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.

© 2020 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.

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).

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety instructions</td>
<td>7</td>
</tr>
<tr>
<td>About this Manual</td>
<td>9</td>
</tr>
<tr>
<td>Key</td>
<td>10</td>
</tr>
<tr>
<td>Notes on the Graphical User Interface</td>
<td>11</td>
</tr>
<tr>
<td><strong>1 Basic Settings</strong></td>
<td></td>
</tr>
<tr>
<td>1.1 System</td>
<td>17</td>
</tr>
<tr>
<td>1.2 Network</td>
<td>21</td>
</tr>
<tr>
<td>1.2.1 Global</td>
<td>22</td>
</tr>
<tr>
<td>1.2.2 IPv4</td>
<td>24</td>
</tr>
<tr>
<td>1.3 Software</td>
<td>25</td>
</tr>
<tr>
<td>1.4 Load/Save</td>
<td>28</td>
</tr>
<tr>
<td>1.5 External Memory</td>
<td>38</td>
</tr>
<tr>
<td>1.6 Port</td>
<td>41</td>
</tr>
<tr>
<td>1.7 Restart</td>
<td>46</td>
</tr>
<tr>
<td><strong>2 Time</strong></td>
<td></td>
</tr>
<tr>
<td>2.1 Basic Settings</td>
<td>49</td>
</tr>
<tr>
<td>2.2 NTP</td>
<td>50</td>
</tr>
<tr>
<td>2.2.1 Global</td>
<td>51</td>
</tr>
<tr>
<td>2.2.2 Server</td>
<td>54</td>
</tr>
<tr>
<td><strong>3 Device Security</strong></td>
<td></td>
</tr>
<tr>
<td>3.1 User Management</td>
<td>57</td>
</tr>
<tr>
<td>3.2 Authentication List</td>
<td>62</td>
</tr>
<tr>
<td>3.3 LDAP</td>
<td>64</td>
</tr>
<tr>
<td>3.3.1 LDAP Configuration</td>
<td>65</td>
</tr>
<tr>
<td>3.3.2 LDAP Role Mapping</td>
<td>70</td>
</tr>
<tr>
<td>3.4 Management Access</td>
<td>72</td>
</tr>
<tr>
<td>3.4.1 Server</td>
<td>73</td>
</tr>
<tr>
<td>3.4.2 IP Access Restriction</td>
<td>85</td>
</tr>
<tr>
<td>3.4.3 Web</td>
<td>88</td>
</tr>
<tr>
<td>3.4.4 Command Line Interface</td>
<td>89</td>
</tr>
<tr>
<td>3.4.5 SNMPv1/v2 Community</td>
<td>92</td>
</tr>
<tr>
<td>3.5 Pre-login Banner</td>
<td>93</td>
</tr>
<tr>
<td><strong>4 Network Security</strong></td>
<td></td>
</tr>
<tr>
<td>4.1 Network Security Overview</td>
<td>95</td>
</tr>
<tr>
<td>4.2 RADIUS</td>
<td>96</td>
</tr>
<tr>
<td>4.2.1 RADIUS Global</td>
<td>98</td>
</tr>
<tr>
<td>4.2.2 RADIUS Authentication Server</td>
<td>99</td>
</tr>
<tr>
<td>4.2.3 RADIUS Authentication Statistics</td>
<td>101</td>
</tr>
<tr>
<td>4.3 Packet Filter</td>
<td>102</td>
</tr>
<tr>
<td>4.3.1 Routed Firewall Mode</td>
<td>103</td>
</tr>
<tr>
<td>4.3.1.1 Global</td>
<td>104</td>
</tr>
</tbody>
</table>
## Contents

4.3.1.2 Firewall Learning Mode .................................................. 106
4.3.1.3 Packet Filter Rule ......................................................... 113
4.3.1.4 Packet Filter Assignment ................................................. 118
4.3.1.5 Packet Filter Overview .................................................. 120
4.3.2.2 Packet Filter Rule ......................................................... 127
4.3.2.1 Packet Filter Global ..................................................... 125
4.3.2.3 Packet Filter Assignment ................................................. 133
4.4 Deep Packet Inspection ......................................................... 138
4.4.3 Deep Packet Inspection - DNP3 Enforcer ................................ 149
4.4.2 Deep Packet Inspection - OPC Enforcer ................................ 146
4.4.1 Deep Packet Inspection - Modbus Enforcer .............................. 139
4.5 DoS .......................................................... 176
4.5.1 DoS Global .......................................................... 177
4.5.2 Rate Limiter .......................................................... 176
4.5.3 DoS Global .......................................................... 177
6.5.1 VLAN Global .......................................................... 235
6.5.3 VLAN Port .......................................................... 238
6.4.2 QoS/Priority Port Configuration ........................................ 232
6.4.1 QoS/Priority Global ..................................................... 231
6.4 QoS/Priority .......................................................... 229
6.6 Intrusion Detection System .................................................... 180
5 Virtual Private Network ......................................................... 183
5.1 VPN Overview .......................................................... 183
5.2 VPN Certificates .......................................................... 192
5.3 VPN Connections .......................................................... 195
6.4.3 802.1D/p Mapping ......................................................... 233
5.3.2 ARP Current .......................................................... 254
7.3.3 ARP Static .......................................................... 255
7.4 Open Shortest Path First .................................................... 256
6.3 Filter for MAC Addresses .................................................... 228
7.4.1 OSPF Global .......................................................... 258
6.4 QoS/Priority .......................................................... 225
7.4.2 OSPF Areas .......................................................... 266
7.4.3 OSPF Stub Areas .......................................................... 268
6.5 VLAN .......................................................... 234
7.1 Routing Global .......................................................... 241
5.3.1 ARP Global .......................................................... 252
7.2 Routing Interfaces .......................................................... 243
7.3.2 ARP Current .......................................................... 254
7.2.1 Routing Interfaces Configuration ....................................... 244
7.4.1 OSPF Global .......................................................... 258
7.2.2 Routing Interfaces Secondary Interface Addresses .................. 250
7.3 ARP .......................................................... 251
7.4 Open Shortest Path First .................................................... 256
7.3.3 ARP Static .......................................................... 255
7.3 ARP .......................................................... 251
7.3.3 ARP Static .......................................................... 255
7.3.2 ARP Current .......................................................... 254
7.7.3 ARP Static .......................................................... 255
7.4.2 OSPF Areas .......................................................... 266
7.4.3 OSPF Stub Areas .......................................................... 268
7.7.2 ARP Current .......................................................... 254
# Safety instructions

<table>
<thead>
<tr>
<th>WARNING</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UNCONTROLLED MACHINE ACTIONS</strong></td>
</tr>
<tr>
<td>To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.</td>
</tr>
<tr>
<td>Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.</td>
</tr>
<tr>
<td>Failure to follow these instructions can result in death, serious injury, or equipment damage.</td>
</tr>
</tbody>
</table>
About this Manual

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 “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 “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 Industrial HiVision Network Management software provides you with additional options for smooth configuration and monitoring:
- Auto-topology discovery
- Browser interface
- Client/server structure
- Event handling
- Event log
- Simultaneous configuration of multiple devices
- Graphical user interface with network layout
- SNMP/OPC gateway
The designations used in this manual have the following meanings:

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>▶️</td>
<td>List</td>
</tr>
<tr>
<td>□️</td>
<td>Work step</td>
</tr>
<tr>
<td>Link</td>
<td>Cross-reference with link</td>
</tr>
<tr>
<td>Note:</td>
<td>A note emphasizes a significant fact or draws your attention to a dependency.</td>
</tr>
<tr>
<td>Courier</td>
<td>Representation of a CLI command or field contents in the graphical user interface</td>
</tr>
</tbody>
</table>

- Execution in the Graphical User Interface
- Execution in the Command Line Interface
Notes on the Graphical User Interface

The Graphical User Interface of the device is divided as follows:
- Navigation area
- Dialog area
- Buttons

Navigation area

The Navigation area is located on the left side of the Graphical User Interface.

The Navigation area contains the following elements:
- Toolbar
- Filter
- Menu

You have the option of collapsing the entire Navigation area, for example when displaying the Graphical User Interface on small screens. To collapse or expand, you click the small arrow at the top of the navigation area.

Toolbar

The toolbar at the top of the navigation area contains several buttons.
- When you position the mouse pointer over a button, a tooltip displays further information.
- If the connection to the device is lost, then the toolbar is grayed out.

The device automatically refreshes the toolbar information every 5 seconds.

Clicking the button refreshes the toolbar manually.

When you position the mouse pointer over the button, a tooltip displays the following information:
- **User:** Name of the logged in user
- **Device name:** Name of the device

Clicking the button opens the **Device Security > User Management** dialog.

When you position the mouse pointer over the button, a tooltip displays the summary of the **Diagnostics > System > Configuration Check** dialog.

Clicking the button opens the **Diagnostics > System > Configuration Check** dialog.
Clicking the button logs out the current user and displays the login dialog.

Displays the remaining time in seconds until the device automatically logs out an inactive user.

Clicking the button opens the Device Security > Management Access > Web dialog. There you can specify the timeout.

When the configuration profile in the volatile memory (RAM) differs from the "Selected" configuration profile in the non-volatile memory (NVM), this button is visible. Otherwise, the button is hidden.

Clicking the button opens the Basic Settings > Load/Save dialog.

By right-clicking the button you can save the current settings in the non-volatile memory (NVM).

When you position the mouse pointer over the button, a tooltip displays the following information:

- **Device Status:** This section displays a compressed view of the Device status frame in the Basic Settings > System dialog. The section displays the alarm that is currently active and whose occurrence was recorded first.
- **Security Status:** This section displays a compressed view of the Security status frame in the Basic Settings > System dialog. The section displays the alarm that is currently active and whose occurrence was recorded first.
- **Boot Parameter:** If you permanently save changes to the settings and at least one boot parameter differs from the configuration profile used during the last restart, then this section displays a note.

The following settings cause the boot parameters to change:
- Basic Settings > External Memory dialog, Software auto update parameter
- Basic Settings > External Memory dialog, Config priority parameter
- Device Security > Management Access > Server dialog, SNMP tab, UDP port parameter
- Diagnostics > System > Selftest dialog, SysMon1 is available parameter
- Diagnostics > System > Selftest dialog, Load default config on error parameter

Clicking the button opens the Diagnostics > Status Configuration > Device Status dialog.

**Filter**

The filter enables you to reduce the number of menu items in the menu. When filtering, the menu displays only menu items matching the search string entered in the filter field.

**Menu**

The menu displays the menu items.

You have the option of filtering the menu items. See section "Filter".
To display the corresponding dialog in the dialog area, you click the desired menu item. If the selected menu item is a node containing sub-items, then the node expands or collapses while clicking. The dialog area keeps the previously displayed dialog.

You have the option of expanding or collapsing every node in the menu at the same time. When you right-click anywhere in the menu, a context menu displays the following entries:

- **Expand**
  - Expands every node in the menu at the same time. The menu displays the menu items for every level.
- **Collapse**
  - Collapses every node in the menu at the same time. The menu displays the top level menu items.

**Dialog area**

The Dialog area is located on the right side of the Graphical User Interface. When you click a menu item in the Navigation area, the Dialog area displays the corresponding dialog.

**Updating the display**

If a dialog remains opened for a longer time, then the values in the device have possibly changed in the meantime.

- To update the display in the dialog, click the button. Unsaved information in the dialog is lost.

**Saving the settings**

Saving, transfers the changed settings to the volatile memory (RAM) of the device. Perform the following step:

- Click the button.

To keep the changed settings, even after restarting the device, perform the following steps:

- Open the **Basic Settings > Load/Save** dialog.
- In the table highlight the desired configuration profile.
- When in the **Selected** column the checkbox is **unmarked**, click the button and then the **Select** item.
- Click the button and then the **Save** item.

**Note:** Unintentional changes to the settings can terminate the connection between your PC and the device. To keep the device accessible, enable the **Undo configuration modifications** function in the **Basic Settings > Load/Save** dialog, before changing any settings. Using the function, the device continuously checks if it can still be reached from the IP address of your PC. If the connection is lost, then the device loads the configuration profile saved in the non-volatile memory (NVM) after the specified time. Afterwards, the device can be accessed again.
Working with tables

The dialogs display numerous settings in table form.

When you modify a table cell, the table cell displays a red mark in its top-left corner. The red mark indicates that your modifications are not yet transferred to the volatile memory (RAM) of the device.

You have the option of customizing the look of the tables to fit your needs. When you position the mouse pointer over a column header, the column header displays a drop-down list button. When you click this button, the drop-down list displays the following entries:

- **Sort ascending**
  Sorts the table entries in ascending order based on the entries of the selected column.
  You recognize sorted table entries by an arrow in the column header.

- **Sort descending**
  Sorts the table entries in descending order based on the entries of the selected column.
  You recognize sorted table entries by an arrow in the column header.

- **Columns**
  Displays or hides columns.
  You recognize hidden columns by an unmarked checkbox in the drop-down list.

- **Filters**
  The table only displays the entries whose content matches the specified filter criteria of the selected column.
  You recognize filtered table entries by an emphasized column header.

You have the option of selecting multiple table entries simultaneously and subsequently applying an action to them. This is useful when you are going to remove multiple table entries at the same time.

- **Select several consecutive table entries:**
  - Click the first desired table entry to highlight it.
  - Press and hold the <SHIFT> key.
  - Click the last desired table entry to highlight every desired table entry.

- **Select multiple individual table entries:**
  - Click the first desired table entry to highlight it.
  - Press and hold the <CTRL> key.
  - Click the next desired table entry to highlight it.
  - Repeat until every desired table entry is highlighted.

Buttons

Here you find the description of the standard buttons. The special dialog-specific buttons are described in the corresponding dialog help text.

✔

Transfers the changes to the volatile memory (RAM) of the device and applies them to the device.

To save the changes in the non-volatile memory, proceed as follows:

- Open the **Basic Settings > Load/Save** dialog.
- In the table highlight the desired configuration profile.
- When in the **Selected** column the checkbox is unmarked, click the button and then the Select item.
- Click the button to save your current changes.
Updates the fields with the values that are saved in the volatile memory (RAM) of the device.

Transfers the settings from the volatile memory (RAM) into the configuration profile designated as “Selected” in the non-volatile memory (NVM).

When in the Basic Settings > External Memory dialog the checkbox in the Backup config when saving column is marked, then the device generates a copy of the configuration profile in the external memory.

Displays a submenu with menu items corresponding to the respective dialog.

Opens the Wizard dialog.

Adds a new table entry.

Removes the highlighted table entry.

Opens the online help.
1 Basic Settings

The menu contains the following dialogs:

- System
- Network
- Software
- Load/Save
- External Memory
- Port
- Restart

1.1 System

In this dialog you monitor individual operating statuses.

Device status

The fields in this frame display the device status and inform you about alarms that have occurred. When an alarm currently exists, the frame is highlighted.

You specify the parameters that the device monitors in the Diagnostics > Status Configuration > Device Status dialog.

Note: If you connect only one power supply unit for the supply voltage to a device with a redundant power supply unit, then the device reports an alarm. To help avoid this alarm, you deactivate the monitoring of the missing power supply units in the Diagnostics > Status Configuration > Device Status dialog.

Alarm counter

Displays the number of currently existing alarms.

When there is at least one currently existing alarm, the icon is visible.

When you position the mouse pointer over the icon, a tooltip displays the cause of the currently existing alarms and the time at which the device triggered the alarm.

If a monitored parameter differs from the desired status, then the device triggers an alarm. The Diagnostics > Status Configuration > Device Status dialog, Status tab displays an overview of the alarms.
**Security status**

The fields in this frame display the security status and inform you about alarms that have occurred. When an alarm currently exists, the frame is highlighted.

You specify the parameters that the device monitors in the Diagnostics > Status Configuration > Security Status dialog.

**Alarm counter**

Displays the number of currently existing alarms.

When there is at least one currently existing alarm, the icon is visible.

When you position the mouse pointer over the icon, a tooltip displays the cause of the currently existing alarms and the time at which the device triggered the alarm.

If a monitored parameter differs from the desired status, then the device triggers an alarm. The Diagnostics > Status Configuration > Security Status dialog, Status tab displays an overview of the alarms.

**Signal contact status**

The fields in this frame display the signal contact status and inform you about alarms that have occurred. When an alarm currently exists, the frame is highlighted.

You specify the parameters that the device monitors in the Diagnostics > Status Configuration > Signal Contact > Signal Contact 1/Signal Contact 2 dialog.

**Alarm counter**

Displays the number of currently existing alarms.

When there is at least one currently existing alarm, the icon is visible.

When you position the mouse pointer over the icon, a tooltip displays the cause of the currently existing alarms and the time at which the device triggered the alarm.

If a monitored parameter differs from the desired status, then the device triggers an alarm. The Diagnostics > Status Configuration > Signal Contact > Signal Contact 1/Signal Contact 2 dialog, Status tab displays an overview of the alarms.
**System data**

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

**System name**

Specifies the name for which the device is known in the network.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters
- The following characters are allowed:
  - 0..9
  - a..z
  - A..Z
  - !#$%&'()*+,-./:;<=>?@[\]^_`{}~
  - <device name>-<MAC address> (default setting)

When creating HTTPS X.509 certificates, the application generating the certificate uses the specified value as the domain name and common name.

The following functions use the specified value as a host name or FQDN (Fully Qualified Domain Name). For compatibility, it is recommended to use only small letters, since not every system compares the case in the FQDN. Verify that this name is unique in the whole network.

- **Syslog**

**Location**

Specifies the location of the device.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

**Contact person**

Specifies the contact person for this device.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

**Device type**

Displays the product name of the device.

**Power supply 1**

**Power supply 2**

Displays the status of the power supply unit on the relevant voltage supply connection.

Possible values:

- present
- defective
- not installed
- unknown
Basic Settings
[Basic Settings > System]

Uptime

Displays the time that has elapsed since this device was last restarted.

Possible values:
- Time in the format day(s), ...h ...m ...s

Temperature [°C]

Displays the current temperature in the device in °C.

You activate the monitoring of the temperature thresholds in the Diagnostics > Status Configuration > Device Status dialog.

Upper temp. limit [°C]

Specifies the upper temperature threshold in °C.

The “Installation” user manual contains detailed information about setting the temperature thresholds.

Possible values:
- -99..99 (integer)
  - If the temperature in the device exceeds this value, then the device generates an alarm.

Lower temp. limit [°C]

Specifies the lower temperature threshold in °C.

The “Installation” user manual contains detailed information about setting the temperature thresholds.

Possible values:
- -99..99 (integer)
  - If the temperature in the device falls below this value, then the device generates an alarm.

LED status

This frame displays the states of the device status LEDs at the time of the last update. The “Installation” user manual contains detailed information about the device status LEDs.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>1</td>
<td>There is currently no device status alarm. The device status is OK.</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>There is currently at least one device status alarm. Therefore, see the Device status frame above.</td>
</tr>
<tr>
<td>Power</td>
<td>1</td>
<td>Device variant with 2 power supply units: Only one supply voltage is active.</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Device variant with 1 power supply unit: The supply voltage is active.</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Device variant with 2 power supply units: Both supply voltages are active.</td>
</tr>
</tbody>
</table>
Port status

This frame displays a simplified view of the ports of the device at the time of the last update.

