“</b>			
State	<ul style="list-style-type: none"> <li>▶ Off: The learning is not active.</li> <li>▶ No data present. Select interface and start learning: The learning is inactive and the Firewall has not learned any data yet.</li> <li>▶ Stopped. Check interface data and release for test: You have interrupted the learning. You now have the option to check the learned data in the “Internal interface” or “External interface” dialog, derive rules from it, modify these rules, and release them for testing.</li> <li>▶ Learning: You have started the learning. The device is collecting traffic data.</li> <li>▶ Testing: You have started the test mode.</li> <li>▶ Currently busy. Please wait: The device is currently busy processing data, or the graphical user interface is exchanging data with the device.</li> </ul>		
Additional Information	<ul style="list-style-type: none"> <li>▶ (No display): The learning is not active.</li> <li>▶ Normal operation: The learning is active. The device still has enough memory for traffic data.</li> <li>▶ Stopped! No free memory: The available memory for learning connections is exhausted. The Firewall has stopped recording traffic data.</li> <li>▶ Some connections have not been recorded: During the internal processing of the connections to be learned, the Firewall has detected too many hash collisions. This means that the Firewall has not recorded a number of connections. It is possible that the rules thus determined are incomplete and do not permit the desired traffic. Test the rules created from this learning procedure thoroughly.</li> </ul>		

Table 40: Firewall Learning Mode, “FLM control” tab page, “Information” frame

Parameter	Meaning	Value range	Default setting
IP Entries	<p>Number of Layer 3 connections learned up to now that have been received at the selected interfaces.</p> <p>For TCP packets, the Firewall only counts the setting up of the connection. For other Layer 4 protocols, it only counts the first packet of a connection.</p> <p>A connection is a unique combination of source and destination addresses, source and destination ports, and the Layer 4 protocol number of the IP header.</p> <p>To update the display while the learning is running, press the "Reload" button.</p>		
Free memory for learning Data [%]	<p>Display the memory remaining for the connections to be learned.</p> <p>The Firewall can learn up to 65,536 different connections.</p> <p>In ICMP packets, the Firewall ignores the codes. The firewall allocates ICMP packets for which only the code differs to a single connection.</p> <p>To update the display while the learning is running, press the "Reload" button.</p>		

*Table 40: Firewall Learning Mode, "FLM control" tab page, "Information" frame*

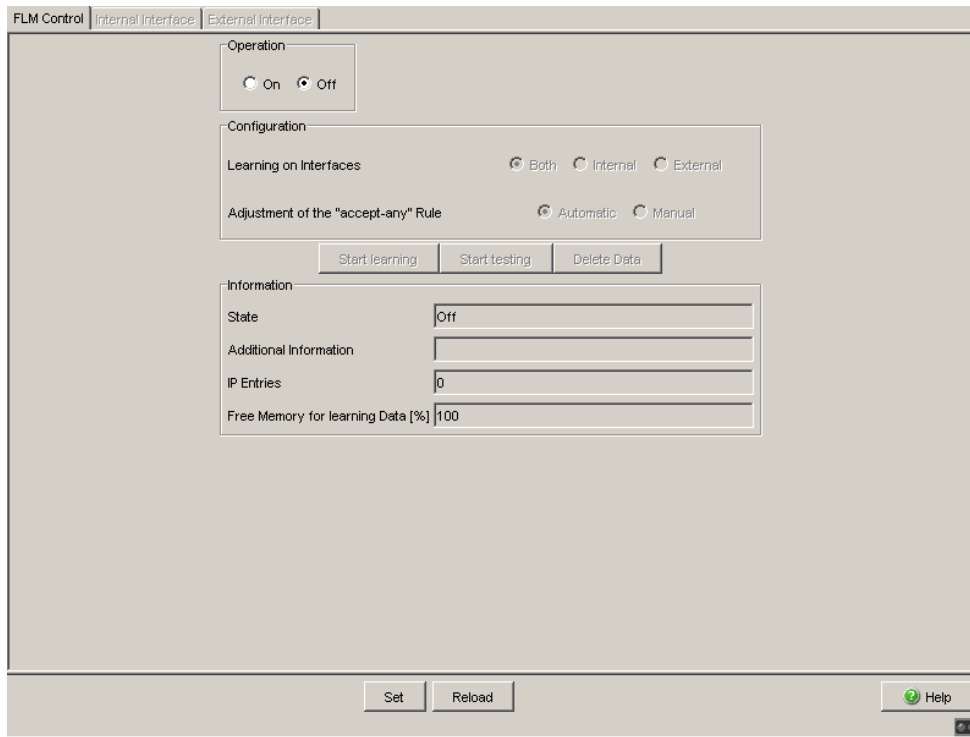


Figure 25: Firewall Learning Mode dialog, "FLM control" tab page

Parameter	Meaning	Value range	Default setting
<b>Frame „Captured Data“</b>			
Index	Sequential line index.		
Source IP	Learned IP source address	IPv4 address	
Source port	Learned UDP or TCP source port	0-65535	
Destination IP	Learned IP destination address	IPv4 address	
Destination Port	Learned UDP or TCP destination port.	0-65535	
Protocol	Learned Layer 4 protocol number from the IP header. The device displays known protocol numbers with their name.	0-255, icmp, tcp, udp	
“Add to Rule Set” button	<p>Adds the selected rows of the learned data to the temporary set of rules. If you have selected multiple rows, the device takes over the first row as a rule.</p> <p>Afterwards you have the option to edit the rule.</p> <p><b>Note:</b> The learned entries that are covered by the entire temporary set of rules are displayed in bright green by the device. The entries that are covered by the currently selected rules are displayed in dark green by the device.</p> <p>When you change a rule, e.g. shorten a netmask, the device automatically adjusts the dark green marking. This enables you to recognize quickly and easily how a changed rule covers the learned entries.</p> <p><b>Note:</b> When you create a rule from an ICMP entry, the device allocates the destination port <code>any</code> to the rule.</p>		
Hide Connections matching the learned Rules	<p>When you activate this function, the device hides the learned entries that are covered by one of the rules instead of displaying them in green.</p> <p>You activate this function if you only want to display the entries not yet covered by rules.</p>		

*Table 41: Firewall Learning Mode, “Internal interface” and “External interface” tab pages, “Recorded data” frame*

Parameter	Meaning	Value range	Default setting
Connections covered by Rule Set	Displays the number of learned connections that are covered by the entire temporary set of rules. In addition, after the forward slash, the device displays the total number of the learned connections.	Format: covered - / total	
Connections covered by Selected	Displays the number of learned connections that are covered by the entire temporary set of rules In addition, after the forward slash, the device displays the total number of the learned connections.	Format: covered - / total	

*Table 41: Firewall Learning Mode, “Internal interface” and “External interface” tab pages, “Recorded data” frame*



Protocoll	Port number
FTP (data, control)	20, 21
SSH	22
Telnet	23
SMTP	25
DHCP/BOOTP (Server, Client)	67, 68
TFTP	69
HTTP (www)	80
POP3	110
NTP	123
NetBIOS (Name, Datagram, Session Service)	137, 138, 139
SNMP, SNMP Trap	161, 162
HTTPS	443
EtherNet/IP I/O	2222
EtherNet/IP Messaging	44818
Foundation Fieldbus Annunciation	1089
Foundation Fieldbus Message Specification	1090
Foundation Fieldbus System Management	1091
Foundation Fieldbus LAN Redundancy Port	3622
LonWorks	2540
LonWorks2	2541
Modbus/TCP	502
Profinet RT Unicast	34962
Profinet RT Multicast	34963
Profinet Context Manager	34964
IEC 60870-5-104	2404
DNP	20000
Ethercat	34980

*Table 42: Examples for registered port numbers*

**Note:** At <http://www.iana.org/assignments/port-numbers> you can find a list of the registered port numbers.

Parameter	Meaning	Value range	Default setting
<b>Frame „Rules“</b>	<b>Note:</b> Most of the columns in this table are identical to those in the <code>Incoming IP packets</code> and <code>Outgoing IP packets</code> dialogs.		
Index	Sequential line index.		
Description	Description of this entry. If the Firewall created the entry from the learned data of the Firewall Learning Mode (FLM), the device enters the text “learned by FLM”.	0-128 ASCII characters	
Active	Activate/deactivate the rule.	On	On
	<b>Note:</b> If you created the rule in the Firewall learn mode, the rule is active. This setting cannot be changed within the FLM dialog. You can modify the rule later in the <code>Incoming IP Packets</code> or <code>Outgoing IP packets</code> dialog.		
Source IP (CIDR)	IP Address with Netmask (CIDR) of the actual source of the data packet.  <b>Note:</b> If you want to use an address template, enter the name of the address template. Put a dollar sign (“\$”) in front of the name to indicate that it is a variable name.	IP Address with any Netmask, any = all, me = own IP address, \$<address template> = address template	
	<b>Note:</b> If you are using address templates in the rules that you have derived from the learned data, these rules will then function correctly. However, the device ignores these rules when marking and hiding the learned data.		

*Table 43: Firewall Learning Mode, “Internal interface” and “External interface” tab pages, “Rules” frame*

Parameter	Meaning	Value range	Default setting
Source Port	<p>Logical source port of the data packet You can also use operators (op) to select multiple ports:</p> <p>= equal to != not equal to &lt; less than &lt;= less than or equal to &gt; greater than &gt;= greater than or equal to &gt;&lt; within &lt;&gt; outside of</p> <p>Use decimal numbers for the port ID. You can also enter the following known ports as ASCII characters:</p> <pre> 7    tcp/udp: echo 9    tcp/udp: discard 20   tcp    :ftp-data 21   tcp    :ftp 22   tcp/udp: ssh 23   tcp    :telnet 53   tcp/udp: domain 67   tcp/udp: bootps 68   tcp/udp: bootpc 69   udp    : tftp 80   tcp/udp: www, http 88   tcp/udp: kerberos 115  tcp    : sftp 123  tcp    : ntp 161  udp    : snmp 162  udp    : snmp-trap 179  tcp/udp: bgp 389  tcp/udp: ldap 443  tcp/udp: https </pre>	<p>any = all</p> <p>op port or port 1 op port 2</p>	any
Source Port (continued)	<p>To selectively check incoming IP packets for specific ICMP traffic criteria, use:</p> <ul style="list-style-type: none"> <li>- the entry <code>icmp</code> for the parameter "Protocol"</li> <li>- for the parameter "Source Port" the following definition for the ICMP type and code:</li> </ul> <pre> type &lt;t&gt; [code &lt;c&gt;] &lt;...&gt; Enter a parameter [...] Optional entry t    Decimal value, 1 to 3 digits c    Decimal value, 1 to 3 digits Examples: type 0 code 0          type 10 </pre> <p>For the possible values for the ICMP type and code, see <a href="#">table 46</a>.</p>	<p>type &lt;t&gt; [code &lt;c&gt;]</p>	any

**Table 43:** Firewall Learning Mode, "Internal interface" and "External interface" tab pages, "Rules" frame

Parameter	Meaning	Value range	Default setting
Destination IP (CIDR)	<p>IP Address with Netmask (CIDR) of the actual destination of the data packet.</p> <p><b>Note:</b> If you want to use an address template, enter the name of the address template. Put a dollar sign (“\$”) in front of the name to indicate that it is a variable name.</p> <p><b>Note:</b> If you are using address templates in the rules that you have derived from the learned data, these rules will then function correctly. However, the device ignores these rules when marking and hiding the learned data.</p>	<p>IP Address with Netmask, any = all, me = own IP address, \$&lt;address template&gt; = address template</p>	
Destination Port	<p>Logical destination port of the data packet</p> <p>To select multiple ports, you can use the same operators as for the source port: Use decimal numbers for the port ID. You can also enter the same known ports, as with the source port, as ASCII characters.</p>	<p>any = all op port port 1 op port 2</p>	any

*Table 43: Firewall Learning Mode, “Internal interface” and “External interface” tab pages, “Rules” frame*

Parameter	Meaning	Value range	Default setting
Protocol	<p>You can enter the following protocols as ASCII characters:</p> <ul style="list-style-type: none"> <li>▶ any Any Layer 4 protocol</li> <li>▶ tcp Transmission Control Protocol (RFC 793)</li> <li>▶ udp User Datagram Protocol (RFC 768)</li> <li>▶ icmp Internet Control Message Protocol (RFC 792)</li> <li>▶ igmp Internet Group Management Protocol (RFCs 1112 (v1), 2236 (v2), 3376 (v3))</li> <li>▶ ipip IP in IP Tunneling (RFC 1853)</li> <li>▶ esp IPsec Encapsulated Security Payload (RFC 2406)</li> <li>▶ ah IPsec Authentication Header (RFC 2402)</li> <li>▶ ipv6-icmp Internet Control Message Protocol for IPv6 (RFC 4443)</li> <li>▶ &lt;0 - 255&gt; Number of the Layer 4 protocol in the IP header</li> </ul> <p><b>Note:</b> With the udp and tcp protocols, you have the option to enter the protocol ports in the “Source port” and “Destination Port” columns. For other protocols you enter any for “Source port” and “Destination Port”.</p> <p><b>Note:</b> The stateful firewall supports the protocols tcp, udp and icmp.</p>	<p>any = all, tcp, udp, icmp, (additionally: igmp, ipip, esp, ah, ipv6-icmp, &lt;0 - 255&gt;)</p> <p><b>Note:</b> You can select the protocols any, tcp, udp and icmp from the list. Manually enter the protocols igmp, ipip, esp, ah, ipv6-icmp and &lt;0 - 255&gt;.</p>	any
Action	<p>Action that the Firewall performs if the rule applies.</p> <p><b>Note:</b> If you created the rule in the Firewall learn mode, the action is accept. This setting cannot be changed within the FLM dialog. You can modify the rule later in the Incoming IP Packets or Outgoing IP packets dialog.</p>	accept	accept

*Table 43: Firewall Learning Mode, “Internal interface” and “External interface” tab pages, “Rules” frame*

Parameter	Meaning	Value range	Default setting
Log	Entry in the event list if the Firewall uses the rule. If applicable, the device also sends a trap.  <b>Note:</b> The <code>logAndTrap</code> setting can generate large quantities of trap data traffic. This is especially the case when sending the trap triggers a match in the Firewall rule again (e.g. if the trap host cannot be reached and a router responds with an ICMP message).	enable, disable, logAndTrap	disable
Error	Shows the last message for an unsuccessful attempt to activate the table entry (usually a detected syntax error).		

Table 43: Firewall Learning Mode, “Internal interface” and “External interface” tab pages, “Rules” frame

Parameter	Meaning	Value range	Default setting
“Release for Test” / “Unrelease” buttons	<ul style="list-style-type: none"> <li>▶ <b>Release for Test:</b> Adds the rules of the temporary set of rules to the provisional productive rule base for testing. In the process, the device helps prevent the released rules from being changed in the productive rule base.</li> <li>▶ <b>Unrelease:</b> Removes the rules of the temporary set of rules from the productive rule base again. The device unblocks the rules for editing in the Firewall learn mode.</li> </ul>		
“Remove Rule” button	Deletes the selected rules from the temporary set of rules.		

Table 44: Firewall learn mode, “Internal interface” and “External interface” tab pages, buttons

**Note:** The buttons in the dialog can display different names. A button enables the action that is possible in the current status.

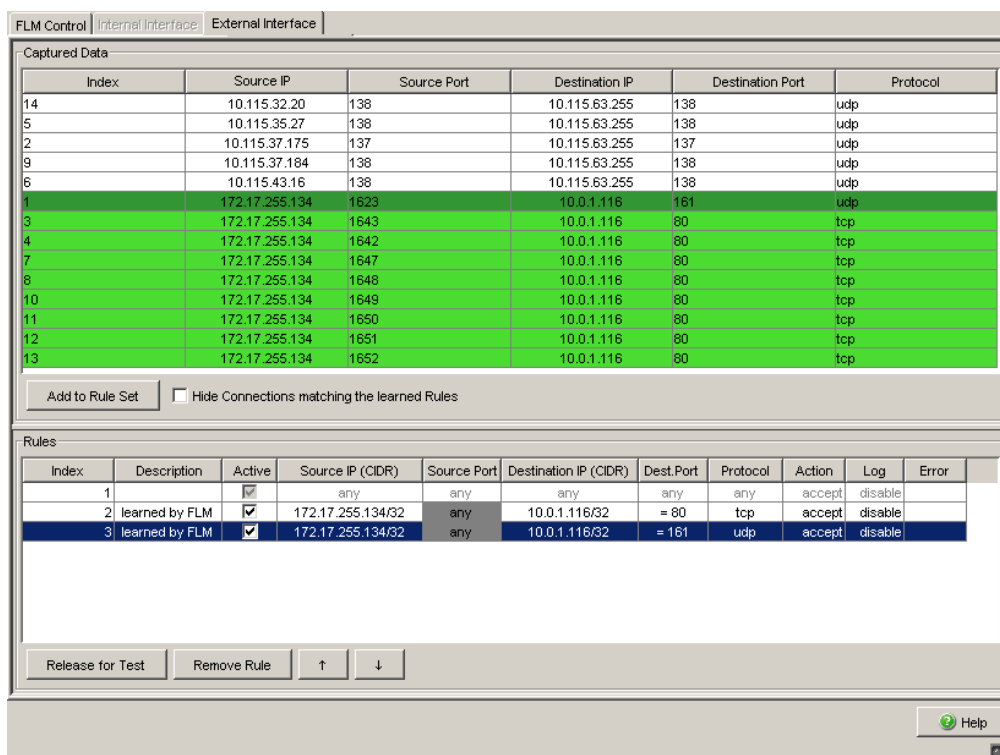


Figure 26: Firewall Learn Mode dialog, “External interface” tab page

### Details of the Example Screenshot

fig. 26 displays the “External interface” dialog tab page after the following steps: The user has:

- started the learning mode,
- accessed the graphical user interface of a switch in the internal network from a work station (has loaded the graphical user interface and opened dialogs),
- interrupted the learning mode again,
- selected the “External Interface” dialog tab page,
- sorted the data entered in ascending order based on the IP source address,
- derived 2 rules from the desired traffic and modified these.

fig. 26 shows the following details:

- ▶ The white rows of the recorded data show that the Firewall at the external interface has learned NetBIOS traffic from different hosts at the network Broadcast address 10.115.63.255. This traffic is undesired, so the user has not created any rules for this.
- ▶ The green rows show that the Firewall has also learned SNMP and HTTP traffic from work station 172.17.255.134 to switch 10.0.1.116. This traffic is desired, so the user has created rules for this.
- ▶ From the data item with the index 3, the user has added a rule to the temporary set of rules (the rule with the index 2) in order to permit the HTTP traffic between the work station and the switch.
  - The Firewall has initially taken TCP source port 1643 into the rule.
  - The user has changed the source port of the rule to `any` (displayed in dark gray) so that the randomly selected source ports are permitted for HTTP traffic.
- ▶ From the data item with the index 1, the user has added a rule to the temporary set of rules (the rule with the index 3) in order to permit the SNMP traffic between the work station and the switch.
  - The Firewall has initially taken UDP source port 1623 into the rule.
  - The user has changed the source port of the rule to `any` so that the randomly selected source ports are permitted for SNMP traffic.
- ▶ The green rows in the recorded data show that now the outgoing HTTP and SNMP traffic from the work station to the switch would be permitted by the rules.
- ▶ The dark green row displays the traffic permitted by rule 3. This rule is currently selected.
- ▶ The light green rows of the recorded data display the traffic permitted by the other rules of the temporary set of rules (here only rule 2). These rules are de-selected.

The user can now:

- select rules 2 and 3 and use the “Release for Test” button to add them to the set of rules to be tested,
- click the “Start Testing Mode” button in the “FLM control” dialog tab page,
- create additional network traffic.

The Firewall will now:

- ▶ permit the SNMP and HTTP traffic from the work station to the switch. The Firewall now ignores this traffic when learning.
- ▶ only learn the traffic not yet permitted. It thus helps the user to detect and analyze any additional desired traffic. It thus assists the user in improving the rules.