The icons represent the status of the individual ports. In some situations, the following icons interfere with one another. When you position the mouse pointer over the appropriate port icon, a tooltip displays a detailed information about the port state.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Status</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACA</td>
<td></td>
<td>No external memory connected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The external memory is connected, but not ready for operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The external memory is connected and ready for operation.</td>
</tr>
</tbody>
</table>

Buttons

You find the description of the standard buttons in section ”Buttons” on page 14.

1.2 Network

The menu contains the following dialogs:
- Global
- IPv4
1.2.1 Global

This dialog lets you specify the VLAN and HiDiscovery settings required for the access to the device management through the network.

Management interface

This frame lets you specify the VLAN in which the device management can be accessed.

VLAN ID

Specifies the VLAN in which the device management is accessible through the network. The device management is accessible through ports that are members of this VLAN.

Possible values:
- 1..4042 (default setting: 1)
  - The prerequisite is that the VLAN is already configured. See the Switching > VLAN > Configuration dialog.
  - Assign a VLAN ID that is not assigned to any router interface.

When you click the button after changing the value, the Information window opens. Select the port, over which you connect to the device in the future. After clicking the Ok button, the new device management VLAN settings are assigned to the port.

- After that the port is a member of the VLAN and transmits the data packets without a VLAN tag (untagged). See the Switching > VLAN > Configuration dialog.
- The device assigns the port VLAN ID of the device management VLAN to the port. See the Switching > VLAN > Port dialog.

After a short time the device is reachable over the new port in the new device management VLAN.

MAC address

Displays the MAC address of the device. The device management is accessible via the network using the MAC address.

HiDiscovery protocol v1/v2

This frame lets you specify settings for the access to the device using the HiDiscovery protocol.

On a PC, the HiDiscovery software displays the Hirschmann devices that can be accessed in the network on which the HiDiscovery function is enabled. You can access these devices even if they have invalid or no IP parameters assigned. The HiDiscovery software lets you assign or change the IP parameters in the device.

**Note:** With the HiDiscovery software you access the device only through ports that are members of the same VLAN as the device management. You specify which VLAN a certain port is assigned to in the Switching > VLAN > Configuration dialog.
Operation

Enables/disables the HiDiscovery function in the device.

Possible values:

- **On** (default setting)
  - HiDiscovery is enabled.
  - You can use the HiDiscovery software to access the device from your PC.

- **Off**
  - HiDiscovery is disabled.

Access

Enables/disables the write access to the device using HiDiscovery.

Possible values:

- **readWrite** (default setting)
  - The HiDiscovery software is given write access to the device.
  - With this setting you can change the IP parameters in the device.

- **readOnly**
  - The HiDiscovery software is given read-only access to the device.
  - With this setting you can view the IP parameters in the device.

Recommendation: Change the setting to the value **readOnly** only after putting the device into operation.

Signal

Activates/deactivates the flashing of the port LEDs as does the function of the same name in the HiDiscovery software. The function lets you identify the device in the field.

Possible values:

- **marked**
  - The flashing of the port LEDs is active.
  - The port LEDs flash until you disable the function again.

- **unmarked** (default setting)
  - The flashing of the port LEDs is inactive.

Buttons

You find the description of the standard buttons in section "Buttons" on page 14.
1.2.2 IPv4

This dialog allows you to specify the IPv4 settings required for the access to the device management through the network.

Management interface

IP address assignment

Specifies the source from which the device management receives its IP parameters.

Possible values:

- **Local**
  - The device uses the IP parameters from the internal memory. You specify the settings for this in the *IP parameter* frame.

IP parameter

This frame lets you assign the IP parameters manually. If you have selected the *Local* radio button in the *Management interface* frame, *IP address assignment* option list, then these fields can be edited.

IP address

Specifies the IP address under which the device management can be accessed through the network.

Possible values:

- **Valid IPv4 address**

Verify that the IP subnet of the device management is not overlapping with any subnet connected to another interface of the device:
  - router interface
  - loopback interface
Netmask

Specifies the netmask.

Possible values:
- Valid IPv4 netmask

Gateway address

Specifies the IP address of a router through which the device accesses other devices outside its own network.

Possible values:
- Valid IPv4 address

If the device does not use the specified gateway, check if another default gateway is specified. The setting in the following dialog has precedence:
- Routing > Routing Table dialog, Next hop IP address column, if the value in the Network address column and in the Netmask column is 0.0.0.0

Buttons

You find the description of the standard buttons in section "Buttons" on page 14.

1.3 Software

This dialog lets you update the device software and display information about the device software.

You also have the option to restore a backup of the device software saved in the device.

Note: Before updating the device software, follow the version-specific notes in the Readme text file.

Version

Stored version

Displays the version number and creation date of the device software stored in the flash memory. The device loads the device software during the next restart.

Running version

Displays the version number and creation date of the device software that the device loaded during the last restart and is currently running.
Basic Settings

[Basic Settings > Software]

Backup version
Displays the version number and creation date of the device software saved as a backup in the flash memory. The device copied this device software into the backup memory during the last software update or after you clicked the Restore button.

Restore
Restores the device software saved as a backup. In the process, the device changes the Stored version and the Backup version of the device software.

Upon restart, the device loads the Stored version.

Bootcode
Displays the version number and creation date of the boot code.

Software update
Alternatively, when the image file is located in the external memory, the device lets you update the device software by right-clicking in the table.

URL
Specifies the path and the file name of the image file with which you update the device software.

The device gives you the following options for updating the device software:

- Software update from the PC
  When the file is located on your PC or on a network drive, drag and drop the file in the area. Alternatively click in the area to select the file.
  You also have the option of transferring the file from your PC to the device through SFTP or SCP. Perform the following steps:
  - On your PC, open an SFTP or SCP client, for example WinSCP.
  - Use the SFTP or SCP client to open a connection to the device.
  - Transfer the file to the directory /upload/firmware in the device.
    When the file transfer is complete, the device starts updating the device software. If the update was successful, then the device creates an ok file in the directory /upload/firmware and deletes the image file.
    The device loads the device software during the next restart.

Start
Updates the device software.

The device installs the selected file in the flash memory, replacing the previously saved device software. Upon restart, the device loads the installed device software.

The device copies the existing software into the backup memory.

To remain logged in to the device during the software update, move the mouse pointer occasionally. Alternatively, specify a sufficiently high value in the Device Security > Management Access > Web dialog, field Web interface session timeout [min] before the software update.
**Table**

**File location**
Displays the storage location of the device software.

Possible values:
- *ram*
  Volatile memory of the device
- *flash*
  Non-volatile memory (NVM) of the device
- *usb*
  External USB memory (ACA21/ACA22)

**Index**
Displays the index of the device software.

For the device software in the flash memory, the index has the following meaning:
- **1**
  Upon restart, the device loads this device software.
- **2**
  The device copied this device software into the backup area during the last software update.

**File name**
Displays the device-internal file name of the device software.

**Firmware**
Displays the version number and creation date of the device software.

**Buttons**
You find the description of the standard buttons in section “Buttons” on page 14.
1.4 **Load/Save**

This dialog lets you save the device settings permanently in a configuration profile.

The device can hold several configuration profiles. When you activate an alternative configuration profile, you change to other device settings. You have the option of exporting the configuration profiles to your PC or to a server. You also have the option of importing the configuration profiles from your PC or from a server to the device.

In the default setting, the device saves the configuration profiles unencrypted. If you enter a password in the *Configuration encryption* frame, then the device saves both the current and the future configuration profiles in an encrypted format.

Unintentional changes to the settings can terminate the connection between your PC and the device. To keep the device accessible, enable the *Undo configuration modifications* function before changing any settings. If the connection is lost, then the device loads the configuration profile saved in the non-volatile memory (*NVM*) after the specified time.

**External memory**

**Selected external memory**

Displays the type of the external memory.

Possible values:

- **usb**
  
  External USB memory (ACA21/ACA22)

**Status**

Displays the operating state of the external memory.

Possible values:

- **notPresent**
  
  No external memory connected.

- **removed**
  
  Someone has removed the external memory from the device during operation.

- **ok**
  
  The external memory is connected and ready for operation.

- **outOfMemory**
  
  The memory space is occupied in the external memory.

- **genericErr**
  
  The device has detected an error.
**Configuration encryption**

Displays if the configuration encryption is active/inactive in the device.

Possible values:

- **marked**
  - The configuration encryption is active.
  - If the configuration profile is encrypted and the password matches the password stored in the device, then the device loads a configuration profile from the non-volatile memory (NVM).  

- **unmarked**
  - The configuration encryption is inactive.
  - If the configuration profile is unencrypted, then the device loads a configuration profile from the non-volatile memory (NVM) only.

If in the Basic Settings > External Memory dialog, the Config priority column has the value first and the configuration profile is unencrypted, then the Security status frame in the Basic Settings > System dialog displays an alarm.

In the Diagnostics > Status Configuration > Security Status dialog, Global tab, Monitor column you specify if the device monitors the Load unencrypted config from external memory parameter.

**Set password**

Opens the Set password window that helps you to enter the password needed for the configuration profile encryption. Encrypting the configuration profiles makes unauthorized access more difficult. To do this, perform the following steps:

- When you are changing an existing password, enter the existing password in the Old password field. To display the password in plain text instead of ***** (asterisks), mark the Display content checkbox.
- In the New password field, enter the password. To display the password in plain text instead of ***** (asterisks), mark the Display content checkbox.
- Mark the Save configuration afterwards checkbox to use encryption also for the Selected configuration profile in the non-volatile memory (NVM) and in the external memory.

*Note:* If a maximum of one configuration profile is stored in the non-volatile memory (NVM) of the device, then use this function only. Before creating additional configuration profiles, decide for or against permanently activated configuration encryption in the device. Save additional configuration profiles either unencrypted or encrypted with the same password.

If you are replacing a device with an encrypted configuration profile, for example due to a defect, then perform the following steps:

- Restart the new device and assign the IP parameters.
- Open the Basic Settings > Load/Save dialog on the new device.
- Encrypt the configuration profile in the new device. See above. Enter the same password you used in the defective device.
- Install the external memory from the defective device in the new device.
- Restart the new device.
  - When you restart the device, the device loads the configuration profile with the settings of the defective device from the external memory. The device copies the settings into the volatile memory (RAM) and into the non-volatile memory (NVM).
Basic Settings

[Basic Settings > Load/Save]

Delete

Opens the Delete window which helps you to cancel the configuration encryption in the device. To cancel the configuration encryption, perform the following steps:

- In the Old password field, enter the existing password.
  To display the password in plain text instead of **** (asterisks), mark the Display content checkbox.
- Mark the Save configuration afterwards checkbox to remove the encryption also for the Selected configuration profile in the non-volatile memory (NVM) and in the external memory.

Note: If you keep additional encrypted configuration profiles in the memory, then the device helps prevent you from activating or designating these configuration profiles as "Selected".

Information

NVM in sync with running config

Displays if the configuration profile in the volatile memory (RAM) and the "Selected" configuration profile in the non-volatile memory (NVM) are the same.

Possible values:
- marked
  The configuration profiles are the same.
- unmarked
  The configuration profiles differ.

External memory in sync with NVM

Displays if the "Selected" configuration profile in the external memory and the "Selected" configuration profile in the non-volatile memory (NVM) are the same.

Possible values:
- marked
  The configuration profiles are the same.
- unmarked
  The configuration profiles differ.

Possible causes:
- No external memory is connected to the device.
- In the Basic Settings > External Memory dialog, the Backup config when saving function is disabled.
Basic Settings

[Basic Settings > Load/Save]

**Backup config on a remote server when saving**

**Operation**

Enables/disables the *Backup config on a remote server when saving* function.

**Possible values:**

- **Enabled**
  - The *Backup config on a remote server when saving* function is enabled.
  - When you save the configuration profile in the non-volatile memory (NVM), the device automatically backs up the configuration profile on the remote server specified in the **URL** field.

- **Disabled** (default setting)
  - The *Backup config on a remote server when saving* function is disabled.

**URL**

Specifies path and file name of the backed up configuration profile on the remote server.

**Possible values:**

- **Alphanumeric ASCII character string with 0..128 characters**
  - **Example:** tftp://192.9.200.1/cfg/config.xml
  - The device supports the following wildcards:
    - **%d**
      - System date in the format **YYYY-mm-dd**
    - **%t**
      - System time in the format **HH_MM_SS**
    - **%i**
      - IP address of the device
    - **%m**
      - MAC address of the device in the format **AA-BB-CC-DD-EE-FF**
    - **%p**
      - Product name of the device

**Set credentials**

Opens the **Credentials** window which helps you to enter the login credentials needed to authenticate on the remote server. To do this, perform the following steps:

- **In the User name field**, enter the user name.
  - To display the user name in plain text instead of ***** (asterisks), mark the **Display content** checkbox.
  - **Possible values:**
    - Alphanumeric ASCII character string with 1..32 characters

- **In the Password field**, enter the password.
  - To display the password in plain text instead of ***** (asterisks), mark the **Display content** checkbox.
  - **Possible values:**
    - **Alphanumeric ASCII character string with 6..64 characters**
      - The following characters are allowed:
        - a..z
        - A..Z
        - 0..9
        - !#$%&'()*+,-./:;<=>?@[\]^_`~
**Undo configuration modifications**

**Operation**

Enables/disables the *Undo configuration modifications* function. Using the function, the device continuously checks if it can still be reached from the IP address of your PC. If the connection is lost, after a specified time period the device loads the “Selected” configuration profile from the non-volatile memory (*NVM*). Afterwards, the device can be accessed again.

Possible values:

- **On**
  - The function is enabled.
  - You specify the time period between the interruption of the connection and the loading of the configuration profile in the *Timeout [s] to recover after connection loss* field.
  - When the non-volatile memory (*NVM*) contains multiple configuration profiles, the device loads the configuration profile designated as “Selected”.

- **Off** (default setting)
  - The function is disabled.
  - Disable the function again before you close the Graphical User Interface. You thus help prevent the device from restoring the configuration profile designated as “Selected”.

**Note:** Before you enable the function, save the settings in the configuration profile. Current changes, that are saved temporarily, are therefore maintained in the device.

**Timeout [s] to recover after connection loss**

Specifies the time in seconds after which the device loads the “Selected” configuration profile from the non-volatile memory (*NVM*) if the connection is lost.

Possible values:

- **30...600** (default setting: 600)

Specify a sufficiently large value. Take into account the time when you are viewing the dialogs of the Graphical User Interface without changing or updating them.

**Watchdog IP address**

Displays the IP address of the PC on which you have enabled the function.

Possible values:

- **IPv4 address** (default setting: 0.0.0.0)

**Table**

**Storage type**

Displays the storage location of the configuration profile.

Possible values:

- **RAM** (volatile memory of the device)
  - In the volatile memory, the device stores the settings for the current operation.
NVM (non-volatile memory of the device)
When applying the *Undo configuration modifications* function or during a restart, the device loads the “Selected” configuration profile from the non-volatile memory.
The non-volatile memory provides space for multiple configuration profiles, depending on the number of settings saved in the configuration profile. The device manages a maximum of 20 configuration profiles in the non-volatile memory.
You can load a configuration profile into the volatile memory (RAM). To do this, perform the following steps:
- In the table highlight the configuration profile.
- Click the **button and then the **Activate** item.

ENVM (external memory)
In the external memory, the device saves a backup copy of the “Selected” configuration profile.
The prerequisite is that in the *Basic Settings > External Memory* dialog you mark the **Backup config when saving** checkbox.

### Profile name
Displays the name of the configuration profile.

Possible values:
- **running-config**
  Name of the configuration profile in the volatile memory (RAM).
- **config**
  Name of the factory setting configuration profile in the non-volatile memory (NVM).
- **User-defined name**
  The device lets you save a configuration profile with a user-specified name by highlighting an existing configuration profile in the table, clicking the **button and then the **Save As..** item.

To export the configuration profile as an XML file on your PC, click the link. Then you select the storage location and specify the file name.

To save the file on a remote server, click the **button and then the **Export...** item.

### Modification date (UTC)
Displays the time (UTC) at which a user last saved the configuration profile.

### Selected
Displays if the configuration profile is designated as “Selected”.

Possible values:
- **marked**
  The configuration profile is designated as “Selected”.
  - When applying the *Undo configuration modifications* function or during a restart, the device loads the configuration profile into the volatile memory (RAM).
  - When you click the **button, the device saves the temporarily saved settings in this configuration profile.
- **unmarked**
  Another configuration profile is designated as “Selected”.

To designate another configuration profile as “Selected”, you highlight the desired configuration profile in the table, click the **button and then the **Activate** item.
Encrypted

Displays if the configuration profile is encrypted.

Possible values:

- **marked**
  The configuration profile is encrypted.

- **unmarked**
  The configuration profile is unencrypted.

You activate/deactivate the encryption of the configuration profile in the Configuration encryption frame.

Encryption verified

Displays if the password of the encrypted configuration profile matches the password stored in the device.

Possible values:

- **marked**
  The passwords match. The device is able to unencrypt the configuration profile.

- **unmarked**
  The passwords are different. The device is unable to unencrypt the configuration profile.

Software version

Displays the version number of the device software that the device ran while saving the configuration profile.

Fingerprint

Displays the checksum saved in the configuration profile.

When saving the settings, the device calculates the checksum and inserts it into the configuration profile.

Fingerprint verified

Displays if the checksum saved in the configuration profile is valid.

The device calculates the checksum of the configuration profile marked as “Selected” and compares it with the checksum saved in this configuration profile.

Possible values:

- **marked**
  The calculated and the saved checksum match. The saved settings are consistent.

- **unmarked**
  For the configuration profile marked as “Selected” applies:
  - The calculated and the saved checksum are different.
  - The configuration profile contains modified settings.
  Possible causes:
  - The file is damaged.
  - The file system in the external memory is inconsistent.
  - A user has exported the configuration profile and changed the XML file outside the device.
  For the other configuration profiles the device has not calculated the checksum.
The device verifies the checksum correctly only if the configuration profile has been saved before as follows:
- on an identical device
- with the same software version, which the device is running

**Note:** This function identifies changes to the settings in the configuration profile. The function does not provide protection against operating the device with modified settings.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

Remove

Removes the configuration profile highlighted in the table from the non-volatile memory (NVM) or from the external memory.

If the configuration profile is designated as “Selected”, then the device helps prevent you from removing the configuration profile.

Save As..

Copies the configuration profile highlighted in the table and saves it with a user-specified name in the non-volatile memory (NVM). The device designates the new configuration profile as “Selected”.

**Note:** Before creating additional configuration profiles, decide for or against permanently activated configuration encryption in the device. Save additional configuration profiles either unencrypted or encrypted with the same password.

If in the **Basic Settings > External Memory** dialog the checkbox in the **Backup config when saving** column is marked, then the device designates the configuration profile of the same name in the external memory as “Selected”.

Activate

Loads the settings of the configuration profile highlighted in the table to the volatile memory (RAM).

- The device terminates the connection to the Graphical User Interface. To access the device management again, perform the following steps:
  - Reload the Graphical User Interface.
  - Log in again.
- The device immediately uses the settings of the configuration profile on the fly.

Enable the **Undo configuration modifications** function before you activate another configuration profile. If the connection is lost afterwards, then the device loads the last configuration profile designated as “Selected” from the non-volatile memory (NVM). The device can then be accessed again.

If the configuration encryption is inactive, then the device loads an unencrypted configuration profile. If the configuration encryption is active and the password matches the password stored in the device, then the device loads an encrypted configuration profile.

When you activate an older configuration profile, the device takes over the settings of the functions contained in this software version. The device sets the values of new functions to their default value.
Select

Designates the configuration profile highlighted in the table as “Selected”. In the Selected column, the checkbox is then marked.

When applying the Undo configuration modifications function or during a restart, the device loads the settings of this configuration profile to the volatile memory (RAM).

- If the configuration encryption in the device is disabled, then designate an unencrypted configuration profile only as “Selected”.
- If the configuration encryption in the device is enabled and the password of the configuration profile matches the password saved in the device, then designate an encrypted configuration profile only as “Selected”.

Otherwise, the device is unable to load and encrypt the settings in the configuration profile the next time it restarts. For this case you specify in the Diagnostics > System > Selftest dialog if the device starts with the default settings or terminates the restart and stops.

Note: You only mark the configuration profiles saved in the non-volatile memory (NVM).

If in the Basic Settings > External Memory dialog the checkbox in the Backup config when saving column is marked, then the device designates the configuration profile of the same name in the external memory as “Selected”.

Import...

Opens the Import... window to import a configuration profile.

The prerequisite is that you have exported the configuration profile using the Export... button or using the link in the Profile name column.

- In the Select source drop-down list, select from where the device imports the configuration profile.
  - PC/URL
    - The device imports the configuration profile from the local PC or from a remote server.
  - External memory
    - The device imports the configuration profile from the external memory.

- When PC/URL is selected above, in the Import profile from PC/URL frame you specify the configuration profile file to be imported.
  - Import from the PC
    - When the file is located on your PC or on a network drive, drag and drop the file in the area. Alternatively click in the area to select the file.
    - You also have the option of transferring the file from your PC to the device through SFTP or SCP:
      - On your PC, open an SFTP or SCP client, for example WinSCP.
      - Use the SFTP or SCP client to open a connection to the device.
      - Transfer the file to the directory /nv/cfg in the device.

- When External memory is selected above, in the Import profile from external memory frame you specify the configuration profile file to be imported.
  - In the Profile name drop-down list, select the name of the configuration profile to be imported.

- In the Destination frame you specify where the device saves the imported configuration profile.
  - In the Profile name field you specify the name under which the device saves the configuration profile.
  - In the Storage type field you specify the storage location for the configuration profile. The prerequisite is that in the Select source drop-down list you select the PC/URL item.
Basic Settings

[Basic Settings > Load/Save]

RAM
The device saves the configuration profile in the volatile memory (RAM) of the device. This replaces the running-config, the device uses the settings of the imported configuration profile immediately. The device terminates the connection to the Graphical User Interface. Reload the Graphical User Interface. Log in again.

NVM
The device saves the configuration profile in the non-volatile memory (NVM) of the device.

When you import a configuration profile, the device takes over the settings as follows:

- If the configuration profile was exported on the same device or on an identically equipped device of the same type, then:
  The device takes over the settings completely.
- If the configuration profile was exported on an other device, then:
  The device takes over the settings which it can interpret based on its hardware equipment and software level.
  The remaining settings the device takes over from its running-config configuration profile.

Regarding configuration profile encryption, also read the help text of the Configuration encryption frame. The device imports a configuration profile under the following conditions:

- The configuration encryption of the device is inactive. The configuration profile is unencrypted.
- The configuration encryption of the device is active. The configuration profile is encrypted with the same password that the device currently uses.

Export...
Exports the configuration profile highlighted in the table and saves it as an XML file on a remote server.

To save the file on your PC, click the link in the Profile name column to select the storage location and specify the file name.

The device gives you the following options for exporting a configuration profile:

Back to factory...
Resets the settings in the device to the default values.

- The device deletes the saved configuration profiles from the volatile memory (RAM) and from the non-volatile memory (NVM).
- The device deletes the HTTPS certificate used by the web server in the device.
- The device deletes the RSA key (Host Key) used by the SSH server in the device.
- When an external memory is connected, the device deletes the configuration profiles saved in the external memory.
- After a brief period, the device reboots and loads the default values.

Back to default
Deletes the current operating (running_config) settings from the volatile memory (RAM).
1.5 **External Memory**

This dialog lets you activate functions that the device automatically executes in combination with the external memory. The dialog also displays the operating state and identifying characteristics of the external memory.

**Table**

**Type**

Displays the type of the external memory.

Possible values:

- **usb**
  
  External USB memory (ACA21/ACA22)

**Status**

Displays the operating state of the external memory.

Possible values:

- **notPresent**
  
  No external memory connected.

- **removed**
  
  Someone has removed the external memory from the device during operation.

- **ok**
  
  The external memory is connected and ready for operation.

- **outOfMemory**
  
  The memory space is occupied in the external memory.

- **genericErr**
  
  The device has detected an error.

**Writable**

Displays if the device has write access to the external memory.

Possible values:

- **marked**
  
  The device has write access to the external memory.

- **unmarked**
  
  The device has read-only access to the external memory. Possibly the write protection is activated in the external memory.

**Software auto update**

Activates/deactivates the automatic device software update during the restart.

Possible values:

- **marked** (default setting)
  
  The automatic device software update during the restart is activated. The device updates the device software when the following files are located in the external memory:
the image file of the device software
- a text file startup.txt with the content autoUpdate=<image_file_name>.bin
  ▶ unmarked
  The automatic device software update during the restart is deactivated.

**Config priority**

Specifies the memory from which the device loads the configuration profile upon reboot.

Possible values:
- **disable**
  The device loads the configuration profile from the non-volatile memory (NVM).
- **first**
  The device loads the configuration profile from the external memory.
  When the device does not find a configuration profile in the external memory, it loads the configuration profile from the non-volatile memory (NVM).

**Note:** When loading the configuration profile from the external memory (ENVM), the device overwrites the settings of the Selected configuration profile in the non-volatile memory (NVM).

If the **Config priority** column has the value **first** and the configuration profile is unencrypted, then the **Security status** frame in the **Basic Settings > System** dialog displays an alarm.

In the **Diagnostics > Status Configuration > Security Status** dialog, **Global** tab, **Monitor** column you specify if the device monitors the **Load unencrypted config from external memory** parameter.

**Backup config when saving**

Activates/deactivates creating a copy of the configuration profile in the external memory.

Possible values:
- **marked** (default setting)
  Creating a copy is activated. When you click in the **Basic Settings > Load/Save** dialog the **Save** button, the device generates a copy of the configuration profile on the active external memory.
- **unmarked**
  Creating a copy is deactivated. The device does not generate a copy of the configuration profile.

**Manufacturer ID**

Displays the name of the memory manufacturer.

**Revision**

Displays the revision number specified by the memory manufacturer.

**Version**

Displays the version number specified by the memory manufacturer.

**Name**

Displays the product name specified by the memory manufacturer.
Serial number

Displays the serial number specified by the memory manufacturer.

**Buttons**

You find the description of the standard buttons in section "Buttons" on page 14.
1.6 Port

This dialog lets you specify settings for the individual ports. The dialog also displays the operating mode, connection status, bit rate and duplex mode for every port.

The dialog contains the following tabs:

- [Configuration]
- [Statistics]

[Configuration]

Table

Port
Displays the port number.

Name
Name of the port.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters
  The following characters are allowed:
  - <space>
  - 0..9
  - a..z
  - A..Z
  - !#$%&'()*+,-./:;<=>?@[\]^_`{}~

Port on
Activates/deactivates the port.

Possible values:

- marked (default setting)
  The port is active.
- unmarked
  The port is inactive. The port does not send or receive any data.

State
Displays if the port is currently physically enabled or disabled.

Possible values:

- marked
  The port is physically enabled.
- unmarked
  The port is physically disabled.
Basic Settings

[Basic Settings > Port]

Power state (port off)

Specifies if the port is physically switched on or off when you deactivate the port with the Port on function.

Possible values:
- **marked**
  The port remains physically enabled. A connected device receives an active link.
- **unmarked** (default setting)
  The port is physically disabled.

Auto power down

Specifies how the port behaves when no cable is connected.

Possible values:
- **no-power-save** (default setting)
  The port remains activated.
- **auto-power-down**
  The port changes to the energy-saving mode.
- **unsupported**
  The port does not support this function and remains activated.

Automatic configuration

Activates/deactivates the automatic selection of the operating mode for the port.

Possible values:
- **marked** (default setting)
  The automatic selection of the operating mode is active.
  The port negotiates the operating mode independently using autonegotiation and detects the devices connected to the TP port automatically (Auto Cable Crossing). This setting has priority over the manual setting of the port.
  Elapse several seconds until the port has set the operating mode.
- **unmarked**
  The automatic selection of the operating mode is inactive.
  The port operates with the values you specify in the Manual configuration column and in the Manual cable crossing (Auto. conf. off) column.
- **Grayed-out display**
  No automatic selection of the operating mode.

Manual configuration

Specifies the operating mode of the ports when the Automatic configuration function is disabled.

Possible values:
- 10 Mbit/s HDX
  Half duplex connection
- 10 Mbit/s FDX
  Full duplex connection
- 100 Mbit/s HDX
  Half duplex connection
100 Mbit/s FDX
Full duplex connection

1000 Mbit/s FDX
Full duplex connection

Note: The operating modes of the port actually available depend on the device configuration.

Link/Current settings
Displays the operating mode which the port currently uses.
Possible values:
- No cable connected, no link.
- 10 Mbit/s HDX
  Half duplex connection
- 10 Mbit/s FDX
  Full duplex connection
- 100 Mbit/s HDX
  Half duplex connection
- 100 Mbit/s FDX
  Full duplex connection
- 1000 Mbit/s FDX
  Full duplex connection

Note: The operating modes of the port actually available depend on the device configuration.

Manual cable crossing (Auto. conf. off)
Specifies the devices connected to a TP port.
The prerequisite is that the Automatic configuration function is disabled.
Possible values:
- mdi
  The device interchanges the send- and receive-line pairs on the port.
- mdix (default setting on TP ports)
  The device helps prevent the interchange of the send- and receive-line pairs on the port.
- auto-mdix
  The device detects the send and receive line pairs of the connected device and automatically adapts to them.
  Example: When you connect an end device with a crossed cable, the device automatically resets the port from mdix to mdi.
- unsupported (default setting on optical ports or TP-SFP ports)
  The port does not support this function.

Flow control
Activates/deactivates the flow control on the port.
Possible values:
- marked (default setting)
  The Flow control on the port is active.
  The sending and evaluating of pause packets (full-duplex operation) or collisions (half-duplex operation) is activated on the port.
To enable the flow control in the device, also activate the *Flow control* function in the *Switching > Global* dialog.

Activate the flow control also on the port of the device that is connected to this port. On an uplink port, activating the flow control can possibly cause undesired sending breaks in the higher-level network segment (“wandering backpressure”).

- **unmarked**
  The Flow control on the port is inactive.

If you are using a redundancy function, then you deactivate the flow control on the participating ports. If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended.

### Send trap (Link up/down)

Activates/deactivates the sending of SNMP traps when the device detects changes in the link up/down status for this port.

Possible values:

- **marked** *(default setting)*
  The sending of SNMP traps is active.
  When the device detects a link up/down status change, the device sends an SNMP trap.

- **unmarked**
  The sending of SNMP traps is inactive.

The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least one trap destination.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

### Clear port statistics

Resets the counter for the port statistics to 0.

### Statistics

This tab displays the following overview per port:

- **Number of data packets/bytes received in the device**
  - *Received packets*
  - *Received octets*
  - *Received unicast packets*
  - *Received multicast packets*
  - *Received broadcast packets*

- **Number of data packets/bytes sent from the device**
  - *Transmitted packets*
  - *Transmitted octets*
  - *Transmitted unicast packets*
  - *Transmitted multicast packets*
  - *Transmitted broadcast packets*

- **Number of errors detected by the device**
  - *Received fragments*
– Detected CRC errors
– Detected collisions

▶ Number of data packets per size category received in the device
  – Packets 64 bytes
  – Packets 65 to 127 bytes
  – Packets 128 to 255 bytes
  – Packets 256 to 511 bytes
  – Packets 512 to 1023 bytes
  – Packets 1024 to 1518 bytes

▶ Number of data packets discarded by the device
  – Received discards
  – Transmitted discards

To sort the table by a specific criterion click the header of the corresponding row.

For example, to sort the table based on the number of received bytes in ascending order, click the header of the Received octets column once. To sort in descending order, click the header again.

To reset the counter for the port statistics in the table to 0, perform the following steps:
▶ In the Basic Settings > Port dialog, click the button and then the Clear port statistics item.
  or
▶ In the Basic Settings > Restart dialog, click the Clear port statistics button.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

Clear port statistics

Resets the counter for the port statistics to 0.
1.7 Restart

This dialog lets you restart the device, reset port counters and address tables, and delete log files.

**Restart**

**Cold start...**

Opens the **Restart** dialog to initiate a restart of the device.

If the configuration profile in the volatile memory (**RAM**) and the "Selected" configuration profile in the non-volatile memory (**NVM**) differ, then the device displays the **Warning** dialog.

- To permanently save the changes, click the **Yes** button in the **Warning** dialog.
- To discard the changes, click the **No** button in the **Warning** dialog.

The device restarts and goes through the following phases:

- The device starts the device software that the **Stored version** field displays in the **Basic Settings > Software** dialog.
- The device loads the settings from the "Selected" configuration profile. See the **Basic Settings > Load/Save** dialog.

**Note:** During the restart, the device does not transfer any data. During this time, the device cannot be accessed by the Graphical User Interface or other management systems.

**Buttons**

You find the description of the standard buttons in section “**Buttons**” on page 14.

**Reset MAC address table**

Removes the MAC addresses from the forwarding table that have in the **Switching > Filter for MAC Addresses** dialog the value **learned** in the **Status** column.

**Reset ARP table**

Removes the dynamically set up addresses from the ARP table.

See the **Diagnostics > System > ARP** dialog.

**Clear port statistics**

Resets the counter for the port statistics to 0.

See the **Basic Settings > Port** dialog, **Statistics** tab.
Delete log file

Removes the logged events from the log file.

See the Diagnostics > Report > System Log dialog.

Delete persistent log file

Removes the log files from the external memory.

See the Diagnostics > Report > Persistent Logging dialog.

Clear firewall table

Removes the information about open connections from the state table of the firewall. It is possible, that the device interrupts open communication connections.
Basic Settings

1.7 Restart
2 Time

The menu contains the following dialogs:

- Basic Settings
- NTP

2.1 Basic Settings

[Time > Basic Settings]

After a restart, the device initializes its clock to January 1, 00:00h. Reset the time if you disconnect the device from the power supply or restart it. Alternatively you specify, that the device automatically obtains the current time from an SNTP server or from a PTP clock.

In this dialog you specify time-related settings independently of the time synchronization protocol specified.

Configuration

System time (UTC)

Displays the current date and time with reference to Universal Time Coordinated (UTC).

Set time from PC

The device uses the time on the PC as the system time.

System time

Displays the current date and time with reference to the local time: System time = System time (UTC) + Local offset [min] + Daylight saving time

Time source

Displays the time source from which the device gets the time information.

The device automatically selects the available time source with the greatest accuracy.

Possible values:

- local
  System clock of the device.
- ntp
  The NTP client is activated and the device is synchronized by an NTP server.
Local offset [min]

Specifies the difference between the local time and *System time (UTC)* in minutes: *Local offset [min] = System time − System time (UTC)*

Possible values:
- **−780..840** (default setting: **60**)

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

## 2.2 NTP

The device lets you synchronize the system time in the device and in the network using the Network Time Protocol (NTP).

The Network Time Protocol (NTP) is a procedure described in RFC 5905 for time synchronization in the network.

On the basis of a reference time source, NTP defines hierarchy levels for time servers and clients. A hierarchy level is known as a “stratum”. Devices of the 1st level (stratum 1) synchronize themselves directly with the reference time source and make the time information available to clients of the 2nd level (stratum 2). A GPS receiver or a radio-controlled clock can serve as the reference time source.

The NTP client in the device evaluates the time information of several servers and adjusts its own clock continuously to attain a high level of accuracy. If you also configure the device as an NTP server, then the device distributes time information to the clients in the subordinate network segment.

The menu contains the following dialogs:
- **Global**
- **Server**
2.2.1 Global

In this dialog you determine if the device functions as an NTP client and server or only as an NTP client.

- As an NTP client, the device takes the coordinated world time (UTC) from one or more NTP servers in the network.

- As an NTP server, the device distributes the coordinated world time (UTC) to NTP clients in the subordinate network segment. The device takes the coordinated world time from one or more NTP servers in the network, if these were previously specified.

Client only

The device transmits the time information without authentication in the VLAN of the device management as well as in Layer 3 on the IP interfaces set up.

Client

Enables/disables the NTP client in the device.

Possible values:

- **On**
  
  The NTP client is enabled.
  
  The device obtains the time information from one or more NTP servers in the network.

- **Off** (default setting)
  
  The NTP client is disabled.

**Note:** Before you enable the client, disable the Server function in the Client and server frame.

Mode

Specifies from where the NTP client takes the time information.

Possible values:

- **unicast** (default setting)
  
  The NTP client takes the time information from unicast responses of the servers that are indicated as active in the Time > NTP > Server dialog.

- **broadcast**
  
  The NTP client takes the time information from broadcast messages or from multicast messages of the servers that are indicated as active in the Time > NTP > Multicast Groups dialog.
**Client and server**

The device transmits the time information without authentication in the VLAN of the device management as well as in Layer 3 on the IP interfaces set up.

**Server**

Enables/disables the NTP client and the NTP server in the device.

Possible values:

- **On**
  - The NTP client and the NTP server are enabled.
  - The NTP client obtains the time information from one or more NTP servers in the network. The NTP server distributes the time information to the NTP clients in the subordinate network segment.

- **Off** (default setting)
  - The NTP client and the NTP server are disabled.

**Note:** If you enable the NTP client and the NTP server, then the device disables the function in the **Client** field in the **Client only** frame.

**Mode**

Specifies in which mode the NTP server works.

Possible values:

- **client-server** (default setting)
  - With this setting, the device obtains the time information from NTP servers in the network and distributes it to NTP clients in the subordinate network segment.
    - The NTP client takes the time information from the unicast responses of the servers that are indicated as active in the **Time > NTP > Server** dialog.
    - The NTP server distributes the time information via unicast to the requesting clients.

- **symmetric**
  - With this setting you integrate the device in a cluster of redundant NTP servers. The device synchronizes the time information with the other NTP servers in the cluster at intervals of 64 seconds.
    - In the **Time > NTP > Server** dialog, indicate the NTP servers participating in the cluster as active.
    - Specify a uniform value for the stratum for the NTP servers participating in the cluster.

**Stratum**

Specifies the hierarchical distance of the device to the referent time source.

Possible values:

- **1..16** (default setting: 12)

**Example:** Devices of the first level (Stratum 1) synchronize themselves directly with the reference time source and make the time information available to the clients of the second level (Stratum 2).

The device evaluates this value under the following circumstances:

- The NTP server in the device is working in **symmetric** mode.
- or
- The device is using the local system clock as the time source. See the **Time source** field in the **Time > Basic Settings** dialog.
Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
2.2.2 Server

In this dialog you specify the NTP servers.

- The NTP client of the device obtains the time information from the unicast responses of the servers specified here.
- If the NTP server of the device is working in symmetric mode, then you specify the servers participating in the cluster here.

Table

Index

Displays the index number to which the table entry relates.

Possible values:

- 1..4

The device automatically assigns this number.

When you delete a table entry, this leaves a gap in the numbering. When you create a new table entry, the device fills the first gap.