### 4.1.3 Incoming and outgoing IP packets

The Firewall allows you to check the incoming IP packets at the external and internal ports based on:

- ▶ the logical port
- ▶ the source IP address
- ▶ the logical destination port
- ▶ the destination IP address
- ▶ the transmission protocol

For every packet that does not match any of the rules in the table, but only the invisible default rule “drop everything”, you have the option of creating a log entry. To do this, activate the setting “Log if non-matching”.

You can create, delete and edit rules, and you can change their order. Select one or more sequential rows to be moved and move your selection with the “↑” and “↓” buttons. You can also duplicate (clone) a rule and then edit it.

Parameter	Meaning	Value range	Default setting
Index	Sequential line index.		
Description	Description of this entry. If the Firewall created the entry from the learned data of the Firewall Learning Mode (FLM), the device enters the text "learned by FLM".	0-128 ASCII characters	
Active	Activate/deactivate the rule	on/off	off
Source IP (CIDR)	IP Address with Netmask (CIDR) of the actual source of the data packet.  <b>Note:</b> If you want to use an address template, enter the name of the address template. Put a dollar sign ("\$\$") in front of the name to indicate that it is a variable name.	IP Address with Netmask, any = all, me = own IP address, \$<address template> = address template	any

*Table 45: Incoming/outgoing IP packets at the external/internal port*

Parameter	Meaning	Value range	Default setting
Source Port	<p>Logical source port of the data packet You can also use operators (op) to select multiple ports:</p> <p>= equal to != not equal to &lt; less than &lt;= less than or equal to &gt; greater than &gt;= greater than or equal to &gt;&lt; within &lt;&gt; outside of</p> <p>Use decimal numbers for the port ID. You can also enter the following known ports as ASCII characters:</p> <pre> 7      tcp/udp: echo 9      tcp/udp: discard 20     tcp      :ftp-data 21     tcp      :ftp 22     tcp/udp: ssh 23     tcp      :telnet 53     tcp/udp: domain 67     tcp/udp: bootps 68     tcp/udp: bootpc 69     udp      : tftp 80     tcp/udp: www, http 88     tcp/udp: kerberos 115    tcp      : sftp 123    tcp      : ntp 161    udp      : snmp 162    udp      : snmp-trap 179    tcp/udp: bgp 389    tcp/udp: ldap 443    tcp/udp: https </pre>	<p>any = all</p> <p>op port or port 1 op port 2</p>	any
Source Port (continued)	<p>To selectively check incoming IP packets for specific ICMP traffic criteria, use:</p> <ul style="list-style-type: none"> <li>- the entry <code>icmp</code> for the parameter "Protocol"</li> <li>- for the parameter "Source Port" the following definition for the ICMP type and code:</li> </ul> <pre> type &lt;t&gt; [code &lt;c&gt;] &lt;...&gt; Enter a parameter [...] Optional entry t   Decimal value, 1 to 3 digits c   Decimal value, 1 to 3 digits Examples: type 0 code 0           type 10 </pre> <p>For the possible values for the ICMP type and code, see <a href="#">table 46</a>.</p>	<p>type &lt;t&gt; [code &lt;c&gt;]</p>	any

*Table 45: Incoming/outgoing IP packets at the external/internal port*

Parameter	Meaning	Value range	Default setting
Destination IP (CIDR)	IP Address with Netmask (CIDR) of the actual destination of the data packet.  <b>Note:</b> If you want to use an address template, enter the name of the address template. Put a dollar sign (“\$”) in front of the name to indicate that it is a variable name.	IP Address with Netmask, any = all, me = own IP address, \$<address template> = address template	
Destination Port	Logical destination port of the data packet To select multiple ports, you can use the same operators as for the source port: Use decimal numbers for the port ID. You can also enter the same known ports, as with the source port, as ASCII characters.	any = all op port port 1 op port 2	any

*Table 45: Incoming/outgoing IP packets at the external/internal port*

Parameter	Meaning	Value range	Default setting
Protocol	<p>You can enter the following protocols as ASCII characters:</p> <ul style="list-style-type: none"> <li>▶ any Any Layer 4 protocol</li> <li>▶ tcp Transmission Control Protocol (RFC 793)</li> <li>▶ udp User Datagram Protocol (RFC 768)</li> <li>▶ icmp Internet Control Message Protocol (RFC 792)</li> <li>▶ igmp Internet Group Management Protocol (RFCs 1112 (v1), 2236 (v2), 3376 (v3))</li> <li>▶ ipip IP in IP Tunneling (RFC 1853)</li> <li>▶ esp IPsec Encapsulated Security Payload (RFC 2406)</li> <li>▶ ah IPsec Authentication Header (RFC 2402)</li> <li>▶ ipv6-icmp Internet Control Message Protocol for IPv6 (RFC 4443)</li> <li>▶ &lt;0 - 255&gt; Number of the Layer 4 protocol in the IP header</li> </ul>	<p>any = all, tcp, udp, icmp, (additionally: igmp, ipip, esp, ah, ipv6-icmp, &lt;0 - 255&gt;)</p>	any
	<p><b>Note:</b> With the udp and tcp protocols, you have the option to enter the protocol ports in the “Source port” and “Destination Port” columns. For other protocols you enter any for “Source port” and “Destination Port”.</p>	<p><b>Note:</b> You can select the protocols any, tcp, udp and icmp from the list. Manually enter the protocols igmp, ipip, esp, ah, ipv6-icmp and &lt;0 - 255&gt;.</p>	
	<p><b>Note:</b> The stateful firewall supports the protocols tcp, udp and icmp.</p>		
Action	Action that the Firewall performs if the rule applies.	accept, drop, reject	drop (incoming) accept (outgoing)

Table 45: Incoming/outgoing IP packets at the external/internal port

---

Parameter	Meaning	Value range	Default setting
Log	Entry in the event list if the Firewall uses the rule. If applicable, the device also sends a trap.  <b>Note:</b> The <code>logAndTrap</code> setting can generate large quantities of trap data traffic. This is especially the case when sending the trap triggers a match in the Firewall rule again (e.g. if the trap host cannot be reached and a router responds with an ICMP message).	enable, disable, logAndTrap	disable
Error	Shows the last message for an unsuccessful attempt to activate the table entry (usually a detected syntax error).		

---

*Table 45: Incoming/outgoing IP packets at the external/internal port*

ICMP Name Type	ICMP Code	Name	Reference
0	0	Echo Reply	RFC792
		No Code	RFC792
3	0	Destination Unreachable	RFC792
		Net Unreachable	RFC792
		Host Unreachable	RFC792
		Protocol Unreachable	RFC792
		Port Unreachable	RFC792
		Fragmentation Needed and Don't Fragment was Set	RFC792
		Source Route Failed	RFC792
		Destination Network Unknown	RFC1122
		Destination Host Unknown	RFC1122
		Source Host Isolated	RFC1122
		Communication with Destination Network is Administratively Prohibited	RFC1122
5	0	Redirect	RFC792
		Redirect Datagram for the Network (or subnet)	RFC792
		Redirect Datagram for the Host	RFC792
		Redirect Datagram for the Type of Service and Network	RFC792
		Redirect Datagram for the Type of Service and Host	RFC792
8	0	Echo	RFC792
		No Code	RFC792
9	0	Router Advertisement	RFC1256
		Normal router advertisement	RFC3344
		Does not route common traffic	RFC3344
10	0	Router Solicitation	RFC1256
		No Code	RFC1256
11	0	Time Exceeded	RFC792
		Time to Live exceeded in Transit	RFC792
		Fragment Reassembly Time Exceeded	RFC792

*Table 46: ICMP types and codes*

**Note:** The Firewall supports up to 1024 IP rules.

In the dialog `Diagnostics:IP Firewall List`, you find the summary of the active rules.

## 4.1.4 Incoming and outgoing MAC packets

The Firewall allows you to check the incoming MAC packets at the external and internal ports based on:

- ▶ the source MAC address
- ▶ the destination MAC address
- ▶ the type field of the MAC data packet

### Transparent Mode

In the transparent mode, the following settings have priority above the entries in the MAC packet filters.

- ▶ “HiDiscovery Relay” in `Basic Settings:Network:Transparent Mode`.
- ▶ “RSTP” in the `Enhanced:Packet Forwarding` dialog.
- ▶ “GMRP” in the `Enhanced:Packet Forwarding` dialog.
- ▶ “DHCP” in the `Enhanced:Packet Forwarding` dialog.

This property saves you from having to create special MAC packet filter rules for these application cases.

### Router Mode

In router mode, the Firewall only transmits IP packets. Other packets are dropped, with the exception of Broadcast and Multicast packets. The rules for MAC packets still apply if an IP packet is addressed to an interface of the Firewall.

To improve the transmission performance of the Firewall, you can deactivate the rules for MAC packets in router mode.

You can create, delete and edit rules, and you can change their order. Select one or more sequential rows to be moved and move your selection with the “↑” and “↓” buttons. You can also duplicate (clone) a rule and then edit it.



Parameter	Meaning	Value range	Default setting
Index	Sequential line index.		
Description	Description of this entry	0-127 ASCII characters	
Active	Activate/deactivate the rule	on/off	off
Source Address	MAC address of the actual source of the data packet. Entry format: 11:22:33:44:55:66 Entering "?" enables wildcards to be used. Example: 1?:22:?:44:55:6?.		
Destination Address	MAC address of the actual destination of the data packet. Entry format: 11:22:33:44:55:66 Entering "?" enables wildcards to be used. Example: 1?:22:?:44:55:6?.		
Protocol	Protocol in the type field of the MAC data packet		any
Action	Action that the Firewall performs if the rule applies.	accept, drop	drop (outgoing) accept (incoming)
Log	Entry in the event list if the Firewall uses the rule. If applicable, the device also sends a trap.  <b>Note:</b> The <code>logAndTrap</code> setting can generate large quantities of trap data traffic. This is especially the case when sending the trap triggers a match in the Firewall rule again (e.g. if the trap host cannot be reached and a router responds with an ICMP message).	enable, disable, logAndTrap	disable
Error	Shows the last message for an unsuccessful attempt to activate the table entry (usually a detected syntax error).		

*Table 47: Incoming/outgoing MAC packets at the external/internal port*

**Note:** The Firewall supports up to 256 MAC rules.

In the dialog `Diagnostics:MAC Firewall List`, you find the summary of the active rules.

### 4.1.5 Incoming PPP packets

The Firewall allows you to check the incoming PPP packets at the external port based on:

- ▶ the logical port
- ▶ the source IP address
- ▶ the logical destination port
- ▶ the destination IP address
- ▶ the transmission protocol

For every packet that does not match any of the rules in the table, but only the invisible default rule “drop everything”, you have the option of creating a log entry. To do this, activate the setting “Log if non-matching”.

Parameter	Meaning	Possible Values	Default Setting
Index	Sequential line index.		
Description	Description of this entry	0-127 ASCII characters	
Active	Activate/deactivate the rule	on/off	off
Source IP (CIDR)	IP Address with Netmask (CIDR) of the actual source of the data packet.	IP Address with Netmask, any = all, me = own IP address	any
Source Port	<p>Logical source port of the data packet You can also use operators (op) to select multiple ports:</p> <p>= equal to != not equal to &lt; less than &lt;= less than or equal to &gt; greater than &gt;= greater than or equal to &gt;&lt; within &lt;&gt; outside of</p> <p>Use decimal numbers for the port ID. You can also enter the following known ports as ASCII characters:</p> <pre> 7      tcp/udp: echo 9      tcp/udp: discard 20     tcp      :ftp-data 21     tcp      :ftp 22     tcp/udp: ssh 23     tcp      :telnet 53     tcp/udp: domain 67     tcp/udp: bootps 68     tcp/udp: bootpc 69     udp      : tftp 80     tcp/udp: www, http 88     tcp/udp: kerberos 115    tcp      : sftp 123    tcp      : ntp 161    udp      : snmp 162    udp      : snmp-trap 179    tcp/udp: bgp 389    tcp/udp: ldap 443    tcp/udp: https </pre>	<p>any = all</p> <p>op port or port 1 op port 2</p>	any
Destination Net	IP Address with Netmask (CIDR) of the actual destination of the data packet.	IP Address with Netmask, any = all, me = own IP address	

*Table 48: Incoming PPP packets at the external port*

---

Parameter	Meaning	Possible Values	Default Setting
Destination Port	Logical destination port of the data packet To select multiple ports, you can use the same operators as for the source port: Use decimal numbers for the port ID. You can also enter the same known ports, as with the source port, as ASCII characters.	any = all op port port 1 op port 2	any

---

*Table 48: Incoming PPP packets at the external port*

Parameter	Meaning	Possible Values	Default Setting
Protocol	<p>You can enter the following protocols as ASCII characters:</p> <ul style="list-style-type: none"> <li>▶ any Any Layer 4 protocol</li> <li>▶ tcp Transmission Control Protocol (RFC 793)</li> <li>▶ udp User Datagram Protocol (RFC 768)</li> <li>▶ icmp Internet Control Message Protocol (RFC 792)</li> <li>▶ igmp Internet Group Management Protocol (RFCs 1112 (v1), 2236 (v2), 3376 (v3))</li> <li>▶ ipip IP in IP Tunneling (RFC 1853)</li> <li>▶ esp IPsec Encapsulated Security Payload (RFC 2406)</li> <li>▶ ah IPsec Authentication Header (RFC 2402)</li> <li>▶ ipv6-icmp Internet Control Message Protocol for IPv6 (RFC 4443)</li> <li>▶ &lt;0 - 255&gt; Number of the Layer 4 protocol in the IP header</li> </ul>	<p>any = all, tcp, udp, icmp, (additionally: igmp, ipip, esp, ah, ipv6-icmp, &lt;0 - 255&gt;)</p> <p><b>Note:</b> You can select the protocols any, tcp, udp and icmp from the list. Manually enter the protocols igmp, ipip, esp, ah, ipv6-icmp and &lt;0 - 255&gt;.</p>	any
	<p><b>Note:</b> With the udp and tcp protocols, you have the option to enter the protocol ports in the “Source port” and “Destination Port” columns. For other protocols you enter any for “Source port” and “Destination Port”.</p>		
	<p><b>Note:</b> The stateful firewall supports the protocols tcp, udp and icmp.</p>		
Action	Action that the Firewall performs if the rule applies.	accept, drop, reject	accept

*Table 48: Incoming PPP packets at the external port*

Parameter	Meaning	Possible Values	Default Setting
Log	Entry in the event list if the Firewall uses the rule. If applicable, the device also sends a trap.  <b>Note:</b> The <code>logAndTrap</code> setting can generate large quantities of trap data traffic. This is especially the case when sending the trap triggers a match in the Firewall rule again (e.g. if the trap host cannot be reached and a router responds with an ICMP message).	<code>enable</code> , <code>disable</code> , <code>logAndTrap</code>	<code>disable</code>
Error	Shows the last message for an unsuccessful attempt to activate the table entry (usually a detected syntax error).		

*Table 48: Incoming PPP packets at the external port*

**Note:** The Firewall supports up to 1024 IP rules. In the dialog `Diagnostics:IP Firewall List`, you find the summary of the active rules.

## 4.2 NAT – Network Address Translation

The Firewall provides you with the following functions of the Network Address Translation protocol:

- ▶ IP Masquerading
- ▶ 1:1 NAT
- ▶ Port Forwarding

1:1 NAT allows you to set up communication connections in both directions.

### 4.2.1 General NAT settings

The settings in this dialog apply to all NAT procedures.

Parameter	Meaning	Value range	Default setting
Maximum Connection Mappings	Maximum for the sum of the assigned connections of all NAT procedures that the Firewall permits.	0-4,096 s	1,024 s
Timeout for Established TCP Connections	Time period in seconds for how long an active TCP connection is allowed to exist before the Firewall interrupts the TCP connection.	0-2,147,483,647 s	3,600 s
Send packet on receiving interface allowed	Activate this setting if you want to permit the Firewall to resend a received packet after the NAT processing at the same interface. This setting is only necessary in certain special cases.	on/off	off

*Table 49: General NAT Settings*

## 4.2.2 IP Masquerading

This dialog allows you to include up to 128 internal networks in the Network Address Translation.

Parameter	Meaning	Value range	Default setting
Index	Sequential line index.		
Description	Description of this entry	0-127 ASCII characters	
Active	Activate/deactivate the rule	on/off	off
Internal Network (CIDR)	IP Address with Netmask (CIDR) of the internal network, e.g. 10.1.2.0/24	IP Address with Netmask	192.168.1.0/24
FTP	Allow active FTP from the internal network	on/off	off
Error	Shows the last message for an unsuccessful attempt to activate the table entry (usually a detected syntax error).		

Table 50: IP Masquerading

## 4.2.3 1:1 NAT

This dialog allows you to enter, edit or delete up to 128 entries for a 1:1 address translation. You can create entries for individual terminal devices with a netmask 32 bits long, and entries for entire network areas with a correspondingly shorter netmask.



With 1:1 NAT, the device operates as a router and allocates an additional IP address in the external network for a terminal device in the internal network. In addition, as a proxy the device answers the ARP queries for the additional IP address in the external network. For outgoing data packets, the device replaces the internal source IP address of the terminal device with its external IP address. For incoming data packets, it replaces the external destination IP address with the internal IP address.

**Note:** Before setting up 1:1 NAT, make sure that the IP address in the external (invert direction: internal) network is unused.

Parameter	Meaning	Value range	Default setting
Index	Sequential line index.		
Description	Description of this entry	0-127 ASCII characters	
Active	Activate/deactivate the rule	on/off	off
Internal Network	IP address of the internal network or the smallest IP address of the network area of the inner network	IP Address	192.168.1.1
External Network	IP address of the external network or the smallest IP address of the network area of the external network	IP Address	10.0.1.1
Netmask	Netmask for the area to be translated	1-32	32
FTP	Allow active FTP from the internal network	on/off	off
Invert Direction	Allocate an additional IP address (via proxy ARP) for an external terminal device at the internal interface, instead of for an internal terminal device at the external interface. Thus terminal devices in the internal network can communicate with external terminal devices without gateway entries.	on/off	off
Double-NAT	With Double NAT, when the source address is implemented in the packets, the device also replaces the destination address if there is a corresponding rule. Thus terminal devices in both the internal and external networks can communicate with terminal devices in the other network without gateway entries.	on/off	off
Error	Shows the last message for an unsuccessful attempt to activate the table entry (usually a detected syntax error).		

**Note:** Before setting up inverse 1:1 NAT, make sure that the IP address in the internal network is unused.

**Note:** For the replacement of the destination address, enter an additional rule for the address conversion of the external terminal device. Activate “Output” (Double NAT). In addition, activate the inversion for this second rule.

Table 51: 1:1 NAT

---

The device allows you to combine 1:1 NAT with router redundancy ([see on page 155 “Router Redundancy”](#)).

## 4.2.4 Port forwarding

A device can set up communication with a device in the internal network from the external network if you have previously entered the forwarding conditions in the table.

Parameter	Meaning	Value range	Default setting
Index	Sequential line index.		
Source IP (CIDR)	IP Address with Netmask (CIDR) of the actual source of the data packet.	IP Address with Netmask, any = all	any
Source Port	Logical source port of the data packet You can optionally use the operator “=: = equal to Use decimal numbers for the port ID. You can also enter the following known ports as ASCII characters:	0..65,535  Syntax: = port-no. or = port-id  e. g.: = http	any
	7 tcp/udp: echo 9 tcp/udp: discard 20 tcp :ftp-data 21 tcp :ftp 22 tcp/udp: ssh 23 tcp :telnet 53 tcp/udp: domain 67 tcp/udp: bootps 68 tcp/udp: bootpc 69 udp : tftp 80 tcp/udp: www, http 88 tcp/udp: kerberos 115 tcp : sftp 123 tcp : ntp 161 udp : snmp 162 udp : snmp-trap 179 tcp/udp: bgp 389 tcp/udp: ldap 443 tcp/udp: https		
Incoming Address	Destination address of the data packet that is received at the external port for forwarding. %extern indicates the IP address of the external port	%extern or IP address	%extern

Table 52: Port Forwarding

Parameter	Meaning	Value range	Default setting
Incoming Port	Logical port at which the data packet at the external port is received for forwarding. Use decimal numbers for the port ID. You can also enter the following known ports as ASCII characters: 7 tcp/udp: echo 9 tcp/udp: discard 20 tcp :ftp-data 21 tcp :ftp 22 tcp/udp: ssh 23 tcp :telnet 53 tcp/udp: domain 67 tcp/udp: bootps 68 tcp/udp: bootpc 69 udp : tftp 80 tcp/udp: www, http 88 tcp/udp: kerberos 115 tcp : sftp 123 tcp : ntp 161 udp : snmp 162 udp : snmp-trap 179 tcp/udp: bgp 389 tcp/udp: ldap 443 tcp/udp: https	0..65.535	80
Forward Address	IP address of the device in the internal network for which the data packet is intended.		127.0.0.1
Forward Port	Logical address of the device in the internal network for which the data packet is intended. You can also enter the same known ports, as with the incoming port, as ASCII characters.	0..65.535	80
Protocol	tcp Transmission Control Protocol (RFC 793) udp User Datagram Protocol (RFC 768) icmp Internet Control Message Protocol (RFC 792)	tcp, udp, icmp	tcp
Log	Entry in the event list if the Firewall uses the rule.	Yes, No	No
Description	Description of this entry	0-127 ASCII characters	
Active	Activate/deactivate the rule	on/off	off
Error	Shows the last message for an unsuccessful attempt to activate the table entry (usually a detected syntax error).		

Table 52: Port Forwarding

---

**Note:** The Firewall supports up to 1024 IP rules.  
In the dialog `Diagnostics:IP Firewall List`, you find the summary of the active rules.

## 4.3 Helping protect against Denial of Service (DoS)

This function helps you to protect your network and your server from unauthorized access via excessive flooding with TCP connections, ping packets or ARP packets.

**Note:** Adjust the values defined by the default settings to the TCP connections, ping packets and ARP packets actually required in your network. The device allows you to generate a log entry when a threshold has been exceeded. You can set this specifically for each threshold.

Parameter	Meaning	Value range	Default setting
Max. incoming TCP Connections per s	Maximum number of new (SYN flag set) incoming TCP connections per second at the external port	1-999,999	25
Max. outgoing TCP Connections per s	Maximum number of new (SYN flag set) incoming TCP connections per second at the internal port	1-999,999	75
Max. incoming Ping Frames per s	Maximum number of incoming ping frames per second at the external port	1-999,999	3
Max. outgoing Ping Frames per s	Maximum number of incoming ping frames per second at the internal port	1-999,999	5
Max. incoming ARP Frames per s	Maximum number of incoming ARP frames per second at the external port	1-999,999	500
Max. outgoing ARP Frames per s	Maximum number of incoming ARP frames per second at the internal port	1-999,999	500

*Table 53: Settings to help protect against Denial of Service*

---

## 4.4 User Firewall

The user firewall allows you to create up to 32 firewall user entries. Every user firewall entry contains:

- ▶ a set of rules that defines which data packets the Firewall may forward or not.
- ▶ a list of the users to which the Firewall should apply these rules.
- ▶ a timeout to limit the usage period.

In the “Configuration” frame of the dialog you can

- ▶ activate or deactivate the user firewall globally and
- ▶ activate or deactivate the group authentication for users.

### Group Authentication:

Group authentication allows you to organize multiple users into groups via a RADIUS server.

If group authentication is active and an unknown person logs in to the user firewall, the Firewall checks the authenticity via the RADIUS server ([see on page 66 “Authentication Lists”](#)).

If the authentication is successful, the RADIUS server sends an “Accept” data packet with the attribute “Filter-ID=<groupname>” to the Firewall.

If the Firewall has a user firewall account with this group name, the Firewall gives the user access.

To be able to use the user firewall, the user must be entered in the dialog `Security:External Authentication:User Firewall Accounts`. To have a clear assignment of “user to user firewall entry”, you can assign exactly one entry to each user. You can assign multiple users to a firewall user entry.

You can create, delete and edit rules, and you can change their order. Select one or more sequential rows to be moved and move your selection with the “↑” and “↓” buttons. You can also duplicate (clone) a rule and then edit it.



Parameter	Meaning	Value range	Default setting
Name	Unique name to identify this entry	0-32 ASCII characters	
Timeout Type	Defines the start of the timeout countdown: <i>static</i> : The countdown of the timeout begins when the user logs on. <i>dynamic</i> : The countdown of the timeout begins after the user logs off.	<i>static</i> , <i>dynamic</i>	<i>static</i>
Source Address (CIDR)	IP Address with Netmask (CIDR) of the user (see table 55).	Unicast IP Address	%authorized_ip
Description	Description of this entry	0-127 ASCII characters	
Active	Activate/deactivate the rule	on/off	off

Table 54: User Firewall Entries

### ■ Editing a user firewall entry

The `Basic Settings` tab page enables you to enter general specifications for this user firewall entry.

Parameter	Meaning	Possible Values	Default Setting
Name	Any name for this entry.	0-32 ASCII characters	
Timeout [s]	Maximum time for the duration of the user access.	1-604,800 (7 days)	28,800 (8 h)
Timeout Type	Defines the start of the timeout countdown: <i>static</i> : The countdown of the timeout begins when the user logs on. <i>dynamic</i> : The countdown of the timeout begins after the user logs off.	<i>static</i> , <i>dynamic</i>	<i>static</i>
Source Address	IP address of the user. If the user does not have a fixed IP address, the expression %authorized_ip allows you to take over the IP address from the user logon as the source address.	IP Address, %authorized_ip	%authorized_ip
Description	Description of this entry	0-127 ASCII characters	

Table 55: Basic Settings

---

The `Users` tab page allows you to name the user(s) to whom this user firewall entry applies. You define the users beforehand in the dialog `Security:External Authentication:Users`.

Parameter	Meaning	Possible Values	Default Setting
Account Name	Name of a user from the table <code>Security:External Authentication:User-Firewall Accounts</code> .		
Active	Activate/deactivate the rule	on/off	off

*Table 56: Accounts*

The **Rules** tab page enables you to create rules for this user firewall entry.

Parameter	Meaning	Possible Values	Default Setting
Source Port	<p>Logical source port of the data packet</p> <p>You can also use operators (op) to select multiple ports:</p> <p>= equal to</p> <p>!= not equal to</p> <p>&lt; less than</p> <p>&lt;= less than or equal to</p> <p>&gt; greater than</p> <p>&gt;= greater than or equal to</p> <p>&gt;&lt; within</p> <p>&lt;&gt; outside of</p> <p>Use decimal numbers for the port ID. You can also enter the following known ports as ASCII characters:</p> <p>7 tcp/udp: echo</p> <p>9 tcp/udp: discard</p> <p>20 tcp :ftp-data</p> <p>21 tcp :ftp</p> <p>22 tcp/udp: ssh</p> <p>23 tcp :telnet</p> <p>53 tcp/udp: domain</p> <p>67 tcp/udp: bootps</p> <p>68 tcp/udp: bootpc</p> <p>69 udp : tftp</p> <p>80 tcp/udp: www, http</p> <p>88 tcp/udp: kerberos</p> <p>115 tcp : sftp</p> <p>123 tcp : ntp</p> <p>161 udp : snmp</p> <p>162 udp : snmp-trap</p> <p>179 tcp/udp: bgp</p> <p>389 tcp/udp: ldap</p> <p>443 tcp/udp: https</p>	<p>any = all</p> <p>op port</p> <p>or</p> <p>port 1 op port 2</p>	any
Destination Network	<p>IP Address with Netmask (CIDR) of the destination network, e.g. 10.1.2.0/24</p>	<p>IP Address with Netmask,</p> <p>any = all,</p> <p>me = own IP address</p>	

*Table 57: Rules*

Parameter	Meaning	Possible Values	Default Setting
Destination Port	Logical destination port of the data packet To select multiple ports, you can use the same operators as for the source port: Use decimal numbers for the port ID. You can also enter the same known ports, as with the source port, as ASCII characters.	any = all op port port 1 op port 2	any
Protocol	You can also enter the following known protocols as ASCII characters: tcp Transmission Control Protocol (RFC 793) udp User Datagram Protocol (RFC 768) icmp Internet Control Message Protocol (RFC 792)	any, tcp, udp, icmp	tcp
Log	Entry in the event list if the Firewall uses the rule.	Yes, No	No
Description	Description of this entry	0-127 ASCII characters	
Active	Activate/deactivate the rule	on/off	off

*Table 57: Rules*

**Note:** The Firewall supports up to 1024 IP rules.

In the dialog `Diagnostics:IP Firewall List`, you find the summary of the active rules.

## **5 VPN – Virtual Private Network**

The device provides you with an assistant for setting up a VPN connection. This assistant takes you through the configuration of a VPN connection step by step. The assistant selects the next step for you, depending on the settings you have already made.

The device also gives you the option of making or editing the settings independently of the assistant in the individual dialogs.

## 5.1 Device connection

With this dialog you can:

- ▶ create up to 256 VPN connections on the external port and give them names. Each row (entry) in the list represents a VPN connection. Up to 64 of the configured connections can be active and in the status `up` at the same time.
- ▶ enter a password for the remote controlled activation/deactivation of a connection.
- ▶ instruct the device to validate received and local certificates before using them (default setting: "Certification validation" activated).
- ▶ use the "VPN" LED of the EAGLE One device to display active VPN connections (default setting: "VPN LED Indication" deactivated).
- ▶ define an IP address range from which the EAGLE One allocates an address to the clients of VPN connections that request an address.
- ▶ define the source for the activation of the service mode.

You can select a VPN entry and:

- ▶ delete it
- ▶ edit it

For a selected entry, you can:

- ▶ display information
- ▶ load a PKCS#12 file from the PC.

You need the name of a VPN connection together with the password in order to activate or deactivate a VPN connection remotely. To do this, you access the following URL of the device:

```
https://vpn:<password>@<firewall_ip>/nph-vpn.cgi?  
name=<connection>&cmd={up|down}
```

Meaning:

- ▶ `<password>` : The password entered in the dialog
- ▶ `<firewall_ip>` : The IP address or the host name of the EAGLE One device
- ▶ `<connection>` : The name of a VPN connection in the table
- ▶ `{up|down}` : up: Set up VPN connect. down: Break VPN connect.

Examples:

```
https://vpn:test@10.1.1.1/nph-vpn.cgi?name=test1&cmd=up
```

<https://vpn:two@fw2.local/nph-vpn.cgi?name=two&cmd=down>

The "VPN LED Indication" field enables you to use the "VPN" LED of the EAGLE One device to display active VPN connections.

The values that can be entered have the following meanings:

Setting	LED VPN	Meaning
off	Not Glowing	
on		Use the "VPN" LED of the EAGLE One device to display active VPN connections.
	Not glowing	One of the following cases applies: <ul style="list-style-type: none"> <li>▶ No VPN connection is active.</li> <li>▶ No active VPN connection is in <code>up</code> status.</li> </ul>
	Glowing green	The LED glows green when one or more active VPN connections are in <code>up</code> status..

*Table 58: Meaning of the values in the "VPN LED Indication" field.*

The "Client IP address allocation" input field allows you to define an IP address range. If a client of an VPN connection requests an address, the EAGLE One dynamically allocates the client an address from this range.

The values that can be entered have the following meanings:

Parameter	Meaning	Possible Values	Default Setting
Client IP address allocation	IPv4 address range in CIDR notation.	Valid IPv4 address range in CIDR notation.	-

*Table 59: IP address range for VPN clients (CIDR)*

**Note:** When defining the address range, verify that the addresses are compatible with the traffic selectors of the VPNs from which clients request addresses. You thus help ensure that a client that receives such an address can also communicate via the VPN.

The "Source for service mode" field enables you to determine the source which starts the service mode.

The values that can be entered have the following meanings:

Parameter	Meaning	Possible Values	Default Setting
Source for service mode	Selecting the source which starts the service mode.	<p>powersupply The service mode starts if</p> <ul style="list-style-type: none"> <li>▶ the redundant power supply of the device is inoperable.</li> <li>▶ you switch off the redundant power supply of the device for this purpose.</li> </ul> <p>digitalinput-low The service mode starts if the low level input voltage (state „0“) is connected to the digital input.</p> <p>digitalinput-high The service mode starts if the high level input voltage (state „1“) is connected to the digital input.</p>	powersupply

*Table 60: Meaning of the values in the "Source for service mode" field.*



Parameter	Meaning	Possible Values	Default Setting
Index	Row index for the unique identification of a connection.		
Name	Any name for this connection. You also use this name in the URL to remotely activate/deactivate the connection.	0-128 ASCII characters	
Startup as	Starting role for mediating the key exchange	responder initiator	responder
Service Mode	<p>Activate/deactivate the service mode. In service mode, the device automatically activates one or more pre-configured VPN connections. You define the source which starts the service mode in the <code>Virtual Private Network:Connection</code> dialog in the "Source for service mode" field (see <a href="#">table 60 on page 136</a>)</p> <p>- Service mode on: Select the "Service Mode" field for one or more VPN connections to switch on the service mode of the device for these connection(s). First configure the selected VPN connection(s) as described in chapter <a href="#">"Editing a connection"</a> on <a href="#">page 138</a>. The device indicates that the service mode is activated as follows:</p> <p>- When the service mode is active, the "Status" field contains the value <code>servicemode-up</code>.</p> <p>- If you have activated the "VPN LED Indication" function, the "VPN" LED glows as described in <a href="#">table 58</a> when the device has activated the VPN connection(s).</p> <p>The device indicates that it has left the service mode with an event log entry: "System service mode is not active".</p> <p>- Service mode off: Remove the checkmark from the Service Mode field to deactivate the service mode of the device.</p>	On/Off	Off
Active	Activate/deactivate the connection	On/Off	Off

*Table 61: Connections*

Parameter	Meaning	Possible Values	Default Setting
Status	State of the connection	up/ down/ negotiation/ constructing/ dormant/ servicemode-up	-
Exchange Mode	<p>mainaggressive: as the initiator, the device uses the main mode when setting up a connection, and as the responder it accepts both the main and the aggressive modes.</p> <p>main: as initiator or responder, the device only uses the main mode when setting up a connection.</p> <p>aggressive: as initiator or responder, the device only uses the aggressive mode when setting up a connection.</p>	mainaggressive/ main/ aggressive	mainaggressive

Table 61: Connections

### ■ Editing a connection

The `Basic Settings` tab page enables you to give the connection any name you want.

Parameter	Meaning	Possible Values	Default Setting
Name	Any name for this connection. You also use this name in the URL to remotely activate/deactivate the connection.	0-128 ASCII characters	

Table 62: Basic Settings

The `Authentication` tab page enables you to set the parameters that the device needs to authenticate itself at the other end of the VPN connection.

Parameter	Meaning	Possible Values	Default Setting
<b>Frame Key Info</b>	Parameters for the key to be used		
Method	Method for selecting and transferring the key	psk x509rsa	psk
Pre-shared key (PSK)	Key that both ends of a VPN connection require to set up the connection and transfer data. When you open a connection to edit it, the Firewall shows the PSK as eight asterisks.	6-128 random ASCII characters	
	<p><b>Note:</b> The Web interface uses the UTF-8 character encoding to exchange the PSK with the device. For the PSK, only use characters and character encoding that the participating devices can interpret immediately. If necessary, restrict the character set used to ASCII (character codes 32-127).</p>		
Load PKCS#12 file from the PC	A PKCS#12 file is a file container that contains the CA certificate, the local certificate and the private key (PEM files).		
<b>Frame Identities</b>	Type of information that an endpoint of the VPN connection uses for identification.		
Local Type	Select the local identification type	default ipaddr keyid fqdn email asnldn	default
Local ID	Identification for the key exchange with the remote terminal in accordance with the local type selected above.		

*Table 63: Authentication*

Parameter	Meaning	Possible Values	Default Setting
Remote Type	Select the remote identification type	any ipaddr keyid fqdn email asn1dn	any
Remote ID	Accepted identification for the key exchange from the remote terminal in accordance with the remote type selected above.		

*Table 63: Authentication*

The identity types that can be selected in the fields “Local type” and “Remote type” have the following meaning:

Possible Values	Meaning
default	Default setting (for PSK: ipaddr; for x509rsa: asn1dn)
any	One of the available options
psk	Pre-shared key
x509rsa	X.509 RSA certificate
ipaddr	IP address of the other end of the VPN connection
keyid	Key identification
fqdn	Fully-qualified domain name
email	E-mail address of a trustworthy person
asn1dn	X.500 Distinguished Name (DN). If the “Local ID” field is empty in this case, then the Firewall uses the DN from the certificate.

*Table 64: Meaning of the values during the authentication*

The `Certificates` tab page provides you with three options for entering certificates that you may need for the authentication:

- ▶ Load PKCS#12 file  
A PKCS#12 file is a file container that contains the CA certificate, the local certificate and the private key.
- ▶ Load PEM files  
A certificate consists of the CA certificate, the local certificate and the private key. One PEM file contains one of these parts.
- ▶ Enter the CA certificate, the local certificate and the private key manually.

<b>Parameter</b>	<b>Meaning</b>
Load PKCS#12 file from the PC	A PKCS#12 file is a data container that contains individual certificate shares. As an alternative to the PKCS#12 file, you can load the individual certificate shares in the form of PEM files below.
<b>Local</b>	Entries for the local certificate
Certificate	The local certificate for authentication at the other end of the VPN connection
Password	The password for the private key, if the key is in encrypted form. When you open a connection to edit it, the Firewall shows the PSK as eight asterisks.
Private key	The private key assigned to the certificate.
<b>Certification Authority (CA)</b>	Entry for the certificate of the certification authority.
Certificate	Certificate of the certification authority.
<b>Remote</b>	Entry for the certificate of the other end of the VPN connection.
Certificate (optional)	Certificate of the other end of the VPN connection (if desired). For a connection to an EAGLE One mGuard, you enter the certificate of the EAGLE One mGuard.

*Table 65: Certificates*

The **IKE - Key Exchange** tab page allows you to set the parameters for the key exchange.

Parameter	Meaning	Possible Values	Default Setting
<b>Mode</b>			
Protocol	Protocol version to be used for the key exchange	auto v1 v2	auto
Startup as	Starting role for mediating the key exchange	responder initiator	responder
DPD Timeout	Dead Peer Detection. Period after which the connection becomes invalid if the other end of the connection does not send a sign of life.	0-86,400 seconds, whereby the value "0" switches off the DPD.	120 seconds
Lifetime	Usage period for the key used to help protect IKE protocol messages, and therefore the maximum lifetime of the IKE security arrangement (IKE SA) itself. Select the lifetime of the initiator as less than or equal to the lifetime of the responder.	1-86,400 seconds (= 24 hours)	28,800 seconds (8 hours)
Compatibility Mode	For LANCOM Client and Hirschmann EAGLE One mGuard.		off
<b>Algorithms</b>			
Select the encryption and hash algorithms to be used for the key exchange.			
Key agreement	Algorithm for the key agreement. The Firewall allows you to enter "any" when it has the starting role "responder". Group assignment: modp768: DH-Group 1 modp1024: DH-Group 2 modp1536: DH-Group 5 modp2048: DH-Group 14 modp3072: DH-Group 15 modp4096: DH-Group 16	any modp768 modp1024 modp1536 modp2048 modp3072 modp4096	modp1024
Hash	Hash algorithm. The Firewall allows you to enter "any" when it has the starting role "responder".	any md5 sha1	sha1

Table 66: IKE Key Exchange

Parameter	Meaning	Possible Values	Default Setting
Integrity	Authentication algorithm for IKE protocol messages. The Firewall allows you to enter “any” when it has the starting role “responder”.	any hmacmd5 hmacsha1	hmacsha1
Encryption	Algorithm for encryption of IKE protocol messages. The Firewall allows you to enter “any” when it has the starting role “responder”.	any des des3 aes128 aes192 aes256	aes128
<b>Endpoints (Peers)</b>	IP addresses of the two endpoints of the VPN connection		
Local IP Address	Host name (FQDN) or IP address of the local security gateway. If the value is “any”, the Firewall uses the first IP address of the external interface. If this address is assigned via DHCP, the setting up of the VPN connection is delayed until a valid IP address is assigned. If a host name is used, the setting up of the VPN connection is delayed until the host name is resolved.	IP Address, any	any
Remote IP Address	Host name (FQDN) or IP address of the remote security gateway. If the value is “any”, the Firewall accepts every IP address when setting up an IKE security arrangement as Responder. The Firewall also accepts a network in CIDR notation when setting up an IKE security arrangement as Responder. As Initiator, the Firewall does not accept such values. If a host name is used, the setting up of the VPN connection is delayed until the host name is resolved.	IP Address, any	any

*Table 66: IKE Key Exchange*

The values that can be selected in the fields “Protocol”, “Start as”, “Key agreement”, “Hash”, “Integrity” and “Encryption” have the following meanings:

Possible Values	Meaning
auto	Automatic selection
v1	IKE protocol version 1
v2	IKE protocol version 2
responder	IKE responder
initiator	IKE initiator
modp	Modular Exponentiation Group, module used for the Diffie-Hellman key exchange.
md5	Message Digest Algorithm 5, cryptographic hash function
sha1	Secure Hash Algorithm 1, cryptographic hash function
hmacmd5	Hash Message Authentication Code, based on MD5
hmacsha1	Hash Message Authentication Code, based on SHA1
des	DES (Data Encryption Standard)
aes	AES (Advanced Encryption Standard)

*Table 67: Meaning of the values for the IKE Key Exchange.*



The **IPsec - Data Exchange** tab page allows you to set the parameters for the data exchange.