Address

Specifies the IP address of the NTP server.

Possible values:

- Valid IPv4 address (default setting: 0.0.0.0)

Port

Displays the UDP Port on which the NTP server provides the time information.

Initial burst

Activates/deactivates the Initial burst mode.

During operation, the NTP client of the device only sends single data packets to request the time information. If the NTP server is unreachable (Status column = notResponding), then the NTP client of the device sends several data packets at once (burst) to synchronize as soon as possible.

Possible values:

- marked
  The Initial burst mode is active.
  - The device sends only once several data packets (burst) when the NTP server is unreachable.
  - Only use this setting if you use a private, non-public NTP server as reference time source.
  - You use this setting with care to speed up the initial synchronization.
- unmarked (default setting)
  The Initial burst mode is inactive.
**Burst**

Activates/deactivates the **Burst** mode.

During operation, the NTP client of the device only sends single data packets to request the time information. In the **Burst** mode, the NTP client of the device sends several data packets at once (burst) when the NTP server is reachable and ready for synchronization.

Possible values:
- **marked**
  - The **Burst** mode is active.
  - For each polling interval, the device sends several data packets (burst) when the NTP server is reachable.
  - Only use this setting if you use a private, non-public NTP server as reference time source.
  - You use this setting with care to improve precision when the connection to the NTP server is unstable.
- **unmarked** (default setting)
  - The **Burst** mode is inactive.

**Preferred**

Marks the NTP server as preferred reference time source when multiple NTP servers are specified.

Without marking, the NTP client of the device uses standard algorithms to select the reference time source.

Mark max. 1 sufficiently precise server as **Preferred**.

Possible values:
- **marked**
  - The device uses the NTP server as the preferred reference time source. You use this setting to help prevent frequent connection changes between equal NTP servers.
- **unmarked** (default setting)
  - No preferred NTP server.

**Status**

Displays the synchronization status.

Possible values:
- **disabled**
  - No server available.
- **protocolError**
- **notSynchronized**
  - The server is available. The server itself is not synchronized.
- **notResponding**
  - The server is available. The device does not receive time information.
- **synchronizing**
  - The server is available. The device receives time information.
- **synchronized**
  - The server is available. The device has synchronized its clock with the server.
- **genericError**
  - Device-internal error.
**Active**

Activates/deactivates the connection to the NTP server.

Possible values:

- **marked**
  - The connection to the NTP server is activated.
  - The NTP client of the device obtains the time information from the unicast responses of this server.
  - If the NTP server of the device is working in symmetric mode, then this server participates in a cluster.

- **unmarked**
  - The connection to the NTP server is deactivated.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.
3 Device Security

The menu contains the following dialogs:
- User Management
- Authentication List
- LDAP
- Management Access
- Pre-login Banner

3.1 User Management

If users log in with valid login data, then the device lets them have access to its device management.

In this dialog you manage the users of the local user management. You also specify the following settings here:
- Settings for the login
- Settings for saving the passwords
- Specify policy for valid passwords

The methods that the device uses for the authentication you specify in the Device Security > Authentication List dialog.

Configuration

This frame lets you specify settings for the login.

Login attempts

Specifies the number of login attempts possible when the user accesses the device management using the Graphical User Interface and the Command Line Interface.

Note: When accessing the device management using the Command Line Interface through the serial connection, the number of login attempts is unlimited.

Possible values:
- 0..5 (default setting: 0)

If the user makes one more unsuccessful login attempt, then the device locks access for the user.

The device lets only users with the administrator authorization remove the lock.

The value 0 deactivates the lock. The user has unlimited attempts to log in.
Login attempts period (min.)

Displays the time period before the device resets the counter in the Login attempts field.

Possible values:
- 0..60 (default setting: 0)

Min. password length

The device accepts the password if it contains at least the number of characters specified here.

The device checks the password according to this setting, regardless of the setting for the Policy check checkbox.

Possible values:
- 1..64 (default setting: 6)

**Password policy**

This frame lets you specify the policy for valid passwords. The device checks every new password and password change according to this policy.

The settings effect the Password column. The prerequisite is that you mark the checkbox in the Policy check column.

Upper-case characters (min.)

The device accepts the password if it contains at least as many upper-case letters as specified here.

Possible values:
- 0..16 (default setting: 1)

The value 0 deactivates this setting.

Lower-case characters (min.)

The device accepts the password if it contains at least as many lower-case letters as specified here.

Possible values:
- 0..16 (default setting: 1)

The value 0 deactivates this setting.

Digits (min.)

The device accepts the password if it contains at least as many numbers as specified here.

Possible values:
- 0..16 (default setting: 1)

The value 0 deactivates this setting.
Special characters (min.)

The device accepts the password if it contains at least as many special characters as specified here.

Possible values:

- 0..16 (default setting: 1)

The value 0 deactivates this setting.

**Table**

Every user requires an active user account to gain access to the device management. The table lets you set up and manage user accounts.

To change settings, click the desired parameter in the table and modify the value.

**User name**

Displays the name of the user account.

To create a new user account, click the button.

**Active**

Activates/deactivates the user account.

Possible values:

- marked
  The user account is active. The device accepts the login of a user with this user name.
- unmarked (default setting)
  The user account is inactive. The device rejects the login of a user with this user name.

When one user account exists with the administrator access role, this user account is constantly active.

**Password**

Displays **** (asterisks) instead of the password with which the user logs in. To change the password, click the relevant field.

Possible values:

- Alphanumeric ASCII character string with 6..64 characters
  The following characters are allowed:
  - a..z
  - A..Z
  - 0..9
  - !#$%&'()*+,-./:;<=>?@[\]^_`{}~

The minimum length of the password is specified in the Configuration frame. The device differentiates between upper and lower case.
If the checkbox in the Policy check column is marked, then the device checks the password according to the policy specified in the Password policy frame.

The device constantly checks the minimum length of the password, even if the checkbox in the Policy check column is unmarked.

Role

Specifies the user role that regulates the access of the user to the individual functions of the device.

Possible values:

- **authorized**
  The user is blocked, and the device rejects the user login.
  Assign this value to temporarily lock the user account. If the device detects an error when another role is being assigned, then the device assigns this role to the user account.

- **guest** (default setting)
  The user is authorized to monitor the device.

- **auditor**
  The user is authorized to monitor the device and to save the log file in the Diagnostics > Report > Audit Trail dialog.

- **operator**
  The user is authorized to monitor the device and to change the settings – with the exception of security settings for device access.

- **administrator**
  The user is authorized to monitor the device and to change the settings.

The device assigns the Service Type transferred in the response of a RADIUS server as follows to a user role:

- Administrative-User: administrator
- Login-User: operator
- NAS-Prompt-User: guest

User locked

Unlocks the user account.

Possible values:

- **marked**
  The user account is locked. The user has no access to the device management.
  If the user makes too many unsuccessful login attempts, then the device automatically locks the user.

- **unmarked** (grayed out) (default setting)
  The user account is unlocked. The user has access to the device management.

Policy check

Activates/deactivates the password check.

Possible values:

- **marked**
  The password check is activated.
  When you set up or change the password, the device checks the password according to the policy specified in the Password policy frame.

- **unmarked** (default setting)
  The password check is deactivated.
SNMP auth type

Specifies the authentication protocol that the device applies for user access via SNMPv3.

Possible values:
- `hmacmd5` (default value)
  For this user account, the device uses protocol HMACMD5.
- `hmacsha`
  For this user account, the device uses protocol HMACSHA.

SNMP encryption type

Specifies the encryption protocol that the device applies for user access via SNMPv3.

Possible values:
- `none`
  No encryption.
- `des` (default value)
  DES encryption
- `aesCfb128`
  AES128 encryption

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.

- In the User name field, you specify the name of the user account.
  Possible values:
  - Alphanumeric ASCII character string with 1..32 characters
### 3.2 Authentication List

In this dialog you manage the authentication lists. In a authentication list you specify which method the device uses for the authentication. You also have the option to assign pre-defined applications to the authentication lists.

If users log in with valid login data, then the device lets them have access to its device management. The device authenticates the users using the following methods:

- User management of the device
- LDAP
- RADIUS

In the default setting the following authentication lists are available:

- `defaultLoginAuthList`
- `defaultV24AuthList`

#### Table

**Note:** If the table does not contain a list, then the access to the device management is only possible using the Command Line Interface through the serial interface of the device. In this case, the device authenticates the user by using the local user management. See the [Device Security > User Management](#) dialog.

<table>
<thead>
<tr>
<th>Name</th>
<th>Displays the name of the list.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To create a new list, click the button.</td>
</tr>
<tr>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>▶ Alphanumeric ASCII character string with 1..32 characters</td>
</tr>
</tbody>
</table>

**Policy**

Specifies the authentication policy that the device uses for access using the application specified in the *Dedicated applications* column.

The device gives you the option of a fall-back solution. For this, you specify another policy in each of the policy fields. If the authentication with the specified policy is unsuccessful, then the device can use the next policy, depending on the order of the values entered in each policy.

**Possible values:**

- **local** (default setting)
  - The device authenticates the users by using the local user management. See the [Device Security > User Management](#) dialog.
  - You cannot assign this value to the authentication list `defaultDot1x8021AuthList`.
- **radius**
  - The device authenticates the users with a RADIUS server in the network. You specify the RADIUS server in the [Network Security > RADIUS > Authentication Server](#) dialog.
Device Security
[Device Security > Authentication List]

- **reject**
  The device accepts or rejects the authentication depending on which policy you try first. The following list contains authentication scenarios:
  - If the first policy in the authentication list is *local* and the device accepts the login credentials of the user, then it logs the user in without attempting the other policies.
  - If the first policy in the authentication list is *local* and the device denies the login credentials of the user, then it attempts to log the user in using the other policies in the order specified.
  - If the first policy in the authentication list is *radius* or *ldap* and the device rejects a login, then the login is immediately rejected without attempting to log in the user using another policy.
    - If there is no response from the RADIUS or LDAP server, then the device attempts to authenticate the user with the next policy.
  - If the first policy in the authentication list is *reject*, then the device immediately rejects the user login without attempting another policy.
  - Verify that the authentication list *defaultV24AuthList* contains at least one policy different from *reject*.

- **ldap**
  The device authenticates the users with authentication data and access role saved in a central location. You specify the Active Directory server that the device uses in the Network Security > LDAP > Configuration dialog.

**Dedicated applications**
Displays the dedicated applications. When users access the device with the relevant application, the device uses the specified policies for the authentication.

To allocate another application to the list or remove the allocation, click the button and then the Allocate applications item. The device lets you assign each application to exactly one list.

**Active**
Activates/deactivates the list.

Possible values:
- **marked**
  The list is activated. The device uses the policies in this list when users access the device with the relevant application.
- **unmarked** (default setting)
  The list is deactivated.
Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Allocate applications

Opens the Allocate applications window.

- The left field displays the applications that can be allocated to the highlighted list.
- The right field displays the applications that are allocated to the highlighted list.

Buttons:
- Moves every entry to the right field.
- Moves the highlighted entries from the left field to the right field.
- Moves the highlighted entries from the right field to the left field.
- Moves every entry to the left field.

Note: When you move the entry WebInterface to the left field, the connection to the device is lost, after you click the Ok button.

3.3 LDAP

The Lightweight Directory Access Protocol (LDAP) lets you authenticate and authorize the users at a central point in the network. A widely used directory service accessible through LDAP is Active Directory®.

The device forwards the login data of the user to the authentication server using the LDAP protocol. The authentication server decides if the login data is valid and transfers the user’s authorizations to the device.

Upon successful login, the device saves the login data temporarily in the cache. This speeds up the login process when users log in again. In this case, no complex LDAP search operation is necessary.

The menu contains the following dialogs:
- LDAP Configuration
- LDAP Role Mapping
3.3.1 LDAP Configuration

This dialog lets you specify up to 4 authentication servers. An authentication server authenticates and authorizes the users when the device forwards the login data to the server.

The device sends the login data to the first authentication server. When no response comes from this server, the device contacts the next server in the table.

**Operation**

Enables/disables the LDAP client.

If in the Device Security > Authentication List dialog you specify the value `ldap` in one of the rows Policy 1 to Policy 5, then the device uses the LDAP client. Prior to this, specify in the Device Security > LDAP > Role Mapping dialog at least one mapping for this role administrator. This provides you access to the device as administrator after logging in through LDAP.

Possible values:

- **On**
  - The LDAP client is enabled.
- **Off** (default setting)
  - The LDAP client is disabled.

**Configuration**

Client cache timeout [min]

Specifies for how many minutes after successfully logging in the login data of a user remain valid. When a user logs in again within this time, no complex LDAP search operation is necessary. The login process is much faster.

Possible values:

- **1..1440** (default setting: 10)

Bind user

Specifies the user ID in the form of the “Distinguished Name” (DN) with which the device logs in to the LDAP server.

If the LDAP server requires a user ID in the form of the “Distinguished Name” (DN) for the login, then this information is necessary. In Active Directory environments, this information is unnecessary.

The device logs in to the LDAP server with the user ID to find the “Distinguished Name” (DN) for the users logging in. The device conducts the search according to the settings in the **Base DN** and **User name attribute** fields.
Possible values:
- Alphanumeric ASCII character string with 0..64 characters

**Bind user password**

Specifies the password which the device uses together with the user ID specified in the *Bind user* field when logging in to the LDAP server.

Possible values:
- Alphanumeric ASCII character string with 0..64 characters

**Base DN**

Specifies the starting point for the search in the directory tree in the form of the “Distinguished Name” (DN).

Possible values:
- Alphanumeric ASCII character string with 0..255 characters

**User name attribute**

Specifies the LDAP attribute which contains a biunique user name. Afterwards, the user uses the user name contained in this attribute to log in.

Often the LDAP attributes *userPrincipalName, mail, sAMAccountName* and *uid* contain a unique user name.

The device adds the character string specified in the *Default domain* field to the user name under the following condition:
- The user name contained in the attribute does not contain the @ character.
- In the *Default domain* field, a domain name is specified.

Possible values:
- Alphanumeric ASCII character string with 0..64 characters
  (default setting: *userPrincipalName*)
Default domain

Specifies the character string which the device adds to the user name of the users logging in if the user name does not contain the @ character.

Possible values:
- Alphanumeric ASCII character string with 0..64 characters

CA certificate

URL

Specifies the path and file name of the certificate.

The device accepts certificates with the following properties:
- X.509 format
- .PEM file name extension
- Base64-coded, enclosed by
  
  -----BEGIN CERTIFICATE-----

  and

  -----END CERTIFICATE-----

For security reasons, we recommend to constantly use a certificate which is signed by a certification authority.

The device gives you the following options for copying the certificate to the device:
- Import from the PC
  
  When the certificate is located on your PC or on a network drive, drag and drop the certificate in the area. Alternatively click in the area to select the certificate.
  
  You also have the option of transferring the certificate from your PC to the device through SFTP or SCP. Perform the following steps:
  
  - On your PC, open an SFTP or SCP client, for example WinSCP.
  - Use the SFTP or SCP client to open a connection to the device.
  - Transfer the certificate file to the directory /upload/ldapcert in the device.
  
  When the file transfer is complete, the device starts installing the certificate. If the installation was successful, then the device creates an ok file in the directory /upload/ldapcert and deletes the certificate file.

Start

Copies the certificate specified in the URL field to the device.

Table

Index

Displays the index number to which the table entry relates.
**Description**

Specifies the description.

You have the option to describe here the authentication server or note additional information.

Possible values:
- Alphanumeric ASCII character string with 0..255 characters

**Address**

Specifies the IP address or the DNS name of the server.

Possible values:
- IPv4 address  (default setting: 0.0.0.0)
- DNS name in the format `<domain>.<tld>` or `<host>.<domain>.<tld>`
- `_ldap._tcp.<domain>.<tld>`
  Using this DNS name, the device queries the LDAP server list (SRV Resource Record) from the DNS server.

If in the **Connection security** row a value other than `none` is specified and the certificate contains only DNS names of the server, then use a DNS name. Enable the **Client** function in the **Advanced > DNS > Client > Global** dialog.

**Destination TCP port**

Specifies the TCP Port on which the server expects the requests.

If you have specified the value `_ldap._tcp.domain.tld` in the **Address** column, then the device ignores this value.

Possible values:
- `0..65535`  (default setting: `389`)
  Exception: Port `2222` is reserved for internal functions.

Frequently used TCP-Ports:
- LDAP: `389`
- LDAP over SSL: `636`
- Active Directory Global Catalogue: `3268`
- Active Directory Global Catalogue SSL: `3269`

**Connection security**

Specifies the protocol which encrypts the communication between the device and the authentication server.

Possible values:
- `none`
  No encryption.
  The device establishes an LDAP connection to the server and transmits the communication including the passwords in clear text.
Device Security

[Device Security > LDAP > Configuration]

- **ssl**
  - Encryption with SSL.
  - The device establishes a TLS connection to the server and tunnels the LDAP communication over it.
- **startTLS** (default setting)
  - Encryption with startTLS extension.
  - The device establishes an LDAP connection to the server and encrypts the communication.

The prerequisite for encrypted communication is that the device uses the correct time. If the certificate contains only the DNS names, then you specify the DNS name of the server in the Address row. Enable the Client function in the Advanced > DNS > Client > Global dialog.

If the certificate contains the IP address of the server in the “Subject Alternative Name” field, then the device is able to verify the identity of the server without the DNS configuration.

### Server status

Displays the connection status and the authentication with the authentication server.

Possible values:

- **ok**
  - The server is reachable.
  - If in the Connection security row a value other than none is specified, then the device has verified the certificate of the server.
- **unreachable**
  - Server is unreachable.
- **other**
  - The device has not established a connection to the server yet.

### Active

Activates/deactivates the use of the server.

Possible values:

- **marked**
  - The device uses the server.
- **unmarked** (default setting)
  - The device does not use the server.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

### Flush cache

Removes the cached login data of the successfully logged in users.
3.3.2 LDAP Role Mapping

This dialog lets you create up to 64 mappings to assign a role to users.

In the table you specify if the device assigns a role to the user based on an attribute with a specific value or based on the group membership.

- The device searches for the attribute and the attribute value within the user object.
- By evaluating the “Distinguished Name” (DN) contained in the member attributes, the device checks group the membership.

When a user logs in, the device searches for the following information on the LDAP server:

- In the related user project, the device searches for attributes specified in the mappings.
- In the group objects of the groups specified in the mappings, the device searches for the member attributes.

On this basis, the device checks any mapping.

- Does the user object contain the required attribute?
- or
- Is the user member of the group?

If the device does not find a match, then the user does not get access to the device.

If the device finds more than one mapping that applies to a user, then the setting in the Matching policy field decides. The user either obtains the role with the more extensive authorizations or the 1st role in the table that applies.

Configuration

Matching policy

Specifies which role the device applies if more than one mapping applies to a user.

Possible values:

- **highest** (default setting)
  - The device applies the role with more extensive authorizations.
- **first**
  - The device applies the rule which has the lower value in the Index column to the user.

Table

Index

Displays the index number to which the table entry relates.
Role

Specifies the user role that regulates the access of the user to the individual functions of the device.

Possible values:
- **unauthorized**
  The user is blocked, and the device rejects the user login.
  Assign this value to temporarily lock the user account. If an error occurs when another role is being assigned, then the device assigns this role to the user account.
- **guest** (default setting)
  The user is authorized to monitor the device.
- **auditor**
  The user is authorized to monitor the device and to save the log file in the Diagnostics > Report > Audit Trail dialog.
- **operator**
  The user is authorized to monitor the device and to change the settings – with the exception of security settings for device access.
- **administrator**
  The user is authorized to monitor the device and to change the settings.