Parameter	Meaning	Possible Values	Default Setting
<b>Mode</b>			
Encapsulation	Selection of VPN operating mode	transport tunnel	transport
Force NAT-T	Network Address Translation - Traversal: If there are NAT routers in the transmission path, corresponding actions are taken by IPsec. In this case, IPsec addresses IKE and IPsec data packets to port 4500 in accordance with RFC 3948. If NAT-T is activated, the Firewall definitely addresses to port 4,500.	on/off	off
Lifetime	Usage period for the key used to help protect data packets, and therefore the maximum lifetime of the IPsec security arrangement (IPsec SA) itself.	1-28,800 (8 h)	3,600 (1 h)
<b>Algorithms</b>			
Key Agreement	Select the encryption and hash algorithms to be used for the key exchange.  Selection of an algorithm for the key agreement. The Firewall allows you to enter "any" when it has the starting role "responder". Group assignment: modp768 DH-Group 1 modp1024 DH-Group 2 modp1536 DH-Group 5 modp2048 DH-Group 14 modp3072 DH-Group 15 modp4096 DH-Group 16	any modp768 modp1024 modp1536 modp2048 modp3072 modp4096 none	modp1024
Integrity	Selection of an algorithm for the integrity protection	any md5 sha1	hmacsha1
Encryption	Selection of an algorithm for the data encryption	any des des3 aes128 aes192 aes256	aes128

*Table 68: IPsec - Data Exchange*

---

The values that can be selected in the fields “Encapsulation”, “Key agreement”, “Integrity” and “Encryption” have the following meanings:

Possible Values	Meaning
modp	Modular Exponentiation Group, module used for the Diffie-Hellman key exchange.
hmacmd5	Hash Message Authentication Code, based on MD5
hmacsha1	Hash Message Authentication Code, based on SHA1
des	DES (Data Encryption Standard)
aes	AES (Advanced Encryption Standard)

*Table 69: Meaning of the values for the IPsec data exchange*

The `IP Networks` tab page enables you to set the parameters for the IP networks at the internal port whose data is to be transferred via the VPN connection.

The firewall only transmits and encrypts through the tunnel that data which corresponds to an entry in this table. The firewall routes the other data according to the existing entries in the packet filters.

Parameter	Meaning	Possible Values	Default Setting
Index	Sequential line index.		
Source Address (CIDR)	IP Address with Netmask (CIDR) of the actual source of the data packet.  <b>Note:</b> If you connect 2 devices via VPN, network addresses are accepted as local source addresses even if they are not identical with the destination addresses entered at the opposite end but are a subset of these destination addresses.  <b>Example:</b> If you enter 192.168.2.0/24 as the source address in the local device and 192.168.1.0/20 as the destination address at the opposite end, this is a valid combination.	IP Address with Netmask, any = all	any

*Table 70: IP Networks at Internal Port*

Parameter	Meaning	Possible Values	Default Setting
Source Port	Logical source port of the data packet. Use decimal numbers for the port ID. You can also enter the following known ports as ASCII characters:	any = all op port op port 1 op port 2	any
	7 tcp/udp: echo		
	9 tcp/udp: discard, sink, null		
	20 tcp: ftp-data		
	21 tcp: ftp		
	22 tcp/udp: ssh		
	23 tcp: telnet		
	53 tcp/udp: dns		
	67 tcp/udp: bootps		
	68 tcp/udp: bootpc		
	69 udp: tftp		
	80 tcp/udp: www, http		
	88 tcp/udp: kerberos, krb5		
	115 tcp: sftp		
	123 tcp/udp: ntp		
	161 udp: snmp		
	162 udp: snmp-trap, snmptrap		
	179 tcp/udp: bgp		
	389 tcp/udp: ldap		
	443 tcp/udp: https		
Destination Address (CIDR)	IP Address with Netmask (CIDR) of the actual destination of the data packet.	IP Address with Netmask, any = all	
Destination Port	Logical destination port of the data packet. Use decimal numbers for the port ID. You can also enter the same known ports, as with the source port, as ASCII characters.	any = all op port op port 1 op port 2	any
Policy	The EAGLE One uses these security specifications for traffic via a VPN connection. The EAGLE One supports the following security specifications: – require: To set up a VPN connection, the EAGLE One requires the data to be encrypted. – use: To set up a VPN connection, the EAGLE One uses the encryption, if you have selected an encryption. Otherwise the EAGLE One forwards the data unencrypted.	require, use	require

Table 70: IP Networks at Internal Port

Parameter	Meaning	Possible Values	Default Setting
Protocol	<p><code>tcp</code> Transmission Control Protocol (RFC 793)</p> <p><code>udp</code> User Datagram Protocol (RFC 768)</p> <p><code>icmp</code> Internet Control Message Protocol (RFC 792)</p> <p><b>Note:</b> If you use a different protocol setting to the standard setting <code>any</code> and connect the EAGLE One to a remote terminal that supports only outdated implementation of IKEv1, then you also activate <code>compatibility mode</code> on the EAGLE One in the <code>IKE key exchange</code> tab so that the devices can set up a connection. The conditions set on the EAGLE One for the traffic selector are also retained in compatibility mode.</p>	<code>any = all, tcp, udp, icmp</code>	<code>any</code>
Description	Description of this entry	0-127 ASCII characters	
Mapped Source Address (CIDR)	<p>The EAGLE One replaces the IP source address of the data sent into the VPN connection with an IP address from this address range.</p> <p>Prerequisite: Protocol = <code>any</code></p>		
Mapped Destination Address (CIDR)	<p>The EAGLE One replaces the IP destination address of the data received out of the VPN connection with an IP address from this address range.</p> <p>Prerequisite: Protocol = <code>any</code></p>		
Active	Activate/deactivate the rule	<code>on/off</code>	<code>off</code>

Table 70: IP Networks at Internal Port

### ■ Deleting a connection

The firewall helps protect an active connection from being deleted. Select the deactivated entry for a connection to be deleted. Click “Delete entry”.



## 6 Redundancy

The redundancy functions allow you to provide redundant paths via a redundant Firewall.

If the Firewall that is currently transmitting detects a loss of communication (e.g. a disconnected link), it sends the information to its partner Firewall, which then takes over the transmission.

Depending on the network operating mode setting, the Firewall offers you:

- ▶ Transparent Redundancy
- ▶ Router Redundancy

## 6.1 Transparent Redundancy

The Transparent Redundancy function allows you to incorporate the Firewall into the path of the redundant ring/network coupling (see the user manual for the redundancy configuration of your Hirschmann device that supports redundant coupling).

You can use the Transparent Redundancy function when you are operating the Firewall in the transparent mode.



Parameter	Meaning	Possible Values	Default Setting
<b>Operation</b>			
	Switch the Transparent Redundancy on/off. Prerequisite: In the Basic Settings:Network:Global dialog, the Transparent mode is selected.	on/off	off
<b>Transparent Redundancy</b>			
Master or Slave Port	The port of the EAGLE One that is connected to the master (via the main line) or the slave (via the redundant line) of the ring coupling. The other port of the EAGLE One is connected to the remote ring or network, which contains neither a ring coupling master or slave. With the external setting: If the connection at the internal port is inoperable, the Firewall deactivates the external port. With the internal setting: If the connection at the external port is inoperable, the Firewall deactivates the internal port.	internal, external	external
<b>Firewall State Table Synchronisation</b>			

*Table 71: Transparent Redundancy*

Parameter	Meaning	Possible Values	Default Setting
Redundancy Partner IP Address	The IP address identifies the redundancy partner with which the Firewall synchronizes its state table, so that the redundancy partner can take over all tasks at any time.	IPv4 address	0.0.0.0
Communication	<p>The communication between the redundant partners is active/inactive.</p> <p>- Active: The communication between master and slave is active. The master sends synchronization packets to the slave and receives its confirmation packets when traffic is going over the device.</p> <p>- Inactive: There is no communication at the moment. Make sure that no data line or net component is down: Check the Layer 2 redundancy status using the switches in the path of the redundant ring/network coupling in which you have incorporated the firewall (see the user manual for the redundancy configuration of your Hirschmann device that supports redundant coupling).</p>	Active, Inactive	Inactive

*Table 71: Transparent Redundancy*

**Note:** Immediately after the main connection is reinstated, the redundant coupling switches the transmission from the redundant line to the main line. If both lines of the main Firewall were previously interrupted, then the two Firewalls were unable to synchronize their state tables.

**Note:** If no packets are received from the other system there can be various reasons including:

- No data transfer via the device is taking place at this moment.
- A data line or net component is inoperable.

The real Layer 2 redundancy state can only be checked on the switches.

## 6.2 Router Redundancy

The Router Redundancy function enables you to provide a redundant Firewall for the Firewall itself in the network. In this case, the Firewall Router Redundancy function combines two Firewalls into a virtual Firewall. Both Firewalls have a shared virtual interface that uses the corresponding Firewall. In the case of a detected error, the redundant Firewall takes over the functions of the first Firewall.

Requirements for using the Router Redundancy function:

- ▶ The Router Mode is active.
- ▶ The packet filter and NAT settings of the Firewall and the redundant Firewall are identical.
- ▶ The Router Redundancy configuration of the Firewall and the redundant Firewall correspond.
- ▶ The entries for the destinations of the ICMP Host Check function are identical and have the same sequence.
- ▶ All VPN connections are deactivated.
- ▶ All devices that have the Firewall entered as a gateway use the virtual IP address of the Firewall Redundancy function.

Parameter	Meaning	Possible Values	Default Setting
<b>Configuration</b>			
Function on/off	Switch the Router Redundancy on/off. Requirement: In the <code>Basics:Network:Global</code> dialog in the "Configuration" frame, the <code>router</code> mode is selected.	On, Off	Off
Priority	The priority is used to specify which device takes over the redundant function. The device with the lower priority (lower number) takes over the redundant function. If the priority is the same, the devices automatically decide which takes over the redundant function.	1-255	100
Status	Displays the redundancy state.		
<b>Internal Interface (Port 1)</b>			
IP Address	Displays the IP address of the internal interface (port 1).		192.168.3.1
Virtual IP Address	IP address of the virtual router on the internal interface.	IP Address	192.168.3.100
VRID	The VRID (virtual router ID) uniquely identifies a virtual router. Select different VRIDs for the internal and external interfaces.	1-255	1
Redundancy Partner IP Address	IP address of the physical redundancy partner that is part of the virtual router.	IP Address	192.168.3.153
<b>External Interface (Port 2)</b>			
IP Address	Displays the IP address of the external interface (port 2).		10.0.0.10
Virtual IP Address	IP address of the virtual router on the external interface.	IP Address	10.0.0.100
VRID	The VRID (virtual router ID) uniquely identifies a virtual router. Select different VRIDs for the internal and external interfaces.	1-255	2
Redundancy Partner IP Address	Physical IP address of the redundancy partner that is part of the virtual router.	IP Address	10.0.0.153

*Table 72: Basic Settings*

The device allows you to combine the router redundancy with 1:1 NAT ([see on page 120 "1:1 NAT"](#)).

The ICMP Host Check function allows you to get the Firewall to check the accessibility of devices in the network in the case of individual connection interruptions. The Firewalls use the check's result to decide which Firewall takes over the active transmission function.

To use this function effectively, configure at least one host for checking at each port of the two Firewalls.

### How the ICMP Host Check works:

If the firewalls' router redundancy protocol detects that they can no longer access each other on all interfaces, the Firewalls start the ICMP Host Check. In the process, the Firewalls go through the affected interface's host list in ascending order of host indices until they find a difference in accessibility for a host. If the current master router cannot access a certain host even though it can be accessed by the backup router, the firewalls swap over their redundancy roles. The current backup router then takes over the master role and the current master router becomes the backup router.

Requirements for using the ICMP Host Check function:

- ▶ Connect at least one host with every interface of the Firewall that can normally be reached by both Firewalls.
- ▶ These hosts are entered in the list for both Firewalls, and the host lists of the Firewalls are identical.

Parameter	Meaning	Possible Values	Default Setting
Operation on/off	Switches the ICMP Host Check on/off.	on, off	off
Status	Displays the state of the check on the reachability of the ping devices entered in the table.	out of service, service enabled, host check running	-
Index	Sequential line index.		
Port	Port to which the Firewall sends the ping request for checking the reachability.	internal, external	internal
IP Address	IP address of the device to which the Firewalls sends the ping request for checking the reachability.	Valid IPv4 Host Address	-
Active	Activate/deactivate the entry.	on, off	on

Table 73: ICMP Host Check

Meanings of the status values displayed are as follows:

- ▶ `out of service`: the ICMP Host Check function is switched off.
- ▶ `not in router mode`: The Firewall is not in router mode.
- ▶ `service enabled`: the function is switched on and is currently not needed as the router redundancy has not detected any problem.
- ▶ `host check running`: The function is switched on and the firewall is currently working through the host list, because the router redundancy has detected a problem.

## 7 Diagnostics

The diagnostics menu contains the following tables and dialogs:

- ▶ Events
  - ▶ Event Log
  - ▶ Syslog Server
  - ▶ Event Settings
  - ▶ Advanced Settings
- ▶ Ports
  - ▶ Utilization
  - ▶ Statistics table
  - ▶ ARP entries
- ▶ Topology Discovery
- ▶ Device Status
- ▶ Signal Contact
- ▶ Alarms (Traps)
- ▶ Report
  - ▶ System Information
- ▶ MAC Firewall List
- ▶ IP Firewall List
- ▶ Configuration Check
- ▶ Reachability Test (Ping)

In service situations, they provide the technician with the necessary information for diagnosis.

---

## 7.1 Events

The dialogs provide you with the following options:

- ▶ **Event Log:**  
Select the events to be logged; display and save the event log file.
- ▶ **Syslog Server:**  
Configuration of the syslog server to transfer event messages to a syslog server.
- ▶ **Event Settings:**  
Select the minimum level to report from which the device transfers events into the event log, and which of them it writes to a connected ACA.

### 7.1.1 Event Log

This function allows you to filter the display for the event log so that it only contains events relevant for you.

In the `Event Log` dialog, you specify which categories of events in the log you want the device to list in the display. Then the device does not display the events of other known categories. The event log itself is not changed by the filtering.

You specify in the event settings ([see on page 163 “Event Settings”](#)) which events the device writes to the event log.



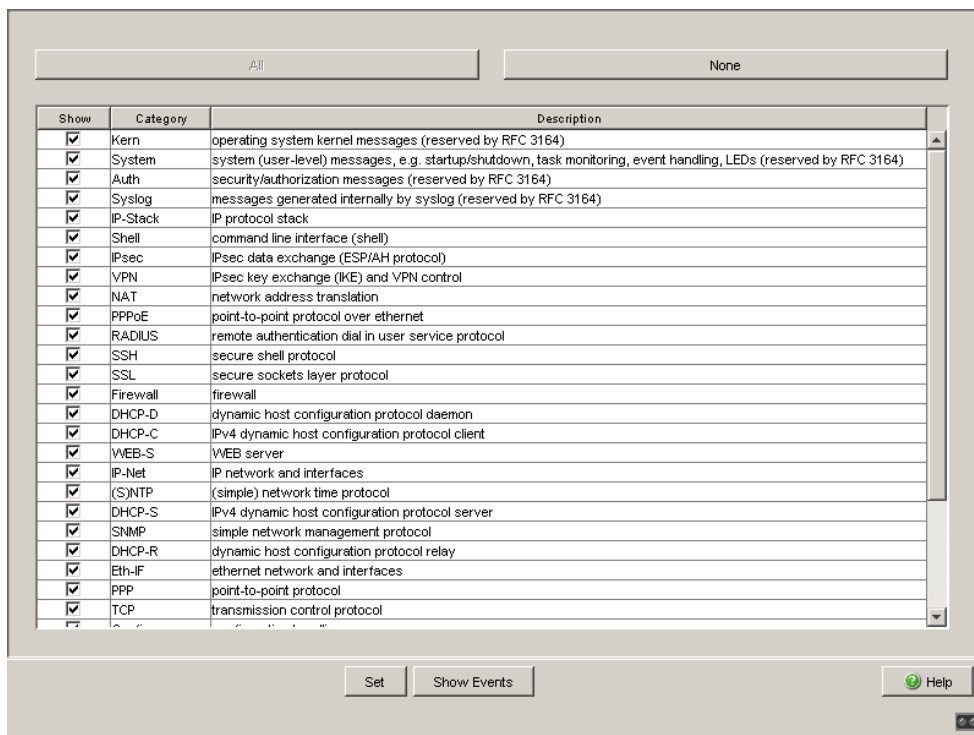


Figure 27: Event Log dialog

- Select the event categories that you want the device to list in the display. See the Event Settings dialog for the meaning of the categories (see [fig. 29](#)).
- Click on “Set” to save the selected categories on your work station (not on the device itself!). They are saved in a file in the home directory of the current user. They are automatically loaded from there the first time the dialog is opened.
- Click on “Show Events” to display the event log file as an HTML file.
- Click on
  - ▶ “Back” to return to the event log window.
  - ▶ “Reload” to update the display.
  - ▶ “Search” to search through the event log file for a key word or a regular expression.
  - ▶ “Save” if you will need the event log file again. In the file selection window, you now select the desired directory, enter a name for the file, and click on “Set”.

**Note:** The log file has the following properties:

- The maximum number of log entries is 4,143.
- If the maximum number of log entries has been reached, the oldest entries will be overwritten by the newer ones.
- Entries that repeat contiguously will be summarized.
- If entries that repeat contiguously are summarized, the log file update may take up to 20 seconds after the last event logged.

## 7.1.2 Syslog Server

This dialog allows you to enter a syslog server. If a syslog server is entered, when an event occurs, the device transfers an event message via the syslog protocol to this server, which for example displays the event messages or triggers an alarm for certain event messages.

If you want to deactivate the sending of event messages via the syslog protocol, you enter the IP address 0.0.0.0.

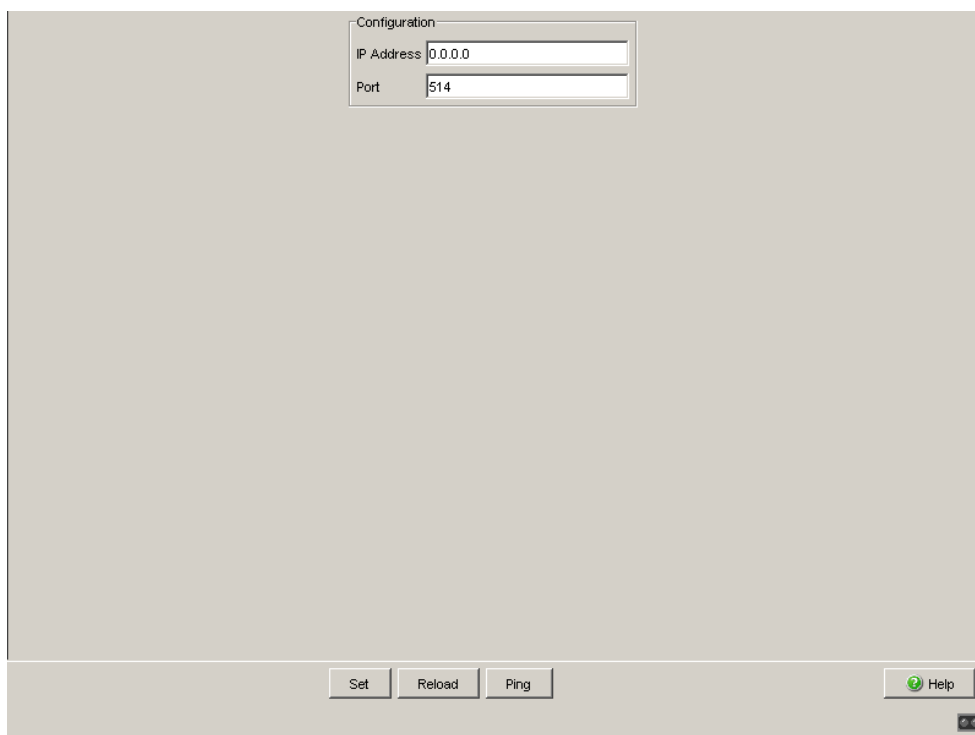


Figure 28: Syslog Server dialog

- Enter the IP address of the syslog server in “IP Address”.
- In “Port” you enter the port number. Default setting: 514 (syslog protocol). Enter the same port number on the device and the syslog server.

### 7.1.3 Event Settings

This dialog allows you to select a minimum level to report for the logging for each event category. The device logs events with the selected level or higher.

You also have the option to select specifically for each event category whether the device writes these events in the persistent log memory on the ACA.

Category	Severity Level	Description	Storing facility persistent
Kern	notice	operating system kernel messages (reserved by RFC 3164)	<input type="checkbox"/>
System	notice	system (user-level) messages, e.g. startup/shutdown, task monitoring, event handling, LEDs (re...	<input type="checkbox"/>
Auth	notice	security/authorization messages (reserved by RFC 3164)	<input type="checkbox"/>
Syslog	notice	messages generated internally by syslog (reserved by RFC 3164)	<input type="checkbox"/>
IP-Stack	notice	IP protocol stack	<input type="checkbox"/>
Shell	notice	command line interface (shell)	<input type="checkbox"/>
IPsec	notice	IPsec data exchange (ESP/AH protocol)	<input type="checkbox"/>
VPN	notice	IPsec key exchange (IKE) and VPN control	<input type="checkbox"/>
NAT	notice	network address translation	<input type="checkbox"/>
PPPoE	notice	point-to-point protocol over ethernet	<input type="checkbox"/>
RADIUS	notice	remote authentication dial in user service protocol	<input type="checkbox"/>
SSH	notice	secure shell protocol	<input type="checkbox"/>
SSL	notice	secure sockets layer protocol	<input type="checkbox"/>
Firewall	notice	firewall	<input type="checkbox"/>
DHCP-D	notice	dynamic host configuration protocol daemon	<input type="checkbox"/>
DHCP-C	notice	IPv4 dynamic host configuration protocol client	<input type="checkbox"/>
WEB-S	notice	WEB server	<input type="checkbox"/>
IP-Net	notice	IP network and interfaces	<input type="checkbox"/>
(S)NTP	notice	(simple) network time protocol	<input type="checkbox"/>
DHCP-S	notice	IPv4 dynamic host configuration protocol server	<input type="checkbox"/>
SNMP	notice	simple network management protocol	<input type="checkbox"/>
DHCP-R	notice	dynamic host configuration protocol relay	<input type="checkbox"/>
Eth-IF	notice	ethernet network and interfaces	<input type="checkbox"/>
PPP	notice	point-to-point protocol	<input type="checkbox"/>
TCP	notice	transmission control protocol	<input type="checkbox"/>
Config	notice	configuration handling	<input type="checkbox"/>
HiDiscovery	notice	discovery of devices	<input type="checkbox"/>
LLDP	notice	link layer discovery protocol	<input type="checkbox"/>
User-Mgmt	notice	user management	<input type="checkbox"/>
Crypto-HW	notice	cryptographic hardware interface	<input type="checkbox"/>
Redundancy	notice	redundancy protocols	<input type="checkbox"/>
CCI	notice	common cryptographic interface	<input type="checkbox"/>

Figure 29: Event Settings dialog

- Under “Level to report” you select for each category the desired event attribute (see table 74) starting from which the device logs the events. By making multiple selections you can assign the same level to report to multiple categories in one step.
- For each category whose events the device is to write to the log file on the ACA, select the checkbox in the “Write in persistent log file”.

Name	Meaning
emergency	The function is no longer available. This affects other functions. The device usually performs a restart.
alert	The function is no longer available. This can affect other functions. Find the cause of the detected error and remove the detected error.
critical	The function was temporarily not available. This may have affected other functions. Find the cause of the detected error and remove the detected error.
error	An error has been detected with this function. This does not affect other functions. The detected error has been handled by the device. Find out whether the detected error was caused by an incorrect configuration or by a temporary event (e.g. an overload) in the network.
warning	An error may have been detected with this function. This does not affect this function or other functions. Find out whether this message resulted from an incorrect configuration or a temporary event (e.g. an overload) in the network.
notice	The function is available. This message is only for information purposes (e.g. reboot, certain configuration changes).
info	The function is available. The message means normal operation, and it can be used for reports or messages. No action is necessary.
debug	The function is available. The message is useful when looking for a detected error, but not for normal operation.

*Table 74: Meaning of the event attributes*

**Note:** The `info` and `debug` levels have been prepared for use in a future software version - while they can be selected in the current software version, they cannot be saved.

## 7.1.4 Advanced Settings

### ■ SNMP Logging

In the “SNMP Logging” frame, the device gives you the option to treat the SNMP requests to the device as events. Here you have the option of treating GET and SET requests separately, and of assigning a “level to report” to the event log entries created.

Parameter	Meaning	Possible Values	Default Setting
<b>Frame „SNMP Logging“</b>	Settings for treating SNMP requests to the device as events.		
Log SNMP Get Requests.	Creates events for SNMP Get requests with the specified “level to report”.	active, inactive	inactive
Level to Report (for logs of SNMP Get Requests)	Specifies the level for which the device creates the event “SNMP Get Request received”.	notice, warning, error, critical, alert, emergency	notice
Log SNMP Set Requests.	Creates events for SNMP Set requests with the specified “level to report”.	active, inactive	inactive
Level to Report (for logs of SNMP Set Requests)	Specifies the level for which the device creates the event “SNMP Set Request received”.	notice, warning, error, critical, alert, emergency	notice

Table 75: SNMP logging settings

### ■ Write in persistent log file

In the “Write in persistent log file” frame, you have the option to configure the maximum size and the maximum number of the persistent log files. In addition, you can stop the current log file. This enables you to replace the while the device is operating, so that the persistent log files remain consistent.

The device writes the persistent log files in the “/log” directory of the ACA. The current log file has the file name “messages”, while older log files in the archive have the names “messages.0” to “messages.97”. When the current log file attains its maximum size, the device renames it to archive file “messages.0” and opens a new current log file. The device renames the previous archive file “messages.0” to “messages.1”, “messages.1” to “messages.2”, etc. When the maximum number for persistent log files has been exceeded, the device deletes the oldest file.

To replace the ACA while the device is operating, the device gives you the option of locking and stopping the current log file. Afterwards, the device closes the current log file.

You can now remove the ACA - the log files on the ACA remain consistent.

Connect another ACA and remove the lock. The device creates a new current log file on the ACA and writes the new events in this file.

Parameter	Meaning	Possible Values	Default Setting
<b>Frame „Store Log persistently“</b>	Settings for persistent log files		
Maximum size of one file in KByte	Displays the maximum size of a log file in KBytes. A maximum size of 0 closes the current log file, archives it, and ends the writing of persistent log files.	0 - 4,096 KBytes	0 KByte
Maximum number of files	Defines the maximum number of log files on the ACA. The number 0 deletes the existing log files and ends the writing of persistent log files.	0 - 99	0
Stop persistent Logging (to remove ACA)	Lock and stop the current persistent log file. Activate the lock to replace the ACA, and deactivate the lock again afterwards.	active, inactive	inactive

*Table 76: Settings for persistent log files*

**Note:** To activate persistent log files, set both the maximum size and the maximum number of log files to values > 0.

**Note:** Only select the events you require to be written in the log file, as the data write rate of the ACA is limited.

**Note:** To replace the ACA while the device is operating, first stop the logging in the persistent log file and click on “Write”. Now replace the ACA. Afterwards, remove the lock on the log file and click “Write” again.

**Note:** Log events that occur while the persistent log file is stopped are only written to the normal event log by the device.

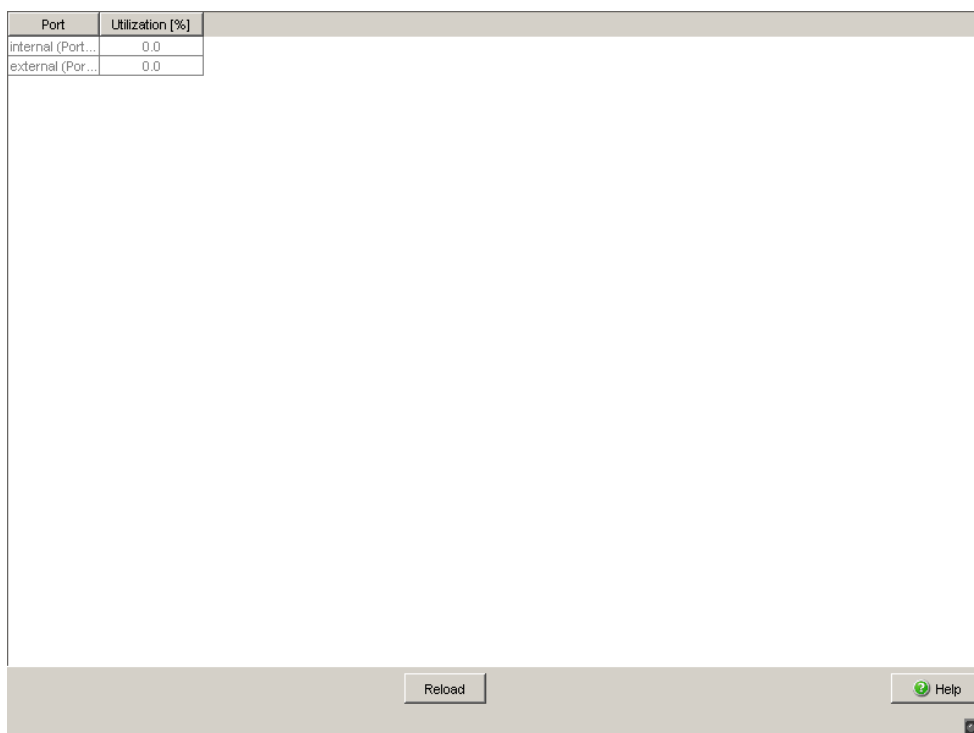
## 7.2 Ports

The port menu contains displays and tables for the individual ports:

- ▶ Utilization
- ▶ Statistics table
- ▶ ARP entries

### 7.2.1 Network Load

This table displays the network load at the individual ports.



Port	Utilization [%]
internal (Port...	0.0
external (Por...	0.0

Figure 30: Network load dialog



## 7.2.2 Statistics table

This table shows you the contents of various port event counters. In the `Basic Settings:Restart` menu item, the device allows you to reset the event counters to 0 using “Cold start” or “Reset port counters”.

Parameter	MIB variable
Port	ifIndex
Received packets	Sum of ifInUcastPkts, ifInMulticastPkts and ifInBroadcastPkts
Received Unicast packets	ifInUcastPkts
Received Multicast packets	ifInMulticastPkts
Received Broadcast packets	ifInBroadcastPkts
Received octets	ifInOctets
Packets discarded on the receiving side	ifInDiscards
Received packets with detected errors	ifInErrors
Received unknown protocols	ifInUnknownProtos
Sent Unicast packets	ifOutUcastPkts
Sent Multicast packets	ifOutMulticastPkts
Sent Broadcast packets	ifOutBroadcastPkts
Sent octets	ifOutOctets
Packets discarded on the sending side	ifOutDiscards
Sent packets with detected errors	ifOutError

*Table 77: MIB variables in the statistics table*

**Note:** In PPPoE mode not all PPPoE packets are counted in the external interface counter statistics.

Port	Received Packets	Received Unicast Packets	Received Multicast Packets	Received Broadcast Packets	Received Octets	Received Discards	Incorrect received Packets	Received unknown Protocols	Transmitted Unicast Packets
internal (Port...	1127	1090	21	16	1148164	0	0	0	79
external (Por...	3297	2104	60	1133	436934	0	0	0	370

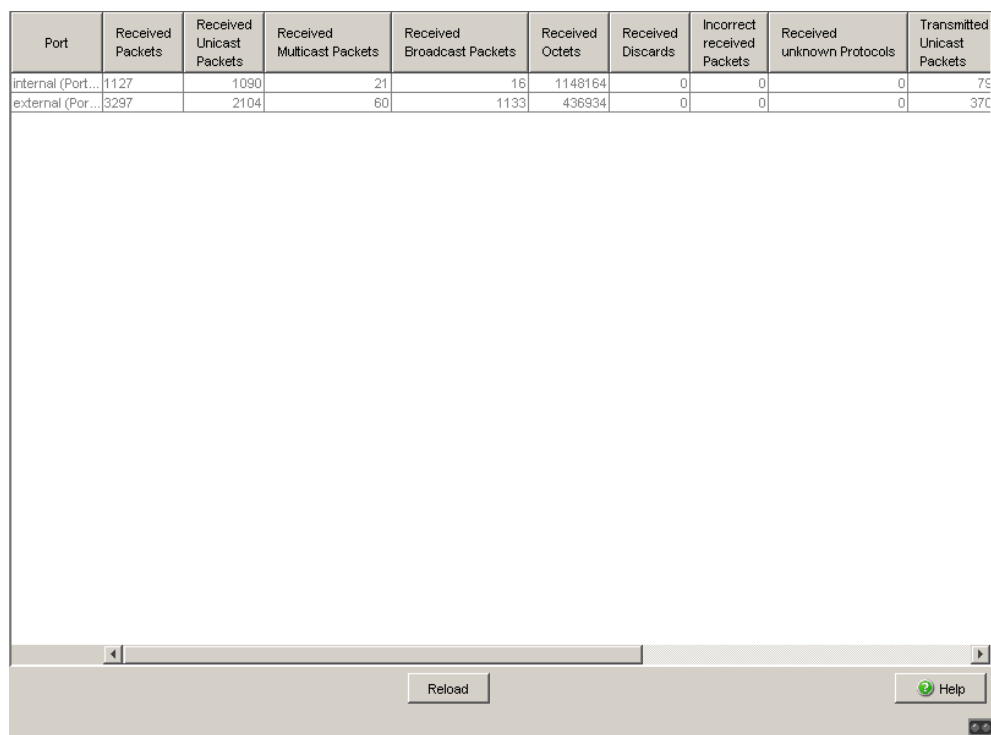


Figure 31: Example of a port statistic table

### 7.2.3 ARP

This table shows you the ARP entries for each port. The device uses the Address Resolution Protocol (ARP) to determine the MAC address relating to the IP address of a device, and it saves this allocation in the ARP table.

Parameter	Meaning
Port	Displays the port to which this entry applies.
IP Address	Displays the IP address of a device that responded to an ARP query to this port.
MAC Address	Displays the MAC address of a device that responded to an ARP query to this port.
Last Updated	Display of the system uptime when this entry was last updated (in days, hours, minutes and seconds).
Type	Displays the type of the entry: <ul style="list-style-type: none"> <li>– static: static ARP entry that remains even after the ARP table is deleted.</li> <li>– dynamic: dynamic entry. If the device does not receive any data during the “Aging Time”, it deletes the entry from the table after the time has elapsed.</li> <li>– local: IP and MAC address of the device's own port</li> </ul>
Active	Displays the status of the entry: <ul style="list-style-type: none"> <li>– Checkmark: ARP active</li> <li>– No checkmark: ARP inactive</li> </ul>

*Table 78: ARP table*

Port	IP Address	MAC Address	Last Updated	Type	Active
internal (Port...	10.115.32.2	00:80:63:CB:1A:47	2 day(s), 3:05:20	dynamic	<input checked="" type="checkbox"/>
internal (Port...	10.115.32.3	00:00:5E:00:01:05	2 day(s), 3:18:05	dynamic	<input checked="" type="checkbox"/>
internal (Port...	10.115.37.173	F0:DE:F1:99:6E:A3	2 day(s), 3:17:47	dynamic	<input checked="" type="checkbox"/>

*Figure 32: Example of ARP entries.*

## 7.3 Topology Discovery

This dialog allows you to switch on/off the Topology Discovery function (Link Layer Discovery Protocol, LLDP). The topology table shows you the collected information for neighboring devices. This information enables the network management station to map the structure of your network.

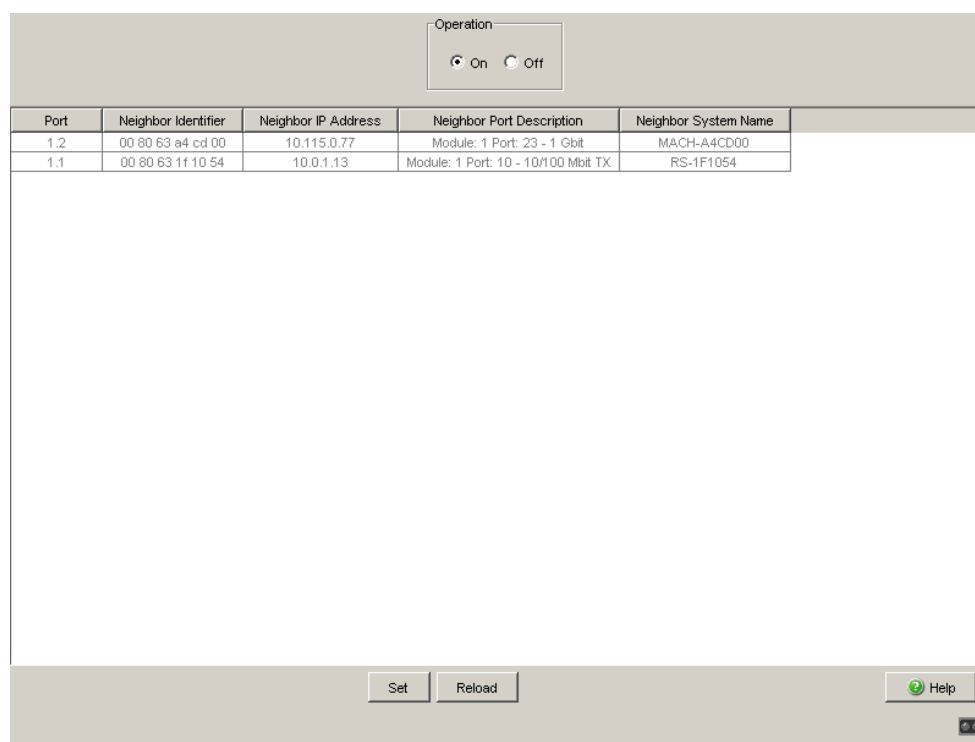


Figure 33: Topology Discovery dialog

If several devices are connected to one port, for example via a hub, the table will contain one line for each connected device.