Type

Specifies if a group or an attribute with an attribute value is set in the Parameter column.

Possible values:
- **attribute** (default setting)
  The Parameter column contains an attribute with an attribute value.
- **group**
  The Parameter column contains the “Distinguished Name” (DN) of a group.

Parameter

Specifies a group or an attribute with an attribute value, depending on the setting in the Type column.

Possible values:
- Alphanumeric ASCII character string with 0..255 characters
  The device differentiates between upper and lower case.
  - If in the Type column the value attribute is specified, then you specify the attribute in the form of Attribute_name=Attribute_value.
    Example: l=Germany
  - If in the Type column the value group is specified, then you specify the “Distinguished Name” (DN) of a group.
    Example: CN=admin-users,OU=Groups,DC=example,DC=com

Active

Activates/deactivates the role mapping.

Possible values:
- **marked** (default setting)
  The role mapping is active.
- **unmarked**
  The role mapping is inactive.
Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.
- In the Index field, you specify the index number.
  Possible values:
  - 1..64

3.4 Management Access

The menu contains the following dialogs:
- Server
- IP Access Restriction
- Web
- Command Line Interface
- SNMPv1/v2 Community
3.4.1 Server

This dialog lets you set up the server services which enable users or applications to access the management of the device.

The dialog contains the following tabs:
- [Information]
- [SNMP]
- [SSH]
- [HTTP]
- [HTTPS]

[Information]

This tab displays as an overview which server services are enabled.

Table

SNMPv1
Displays if the server service is active or inactive, which authorizes access to the device using SNMP version 1. See the SNMP tab.

Possible values:
- marked
  Server service is active.
- unmarked
  Server service is inactive.

SNMPv2
Displays if the server service is active or inactive, which authorizes access to the device using SNMP version 2. See the SNMP tab.

Possible values:
- marked
  Server service is active.
- unmarked
  Server service is inactive.
SNMPv3

Displays if the server service is active or inactive, which authorizes access to the device using SNMP version 3. See the SNMP tab.

Possible values:
- marked
  - Server service is active.
- unmarked
  - Server service is inactive.

SSH server

Displays if the server service is active or inactive, which authorizes access to the device using Secure Shell. See the SSH tab.

Possible values:
- marked
  - Server service is active.
- unmarked
  - Server service is inactive.

HTTP server

Displays if the server service is active or inactive, which authorizes access to the device using the Graphical User Interface through HTTP. See the HTTP tab.

Possible values:
- marked
  - Server service is active.
- unmarked
  - Server service is inactive.

HTTPS server

Displays if the server service is active or inactive, which authorizes access to the device using the Graphical User Interface through HTTPS. See the HTTPS tab.

Possible values:
- marked
  - Server service is active.
- unmarked
  - Server service is inactive.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
This tab lets you specify settings for the SNMP agent of the device and to enable/disable access to the device with different SNMP versions.

The SNMP agent enables access to the device management with SNMP-based applications.

**Configuration**

**SNMPv1**

Activates/deactivates the access to the device with SNMP version 1.

Possible values:

- **marked** (default setting)
  - Access is activated.

- **unmarked**
  - Access is deactivated.

You specify the community names in the Device Security > Management Access > SNMPv1/v2 Community dialog.

**SNMPv2**

Activates/deactivates the access to the device with SNMP version 2.

Possible values:

- **marked** (default setting)
  - Access is activated.

- **unmarked**
  - Access is deactivated.

You specify the community names in the Device Security > Management Access > SNMPv1/v2 Community dialog.

**SNMPv3**

Activates/deactivates the access to the device with SNMP version 3.

Possible values:

- **marked** (default setting)
  - Access is activated.

- **unmarked**
  - Access is deactivated.

Network management systems like Industrial HiVision use this protocol to communicate with the device.
Device Security

[Device Security > Management Access > Server]

UDP port

Specifies the number of the UDP port on which the SNMP agent receives requests from clients.

Possible values:

- **1..65535** (default setting: **161**)
  - Exception: Port **2222** is reserved for internal functions.

To enable the SNMP agent to use the new port after a change, you proceed as follows:

- Click the **button.
- Select in the **Basic Settings > Load/Save** dialog the active configuration profile.
- Click the **button to save the current changes.
- Restart the device.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

[SSH]

This tab lets you enable/disable the SSH server in the device and specify its settings required for SSH. The server works with SSH version 2.

The SSH server enables access to the device management remotely through the Command Line Interface. SSH connections are encrypted.

To access the device and the connected external memory using SFTP or SCP, you also need access to the SSH server. With an SFTP or SCP client, for example WinSCP, you have the option of loading configuration files or a software update to the device.

The SSH server identifies itself to the clients using its public RSA key. When first setting up the connection, the client program displays the user the fingerprint of this key. The fingerprint contains a Base64-coded character sequence that is easy to check. When you make this character sequence available to the users via a reliable channel, they have the option to compare both fingerprints. If the character sequences match, then the client is connected to the correct server.

The device lets you create the private and public keys (host keys) required for RSA directly in the device. Otherwise you have the option to copy your own keys to the device in PEM format.

As an alternative, the device lets you load the RSA key (host key) from an external memory upon restart. You activate this function in the **Basic Settings > External Memory** dialog, **SSH key auto upload** column.
Operation

Enables/disables the SSH server.

Possible values:

- **On** (default setting)
  - The SSH server is enabled.
  - The access to the device management is possible through the Command Line Interface using an encrypted SSH connection.
  - You can start the server only if there is an RSA signature in the device.

- **Off**
  - The SSH server is disabled.
  - When you disable the SSH server, the existing connections remain established. However, the device helps prevent new connections from being set up.

**Note:** If you disable the SSH server, then the access to the Command Line Interface is only possible through the serial interface of the device.

Configuration

TCP port

Specifies the number of the TCP port on which the device receives SSH requests from clients.

Possible values:

- **1..65535** (default setting: 22)
  - Exception: Port 2222 is reserved for internal functions.

The server restarts automatically after the port is changed. Existing connections remain in place.

Sessions

Displays how many SSH connections are currently established to the device.

Sessions (max.)

Specifies the maximum number of SSH connections to the device that can be set up simultaneously.

When you access the device using Command Line Interface, SFTP or SCP, each of these applications establishes a separate SSH connection to the device.

Possible values:

- **1..5** (default setting: 5)

Session timeout [min]

Specifies the timeout in minutes. After the user logged in has been inactive for this time, the device ends the connection.

A change in the value takes effect the next time a user logs in.
Possible values:

- **0**
  - Deactivates the function. The connection remains established in the case of inactivity.
- **1..160**
  - (default setting: 5)

**Fingerprint**

The fingerprint is an easy to verify string that uniquely identifies the host key of the SSH server.

After importing a new host key, the device continues to display the existing fingerprint until you restart the server.

**Fingerprint type**

Specifies which fingerprint the *RSA Fingerprint* field displays.

Possible values:

- **md5**
  - The *RSA Fingerprint* field displays the fingerprint as hexadecimal MD5 hash.
- **sha256**
  - The device does not support this setting. The *RSA Fingerprint* field retains the previous display.

**RSA Fingerprint**

Displays the fingerprint of the public host key of the SSH server.

When you change the settings in the *Fingerprint type* field, click afterwards the ✔ button and then the ◁ button to update the display.

**Signature**

**RSA present**

Displays if an RSA host key is present in the device.

Possible values:

- **marked**
  - A key is present.
- **unmarked**
  - No key is present.
Create

Generates a host key in the device. The prerequisite is that the SSH server is disabled.

Length of the key created:
- 2048 bit (RSA)

To get the SSH server to use the generated host key, re-enable the SSH server.

Alternatively, you have the option to copy your own host key to the device in PEM format. See the Key import frame.

Delete

Removes the host key from the device. The prerequisite is that the SSH server is disabled.

Oper status

Displays if the device currently generates a host key.

It is possible that another user triggered this action.

Possible values:
- rsa
  The device currently generates an RSA host key.
- none
  The device does not generate a host key.

Key import

URL

Specifies the path and file name of your own RSA host key.

The device accepts the RSA key if it has the following key length:
- 2048 bit (RSA)

The device gives you the following options for copying the key to the device:
- Import from the PC
  When the host key is located on your PC or on a network drive, drag and drop the file that contains the key in the area. Alternatively click in the area to select the file.
  You also have the option of transferring the key from your PC to the device through SFTP or SCP. Perform the following steps:
  - On your PC, open an SFTP or SCP client, for example WinSCP.
  - Use the SFTP or SCP client to open a connection to the device.
  - Transfer the file that contains the key to the directory upload/ssh-key in the device.
    When the file transfer is complete, the device starts installing the key. If the installation was successful, then the device creates an ok file in directory upload/ssh-key and deletes the file that contains the key.
  - To get the server to use this key, you restart the server.

Start

Copies the key specified in the URL field to the device.
Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

[HTTP]

This tab lets you enable/disable the HTTP protocol for the web server and specify the settings required for HTTP.

The web server provides the Graphical User Interface via an unencrypted HTTP connection. For security reasons, disable the HTTP protocol and use the HTTPS protocol instead.

The device supports up to 10 simultaneous connections using HTTP or HTTPS.

Note: If you change the settings in this tab and click the button, then the device ends the session and disconnects every opened connection. To continue working with the Graphical User Interface, log in again.

Operation

Operation enables/disables the HTTP protocol for the web server.

Possible values:

- **On** (default setting)
  - The HTTP protocol is enabled.
  - The access to the device management is possible through an unencrypted HTTP connection.
  - When the HTTPS protocol is also enabled, the device automatically redirects the request for a HTTP connection to an encrypted HTTPS connection.

- **Off**
  - The HTTP protocol is disabled.
  - When the HTTPS protocol is enabled, the access to the device management is possible through an encrypted HTTPS connection.

Note: If the HTTP and HTTPS protocols are disabled, then you can enable the HTTP protocol using the Command Line Interface command `http server` to get to the Graphical User Interface.

Configuration

TCP port

Specifies the number of the TCP port on which the web server receives HTTP requests from clients.

Possible values:

- **1..65535** (default setting: 80)
  - Exception: Port 2222 is reserved for internal functions.
Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

[HTTPS]

This tab lets you enable/disable the HTTPS protocol for the web server and specify the settings required for HTTPS.

The web server provides the Graphical User Interface via an encrypted HTTP connection.

A digital certificate is required for the encryption of the HTTP connection. The device lets you create this certificate yourself or to load an existing certificate onto the device.

The device supports up to 10 simultaneous connections using HTTP or HTTPS.

Note: If you change the settings in this tab and click the button, then the device ends the session and disconnects every opened connection. To continue working with the Graphical User Interface, log in again.

Operation

Operation

Enables/disables the HTTPS protocol for the web server.

Possible values:

- **On** (default setting)
  The HTTPS protocol is enabled.
  The access to the device management is possible through an encrypted HTTPS connection. When there is no digital certificate present, the device generates a digital certificate before it enables the HTTPS protocol.
  
- **Off**
  The HTTPS protocol is disabled.
  When the HTTP protocol is enabled, the access to the device management is possible through an unencrypted HTTP connection.

Note: If the HTTP and HTTPS protocols are disabled, then you can enable the HTTPS protocol using the Command Line Interface command `https server` to get to the Graphical User Interface.
Configuration

TCP port

Specifies the number of the TCP port on which the web server receives HTTPS requests from clients.

Possible values:
- 1..65535 (default setting: 443)
  Exception: Port 2222 is reserved for internal functions.

Fingerprint

The fingerprint is an easily verified hexadecimal number sequence that uniquely identifies the digital certificate of the HTTPS server.

After importing a new digital certificate, the device displays the current fingerprint until you restart the server.

Fingerprint type

Specifies which fingerprint the Fingerprint field displays.

Possible values:
- sha1
  The Fingerprint field displays the SHA1 fingerprint of the certificate.
- sha256
  The Fingerprint field displays the SHA256 fingerprint of the certificate.

Fingerprint

Character sequence of the digital certificate used by the server.

When you change the settings in the Fingerprint type field, click afterwards the ✔ button and then the ✂ button to update the display.

Certificate

Note: If the device uses a certificate that is not signed by a certification authority, then the web browser displays a message while loading the Graphical User Interface. To continue, add an exception rule for the certificate in the web browser.

Present

Displays if the digital certificate is present in the device.

Possible values:
- marked
  The certificate is present.
- unmarked
  The certificate has been removed.
Create

Generates a digital certificate in the device.

Until restarting the web server uses the previous certificate.

To get the web server to use the newly generated certificate, restart the web server. Restarting the web server is possible only through the Command Line Interface.

Alternatively, you have the option of copying your own certificate to the device. See the Certificate import frame.

Delete

Deletes the digital certificate.

Until restarting the web server uses the previous certificate.

Oper status

Displays if the device currently generates or deletes a digital certificate.

It is possible that another user has triggered the action.

Possible values:

▸ none
  The device does currently not generate or delete a certificate.

▸ delete
  The device currently deletes a certificate.

▸ generate
  The device currently generates a certificate.

Certificate import

URL

Specifies the path and file name of the certificate.

The device accepts certificates with the following properties:

• X.509 format

• .PEM file name extension

• Base64-coded, enclosed by
  
  -----BEGIN PRIVATE KEY-----
  and
  -----END PRIVATE KEY-----
  as well as

  -----BEGIN CERTIFICATE-----
  and
  -----END CERTIFICATE-----

• RSA key with 2048 bit length
The device gives you the following options for copying the certificate to the device:

- Import from the PC
  When the certificate is located on your PC or on a network drive, drag and drop the certificate in the area. Alternatively click in the area to select the certificate.
  You also have the option of transferring the certificate from your PC to the device through SFTP or SCP. Perform the following steps:
  - On your PC, open an SFTP or SCP client, for example WinSCP.
  - Use the SFTP or SCP client to open a connection to the device.
  - Transfer the certificate file to the directory /upload/https-cert in the device.
    When the file transfer is complete, the device starts installing the certificate. If the installation was successful, then the device creates an ok file in the directory /upload/https-cert and deletes the certificate file.
  - To get the web server to use this certificate, restart the web server. Restarting the web server is possible only through the Command Line Interface.

**Start**

Copies the certificate specified in the **URL** field to the device.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.
3.4.2 IP Access Restriction

This dialog enables you to restrict the access to the device management to specific IP address ranges and selected IP-based applications.

► If the function is disabled, then the access to the device management is possible from any IP address and using every application.

► If the function is enabled, then the access is restricted. You have access to the device management only under the following conditions:
  – At least one table entry is activated.
  – You are accessing the device with a permitted application from a permitted IP address range.

**Operation**

**Note:** Before you enable the function, verify that at least one active entry in the table lets you access. Otherwise, if you change the settings, then the connection to the device terminates. The access to the device management is possible only using the Command Line Interface through the serial interface.

Enables/disables the *IP Access Restriction* function.

Possible values:

► **On**
  
The *IP Access Restriction* function is enabled.
  
The access to the device management is restricted.

► **Off** (default setting)
  
The *IP Access Restriction* function is disabled.

**Table**

You have the option of defining up to 16 table entries and activating them separately.

**Index**

Displays the index number to which the table entry relates.

When you delete a table entry, this leaves a gap in the numbering. When you create a new table entry, the device fills the first gap.
Device Security
[Device Security > Management Access > IP Access Restriction]

Possible values:
▶ 1..16

Address

Specifies the IP address of the network from which you allow the access to the device management. You specify the network range in the Netmask column.

Possible values:
▶ Valid IPv4 address (default setting: 0.0.0.0)

Netmask

Specifies the range of the network specified in the Address column.

Possible values:
▶ Valid netmask (default setting: 0.0.0.0)

HTTP

Activates/deactivates the HTTP access.

Possible values:
▶ marked (default setting)
   Access is activated for the adjacent IP address range.
▶ unmarked
   Access is deactivated.

HTTPS

Activates/deactivates the HTTPS access.

Possible values:
▶ marked (default setting)
   Access is activated for the adjacent IP address range.
▶ unmarked
   Access is deactivated.

SNMP

Activates/deactivates the SNMP access.

Possible values:
▶ marked (default setting)
   Access is activated for the adjacent IP address range.
▶ unmarked
   Access is deactivated.
SSH

Activates/deactivates the SSH access.

Possible values:
- marked (default setting)
  Access is activated for the adjacent IP address range.
- unmarked
  Access is deactivated.

Active

Activates/deactivates the table entry.

Possible values:
- marked (default setting)
  Table entry is activated. The device restricts the access to the device management to the adjacent IP address range and the selected IP-based applications.
- unmarked
  Table entry is deactivated.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
3.4.3 Web

In this dialog you specify settings for the Graphical User Interface.

Configuration

Web interface session timeout [min]

Specifies the timeout in minutes. After the device has been inactive for this time it ends the session for the user logged in.

Possible values:

- 0..160 (default setting: 5)

The value 0 deactivates the function, and the user remains logged in when inactive.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
3.4.4 Command Line Interface

In this dialog you specify settings for the Command Line Interface. You find detailed information about the Command Line Interface in the “Command Line Interface” reference manual.

The dialog contains the following tabs:
- [Global]
- [Login banner]

[Global]

This tab lets you change the prompt in the Command Line Interface and specify the automatic closing of sessions through the serial interface when they have been inactive.

The device has the following serial interfaces.
- V.24 interface

Configuration

Login prompt

Specifies the character string that the device displays in the Command Line Interface at the start of every command line.

Possible values:
- Alphanumeric ASCII character string with 0..128 characters (0x20..0x7E) including space characters
  Wildcards
  - %d date
  - %i IP address
  - %m MAC address
  - %p product name
  - %t time
  Default setting: (EAGLE)

Changes to this setting are immediately effective in the active Command Line Interface session.

Serial interface timeout [min]

Specifies the time in minutes after which the device automatically closes the session of an inactive user logged in with the Command Line Interface through the serial interface.

Possible values:
- 0..160 (default setting: 5)
  The value 0 deactivates the function, and the user remains logged in when inactive.

A change in the value takes effect the next time a user logs in.
Buttons
You find the description of the standard buttons in section “Buttons” on page 14.

[Login banner]
In this tab you replace the start screen of the Command Line Interface with your own text.

In the default setting, the start screen displays information about the device, such as the software version and the device settings. With the function in this tab, you deactivate this information and replace it with an individually specified text.

To display your own text in the Command Line Interface and in the Graphical User Interface before the login, you use the Device Security > Pre-login Banner dialog.

Operation
Enables/disables the Login banner function.

Possible values:

- **On**
  The Login banner function is enabled.
  The device displays the text information specified in the Banner text field to the users that log in with the Command Line Interface.

- **Off** (default setting)
  The Login banner function is disabled.
  The start screen displays information about the device. The text information in the Banner text field is kept.

Banner text
Specifies the character string that the device displays in the Command Line Interface at the start of every session.

Possible values:

- Alphanumeric ASCII character string with 0..1024 characters (0x20..0x7E) including space characters
- `<Tab>`
- `<Line break>`
Remaining characters

Displays how many characters are still remaining in the Banner text field for the text information.

Possible values:

- 1024..0

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
3.4.5  **SNMPv1/v2 Community**

In this dialog you specify the community name for SNMPv1/v2 applications.

Applications send requests via SNMPv1/v2 with a community name in the SNMP data packet header. Depending on the community name, the application gets read authorization or read and write authorization for the device.

You activate the access to the device via SNMPv1/v2 in the *Device Security > Management Access > Server* dialog.

**Table**

<table>
<thead>
<tr>
<th>Community</th>
<th>Displays the authorization for SNMPv1/v2 applications to the device:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Write</strong> For requests with the community name entered, the application receives read and write authorization for the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Read</strong> For requests with the community name entered, the application receives read authorization for the device.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies the community name for the adjacent authorization.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td><strong>Alphanumeric ASCII character string with 0..32 characters</strong></td>
</tr>
<tr>
<td>private</td>
<td>(default setting for read and write authorizations)</td>
</tr>
<tr>
<td>public</td>
<td>(default setting for read authorization)</td>
</tr>
</tbody>
</table>

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.
3.5 Pre-login Banner

This dialog lets you display a greeting or information text to users before they log in.

The users see this text in the login dialog of the Graphical User Interface and of the Command Line Interface. Users logging in with SSH see the text - regardless of the client used - before or during the login.

To display the text only in the Command Line Interface, use the settings in the Device Security > Management Access > CLI dialog.

Operation

Enables/disables the Pre-login Banner function.

Using the Pre-login Banner function, the device displays a greeting or information text in the login dialog of the Graphical User Interface and of the Command Line Interface.

Possible values:

- **On**
  - The Pre-login Banner function is enabled.
  - The device displays the text specified in the Banner text field in the login dialog.
- **Off** (default setting)
  - The Pre-login Banner function is disabled.
  - The device does not display a text in the login dialog. When you enter a text in the Banner text field, this text is saved in the device.

Banner text

Specifies information text that the device displays in the login dialog of the Graphical User Interface and of the Command Line Interface.

Possible values:

- Alphanumeric ASCII character string with 0..512 characters (0x20..0x7E) including space characters
- `<Tab>`
- `<Line break>`
Remaining characters

Displays how many characters are still remaining in the Banner text field.

Possible values:

► 512...0

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
4 Network Security

The menu contains the following dialogs:

- Network Security Overview
- RADIUS
- Packet Filter
- Deep Packet Inspection
- DoS
- Intrusion Detection System

4.1 Network Security Overview

This dialog displays the network security rules used in the device.

Parameter

Port/VLAN

Specifies if the device displays VLAN- and/or port-based rules.

Possible values:

- **All** (default setting)
  The device displays the VLAN- and port-based rules specified by you.

- **Port: <Port Number>**
  The device displays port-based rules for a specific port. This selection is available, when you specified one or more rules for this port.

- **VLAN: <VLAN ID>**
  The device displays VLAN-based rules for a specific VLAN. This selection is available, when you specified one or more rules for this VLAN.

Packet filter

Displays the *Packet Filter* rules in the overview.


DNAT

Displays the *Destination NAT* rules in the overview.

You edit *Destination NAT* rules in the *Routing > NAT > Destination NAT* dialog.

Double NAT

Displays the *Double NAT* rules in the overview.

You edit *Double NAT* rules in the *Routing > NAT > Double NAT* dialog.
Network Security

[Network Security > RADIUS]

Masquerading NAT

Displays the Masquerading NAT rules in the overview.

You edit Masquerading NAT rules in the Routing > NAT > Masquerading NAT dialog.

1:1 NAT

Displays the 1:1 NAT rules in the overview.

You edit 1:1 NAT rules in the Routing > NAT > 1:1 NAT dialog.

All

Marks the adjacent checkboxes. The device displays the related rules in the overview.

None

Unmarks the adjacent checkboxes. The device does not display any rules in the overview.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

4.2 RADIUS

[Network Security > RADIUS]

With its factory settings, the device authenticates users based on the local user management. However, as the size of a network increases, it becomes more difficult to keep the login data of the users consistent across the devices.

RADIUS (Remote Authentication Dial-In User Service) lets you authenticate and authorize the users at a central point in the network. A RADIUS server performs the following tasks here:

- **Authentication**
  
  The authentication server authenticates the users when the RADIUS client at the access point forwards the login data of the users to the server.

- **Authorization**
  
  The authentication server authorizes logged in users for selected services by assigning various parameters for the relevant end device to the RADIUS client at the access point.

If you assign the radius policy to an application in the Device Security > Authentication List dialog, then the device operates in the role of the RADIUS client. The device forwards the users’ login data to the primary authentication server. The authentication server decides if the login data is valid and transfers the user’s authorizations to the device.

The device assigns the Service Type transferred in the response of a RADIUS server as follows to a user role existing in the device:

- Administrative-User: administrator
- Login-User: operator
- NAS-Prompt-User: guest
The menu contains the following dialogs:

- RADIUS Global
- RADIUS Authentication Server
- RADIUS Authentication Statistics
4.2.1 **RADIUS Global**

This dialog lets you specify basic settings for RADIUS.

**RADIUS configuration**

**Retransmits (max.)**

Specifies how many times the device retransmits an unanswered request to the authentication server before the device sends the request to an alternative authentication server.

Possible values:

- 1..15 (default setting: 4)

**Timeout [s]**

Specifies how many seconds the device waits for a response after a request to an authentication server before it retransmits the request.

Possible values:

- 1..30 (default setting: 5)

**NAS IP address (attribute 4)**

Specifies the IP address that the device transfers to the authentication server as attribute 4. Specify the IP address of the device or another available address.

Possible values:

- Valid IPv4 address (default setting: 0.0.0.0)

In many cases, there is a firewall between the device and the authentication server. In the Network Address Translation (NAT) in the firewall changes the original IP address, and the authentication server receives the translated IP address of the device.

The device transfers the IP address in this field unchanged across the Network Address Translation (NAT).

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

**Reset**

Deletes the statistics in the **Network Security > RADIUS > Authentication Statistics** dialog.
4.2.2 RADIUS Authentication Server

This dialog lets you specify up to 8 authentication servers. An authentication server authenticates and authorizes the users when the device forwards the login data to the server.

The device sends the login data to the specified primary authentication server. When the server does not respond, the device contacts the specified authentication server that is highest in the table. When no response comes from this server either, the device contacts the next server in the table.

Table

<table>
<thead>
<tr>
<th>Index</th>
<th>Displays the index number to which the table entry relates.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the name of the server. To change the value, click the relevant field.</td>
</tr>
<tr>
<td></td>
<td>Possible values: Alphanumeric ASCII character string with 1..32 characters (default setting: Default-RADIUS-Server)</td>
</tr>
<tr>
<td>Address</td>
<td>Specifies the IP address of the server. Possible values: Valid IPv4 address</td>
</tr>
<tr>
<td>Destination UDP port</td>
<td>Specifies the number of the UDP port on which the server receives requests. Possible values: 0..65535 (default setting: 1812) Exception: Port 2222 is reserved for internal functions.</td>
</tr>
<tr>
<td>Secret</td>
<td>Displays ****** (asterisks) when you specify a password with which the device logs in to the server. To change the password, click the relevant field. Possible values: Alphanumeric ASCII character string with 1..64 characters You get the password from the administrator of the authentication server.</td>
</tr>
</tbody>
</table>
Network Security
[Network Security > RADIUS > Authentication Server]

Primary server

Specifies the authentication server as primary or secondary.

Possible values:

► marked
  The server is specified as the primary authentication server. The device sends the login data for
  authenticating the users to this authentication server.
  When you activate multiple servers, the device specifies the last server activated as the primary
  authentication server.

► unmarked (default setting)
  The server is the secondary authentication server. When the device does not receive a
  response from the primary authentication server, the device sends the login data to the
  secondary authentication server.

Active

Activates/deactivates the connection to the server.

The device uses the server, if you specify in the Device Security > Authentication List dialog the value
radius in one of the rows Policy 1 to Policy 5.

Possible values:

► marked (default setting)
  The connection is active. The device sends the login data for authenticating the users to this
  server if the preconditions named above are fulfilled.

► unmarked
  The connection is inactive. The device does not send any login data to this server.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.

► In the Index field, you specify the index number.

► In the Address field, you specify the IP address of the server.
4.2.3 RADIUS Authentication Statistics

This dialog displays information about the communication between the device and the authentication server. The table displays the information for each server in a separate row.

To delete the statistic, click in the Network Security > RADIUS > Global dialog the Clear RADIUS statistics? button.

Table

<table>
<thead>
<tr>
<th>Name</th>
<th>Displays the name of the server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Displays the IP address of the server.</td>
</tr>
<tr>
<td>Round trip time</td>
<td>Displays the time interval in hundredths of a second between the last response received from the server (Access Reply/Access Challenge) and the corresponding data packet sent (Access Request).</td>
</tr>
<tr>
<td>Access requests</td>
<td>Displays the number of access data packets that the device sent to the server. This value does not take repetitions into account.</td>
</tr>
<tr>
<td>Retransmitted access-request packets</td>
<td>Displays the number of access data packets that the device retransmitted to the server.</td>
</tr>
<tr>
<td>Access accepts</td>
<td>Displays the number of access accept data packets that the device received from the server.</td>
</tr>
<tr>
<td>Access rejects</td>
<td>Displays the number of access reject data packets that the device received from the server.</td>
</tr>
<tr>
<td>Access challenges</td>
<td>Displays the number of access challenge data packets that the device received from the server.</td>
</tr>
<tr>
<td>Malformed access responses</td>
<td>Displays the number of malformed access response data packets that the device received from the server (including data packets with an invalid length).</td>
</tr>
</tbody>
</table>
Bad authenticators

Displays the number of access response data packets with an invalid authenticator that the device received from the server.

Pending requests

Displays the number of access request data packets that the device sent to the server to which it has not yet received a response from the server.

Timeouts

Displays how many times no response to the server was received before the specified waiting time elapsed.

Unknown types

Displays the number data packets with an unknown data type that the device received from the server on the authentication port.

Packets dropped

Displays the number of data packets that the device received from the server on the authentication port and then discarded them.

Buttons

You find the description of the standard buttons in section "Buttons" on page 14.

4.3 Packet Filter

In this menu, you specify the settings for the Packet Filter functions.

The menu contains the following dialogs:

- Routed Firewall Mode
- Transparent Firewall Mode
4.3.1 Routed Firewall Mode

In this menu, you specify the settings for the *Routed Firewall Mode* packet filter.

The *Routed Firewall Mode* packet filter contains rules which the device applies successively to the data stream on its router interfaces. The *Routed Firewall Mode* packet filter evaluates the data stream statefully and filters undesired data packets selectively. The device considers the status of the connection, and also determines if the data packets belong to a specific connection (*Stateful Packet Inspection*).

If a data packet matches the criteria of one or more rules, then the device applies the action specified in the first rule that matches to the data stream. The device ignores the rules that follow the first rule that matches.

If no rule matches, then the device applies the default rule. In the default setting, the standard rule has the value *accept*. The device lets you change the standard rule in the *Network Security > Packet Filter > Routed Firewall Mode > Global* dialog.

The device provides a multi-step approach to set up and apply the *Packet Filter* rules:
- You create a rule.
- You assign the rule to a router interface.
  - Up to this step, changes have no effect on the behavior of the device and the data stream.
- The device applies the rule to the data stream.

The data packets go through the filter functions of the device in the following sequence:

![Diagram of data packet processing sequence]

*Figure 1: Processing sequence of the data packets in the device*

The menu contains the following dialogs:
- Global
- Firewall Learning Mode
- Packet Filter Rule
- Packet Filter Assignment
- Packet Filter Overview
4.3.1.1 Global

In this dialog you specify the global settings for the Routed Firewall Mode packet filter.

Configuration

Allowed rules for L3 firewalling (max.)

Displays the maximum number of allowed firewall rules for data packets.

Default policy

Specifies how the firewall processes data packets if no rule applies.

Possible values:
- `accept` (default setting)
  The device accepts the data packets.
- `drop`
  The device discards the data packets.
- `reject`
  The device discards the data packet and sends an ICMP Admin Prohibited message to the sender.

Validate checksum

Specifies how the firewall handles connection tracking on the basis of data packet checksum.

Possible values:
- `marked` (default setting)
  The device evaluates the checksum in the data packet. If the value is invalid, then the device drops the data packet.
- `unmarked`
  The device ignores the checksum. The device forwards the data packet even if the value is invalid.

Information

Uncommitted changes present

Displays if the Packet Filter rules applied to the data stream differ from the Packet Filter rules saved in the device.

Possible values:
- `marked`
  At least one of the Packet Filter rules saved in the device contains modified settings. When you click the Commit button, the device applies the Packet Filter rules to the data stream.
- `unmarked`
  The device applies the saved Packet Filter rules to the data stream.
**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

**Commit**

Applies the rules saved in the device to the data stream.

In the process, the device also removes the state information from the packet filter. This includes potential DCE RPC information of the **OPC Enforcer**. In the process, the device interrupts open communication connections.

**Note:** While the device activates the saved rules, you cannot set up any new communication connections.
4.3.1.2 Firewall Learning Mode

This dialog lets you specify the connections which you allow to have access to your network.

The maximum number of rules that you can configure using the FLM function depends on the number of rules already configured in the Packet Filter Rule dialog. The device lets you configure up to a total of 2048 rules.

The FLM function only applies to packets that pass through the device matching the FORWARD chain. The packets that the device receives on the INPUT chain, and those that the device creates on the OUTPUT chain traverse the device unrestricted. During the learning phase the device retains SSH, SNMP, and GUI access.

The FLM function requires you to configure and select at least 2 router interfaces in the device.

The maximum number of connections that the FLM function can learn is 65535.

Note: During the learning phase your network is temporarily exposed, because Firewall Learning Mode configures rules to accept every data packet on the selected ports.

Note: If you enable the VRRP function on a router interface, then the FLM function is ineffective on this router interface.

The dialog contains the following tabs:
- [Configuration]
- [Rules]

[Configuration]

The tab lets you enable the FLM function. The device monitors up to 4 interfaces to discover what type of data traverses the port into your network.

Operation

Enables/disables the FLM function.

Possible values:
- **On**
  The FLM function is enabled.
- **Off** (default setting)
  The FLM function is disabled.
Network Security
[Network Security > Packet Filter > Routed Firewall Mode > FLM]

Information

Status

Displays the state of the running Firewall Learning Mode application.

Possible values:

- \textit{off}
  The function is inactive.
- \textit{stopped-data-notpresent}
- \textit{stopped-data-present}
  The device stopped the learning mode. Check the Rule tab for learned data.
- \textit{learning}
  The device is learning data.
- \textit{pending}
  The device is busy processing learned data.

Information

Displays the status of Firewall Learning Mode application memory.

Additional information

Displays a special status message.

Learned entries

Displays the number of Layer 3 entries in the connection table.

Free memory for learning data [%]

Displays the percentage of free memory available for learning data.

Configuration

Available Interfaces

Displays the interfaces that are available for the FLM function.

Selected Interfaces

Specifies the interfaces that the FLM function is actively monitoring. The maximum number of interfaces that the device can monitor is 4.
Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Moves the entries highlighted in the Available Interfaces field to the Selected Interfaces field. For the FLM function, you can only select active router interfaces.

Moves the entries highlighted in the Selected Interfaces field to the Available Interfaces field.

Start

Starts the learning phase. The device filters the data packets on the active interfaces.

Stop

Stops the learning phase.

Continue

Continues the learning phase from a previous session, without clearing the memory.

Clear

Clears the memory. Learned data can be cleared only when the FLM function is stopped.

[Rules]

This tab displays the type of data that is traversing the selected ports. This lets you create rules to manage the data stream traversing the device. Using the data displayed in the Learned entries frame you can accept or reject data as required.

The tab is active after the device forwards one data packet and the FLM function is disabled again.

Learned entries

Source address

Displays the source address of the packets.

Destination address

Displays the destination address of the packet.

Destination port

Displays the destination port of the packet.
Network Security

Ingress interface
Displays the interface that received the packet.

Egress interface
Displays the interface that sent the packet.

Protocol
Displays the IP protocol, based on RFC 791, for protocol filtering.

First Occurrence
Displays the first time that the device has determined the packet.

Connections by Rule Set
Displays the number of connections that match the rules set in the table below.

Connections by Selection
Displays the number of connections that match the selections in the table below.

Packetfilter Rules

Rule index
Displays the sequential number of the Packet Filter rule. The device automatically assigns the number.

Source address
Specifies the source address of the data packets to which the device applies the rule.
Possible values:
- any (default setting)
  The device applies the Packet Filter rule to data packets with any source address.
- Valid IPv4 address
  The device applies the rule to data packets with the specified source address.
- Valid IPv4 address and netmask in CIDR notation
  The device applies the rule to data packets with the specified source address in the specified subnet.
- An exclamation mark (!) preceding the IP address reverses the expression into its opposite. The device applies the rule to data packets which do not contain the source address specified here.

Destination address
Specifies the destination address of the data packets to which the device applies the rule.
Possible values:
- any (default setting)
  The device applies the Packet Filter rule to data packets with any destination address.
Valid IPv4 address
The device applies the rule to data packets with the specified destination address.

Valid IPv4 address and netmask in CIDR notation
The device applies the rule to data packets with the specified destination address in the specified subnet.

An exclamation mark (!) preceding the IP address reverses the expression into its opposite. The device applies the rule to data packets which do not contain the destination address specified here.

Protocol
Specifies the protocol type of the data packets to which the device applies the rule. The device applies the rule only to data packets with a Protocol field of the specified value.

Possible values:
- **any** (default setting)
  The device applies the rule to every data packet without evaluating the protocol.
- **icmp**
  Internet Control Message Protocol (RFC 792)
- **igmp**
  Internet Group Management Protocol
- **ipip**
  IP in IP tunneling (RFC 2003)
- **tcp**
  Transmission Control Protocol (RFC 793)
- **udp**
  User Datagram Protocol (RFC 768)
- **esp**
  IPsec Encapsulated Security Payload (RFC 2406)
- **ah**
  IPsec Authentication Header (RFC 2402)
- **icmpv6**
  Internet Control Message Protocol for IPv6

Destination port
Specifies the destination port of the data packets to which the device applies the rule.

Possible values:
- **any** (default setting)
  The device applies the Packet Filter rule to every data packet without evaluating the destination port.
- **1..65535**
  The device applies the Packet Filter rule only to data packets containing the specified destination port.
  The field lets you specify the following options:
  - You specify a port with a single numerical value, for example **21**.
  - You specify multiple individual ports with numerical values separated by commas, for example **21,80,110**.
  - You specify a port range with numerical values connected by dashes, for example **2000-3000**.
  - You can also combine ports and port ranges, for example **21,2000-3000,65535**.
  The field lets you specify up to 15 numerical values. When you enter **21,2000-3000,65535**, for example, you use 4 of 15 numerical values.
Action

Specifies how the device handles received data packets when the device applies the rule.

Possible values:

- `accept` (default setting)
  The device accepts the data packets according to the ingress rules. Afterwards, the device applies the egress rules before sending the data packets.

- `drop`
  The device discards the data packet without informing the sender.

- `reject`
  The device discards the data packet and informs the sender.

- `enforce-modbus`
  The device applies the rule specified in the DPI profile index column to the data packets.

- `enforce-opc`
  The device applies the rule specified in the DPI profile index column to the data packets.

Description

Specifies a name or description for the rule.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters

Ingress interface

Displays if the device applies the Packet Filter rule to data packets received or sent on a router interface.