When devices both with and without an active topology discovery function are connected to a port, the topology table hides the devices without active topology discovery.

When only devices without active topology discovery are connected to a port, the table will contain one line for this port to represent all devices. This line contains the number of connected devices.

## 7.4 Device Status

The device status provides an overview of the overall condition of the device. Many process visualization systems record the device status for a device in order to present its condition in graphic form.

The device displays its current status as "Error" or "OK" in the "Device Status" frame. The device determines this status from the individual monitoring results.

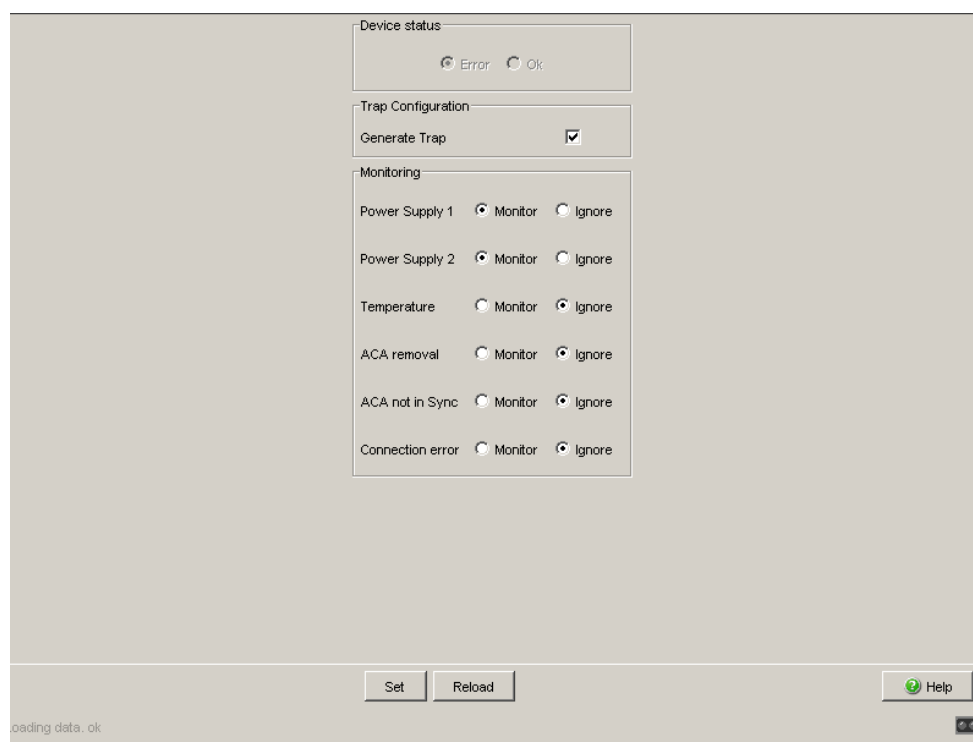


Figure 34: Device Status Dialog

The events which can be selected are:

Name	Meaning
Power Supply ...	Monitor/ignore supply voltage(s).
Temperature	Monitor/ignore the temperature threshold setting ( <a href="#">see on page 16 "System"</a> ) for temperatures that are too high/too low.
ACA Removal	Monitor/ignore the removal of the ACA.
ACA not in sync	Monitor/ignore non-matching of the configuration on the device and on the ACA <sup>a</sup> .
Connection Error	Monitor/ignore the link status of at least one port. The reporting of the link status can be masked for each port by the management ( <a href="#">see on page 33 "Port Configuration"</a> ). In order to monitor connection errors, you also need to select the box for each required port in the <code>Basic settings:Portconfiguration</code> dialog in the column „Propagate connection error“. Link status is not monitored in the state on delivery.

*Table 79: Device Status*

- a. The configurations are non-matching if only one file exists or the two files do not have the same content.

- Select "Generate Trap" in the "Trap Configuration" field to activate the sending of a trap if the device state changes.

**Note:** With a non-redundant voltage supply, the device reports the absence of a supply voltage. If you do not want this message to be displayed, feed the supply voltage over both inputs or switch off the monitoring ([see on page 176 "Signal contact"](#)).

## 7.5 Signal contact

The signal contacts are used for

- ▶ monitoring the functions of the device,
- ▶ controlling external devices by manually setting the signal contacts,
- ▶ reporting the device state of the device (default setting).

### 7.5.1 Function Monitoring

- In the “Mode Signal contact” box, you select the “Monitoring correct operation” mode. In this mode, the signal contact is used to monitor the operation of the device, thus enabling remote diagnostics.

The device uses the potential-free signal contacts (relay contact, closed circuit) to report a break in contact:

- ▶ detected outage of power supply 1/2 or detected continuous device malfunction (internal voltage). Select “Monitor” for power supply 1/2 if the signal contact should report the detected outage of a power supply or the internal 3.3 V voltage.
- ▶ the temperature thresholds set have been exceeded or have not been reached ([see on page 17 “System Data”](#)). Select “Monitor” for the temperature if the signal contact should report an impermissible temperature.
- ▶ removal of the ACA. Select “Monitor” for the ACA removal if the signal contact should report the removal of the ACA.



- ▶ the current configuration on the device and the ACA do not match. Select “Monitor” for a non-synchronous ACA if the signal contact should report this non-matching.
- ▶ the interrupted connection to at least one port. In its delivery state, the device ignores the link status. In order to monitor detected connection errors, you also need to select the box for each required port in the `Propagate connection error` table column in the `Basic settings: Port configuration` dialog.

## 7.5.2 Manual Setting

- In the “Signal Contact Mode” field, you select the “Manual setting” mode. With this mode you can control this signal contact remotely.
- Select “Opened” in the “Manual setting” field to open the contact.
- Select “Closed” in the “Manual setting” field to close the contact.

Application options:

- ▶ Simulation of a detected error during SPS error monitoring.
- ▶ Remote control of a device via SNMP, such as switching on a camera.

### 7.5.3 Device Status

- In the “Signal Contact Mode” field, you select the “Device Status” mode. In this mode, the signal contact is used to monitor the device status of the device (see on page 174 “Device Status”) and thereby makes remote diagnosis possible.  
A break in contact is reported with the device status “Error” via the potential-free signal contact (relay contact, closed circuit) (see on page 174 “Device Status”).

### 7.5.4 Configuring Traps

- Select `Generate Trap`, if the device is to create a trap as soon as the position of a signal contact changes when function monitoring is active.

Signal Contact 1

Signal Contact Mode

Monitoring Correct Operation  Manual Setting  Device Status

Trap Configuration

Generate Trap

Set Reload Help

*Figure 35: Signal Contact Dialog*

## 7.6 Alarms (Traps)

This dialog allows you to determine which events trigger an alarm (trap) and where these alarms should be sent.

- Click “Create Entry...” to open the dialog window for entering a name and the IP address of the recipient to whom the traps are to be sent.
- Confirm the entries with “OK”. You thus create a new row in the table for this recipient.
- In the “Enabled” column, you mark the entries that the device should take into account when it sends traps. Default setting: inactive.
- In the “Configuration” frame, select the trap categories from which you want to send traps. Default setting: all trap categories are active.

The events which can be selected are:

Name	Meaning
Login	An access or an access attempt to the device has been made via the serial interface or via the network (SSH).
Authentication	The device has rejected an unauthorized access attempt, see dialog on <a href="#">page 50</a> .
Chassis	<p>Summarizes the following events:</p> <ul style="list-style-type: none"> <li>– The status of a supply voltage has changed (<a href="#">see on page 16 “System”</a>).</li> <li>– The status of the signal contact (<a href="#">see on page 176 “Signal contact”</a>) has changed. To take this event into account, you activate “Create trap when status changes” in the <code>Diagnostics:Signal Contact</code> dialog (<a href="#">see on page 176 “Signal contact”</a>).</li> <li>– The device status has changed. To take this event into account, you activate “Create trap when status changes” in the dialog “<a href="#">Device Status</a>”.</li> <li>– If the SNTP function is active: the synchronization with the SNTP server (<a href="#">see on page 77 “SNTP configuration”</a>) was created or interrupted.</li> <li>– If the NTP function is active: the synchronization with the NTP server (<a href="#">see on page 80 “NTP Configuration”</a>) was created or interrupted.</li> <li>– The AutoConfiguration Adapter, ACA, has been added or removed.</li> <li>– The temperature threshold has been exceeded/not reached.</li> </ul>
Cold Start	The device has been powered on and can be managed.
Link Status	At one port of the device, the link to a device connected there has been established/interrupted.
Redundancy	If router redundancy is active: the router redundancy status (master router/backup router) ( <a href="#">see on page 155 “Router Redundancy”</a> ) of the device has changed.
Firewall	A user ( <a href="#">see on page 64 “User Firewall Accounts”</a> ) of the firewall ( <a href="#">see on page 128 “User Firewall”</a> ) has logged in, logged off, or the login has been unsuccessful.
VPN	A VPN connection was created or interrupted.

*Table 80: Trap categories*

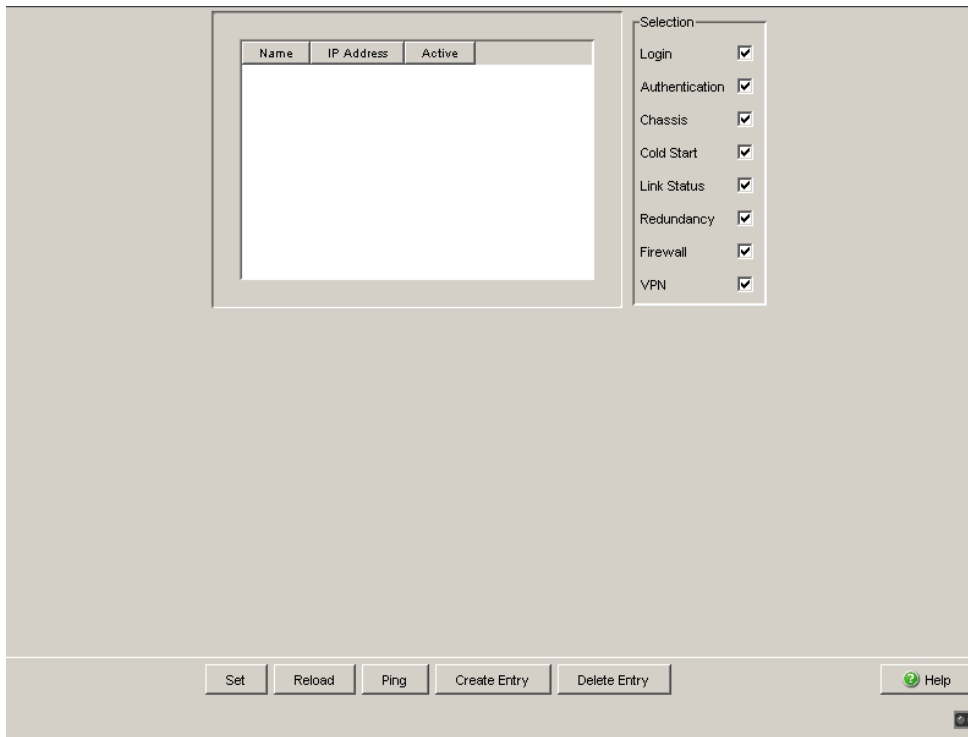


Figure 36: Alarms (Traps) Dialog

## 7.7 Report

The following reports are available for the diagnostics:

- ▶ System Information

### 7.7.1 System Information

The system information is a HTML file containing the relevant data about the system.

## System Information

### Hirschmann EAGLE Security Device

System software: EAGLEONE ONE-05.3.00-B05 2013-10-21 16:58 RAM: ONE-05.3.00-B05 2013-10-21 16:58 BAK: ONE-05.3.00-B04 2013-10-15 11:54

Network operation mode: **Transparent Mode**

Network management interface IP address: 10.115.47.16 MAC address: ec:e5:55:f5:f3:2d

System name: EAGLEONE-F5F32D

System uptime: 0 days 8 hours 3 minutes 28 seconds

System operating hours: 116 days 19 hours 4 minutes 5 seconds

System local time: 2013-10-22 16:06:07

Hardware description: **EagleOne**

Hardware serial number: 016

Hardware revision: 0512

CPLD code revision: 0002

EEPROM information: SW=0x07, HW=0x13

Power supply 1: **OK**

Power supply 2: **Failed**

Temperature: 56 °C

ACAsatus: **Removed**

#### Task list of all tasks with current task information

Taskname	Status	Task ID	Observed	Can terminate	Priority	Err. No	Delay	Stack size in bytes	In use	Maximum	Minimum remain
tCli	PEND+T	0x2102188	yes	yes	110	0x003D0004	63	65536	688	3680	61856
ipssh_10.115.35.68_10911	PEND+T	0x2100210	yes	yes	130	0x00000046	1436845	24576	720	2944	21632

Figure 37: System Information Dialog

- Click on “Show System Info”. The device displays the system information as a HTML file.
- Click on
  - ▶ “Back” to return to the system information window.
  - ▶ “Reload” to update the display.
  - ▶ “Search...” to search the system information file for a keyword or a regular expression.
  - ▶ “Save...” if you need the system information as an external file. In the file selection window, select the desired directory, enter a name for the file, and click on “Save”.



## 7.8 MAC Firewall List

The MAC Firewall List shows the rules created by the user, together with the implicit rules of the Layer 2 (MAC) Firewall entered by the system. This list can help you to understand event log entries, and it enhances your overview of the Firewall configuration.

Parameter	Meaning	Possible Values
Index	Sequential line index	-
Rule Group	Internal classification of the rules	- Default Rules - Miscellaneous - Rate Limits (DoS) - Special Traffic
Reference	Internal information for the service technician.	
Interface	Interface to which this rule applies.	- any = all - egress = device-specific data - external = external port - internal = internal port - mirror = bridge interface in Transparent Mode.
Source Address	MAC address of the actual source of the data packet. Entry format: 11:22:33:44:55:66 Entering "?" enables wildcards to be used. Example: 1?:22:?:?:44:55:6?.	
Destination Address	MAC address of the actual destination of the data packet. Entry format: 11:22:33:44:55:66 Entering "?" enables wildcards to be used. Example: 1?:22:?:?:44:55:6?.	
Protocol	Protocol in the type field of the MAC data packet.	
Action	Action that the Firewall performs if the rule applies.	accept, drop

*Table 81: MAC Firewall List*

---

Parameter	Meaning	Possible Values
Log	Entry in the event list if the rule applies.	Yes, No
Match Count	Counter that records how often the rule has already applied	0 - 4,294,967,295 ( $2^{32} - 1$ )

*Table 81: MAC Firewall List*

## 7.9 IP Firewall List

The IP Firewall List shows the rules created by the user, together with the implicit rules of the Layer 3 (IP) Firewall entered by the system. This list can help you to understand event log entries, and it enhances your overview of the Firewall configuration.

Parameter	Meaning	Possible Values
Index	Sequential line index	
Rule Group	Internal classification of the rules	<ul style="list-style-type: none"> <li>- Special Traffic</li> <li>- Miscellaneous</li> <li>- Rate Limits</li> <li>- VPN</li> <li>- HTTPS Access</li> <li>- SSH Access</li> <li>- SNMP Access</li> <li>- PPP Packet Filter</li> <li>- Packet Filter IP Outgoing</li> <li>- Packet Filter IP Incoming</li> <li>- Default Rules</li> </ul>
Reference	Internal information for the service technician.	
Interface	Interface to which this rule applies.	<ul style="list-style-type: none"> <li>- any = all</li> <li>- egress = device-specific data</li> <li>- external = external port</li> <li>- internal = internal port</li> <li>- mirror = bridge interface in Transparent Mode.</li> <li>- loopback</li> <li>- ppp (serial) = V.24 port</li> </ul>
Source Network	IP Address with Netmask (CIDR) of the actual source of the data packet.	IP Address with Netmask, any = all, me = own IP address
Source Port	Logical source port of the data packet.	any = all op port port 1 op port 2
Destination Network	IP Address with Netmask (CIDR) of the actual destination of the data packet.	IP Address with Netmask, any = all, me = own IP address

*Table 82: IP Firewall List*

Parameter	Meaning	Possible Values
Destination Port	Logical destination port of the data packet	any = all op port port 1 op port 2
Protocol	IP protocol	any = all, tcp, udp, icmp
Action	Action that the Firewall performs if the rule applies.	accept, drop, reject
Log	Entry in the event list if the rule applies.	Yes, No
Match Count	Counter that records how often the rule has already applied	0 - 4,294,967,295 ( $2^{32} - 1$ )

*Table 82: IP Firewall List*

## 7.10 Configuration Check

The device enables you to compare its configuration with those of its neighboring devices.


For this purpose, it uses the data that it received from its neighboring devices via topology recognition (LLDP).

The dialog lists the deviations detected, which affect the performance of the communication between the device and the recognized neighboring devices.

- You update the table's content via the "Reload" button. If the table remains empty, the configuration check was successful and the device's configuration is compatible for the recognized neighboring devices.

**Note:** A neighboring device without LLDP support, which forwards LLDP packets, may be the cause of equivocal messages in the dialog. This occurs if the neighboring device is a hub or a switch without management, which ignores the IEEE 802.1D-2004 standard.

In this case, the dialog displays the devices recognized and connected to the neighboring device as connected to the switch port, even though they are connected to the neighboring device.

Port	Neighbour System ...	Neighbour IP Address	Neighbour Port	Neighbour Type	Status	Reason
1	RS-1F1054	10.0.1.13	Unit: 1 Slot: 1 Port: 1...	BRIDGE		

Select a neighbour device from the table.


Reload  Help

Figure 38: Configuration Check

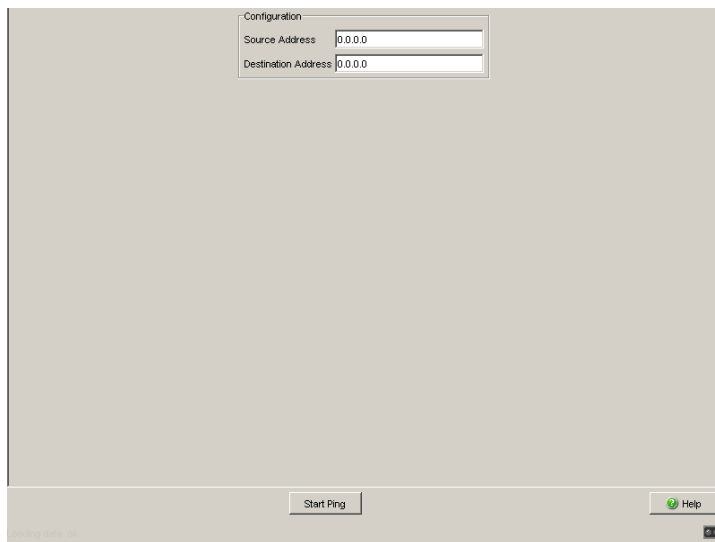
Parameter	Meaning
Port	Port to which this entry applies.
Neighbour System Name	System name of the neighboring device ( <a href="#">see on page 17 “System Data”</a> )
Neighbour IP Address	IP address of the neighboring device with LLDP function ( <a href="#">see on page 20 “Network”</a> )
Neighbour Port	Displays information on the neighboring device.
Neighbour Type	Displays the type of the neighboring device. Written in <ul style="list-style-type: none"> <li>– Capital letters: The device has this function, and the function is activated.</li> <li>– Lower-case letters: The device has this function, and the function is deactivated.</li> </ul>
Status	Displays the configuration status <ul style="list-style-type: none"> <li>– Green circle with checkmark: The configuration of this device and the configuration of the neighboring device are compatible. Communication between the two devices is okay.</li> <li>– Yellow triangle: The configuration of this device and the configuration of the neighboring device do not match. The performance of the communication between the two devices could be endangered. Select this row to obtain further information in the window below.</li> <li>– Red square with X: The configuration of this device and the configuration of the neighboring device are not compatible. Communication between the two devices is endangered. Select this row to obtain further information in the window below.</li> <li>– Blue circle with question mark: Configuration data is not available for the neighboring device. Select this row to obtain further information in the window below.</li> </ul>
Reason	If a reason is entered in a row, selecting this row displays more detailed information on this reason in the window below.

*Table 83: Configuration Check table*

## 7.11 Reachability Test (Ping)

This dialog allows you to perform a reachability test (ping) for any IP address directly from the device.

For special cases, such as a reachability test through a VPN tunnel, you can specify the source address of the pings manually.



*Figure 39: Ping dialog (reachability test)*



Parameter	Meaning	Possible Values
Source Address	<p>Sending address for the ICMP Echo requests (pings), normally 0.0.0.0.</p> <p>When the source address is 0.0.0.0, the Firewall uses the IP address of the interface at which the pings are sent. The Firewall determines the interface from the destination address and the routing table.</p> <p>For special cases (e.g. to help ensure that the reachability test uses a specific VPN tunnel), use a different IP address.</p> <p>State on delivery: 0.0.0.0</p>	IPv4 address, normally 0.0.0.0
Destination Address	<p>Destination address for the ICMP Echo requests (pings). State on delivery: 0.0.0.0</p>	Any IPv4 address to be tested, not 0.0.0.0
Start Ping	Click "Start Ping" to start the reachability test. After some seconds, the device displays the result as a text in a new dialog window.	-

*Table 84: Ping dialog table*



## 8 Advanced

The Advanced menu contains the dialogs:

- ▶ DNS
- ▶ Packet Forwarding
- ▶ DHCP Relay Agent
- ▶ DHCP Server

## 8.1 DNS

The Domain Name System (DNS) allows names (e.g. www.example.de) to be used on the Internet instead of IP addresses. When entering host names, e.g. to create a connection with a remote terminal, a device (e.g. a PC) starts a DNS request on one or more DNS servers for the related IP address (name resolution). The DNS server that knows the requested name resolution passes the related IP address to the requesting device (DNS client). The DNS servers can be reached via the Internet service provider, or they can be installed in the local network.

The EAGLE One device provides you with a DNS cache function. It saves the result of the name resolution for a specific period - the maximum period is until a restart - in the temporary memory (cache). Thus the EAGLE One device can reply to additional DNS requests for which the result is already stored in the cache, without requiring a repeat DNS request at a DNS server. This reduces the workload of the responsible DNS server, and you receive the reply faster.

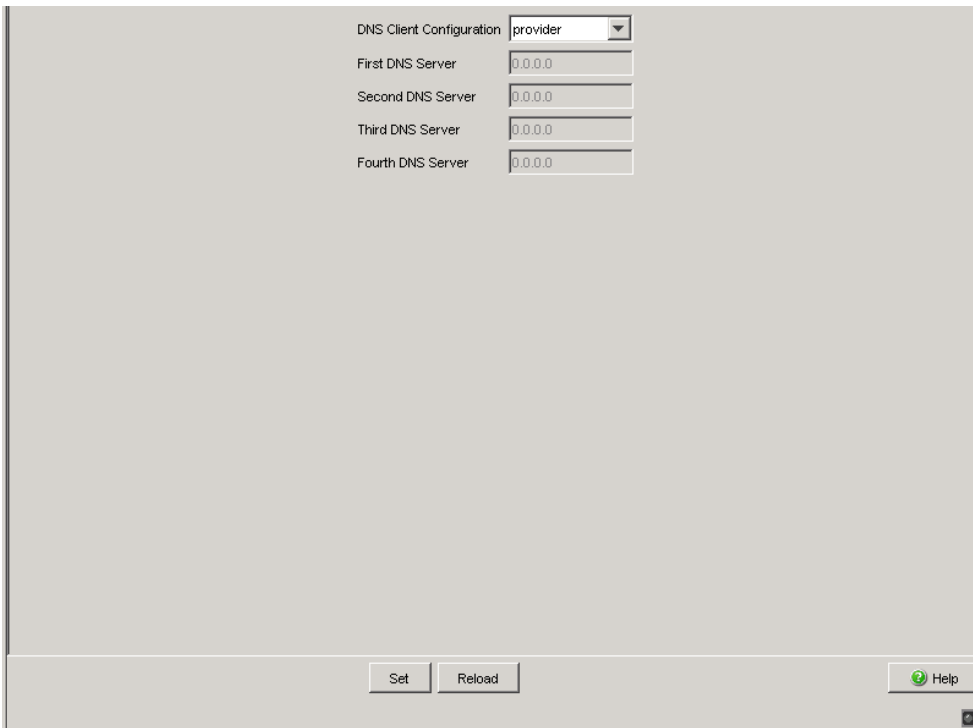
A DynDNS service enables you to have a name (DynDNS host name) registered there, by means of which a device (e.g. PC for administering the Firewall) can also determine dynamically allocated IP addresses.

### 8.1.1 DNS Server

This dialog allows you to enter one or more DNS servers on which the device searches for a name resolution. Thus, when a device is setting up a connection to a remote terminal via a host name (e.g. VPN gateway), the device can determine the related IP address for this host name as a DNS client.

In the “DNS Client Configuration” field, select the DNS server which the device accesses for a name resolution.

- ▶ **Provider:** The DNS client of the device sends DNS requests to the DNS servers that were allocated to the device by the Internet service provider (e.g. via DHCP Client or PPPoE).
- ▶ **User:** The DNS client of the device sends DNS requests to the DNS (root) servers entered in the four fields by the user, in the sequence of the entries. If a DNS (root) server is not available, then entering more than one DNS (root) server enables the device to switch to another DNS (root) server. In user mode, the device ignores the DNS servers allocated by an Internet service provider.



DNS Client Configuration provider

First DNS Server 0.0.0.0

Second DNS Server 0.0.0.0

Third DNS Server 0.0.0.0

Fourth DNS Server 0.0.0.0

Set Reload Help

Figure 40: DNS server

## 8.1.2 DynDNS

Register with the DynDNS service before using the DynDNS function. The device allows you to register on the [www.DynDNS.org](http://www.DynDNS.org) website or on another website of your choice:

This dialog allows you to enter the registration data from this registration at the DynDNS service. Via the registered host name, the device can also be accessed via the Internet under this name in the case of dynamically allocated IP addresses (in PPPoE mode).

Parameter	Meaning
Provider	Select the website of the DynDNS provider: – dyndns-org: website <a href="http://www.DynDNS.org">www.DynDNS.org</a> – other: your choice for another DynDNS provider  If you reset the provider from “other” to “dyndns-org”, the device resets the settings for “Server” and “CheckIP Server” to the default settings of DynDNS.org.
Register	Checkmarked: The DynDNS service is activated. At the intervals entered under “Refresh”, the device checks its IP address, and if this changes it passes the new address to the DynDNS service for registration. Not checkmarked: The DynDNS service is deactivated.
Server	Enter the DNS server. Use the default settings of the DynDNS provider you have selected under “Provider”. Default setting: DNS server “members.dyndns.org” proposed by DynDNS.org.
CheckIP Server	Enter the CheckIP server for checking the IP address of a device. Use the default settings of the DynDNS provider you have selected under “Provider”. Default setting: CheckIP server “checkip.dyndns.org” proposed by DynDNS.org.
Login	Enter the login name from the registration at the DynDNS provider selected by you, e.g. at DynDNS.org.
Password	Enter the password from the registration at the DynDNS provider selected by you, e.g. at DynDNS.org.
Hostname	Enter the host name from the registration at the DynDNS provider selected by you, e.g. at DynDNS.org.
Refresh	Refresh interval in minutes. Possible values: 1-6000, default setting 10.
Status	Display the status of the DynDNS client, ( <a href="#">see on page 199 “DynDNS - Status of DynDNS Client”</a> )

Table 85: DynDNS

Possible Values	Meaning
Inactive	DynDNS is not active (e.g. "Register" is not selected, DNS server ( <a href="#">see on page 196 "DNS Server"</a> ) is not configured).
No change / in progress	DynDNS is active and checks whether the IP address has changed, and thus whether the device has to refresh the IP address stored in the DynDNS service.
Good / update done	The device has successfully updated the IP address stored in the DynDNS service.
Bad user / bad password	The DNS server of the DynDNS service has rejected the login of the user (login and/or password incorrect).
No such host in system	The DynDNS service does not recognize the host name entered.
Invalid hostname format	The host name entered does not have a valid format (FQDN = Fully Qualified Domain Name).
Host not in this account	The host name entered is not known for this DynDNS account (the host name does not belong to this user).
No change	The DynDNS service has registered the same host name/IP address pair twice.
Host has been blocked	The DynDNS service has registered the same host name/IP address pair multiple times (the entry on the DynDNS service was thus blocked).

*Table 86: DynDNS - Status of DynDNS Client*

The screenshot displays a configuration window for DynDNS. It contains the following fields and controls:

- Configuration:**
  - Provider: dropdown menu set to "dyndns-org"
  - Register: checkbox (unchecked)
  - Server: text input field containing "members.dyndns.org"
  - CheckIP Server: text input field containing "checkip.dyndns.org"
  - Login: text input field containing "test"
  - Password: text input field containing "\*\*\*\*\*"
  - Hostname: text input field containing "test.dyndns.org"
  - Refresh [min]: text input field containing "10"
- Information:**
  - Status: text input field containing "inactive"

At the bottom of the window, there are three buttons: "Set", "Reload", and "Help" (with a green question mark icon). A small status indicator at the bottom left reads "Loading data, ok".

*Figure 41: DynDNS*

## 8.2 Packet Forwarding

This dialog allows you to activate and deactivate the forwarding of RSTP, GMRP and DHCP data packets in the Transparent Mode ([see on page 22 “Transparent Mode”](#)).

If packet forwarding is activated, then the device is transparent for these packets.

In Router mode, these setting have no effect, because the device does not forward any packets on layer 2 in Router mode.

Parameter	Meaning	Default setting
RSTP	Activate/deactivate the forwarding of Rapid Spanning Tree Protocol (RSTP) data packets. The RSTP enables redundancy by interrupting loops in multiple, redundant connections between subnetworks.	On
GMRP	Activate/deactivate the forwarding of GMRP data packets. The GMRP (GARP Multicast Registration Protocol) controls the forwarding of multicasts. The network load is reduced by the device only forwarding the multicasts to the devices registered using GMRP.	Off
DHCP	Activate/deactivate the forwarding of DHCP data packets. Devices with DHCP as the configuration mode get their configuration data from a DHCP server. Thus they can be very easily incorporated or replaced.	Off

*Table 87: Packet Forwarding*

**Note:** Forwarding of DHCP data packets only works in Transparent mode. If you are operating the device in Router mode, the device allows you to enable DHCP traffic via the DHCP relay ([see on page 202 “DHCP Relay Agent”](#)).



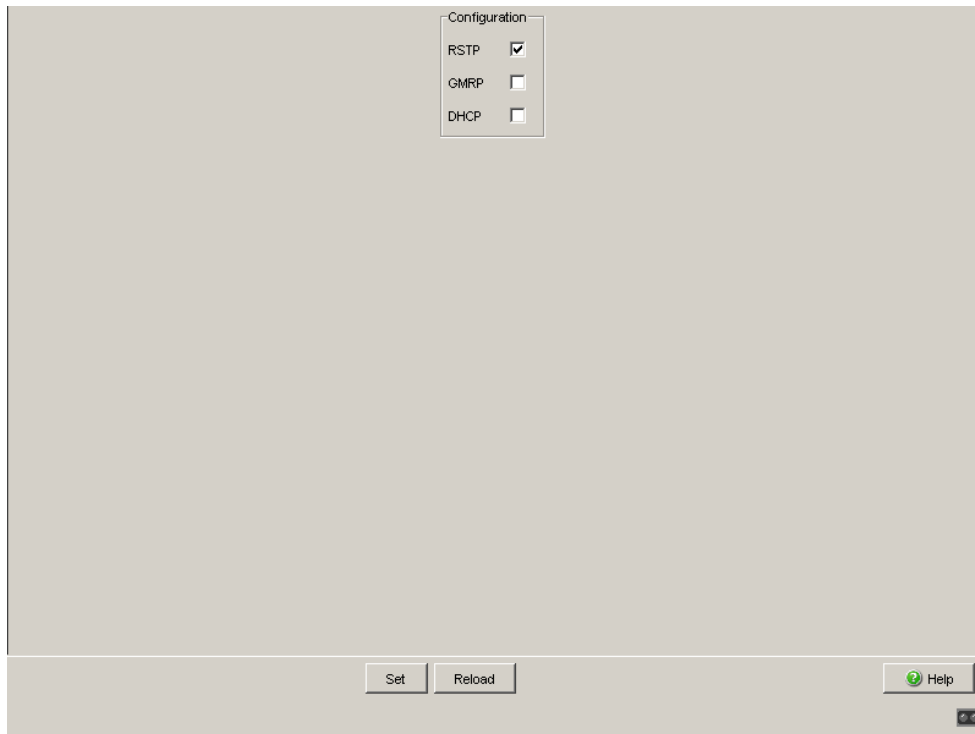


Figure 42: Packet Forwarding

## 8.3 DHCP Relay Agent

This dialog allows you to configure the DHCP relay agent.

**Note:** The DHCP relay agent only works in router mode. If you are running the device in transparent mode, you can enable DHCP traffic via the “Packet forwarding” setting ([see on page 200 “Packet Forwarding”](#)).

**Note:** The DHCP relay agent enters the IP address for the interface at which the packet was received as the source address when forwarding DHCP packets to the server. Enter a route for this interface address in the configuration of your DHCP server to help assuring communication.

- Enter the DHCP server IP address.  
If one DHCP server is not available, you can enter up to three additional DHCP server IP addresses so that the device can change to another DHCP server.

Parameter	Meaning
Server IP address	Enter the DHCP server IP address. If one DHCP server is not available, then you can enter up to three additional DHCP server IP addresses, so that the device can change to another DHCP server.
DHCP Relay Status	Display the DHCP relay status. The DHCP relay function is active if <ul style="list-style-type: none"> <li>– at least one IP address is entered in “Server IP Address” and</li> <li>– the DHCP server (<a href="#">see on page 206 “Pool”</a>) is not active on either of the two interfaces.</li> </ul>
Hirschmann Device	Checkmark the interfaces to which a Hirschmann device is connected. You thus help ensure that the DHCP server allocates the same IP address to a replacement Hirschmann device. <b>Note:</b> Because the Firewall is a security device, it only supports standard DHCP. For this reason, do not checkmark the interfaces to which an EAGLE One is connected.

*Table 88: DHCP Relay Agent*

Port	Hirschmann Device
internal (Port 1)	<input type="checkbox"/>
external (Port 2)	<input type="checkbox"/>

Figure 43: DHCP Relay Agent dialog

**Note:** In the Enhanced:Packet Forwarding dialog (see page 200), deactivate the forwarding of DHCP packets.

## 8.4 DHCP Server

The DHCP Server dialogs allow you to very easily include new devices (clients) in your network or exchange them in your network: When you select DHCP as the configuration mode for the client, the client gets the configuration data from the DHCP server.

The DHCP server assigns to the client:

- a fixed IP address (static) or an address from an address range (dynamic),
- the netmask,
- the gateway address,
- the DNS server address,
- the WINS server address and
- the lease time.

You can also specify for each port a URL for transferring additional configuration parameters to the client.

## 8.4.1 Pool

This dialog allows you to closely control the allocation of IP addresses. You can activate or deactivate the DHCP server for each port or for each VLAN. For this purpose, the DHCP server provides what is known as an IP address pool (in short “pool”) from which it allocates IP addresses to clients. The pool consists of a list of entries. An entry can define a specific IP address or a connected IP address range.

You can choose between dynamic and static allocation.

► An entry for dynamic allocation applies to the port of the device for which you activate the DHCP server. If a client makes contact at this port, the DHCP server allocates a free IP address from the pool entry for this port. For dynamic allocation, create a pool entry for a port and enter the first and last IP addresses for the IP address range. Leave the MAC Address, Client ID, Remote ID and Circuit ID fields empty. You have the option to create 1 pool entry for each port.

► With static allocation, the DHCP server each time allocates the same IP address to a client. The DHCP server identifies the client using a unique hardware ID.

A static address entry can only contain 1 IP address and applies to the related port of the device.

For static allocation, create a pool entry for the port, enter the IP address, and leave the “Last IP Address” field empty. Enter a hardware ID with which the DHCP server uniquely identifies the client. This ID can be a MAC address, a client ID, a remote ID or a circuit ID. If a client makes contact with a known hardware ID, the DHCP server allocates the static IP address.

The table shows you the configured entries of the DHCP server pool. You have the option to create a new entry, edit an existing entry or delete entries. You have the option to create 1 pool entry for each port of the device. The pools can contain up to 64 entries altogether.

Click “Create entry” to create a new entry. The device displays a new dialog. Fill in the fields you require, then click “Write”. Click on “Back” to return to the “Pool” dialog.

Parameter	Meaning	Value range	Default setting
Port	Port to which this entry applies.	internal (port 1), external (port 2)	internal (port 1)
Active	Activates or deactivates the pool entry.	On, Off	Off
IP Address	<ul style="list-style-type: none"> <li>▶ For a dynamic address entry: the 1st address of the IP address pool that the DHCP server allocates to a client.</li> <li>▶ For a static address entry: the IP address that the server each time allocates to the same client.</li> </ul>	Valid IPv4 address	-
Last IP Address	For a dynamic address entry: the last address of the IP address pool that the DHCP server allocates to a client.	Valid IPv4 address	-

*Table 89: DHCP server pool settings, IP address basic settings*

Parameter	Meaning	Value range	Default setting
Lease time [s]	Time in s for which the DHCP server allocates the address to the client. Within the lease time, the client can apply for an extension. If the client does not apply for an extension, after it has elapsed the DHCP server takes the IP address back into the pool and allocates it to any client that requires it.	1 s - 4294967295 s ( $2^{32}-1$ s)	86400 s (1 day)
MAC Address	For a static address entry: MAC address with which the client identifies itself.	MAC address of the client that contains the static IP address	-
Gateway	IP address of the DHCP relay via which the client makes its request. If the DHCP server receives a request via another DHCP relay, it ignores this. If there is no DHCP relay between the client and the DHCP server, leave these fields empty.	IPv4 address of the DHCP relay.	-
Client ID	For a static address entry: Client ID with which the client identifies itself.	Client ID of the client that contains the static IP address <sup>a</sup>	-
Remote ID	For a static address entry: Remote ID with which the client identifies itself.	Remote ID of the client that contains the static IP address <sup>a</sup>	-

Table 90: DHCP server pool settings, mode of address allocation



Parameter	Meaning	Value range	Default setting
Circuit ID	For a static address entry: Circuit ID with which the client identifies itself.	Circuit ID of the client that contains the static IP address <sup>a</sup>	-
Hirschmann Device	Checkmark the rows in which a Hirschmann device is entered as a client. You thus help ensure that the DHCP server allocates the same IP address to a replacement Hirschmann device. <b>Note:</b> Because an EAGLE One device is a security device, it only supports standard DHCP. For this reason, do not checkmark the rows in which an EAGLE One device is entered. <b>Note:</b> When replacing a client device, change the MAC address to that of the new client.	On, Off	Off

*Table 90: DHCP server pool settings, mode of address allocation*

- <sup>a</sup> A client, remote or circuit ID consists of 1 - 255 bytes in hexadecimal form (00 - ff), separated by spaces.