Possible values:

- `ingress`
  The device applies the Packet Filter rule to data packets received on the router interface.

- `egress`
  The device applies the Packet Filter rule to data packets sent on the router interface.

Active

Activates/deactivates the rule.

Possible values:

- `marked` (default setting)
  The rule is active.

- `unmarked`
  The rule is inactive.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

Create

Creates a new rule when the Learned entries frame displays at least an entry. The Packetfilter Rules frame displays the newly created rule.
Edit

Lets you edit the rule highlighted in the Packetfilter Rules frame.

Delete

Deletes the rule highlighted in the Packetfilter Rules frame.
4.3.1.3 Packet Filter Rule

This dialog lets you set up rules for the packet filter. You assign the rules specified here to the desired ports in the Network Security > Packet Filter > Routed Firewall Mode > Assignment dialog.

Table

<table>
<thead>
<tr>
<th>Rule index</th>
<th>Displays the sequential number of the Packet Filter rule. The device automatically assigns this number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Specifies a name or description for the rule. Possible values:</td>
</tr>
<tr>
<td></td>
<td>► Alphanumeric ASCII character string with 0..64 characters</td>
</tr>
<tr>
<td>Source address</td>
<td>Specifies the source address of the data packets to which the device applies the rule. Possible values:</td>
</tr>
<tr>
<td></td>
<td>► any (default setting) The device applies the Packet Filter rule to data packets with any source address.</td>
</tr>
<tr>
<td></td>
<td>► Valid IPv4 address The device applies the rule to data packets with the specified source address.</td>
</tr>
<tr>
<td></td>
<td>► Valid IPv4 address and netmask in CIDR notation The device applies the rule to data packets with the specified source address in the specified subnet.</td>
</tr>
<tr>
<td></td>
<td>► An exclamation mark (!) preceding the IP address reverses the expression into its opposite. The device applies the rule to data packets which do not contain the source address specified here.</td>
</tr>
<tr>
<td>Destination address</td>
<td>Specifies the destination address of the data packets to which the device applies the rule. Possible values:</td>
</tr>
<tr>
<td></td>
<td>► any (default setting) The device applies the Packet Filter rule to data packets with any destination address.</td>
</tr>
<tr>
<td></td>
<td>► Valid IPv4 address The device applies the rule to data packets with the specified destination address.</td>
</tr>
<tr>
<td></td>
<td>► Valid IPv4 address and netmask in CIDR notation The device applies the rule to data packets with the specified destination address in the specified subnet.</td>
</tr>
<tr>
<td></td>
<td>► An exclamation mark (!) preceding the IP address reverses the expression into its opposite. The device applies the rule to data packets which do not contain the destination address specified here.</td>
</tr>
</tbody>
</table>
Protocol

Specifies the IP protocol or Layer 4 protocol type of the data packets to which the device applies the rule. The device applies the rule only to data packets with a Protocol field of the specified value.

Possible values:
- `any` (default setting)
  The device applies the rule to every data packet without evaluating the protocol.
- `icmp`
  Internet Control Message Protocol (RFC 792)
- `igmp`
  Internet Group Management Protocol
- `ipip`
  IP in IP tunneling (RFC 2003)
- `tcp`
  Transmission Control Protocol (RFC 793)
- `udp`
  User Datagram Protocol (RFC 768)
- `esp`
  IPsec Encapsulated Security Payload (RFC 2406)
- `ah`
  IPsec Authentication Header (RFC 2402)
- `icmpv6`
  Internet Control Message Protocol for IPv6

Source port

Specifies the source port of the data packets to which the device applies the rule.

Possible values:
- `any` (default setting)
  The device applies the Packet Filter rule to every data packet without evaluating the source port.
- `1..65535`
  The device applies the Packet Filter rule only to data packets containing the specified source port.
  The field lets you specify the following options:
  - You specify a port with a single numerical value, for example 21.
  - You specify multiple individual ports with numerical values separated by commas, for example 21,80,110.
  - You specify a port range with numerical values connected by dashes, for example 2000-3000.
  - You can also combine ports and port ranges, for example 21,2000-3000,65535.
  The field lets you specify up to 15 numerical values. When you enter 21,2000-3000,65535, for example, you use 4 of 15 numerical values.

Destination port

Specifies the destination port of the data packets to which the device applies the rule.

Possible values:
- `any` (default setting)
  The device applies the Packet Filter rule to every data packet without evaluating the destination port.
- `1..65535`
  The device applies the Packet Filter rule only to data packets containing the specified destination port.
  The field lets you specify the following options:
– You specify a port with a single numerical value, for example 21.
– You specify multiple individual ports with numerical values separated by commas, for example 21,80,110.
– You specify a port range with numerical values connected by dashes, for example 2000-3000.
– You can also combine ports and port ranges, for example 21,2000-3000,65535.

The field lets you specify up to 15 numerical values. When you enter 21,2000-3000,65535, for example, you use 4 of 15 numerical values.

Parameters

Specifies additional parameters for this rule.

Enter parameters in the form <param>=<val>. If you enter multiple parameters, then separate them using a comma. If you enter multiple values, then separate them using a vertical bar.

Some parameters are valid when you use a specific protocol. Exception: the value mac is valid independently of the protocol. You also have the option of entering a combination of valid rules and protocol-specific rules.

Possible values:

- none (default setting)
  You have not specified any additional parameters for this rule.
- mac=de:ad:de:ad:be:ef
  This rule applies to packets with the source MAC address de:ad:de:ad:be:ef.
- type=<0..255>
  This rule applies to packets with a specific ICMP type. Enter exactly one value (for the meaning of these values see RFC 792).
- code=<0..255>
  This rule applies to packets with a specific ICMP code. Enter exactly one value (for the meaning of these values see RFC 792).
- frags=true|false
  When true, this rule applies to fragmented packets for which you set specific rules.
- flags=syn|ack|fin
  This rule applies to packets for which you set specific flags.
- flags=syn
  This rule applies to packets for which you set the syn flag.
- flags=syn|ack|fin
  This rule applies to packets for which you set the syn, ack, or fin flag.
- mac=de:ad:de:ad:be:ef, state=new|rel, flags=syn
  This rule applies to packets that come from the de:ad:de:ad:be:ef MAC address, are in a new or relative connection, and for which you set the syn flag.

Action

Specifies how the device processes received data packets when the device applies the rule.

Possible values:

- accept (default setting)
  The device accepts the data packets according to the ingress rules. Afterwards, the device applies the egress rules before transmitting the data packets.
- drop
  The device discards the data packet without informing the sender.
- reject
  The device discards the data packet and informs the sender.
Network Security
[Network Security > Packet Filter > Routed Firewall Mode > Rule]

- **enforce-modbus**
  The device applies the rule specified in the **DPI profile index** column to the data packets. The value is only available in the device variant **MB** or **01**. Refer to the **Software level** characteristic value in the product code.

- **enforce-opc**
  The value is only available in the device variant **OP** or **01**. Refer to the **Software level** characteristic value in the product code.

- **enforce-dnp3**
  The device applies the rule specified in the **DPI profile index** column to the data packets. The value is only available in the device variant **SU** or **UN**. Refer to the **Software level** characteristic value in the product code.

**Log**

Activates/deactivates the logging in the log file.

Possible values:
- **marked**
  Logging is active.
  When the device applies the **Packet Filter** rule to a data packet, the device places an entry in the log file. See the **Diagnostics > Report > System Log** dialog.
- **unmarked** (default setting)
  Logging is inactive.

**Trap**

Activates/deactivates the sending of SNMP traps when the **Packet Filter** rule is applied to data packets.

Possible values:
- **marked**
  If the device applies the **Packet Filter** rule to a data packet, then the device sends an SNMP trap.
- **unmarked** (default setting)
  The sending of SNMP traps is deactivated.

The prerequisite for sending SNMP traps is that you enable the function in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog and specify at least one trap destination.

**DPI profile index**

Specifies which rule the device applies to the data packets. The prerequisite for changing the value is that you specify one of the following values in the **Action** column.
- **enforce-modbus**
- **enforce-opc**
- **enforce-dnp3**

Possible values:
- **0** (default setting)
  The device does not apply any rule to the data packets.
- **1..32**
  The device applies the rule with the specified **Index number** to the data packets.
Active

Activates/deactivates the rule.

Possible values:
- **marked** (default setting)
  The rule is active.
- **unmarked**
  The rule is inactive.

To apply the changes to the data stream, click the ✓ button, then the button and then the Commit item in the Network Security > Packet Filter > Routed Firewall Mode > Global dialog or in the Network Security > Packet Filter > Routed Firewall Mode > Assignment dialog.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.
4.3.1.4 Packet Filter Assignment

This dialog lets you assign one or more Packet Filter rules to the router interfaces of the device. You set up router interfaces in the Routing > Interfaces > Configuration dialog.

**Information**

**Assignments**
Display how many rules are active for the ports.

**Uncommitted changes present**
Displays if the Packet Filter rules applied to the data stream differ from the Packet Filter rules saved in the device.

Possible values:
- **marked**
  At least one of the Packet Filter rules saved in the device contains modified settings. When you click the Commit button, the device applies the Packet Filter rules to the data stream.
- **unmarked**
  The device applies the saved Packet Filter rules to the data stream.

**Table**

**Description**
Displays the name or description of the rule. You specify the description in the Network Security > Packet Filter > Routed Firewall Mode > Rule dialog.

**Rule index**
Displays the sequential number of the Packet Filter rule. To specify this number, click the button.

**Interface**
Displays the interface to which the device applies the rule. To specify this interface, click the button. The device displays ports to which you enable the Routing function.

**Direction**
Displays if the device applies the Packet Filter rule to data packets received or sent.

Possible values:
- **ingress**
  The device applies the Packet Filter rule to data packets received on the router interface.
- **egress**
  The device applies the Packet Filter rule to data packets sent on the router interface.
Priority

Specifies the priority of the Packet Filter rule.

Using the priority, you specify the sequence in which the device applies the rules to the data stream. The device applies the rules in ascending order which starts with priority 0.

Possible values:
- 0..4294967295

Active

Activates/deactivates the rule.

Possible values:
- marked (default setting)
  - The rule is active.
- unmarked
  - The rule is inactive.

To apply the changes to the data stream, click the ✔ button, then the ▪ button and then the Commit item.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create dialog to assign a rule to a router interface.

- In the Interface field, you specify the router interface to which the device applies the rule.
- In the Direction field, you specify if the device applies the rule to data packets received or sent.
- In the Rule index field, you specify the rule which you assign to the router interface.

Commit

Applies the rules saved in the device to the data stream.

In the process, the device also removes the state information from the packet filter. This includes potential DCE RPC information of the OPC Enforcer. In the process, the device interrupts open communication connections.

Note: While the device activates the saved rules, you cannot set up any new communication connections.
4.3.1.5 Packet Filter Overview

This dialog gives you an overview of the specified Packet Filter rules.

**Table**

Description

Displays the name or description of the rule. You specify the description in the Network Security > Packet Filter > Routed Firewall Mode > Rule dialog.

Rule index

Displays the sequential number of the Packet Filter rule.

Interface

Displays the interface to which the device applies the rule.

Direction

Displays if the device applies the Packet Filter rule to data packets received or sent.

Possible values:

- **ingress**
  The device applies the Packet Filter rule to data packets received on the router interface.

- **egress**
  The device applies the Packet Filter rule to data packets sent on the router interface.

Priority

Displays the priority of the Packet Filter rule. The device applies the rules in ascending order which starts with priority 0.

Source address

Displays the source address of the data packets to which the device applies the rule.

Possible values:

- **any**
  The device applies the Packet Filter rule to data packets with any source address.

- **Valid IPv4 address**
  The device applies the Packet Filter rule only to data packets containing the source address specified here.

- **Valid IPv4 address and netmask in CIDR notation**
  The device applies the Packet Filter rule only to data packets containing a source address in the subnet specified here.

- **An exclamation mark (!) preceding the IP address** reverses the expression into its opposite. The device applies the rule to data packets which do not contain the source address specified here.
Source port

Displays the source port of the data packets to which the device applies the rule.

Possible values:

- any
  - The device applies the Packet Filter rule to every data packet without evaluating the source port.
- 1..65535
  - The device applies the Packet Filter rule only to data packets containing the specified source port.

Destination address

Specifies the destination address of the data packets to which the device applies the rule.

Possible values:

- any (default setting)
  - The device applies the Packet Filter rule to data packets with any destination address.
- Valid IPv4 address
  - The device applies the rule to data packets with the specified destination address.
- Valid IPv4 address and netmask in CIDR notation
  - The device applies the rule to data packets with the specified destination address in the specified subnet.
- An exclamation mark (!) preceding the IP address reverses the expression into its opposite. The device applies the rule to data packets which do not contain the destination address specified here.

Destination port

Displays the destination port of the data packets to which the device applies the rule.

Possible values:

- any
  - The device applies the Packet Filter rule to every data packet without evaluating the destination port.
- 1..65535
  - The device applies the Packet Filter rule only to data packets containing the specified destination port.

Protocol

Displays the IP protocol to which the Packet Filter rule is restricted. The device applies the rule only to data packets with a Protocol field of the specified value.

Possible values:

- icmp
  - Internet Control Message Protocol (RFC 792)
- igmp
  - Internet Group Management Protocol
- ipip
  - IP in IP tunneling (RFC 1853)
- tcp
  - Transmission Control Protocol (RFC 793)
- udp
  - User Datagram Protocol (RFC 768)
Network Security

[Network Security > Packet Filter > Routed Firewall Mode > Overview]

- **esp**
  IPsec Encapsulated Security Payload (RFC 2406)

- **ah**
  IPsec Authentication Header (RFC 2402)

- **icmpv6**
  Internet Control Message Protocol for IPv6

- **any**
  The device applies the **Packet Filter** rule to every data packet without evaluating the IP protocol.

### Parameters

Displays additional parameters for this rule.

#### Possible values:

- **none**  
  (default setting)
  You have not specified any additional parameters for this rule.

- **mac=de:ad:de:ad:be:ef**
  This rule applies to packets with the source MAC address **de:ad:de:ad:be:ef**.

- **type=<0..255>**
  This rule applies to packets with a specific ICMP type. Enter exactly one value (for the meaning of these values see RFC 792).

- **code=<0..255>**
  This rule applies to packets with a specific ICMP code. Enter exactly one value (for the meaning of these values see RFC 792).

- **frags=<true|false>**
  When **true**, this rule applies to fragmented packets for which you set specific rules.

- **flags=<syn|ack|fin>**
  This rule applies to packets for which you set specific flags.

- **flags=syn**
  This rule applies to packets for which you set the **syn** flag.

- **flags=syn|ack|fin**
  This rule applies to packets for which you set the **syn**, **ack**, or **fin** flag.

- **mac=de:ad:de:ad:be:ef,state=new|rel,flags=syn**
  This rule applies to packets that come from the **de:ad:de:ad:be:ef** MAC address, are in a new or relative connection, and for which you set the **syn** flag.

### Action

Displays how the device processes received data packets when the device applies the rule.

#### Possible values:

- **accept**
  The device accepts the data packets.

- **drop**
  The device drops the data packets.

- **reject**
  The device rejects the data packets.

- **enforce-modbus**
  The device applies the **Modbus Enforcer** rule to the data packets.

- **enforce-opc**
  The device applies the **OPC Enforcer** rule to the data packets.

- **enforce-dnp3**
  The device applies the **DNP3 Enforcer** rule to the data packets.
Log

Displays if the device places an entry in the log file when the device applies the rule to a data packet.

Possible values:
- marked
  When the device applies the Packet Filter rule to a data packet, the device places an entry in the log file. See the Diagnostics > Report > System Log dialog.
- unmarked
  Logging is disabled.

Trap

Displays if the device sends an SNMP trap when the device applies the rule to a data packet.

Possible values:
- marked
  The device sends an SNMP trap.
- unmarked
  The device does not send an SNMP trap.

The prerequisite for sending SNMP traps is that you enable the function in the Diagnostics > Status Configuration > Alarms (Traps) dialog and specify at least one trap destination.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

4.3.2 Transparent Firewall Mode

In this menu, you specify the settings for the Transparent Firewall Mode packet filter. The Transparent Firewall Mode packet filter contains rules which the device applies successively to the data stream on its non-routing ports or VLAN interfaces. The Transparent Firewall Mode packet filter evaluates every data packet that passes through the firewall regardless of the connection status (Stateless Packet Inspection).

The device filters the undesired data packets selectively while the connection is unknown.
- If a data packet matches the criteria of one or more rules, then the device applies the action specified in the first applicable rule to the data stream. The device ignores the rules that follow the first applicable rule.
- If no rule matches, then the device applies the default rule. In the default setting, the standard rule has the value accept. The device lets you change the standard rule in the Network Security > Packet Filter > Transparent Firewall Mode > Global dialog.

The device provides a multi-step approach to set up and apply the Packet Filter rules:
- You create a rule.
- You assign the rule to a non-routing port or VLAN.
  Up to this step, changes have no effect on the behavior of the device and the data stream.
- The device applies the rule to the data stream.
The device processes data packets in the following sequence:

![Processing sequence of the data packets in the device](image)

**Figure 2:** Processing sequence of the data packets in the device

The menu contains the following dialogs:
- Packet Filter Global
- Packet Filter Rule
- Packet Filter Assignment
- Packet Filter Overview
4.3.2.1 **Packet Filter Global**

In this dialog you specify the global settings for the *Transparent Firewall Mode* packet filter.

**Configuration**

- **Allowed rules for L2 firewalling (max.)**
  Displays the maximum number of allowed firewall rules for data packets.

- **Default policy**
  Specifies how the firewall processes data packets if no rule applies.
  
  Possible values:
  - `accept` (default setting)
    The device accepts the data packets.
  - `drop`
    The device discards the data packets.

- **Validate FCS**
  Specifies if the firewall evaluates the *Frame Check Sequence* of data packets.
  
  Possible values:
  - `marked` (default setting)
    The device evaluates the *Frame Check Sequence* in the data packet. If the value is invalid, then the device drops the data packet.
  - `unmarked`
    The device ignores the *Frame Check Sequence*. The device forwards the data packet even if the value is invalid.

**Information**

- **Uncommitted changes present**
  Displays if the *Packet Filter* rules applied to the data stream differ from the *Packet Filter* rules saved in the device.
  
  Possible values:
  - `marked`
    At least one of the *Packet Filter* rules saved in the device contains modified settings. When you click the *Commit* button, the device applies the *Packet Filter* rules to the data stream.
  - `unmarked`
    The device applies the saved *Packet Filter* rules to the data stream.
**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

**Commit**

Applies the rules saved in the device to the data stream.

**Note:** While the device activates the saved rules, you cannot set up any new communication connections.
### 4.3.2.2 Packet Filter Rule

This dialog lets you set up rules for the packet filter. You assign the rules specified here to the desired non-routing ports or VLANs in the Network Security > Packet Filter > Transparent Firewall Mode > Assignment dialog.

#### Table

<table>
<thead>
<tr>
<th>Index</th>
<th>Displays the sequential number of the Packet Filter rule. The device automatically assigns this number.</th>
</tr>
</thead>
</table>
| **Description** | Specifies a name or description for the rule. Possible values:  
  - Alphanumeric ASCII character string with 0..64 characters |
| **Action** | Specifies how the device processes received data packets when the device applies the rule. Possible values:  
  - accept (default setting)  
    The device accepts the data packets according to the ingress rules. Afterwards, the device applies the egress rules before transmitting the data packets.  
  - drop  
    The device discards the data packet without informing the sender. |
| **Source MAC address** | Specifies the source address of the MAC data packets to which the device applies the rule. Possible values:  
  - any (default setting)  
    The device applies the rule to MAC data packets with any source address.  
  - Valid MAC address  
    The device applies the rule to MAC data packets with the specified source address.  
  - Example: 00:11:22:33:44:55 |
Destination MAC address

Specifies the destination address of the MAC data packets to which the device applies the rule.