Parameter	Meaning	Value range	Default setting
Configuration URL	TFTP URL, from which the client can obtain additional configuration information. Enter the URL in the form <code>tftp://server name or ip address/directory/file</code> .	Valid TFTP URL	-
Default gateway	Default gateway entry for the client.	Valid IPv4 address	-
Netmask	Netmask entry for the client.	Valid IPv4 netmask	-
WINS Server	WINS (Windows Internet Name Service) entry for the client.	Valid IPv4 address	-
DNS Server	DNS server entry for the client.	Valid IPv4 address	-
Hostname	Host name for the client. If this name is entered, it overwrites the system name of the client (see on page 17 “System Data”).	Max. 64 ASCII characters in the range 0x21 (!) - 0x7e (~).	- (no host name)

Table 91: DHCP server pool settings, option allocation to the client

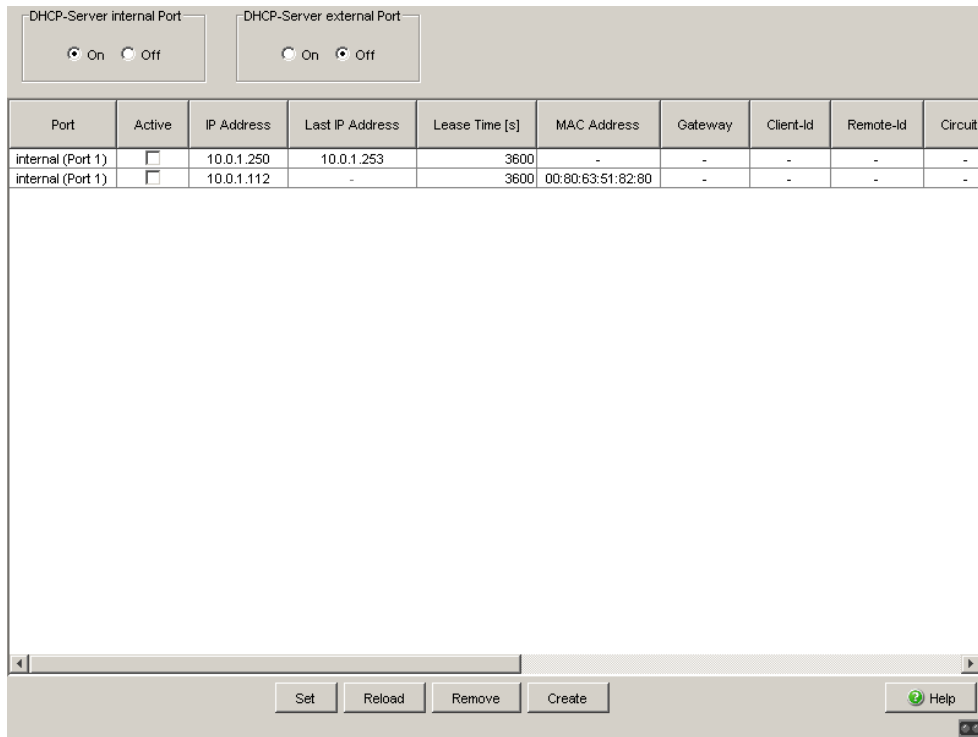


Figure 44: DHCP Server Pool per Port dialog

## 8.4.2 Lease Table

The lease table shows you the IP addresses that the DHCP server has currently allocated.

The device displays the related details for every IP address allocated.

The device allows you to allocate up to 1,024 addresses.

Parameter	Meaning	Value range
Port	Port to which this entry applies.	internal (port 1), external (port 2)
IP address	IP address that the DHCP server has allocated to the device with the specified MAC address.	An IPv4 address from the pool.
Status	Status of the DHCP address allocation according to the Dynamic Host Configuration Protocol.	bootp, offering, requesting, bound, renewing, rebinding, declined, released
Remaining Lifetime [s]	Time remaining in seconds until the validity of the IP address elapses, unless the client applies for an extension.	-
Leased MAC Address	MAC address of the client that is currently leasing the IP address.	Format xx:xx:xx:xx:xx
Gateway	IP address of the DHCP relay via which the client has made the request.	IPv4 address or empty
Local (client) ID	The client ID that the client submitted for the DHCP request.	<sup>a</sup>
Remote ID	The remote ID that the client submitted for the DHCP request.	<sup>a</sup>
Circuit ID	The circuit ID that the client submitted for the DHCP request.	<sup>a</sup>

*Table 92: DHCP lease table*

- <sup>a</sup> A client, remote or circuit ID consists of 1 - 255 bytes in hexadecimal form (00 - ff), separated by spaces.

---

Port	IP Address	Status	Remaining Lifetime	Leased MAC Address	Gateway	Client ID	Remote ID	Circuit ID
------	------------	--------	--------------------	--------------------	---------	-----------	-----------	------------

Reload Help

Figure 45: DHCP Server Lease Table dialog



## 9 Logout

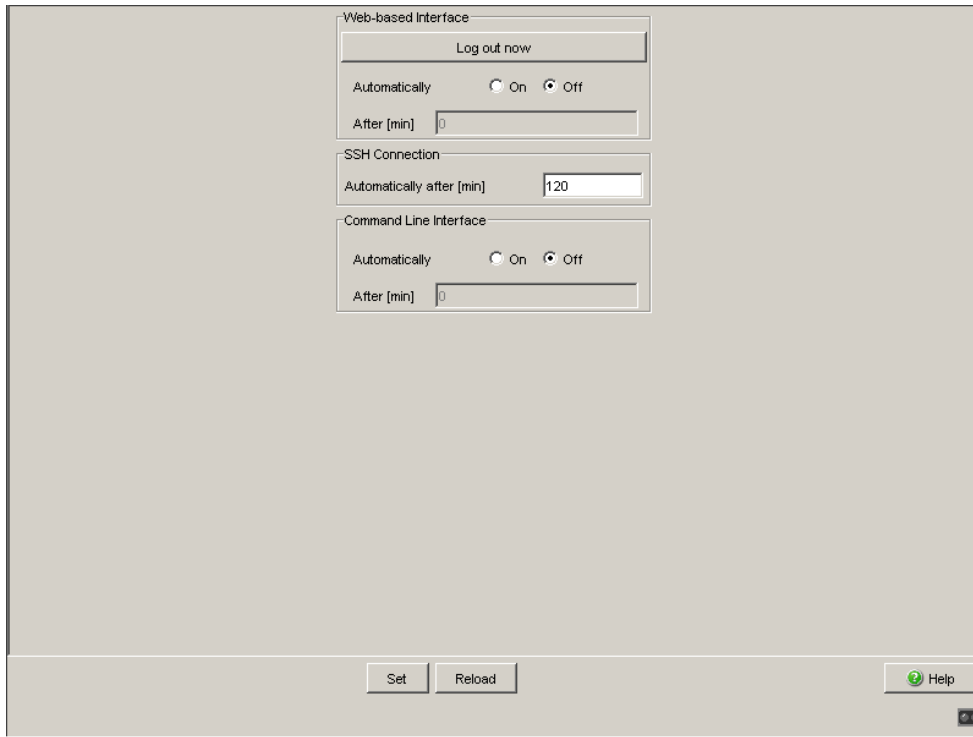
This dialog allows you to configure automatic logging out for the various user interfaces. In addition, you can also log out from the graphical user interface immediately.

- ▶ Graphical user interface: activate/deactivate the automatic logging out and set the time period for automatic logging out. Also immediate logging out from the graphical user interface.
- ▶ SSH connection: time period for automatic logging out.
- ▶ Command Line Interface (V.24): activate/deactivate the automatic logging out and set the time period for automatic logging out.

Parameter	Meaning	Possible Values	Default Setting
<b>Graphical user interface</b>			
Log out now	Immediate logout by clicking on "Log out now".		
Automatically	Switch the automatic logout function on/off.	On/Off	On
After [min]	Enter the time in minutes after which the device ends the connection if you have not made any entries.	0-120 (0: Off)	5 (On)
<b>SSH Connection</b>			
Automatically after [min]	Enter the time in minutes after which the device ends the connection if you have not made any entries.	1-120	5
<b>Command Line Interface</b>			
Automatically	Switch the automatic logout function on/off.	On/Off	On
After [min]	Enter the time in minutes after which the device ends the connection if you have not made any entries.	0-120 (0: Off)	5 (On)

Table 93: Logout

**Note:** To get access to the device via the graphical user interface again after a logout, restart the graphical user interface to login.



*Figure 46: Logout*



# **A General Information**

## A.1 List of RFCs

RFC 768	UDP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1769	SNTP
RFC 1867	Form-Based File Upload in HTML
RFC 1901	Community based SNMP v2
RFC 1905	Protocol Operations for SNMP v2
RFC 1906	Transport Mappings for SNMP v2
RFC 1907	Management Information Base for SNMP v2
RFC 1908	Coexistence between SNMP v1 and SNMP v2
RFC 1918	Address Allocation for Private Internets
RFC 1945	HTTP/1.0
RFC 2068	HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03
RFC 2131	DHCP
RFC 2132	DHCP-Options
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2271	SNMP Framework MIB
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 24xx	IPsec, IKEv1 - there are several RFCs that apply to IPsec, IKEv1
RFC 2570	Introduction to SNMP v3
RFC 2571	Architecture for Describing SNMP Management Frameworks
RFC 2572	Message Processing and Dispatching for SNMP
RFC 2573	SNMP v3 Applications
RFC 2574	User Based Security Model for SNMP v3
RFC 2575	View Based Access Control Model for SNMP
RFC 2576	Coexistence between SNMP v1, v2 & v3
RFC 2578	SMIv2
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance statements for SMI v2
RFC 2618	RADIUS Authentication Client MIB
RFC 2663	IP Network Address Translator (NAT) Terminology and Considerations
RFC 2818	HTTP over TLS

---

RFC 2851	Internet Addresses MIB
RFC 2865	RADIUS Client
RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 2869	RADIUS Extensions
RFC 3022	Traditional IP Network Address Translator
RFC 3164	The BSD syslog Protocol
RFC 3947	Negotiation of NAT-Traversal in the IKE
RFC 3948	UDP Encapsulation of IPsec ESP Packets
RFC 43xx	IPsec, IKEv2 - there are several RFCs that apply to IPsec, IKEv2
RFC 5905	NTPv4

## A.2 Underlying IEEE Standards

IEEE 802.1AB	Link aggregation
IEEE 802.1D	Switching, GARP, GMRP, Spanning Tree (the device supports packet forwarding only)
IEEE 802.1D-1998, IEEE 802.1D-2004	Media access control (MAC) bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering, GARP, GMRP)
IEEE 802.3-2002	Ethernet
IEEE 802.3ac	VLAN Tagging

## A.3 Technical Data

### VLAN

VLAN ID	1 to 4094
---------	-----------

### Routing/Switching

Number of additional IP addresses	32
Maximum number of static routing entries	64

### Firewall

Maximum number of IP rules (in total)	1024
Maximum number of MAC rules (in total)	256
Maximum number of SPI (Stateful Packet Inspection) entries	4096

### NAT

Maximum number of NAT rules	up to 512, depending on NAT type
Maximum number of 1:1 NAT address translation entries (mapping table)	4096 (adjustable), default setting: 1024

### VPN

Maximum number of configurable connections	256
Maximum number simultaneously active connections	64

### DHCP Server

Maximum number of configurable IP addresses that can be leased out	1024
Lease Time	Configurable per pool entry, default 86,400 s (1 day)

## A.4 Maintenance

Hirschmann is continually working to improve and develop our software. You should regularly check whether there is a new version of the software that provides you with additional benefits. You will find software information and downloads on the product pages of the Hirschmann website.

### A.4.1 Service-Shell

A service technician uses the Service Shell function for maintenance of your functioning device. If you need service support, this function allows the service technician to access internal functions of your device from an external location.

**Note:** The Service Shell function is for service purposes exclusively. This function allows the access on internal functions of the device. In no case, execute internal functions without service technician instructions. Executing internal functions such as deleting the content of the NVM (non-volatile memory) possibly leads to inoperability of your device.

**Note:** Disabling the Service Shell function produces a permanent effect. To reactivate the Service Shell function, send the device back to the manufacturer.

## **A.5 Copyright of Integrated Software**

### **A.5.1 Bouncy Castle Crypto APIs (Java)**

The Legion Of The Bouncy Castle  
Copyright (c) 2000 - 2004 The Legion Of The Bouncy Castle  
(<http://www.bouncycastle.org>)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

---

## A.5.2 Network Time Protocol Version 4 Distribution

Copyright © David L. Mills 1992-2007

Permission to use, copy, modify, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty

The following individuals contributed in part to the Network Time Protocol Distribution Version 4 and are acknowledged as authors of this work.

- Mark Andrews <mark\_andrews@isc.org> Leitch atomic clock controller
- Bernd Altmeier <altmeier@atsoft.de> hopf Elektronik serial line and PCI-bus devices
- Viraj Bais <vbais@mailman1.intel.com> and Clayton Kirkwood <kirkwood@striderfm.intel.com> port to Windows NT 3.5
- Michael Barone <michael.barone@lmco.com> GPSVME fixes
- Jean-Francois Boudreault <Jean-Francois.Boudreault@viagenie.qc.ca>, IPv6 support
- Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
- Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT port. Clean up recvbuf and iosignal code into separate modules.
- Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
- Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver, Trimble PARSE support
- Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)
- Steve Clift <clift@ml.csiro.au> OMEGA clock driver
- Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration
- Sven Dietrich <sven\_dietrich@trimble.com> Palisade reference clock driver, NT adj. residuals, integrated Greg's Winnt port.
- John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
- Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port
- Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified in RFC-1119
- John Hay <jhay@@icomtek.csr.co.za> IPv6 support and testing
- Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver



- 
- Mike Iglesias <iglesias@uci.edu> DEC Alpha port
  - Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
  - Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
  - Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or <H.Lambermont@chello.nl> ntpswEEP
  - Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)
  - Frank Kardel <kardel (at) ntp (dot) org> PARSE <GENERIC> driver (>14 reference clocks), STREAMS modules for PARSE, support scripts, syslog cleanup, dynamic interface handling
  - William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications
  - Dave Katz <dkatz@cisco.com> RS/6000 AIX port
  - Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver
  - George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
  - Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
  - Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
  - Danny Mayer <mayer@ntp.org> Network I/O, Windows Port, Code Maintenance
  - David L. Mills <mills@udel.edu> Version 4 foundation: clock discipline, authentication, precision kernel; clock drivers: Spectracom, Austron, Arbiter, Heath, ATOM, ACTS, KSI/Odetics; audio clock drivers: CHU, WWV/H, IRIG
  - Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port
  - Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
  - Tom Moore <tmoore@fiemel.daytonoh.ncr.com> i386 svr4 port
  - Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
  - Derek Mulcahy <derek@toybox.demon.co.uk> and Damon Hart-Davis <d@hd.org> ARCRON MSF clock driver
  - Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling
  - Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
  - Wilfredo Sánchez <wsanchez@apple.com> added support for NetInfo
  - Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules
  - Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory
  - Ray Schnitzler <schnitz@unipress.com> Unixware1 port
  - Michael Shields <shields@tembel.org> USNO clock driver
  - Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver

- Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the ChangeLog)
- Kenneth Stone <ken@sdd.hp.com> HP-UX port
- Ajit Thyagarajan <ajit@ee.udel.edu> IP multicast/anycast support
- Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp> TRAK clock driver
- Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic TrueTime clock driver
- Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and validated HTML documents according to the HTML DTD

## B Readers' Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

	Very Good	Good	Satisfactory	Mediocre	Poor
Precise description	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Readability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Understandability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Examples	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Structure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Comprehensive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Graphics	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Drawings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tables	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Did you discover any errors in this manual?  
If so, on what page?

---



---



---



---



---



---



---



---

## Readers' Comments

---

Suggestions for improvement and additional information:

---

---

---

---

General comments:

---

---

---

---

Sender:

---

Company / Department:

---

Name / Telephone number:

---

Street:

---

Zip code / City:

---

E-mail:

---

Date / Signature:

---

Dear User,

Please fill out and return this page

- ▶ as a fax to the number +49 (0)7127/14-1600 or
- ▶ per mail to

Hirschmann Automation and Control GmbH  
Department 01RD-NT  
Stuttgarter Str. 45-51  
72654 Neckartenzlingen

# C Index

<b>1</b>			
1 to 1 NAT	120, 121	Firmware update	31
<b>A</b>		FLM	87
ACA	40, 42, 181	Function Monitoring	176, 176
Accept SNTP Broadcasts	78	<b>G</b>	
Access with Web-based interface, password	48	GMRP data packet	200
Address templates	86	Graphical User Interface (GUI)	11
Administration (login type)	13	Group Authentication	128
Advanced menu	195	<b>H</b>	
Alarm	180	HDX mode	18
Anforderungsintervall (SNTP)	81	HIPER-Ring	151
Asymmetrical firewall	85	HiView	11
Authentication	64, 139	HTTPS-Port	56
Authentication List	66	<b>I</b>	
Authentication list	64	ICMP Host Check	157
AutoConfiguration Adapter	40, 42, 181	IKE - Key Exchange	142
<b>C</b>		Industrial HiVision	7
Certificate	56	IPsec - Data Exchange	145
Certificates	140	IP address templates	86
CLI access, password	48	IP Firewall List	187
Configuration Check	189	IP Masquerading	120
<b>D</b>		IP Networks	147
Denial of Service	127	<b>L</b>	
Device Connection	134	Learn mode	87
Device Status	178	Level to report	163
DHCP data packet	200	LLDP	172, 189
DHCP Relay Agent	202, 202	Login Banner	71
DHCP Server (overview)	205	Login Type	13
DHCP server pool	206	Login window	12
DHCP server (lease table)	211	Logout	215
DNS	196	<b>M</b>	
DNS Server	196	MAC Firewall List	185
Domain Name Server	196	Manual setting	177
DoS	127	Modem interface	37
DynDNS	198	<b>N</b>	
<b>E</b>		NAT	119, 119
Event log	160	Network Address Translation	119, 119
Event settings	160, 163	Network Load	168
<b>F</b>		Network Management Station	172
FAQ	231	Network Security	83
Filter-ID=<groupname>	128	Non-volatile memory	41
Fingerprint	60	NTP	80
Firewall Learn Mode	87	NTP client	80
		NTP operation mode	80

NTP server	80	<b>T</b>	
NVM	41	Technical Questions	231
<b>P</b>		Temperature (device)	17
Packet Filter	84	Templates (IP addresses)	86, 86
Packet Forwarding	200	Terminal/CLI interface	36
Password	13, 48	Time	73
Password for access with Web-based interface	48	Timeout	128
Password for CLI access	48	Topology	172
Password for SNMPv3 access	48	Topology Recognition	189
Ports	168	Training Courses	231
Port configuration	33	Transparent Mode	22, 200
Port forwarding	124	Transparent Redundancy	151, 152
Port statistics table	169	Trap	180
PPPoE Mode	27	Trap configuration	178
<b>R</b>		<b>U</b>	
RADIUS Server	69	Universal Time Coordinated	80
Radius server	128	User Firewall	64, 128
Read access	13	User Firewall (login type)	13
Report	183	UTC	80
Request interval (SNTP)	78	<b>V</b>	
RFC	218	VPN	133
Router Mode	24	<b>W</b>	
Router Redundancy	155	Web Access	56
<b>S</b>		Write access	13
Serial Port	35		
Set	13		
SFTP access	60		
Signal Contact	176, 181		
SNMPv3 access, password	48		
SNMP Access	50		
SNMP access	54, 54		
SNMP logging	166		
SNMP port	50		
SNTP	77		
Software update	31		
SSH Access	60		
SSH Port	60		
STP data packet	200		
Starting the graphical user interface (GUI)	11		
Static routes	30		
Statistics table	169		
Supply voltage	181		
Symbol	9		
Syslog Server	162		
Syslog server	160		
System	16		
Systemzeit	81		
System Information	183		
System requirements (GUI)	11		
System time (taken from an SNTP server)	78		

## D Further Support

### ■ Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You will find the addresses of our partners on the Internet at <http://www.hirschmann.com>

Contact our support at <https://hirschmann-support.belden.eu.com>

You can contact us

in the EMEA region at

- ▶ Tel.: +49 (0)1805 14-1538
- ▶ E-mail: [hac.support@belden.com](mailto:hac.support@belden.com)

in the America region at

- ▶ Tel.: +1 (717) 217-2270
- ▶ E-mail: [inet-support.us@belden.com](mailto:inet-support.us@belden.com)

in the Asia-Pacific region at

- ▶ Tel.: +65 6854 9860
- ▶ E-mail: [inet-ap@belden.com](mailto:inet-ap@belden.com)

### ■ Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

- ▶ 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.

The current technology and product training courses can be found at <http://www.hicomcenter.com>

- ▶ 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