Possible values:
- **any** (default setting)
  The device applies the rule to MAC data packets with any destination address.
- **Valid MAC address**
  The device applies the rule to MAC data packets with the specified destination address.
  Example: `00:11:22:33:44:55`

Ethertype

Specifies the *Ethertype* keyword of the MAC data packets to which the device applies the rule.

Possible values:
- **custom** (default setting)
  The device applies the value specified in the *Ethertype custom value* column.
- **appletalk**
- **arp**
- **ibmsna**
- **ipv4**
- **ipv6**
- **ipxold**
- **mplsmcast**
- **mplsucast**
- **netbios**
- **novell**
- **pppoedisc**
- **rarp**
- **pppoesess**
- **ipxnew**
- **profinet**
- **powerlink**
- **ethercat**
- **vlan8021q**

Ethertype custom value

Specifies the *Ethertype* value of the MAC data packets to which the device applies the rule. The prerequisite is that in the *Ethertype* column the value *custom* is specified.

Possible values:
- **any** (default setting)
  The device applies the rule to every MAC data packet without evaluating the *Ethertype* value.
- **1..5ff**
  The device applies the rule to Logical Link Control (LLC) data packets whose length field contains the specified value. These values are available only for port-based rules.
- **600..ffff**
  The device applies the rule only to MAC data packets that contain the *Ethertype* value specified here.
VLAN ID

Specifies the VLAN ID of the data packets to which the device applies the rule. The prerequisite is that you specify the value `vlan8021q` in the `Ethertype` column.

Possible values:
- `any` (default setting)
  The device applies the rule to every data packet without evaluating the VLAN ID.
- `1..4042`
  The device applies the rule only to data packets with the specified VLAN ID.

Source IP address

Specifies the source address of the IP data packets to which the device applies the rule. The prerequisite is that you specify the value `ipv4` in the `Ethertype` column.

Possible values:
- `any` (default setting)
  The device applies the rule to IP data packets with any source address.
- Valid IPv4 address and netmask in CIDR notation
  The device applies the rule to data packets with the specified source address in the specified subnet.

Destination IP address

Specifies the destination address of the IP data packets to which the device applies the rule. The prerequisite is that you specify the value `ipv4` in the `Ethertype` column.

Possible values:
- `any` (default setting)
  The device applies the rule to IP data packets with any destination address.
- Valid IPv4 address and netmask in CIDR notation
  The device applies the rule to data packets with the specified destination address in the specified subnet.

Protocol

Specifies the IP protocol or Layer 4 protocol type of the data packets to which the device applies the rule. The device applies the rule only to data packets with a `Protocol` field of the specified value.

Possible values:
- `any` (default setting)
  The device applies the rule to every data packet without evaluating the protocol.
- `icmp`
  Internet Control Message Protocol (RFC 792)
- `igmp`
  Internet Group Management Protocol
- `ipip`
  IP in IP tunneling (RFC 2003)
- `tcp`
  Transmission Control Protocol (RFC 793)
- `udp`
  User Datagram Protocol (RFC 768)
- `esp`
  IPsec Encapsulated Security Payload (RFC 2406)
Network Security
[Network Security > Packet Filter > Transparent Firewall Mode > Rule]

- **ah**
  IPsec Authentication Header (RFC 2402)

- **icmpv6**
  Internet Control Message Protocol for IPv6

**TOS priority**

Specifies the *IP precedence* (ToS value) in the header of the IP data packets to which the device applies the rule.

Possible values:
- **0** (default setting)
  The device applies the rule to every IP data packet without evaluating the ToS value.
- **1..255**
  The device applies the rule only to IP data packets containing the specified ToS value.

**Source port**

Specifies the source port of the data packets to which the device applies the rule. The prerequisite is that you specify the value **TCP** or **UDP** in the **Protocol** column.

Possible values:
- **any** (default setting)
  The device applies the rule to every data packet without evaluating the source port.
- **1..65535**
  The device applies the rule only to data packets containing the specified source port.
  The field lets you specify the following options:
  - You specify a port with a single numerical value, for example **21**.
  - You specify multiple individual ports with numerical values separated by commas, for example **21,80,110**.
  - You specify a port range with numerical values connected by dashes, for example **2000-3000**.
  - You can also combine ports and port ranges, for example **21,2000-3000,65535**.
  The column lets you specify up to 15 numerical values. When you enter **21,2000-3000,65535**, for example, you use 4 of 15 numerical values.

**Destination port**

Specifies the destination port of the data packets to which the device applies the rule. The prerequisite is that you specify the value **TCP** or **UDP** in the **Protocol** column.

Possible values:
- **any** (default setting)
  The device applies the rule to every data packet without evaluating the destination port.
- **1..65535**
  The device applies the rule only to data packets containing the specified destination port.
  The field lets you specify the following options:
  - You specify a port with a single numerical value, for example **21**.
  - You specify multiple individual ports with numerical values separated by commas, for example **21,80,110**.
  - You specify a port range with numerical values connected by dashes, for example **2000-3000**.
  - You can also combine ports and port ranges, for example **21,2000-3000,65535**.
  The column lets you specify up to 15 numerical values. When you enter **21,2000-3000,65535**, for example, you use 4 of 15 numerical values.
Assigned queue ID

Specifies the priority queue to which the device assigns the data packets.

Possible values:
- 0..7 (default setting: 0)

Rate limit

Specifies the data rate limit for the non-routing port or VLAN. The limit applies to the sum of the sizes of data packets sent and received. The prerequisite is that you specify a value between 1 and 7 in the Assigned queue ID column.

Possible values:
- 0 (default setting)
  - No limitation of the data transfer rate.
- 1..4294967295
  - If the data transfer rate on the port exceeds the value specified, then the device discards surplus IP data packets. The prerequisite is that you specify in the Burst size column a value > 0. You specify the measurement unit of the limit in the Unit column.

Burst size

Specifies the limit in KByte for the data volume during temporary bursts. The prerequisite is that you specify a value between 1 and 7 in the Assigned queue ID column.

Possible values:
- 0 (default setting)
  - No limitation of the data volume.
- 1..128
  - If during temporary bursts on the port the data volume exceeds the value specified, then the device discards surplus MAC data packets.

Recommendation:
- If the bandwidth is known:
  \[ \text{Burst size} = \text{bandwidth} \times \text{allowed duration of a burst} / 8. \]
- If the bandwidth is unknown:
  \[ \text{Burst size} = 10 \times \text{MTU (Maximum Transmission Unit)} \] of the port.
Unit

Specifies the measurement unit for the data transfer rate specified in the Rate limit column. The prerequisite is that you specify a value between 1 and 7 in the Assigned queue ID column.

Possible values:

Trap

Activates/deactivates the sending of SNMP traps when the Packet Filter rule is applied to data packets.

Possible values:

➤ marked
  If the device applies the Packet Filter rule to a data packet, then the device sends an SNMP trap.
➤ unmarked (default setting)
  The sending of SNMP traps is deactivated.

The prerequisite for sending SNMP traps is that you enable the function in the Diagnostics > Status Configuration > Alarms (Traps) dialog and specify at least one trap destination.

Log

Activates/deactivates the logging in the log file.

Possible values:

➤ marked
  Logging is active.
  When the device applies the Packet Filter rule to a data packet, the device places an entry in the log file. See the Diagnostics > Report > System Log dialog.
➤ unmarked (default setting)
  Logging is inactive.

Active

Activates/deactivates the rule.

Possible values:

➤ marked (default setting)
  The rule is active.
➤ unmarked
  The rule is inactive.

To apply the changes to the data stream, click the ✔ button, then the ➔ button and then the Commit item in the Network Security > Packet Filter > Transparent Firewall Mode > Global dialog or in the Network Security > Packet Filter > Transparent Firewall Mode > Assignment dialog.

Buttons

You find the description of the standard buttons in section "Buttons" on page 14.
4.3.2.3 Packet Filter Assignment

This dialog lets you assign one or more Packet Filter rules to the non-routing ports or VLANs.

Information

Assignments
Displays how many rules are active for the non-routing ports or VLANs.

Uncommitted changes present
Displays if the Packet Filter rules applied to the data stream differ from the Packet Filter rules saved in the device.

Possible values:
- marked
  At least one of the Packet Filter rules saved in the device contains modified settings. When you click the Commit button, the device applies the Packet Filter rules to the data stream.
- unmarked
  The device applies the saved Packet Filter rules to the data stream.

Table

Description
Displays the name or description of the rule. You specify the description in the Network Security > Packet Filter > Transparent Firewall Mode > Rule dialog.

Index
Displays the sequential number of the Packet Filter rule. To specify this number, click the Create entry button.

Type
Displays where the device applies the rule to.

Possible values:
- PORT
  The device already applies the Packet Filter rule to a non-routing port. You find the corresponding port number in the Port/VLAN column.
- VLAN
  The device already applies the Packet Filter rule to a non-routing VLAN interface. You find the corresponding VLAN ID in the Port/VLAN column.
Network Security

[Network Security > Packet Filter > Transparent Firewall Mode > Assignment]

Port/VLAN

Displays the number of the non-routing port or VLAN ID to which the device applies the rule. To specify the port number or VLAN ID, click the **Create entry** button.

Direction

Displays if the device applies the **Packet Filter** rule to data packets received or sent.

Possible values:
- **ingress**
  The device applies the **Packet Filter** rule to data packets received on the non-routing port or VLAN interface.
- **egress**
  The device applies the **Packet Filter** rule to data packets sent on the non-routing port or VLAN interface.

Priority

Specifies the priority of the **Packet Filter** rule.

Using the priority, you specify the sequence in which the device applies the rules to the data stream. The device applies the rules in ascending order which starts with priority 0.

Possible values:
- 0..4294967295

Active

Activates/deactivates the rule.

Possible values:
- **marked** *(default setting)*
  The rule is active.
- **unmarked**
  The rule is inactive.

To apply the changes to the data stream, click the ✓ button, then the button and then the **Commit** item.

**Buttons**

You find the description of the standard buttons in section “**Buttons**” on page 14.

Opens the **Create** dialog to assign a rule to a non-routing port or VLAN.

- In the **Port/VLAN** field, you specify the number of the non-routing port or the VLAN-ID to which the device applies the rule.
- In the **Direction** field, you specify if the device applies the rule to data packets received or sent.
- In the **Index** field, you specify the rule which you assign to the non-routing port or VLAN.
Applies the rules saved in the device to the data stream.

**Note:** While the device activates the saved rules, you cannot set up any new communication connections.
4.3.2.4  **Packet Filter Overview**

This dialog gives you an overview of the specified *Packet Filter* rules.

**Table**

<table>
<thead>
<tr>
<th>Description</th>
<th>Displays the name or description of the rule. You specify the description in the <em>Network Security &gt; Packet Filter &gt; Transparent Firewall Mode &gt; Rule</em> dialog.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Displays the sequential number of the <em>Packet Filter</em> rule.</td>
</tr>
<tr>
<td>Direction</td>
<td>Displays if the device applies the <em>Packet Filter</em> rule to data packets received or sent. Possible values:</td>
</tr>
<tr>
<td></td>
<td>- <code>ingress</code>  The device applies the <em>Packet Filter</em> rule to data packets received on the non-routing port or VLAN interface.</td>
</tr>
<tr>
<td></td>
<td>- <code>egress</code>   The device applies the <em>Packet Filter</em> rule to data packets sent on the non-routing port or VLAN interface.</td>
</tr>
<tr>
<td>Priority</td>
<td>Displays the priority of the <em>Packet Filter</em> rule. The device applies the rules in ascending order which starts with priority 0.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays where the device applies the rule to.</td>
</tr>
<tr>
<td>Port/VLAN</td>
<td>Displays the number of the non-routing port or VLAN ID to which the device applies the rule.</td>
</tr>
<tr>
<td>Source MAC address</td>
<td>Displays the source address of the MAC data packets to which the device applies the rule.</td>
</tr>
<tr>
<td>Destination MAC address</td>
<td>Displays the destination address of the MAC data packets to which the device applies the rule.</td>
</tr>
<tr>
<td>Ethertype</td>
<td>Displays the <em>Ethertype</em> keyword of the MAC data packets to which the device applies the rule.</td>
</tr>
</tbody>
</table>
Ethertype custom value

Displays the Ethertype value of the MAC data packets to which the device applies the rule. The prerequisite is that in the Ethertype column the value custom is specified.

Source IP address

Displays the source address of the IP data packets to which the device applies the rule.

Destination IP address

Displays the destination address of the IP data packets to which the device applies the rule.

Protocol

Displays the IP protocol to which the Packet Filter rule is restricted. The device applies the Packet Filter rule only to packets of the specified IP protocol.

TOS priority

Displays the IP precedence (ToS value) in the header of the IP data packets to which the device applies the rule.

Action

Displays how the device processes received data packets when the device applies the rule.

Source port

Displays the source TCP or UDP port of the data packets to which the device applies the rule.

Destination port

Displays the destination TCP or UDP port of the data packets to which the device applies the rule.

Assigned queue ID

Displays the priority queue to which the device assigns the IP or MAC data packets.

Rate limit

Displays the data rate limit for the non-routing port or VLAN. The limit applies to the sum of the sizes of data packets sent and received.

Burst size

Displays the limit in KByte for the data volume during temporary bursts.

Unit

Displays the measurement unit for the data transfer rate specified in the Rate limit column.

Trap

Displays if the device sends an SNMP trap when the device applies the rule to a data packet.
Log

Displays if the device places an entry in the log file when the device applies the rule to a data packet.

Active

Displays if the rule is active or inactive.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

4.4 Deep Packet Inspection

The DPI function lets you monitor and filter data packets. The function supports you in protecting your network from undesirable content, such as spam or viruses.

The DPI function inspects data packets for undesirable characteristics and protocol violations. The protocol inspects the header and the payload of the data packets.

This dialog lets you specify the DPI settings. The device blocks data packets that violate the specified rules. If an error is detected, then the device terminates the data connection upon user request.

The menu contains the following dialogs:

- Deep Packet Inspection - Modbus Enforcer
- Deep Packet Inspection - OPC Enforcer
- Deep Packet Inspection - DNP3 Enforcer
4.4.1 Deep Packet Inspection - Modbus Enforcer

This dialog lets you specify the Modbus Enforcer settings and define Modbus TCP specific rules.

The rules specify function codes and register or coil addresses. The function code in the Modbus TCP protocol specifies the purpose of the data transfer. The device blocks the data packets that violate the specified rules. If an error is detected, then the device terminates the data connection upon user request. The predefined function code lists and the function code generator support you when specifying the function codes.

When the Modbus Enforcer rule is active (checkbox in the Profile active column is marked), the device applies the rules to the data stream.
- The device permits data packets containing only the function codes specified in the Function code column.
- The device rejects the data packets containing any other function codes that are not specified in the Function code column.

**Operation**

Uncommitted changes present

Displays if the Modbus Enforcer rules applied to the data stream differ from the rules saved in the device.

Possible values:
- marked
  
  At least one of the active Modbus Enforcer rules saved in the device contains modified settings.

  When you click the button and then the Commit changes item, the device applies the specified Modbus Enforcer rules and refreshes the display in the Function code column.

- unmarked
  
  The device applies the saved Modbus Enforcer rules to the data stream.

**Table**

Index

Displays the sequential number of the rule to which the table entry relates.

Description

Specifies the name for the rule.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters
  (default setting: modbus)

  The device differentiates between upper and lower case.
Function type

Specifies the function type for the *Modbus Enforcer* rule.

Possible values:
- **readOnly** (default setting)
  - Assigns the *function codes* for the read function of the *Modbus TCP* protocol.
  - After clicking the ✓ button, the *Function code* column displays the values 1,2,3,4,7,11,12,17,20,24.
- **readWrite**
  - Assigns the *function codes* for the read/write functions of the *Modbus TCP* protocol.
  - After clicking the ✓ button, the *Function code* column displays the values 1,2,3,4,5,6,7,11,12,15,16,17,20,21,22,23,24.
- **programming**
  - Assigns the *function codes* for the programming functions of the *Modbus TCP* protocol.
  - After clicking the ✓ button, the *Function code* column displays the values 1,2,3,4,5,6,7,11,12,15,16,17,20,21,22,23,24,40,42,90, 125,126.
- **all**
  - Assigns the *function codes* for every function of the *Modbus TCP* protocol.
  - After clicking the ✓ button, the *Function code* column displays the values 1,2,...,254,255.
- **advanced**
  - Lets you specify user-defined values in the *Function code* column.

**Note:** If you have specified the value *advanced*, then for your own security the device does not allow any subsequent changes to be made to the value. The device helps prevent a change to *readOnly*, *readWrite* or *programming*. This helps avoid overwriting the manually specified values in the *Function code* column. To specify an entry with the value *readOnly*, *readWrite* or *programming*, create a new entry.

Function code

Displays the *function codes* for the *Modbus Enforcer* rule. The device permits data packets with the specified properties.

The column displays different values depending on the value specified in the *Function type* column:
- If in the *Function type* column the value *readOnly*, *readWrite* or *programming* is specified, then the device automatically enters the related *function codes*.
- If in the *Function type* column the value *advanced* is specified, then the device lets you specify user-defined *function codes*. To do this, perform the following steps:
  - Highlight the row for the relevant rule.
  - Click the ✓ button and then the *Edit* item.
  - The dialog displays the *Edit* window.
    - If in the *Function type* column a value other than *advanced* is specified, the device displays a message. Confirm that you agree with changing the value in the *Function type* column to *advanced*. The device automatically changes the value in the *Function type* column to *advanced*.
  - Click the ✓ button.
  - Click the *Ok* button.

Possible values:
- `<FC> | <AR>, <FC> | <AR>, ...`
  - The device lets you specify multiple *function codes* and for some *function codes* an additional address range. You find the meaning of the values in section "Meaning of the Function code values" on page 144.
Network Security

[Network Security > DPI > Modbus Enforcer]

- **Function code** \( <FC> = 1..255 \)
  You separate each function code with a comma, for example 1,2,3.
  For some function codes the device lets you specify an additional address range. You separate the address range from the function code with a vertical bar (pipe), for example 1|128-255.

- **Address range** \( <AR> = 0..65535 \) and \( 0..65535|0..65535 \) (for Function code = 23)
  You join the start value and end value of the range with a hyphen, for example 128-255.

### Unit identifier

Specifies the Modbus TCP identification unit for the Modbus Enforcer rule.

Possible values:

- **none** (default setting)
  The device permits data packets without an identification unit.
- **0..255**
  The device permits data packets with the specified identification unit.
  The field lets you specify the following options:
  - A single Modbus TCP identification unit with a single numerical value, for example 1.
  - Multiple Modbus TCP identification units with numerical values separated by a comma, for example 1,2,3.

### Sanity check

Activates/deactivates the plausibility check for the data packets.

Possible values:

- **marked** (default setting)
  The plausibility check is active.
  The device checks the plausibility of the data packets in regards to format and specification.
- **unmarked**
  The plausibility verification is inactive.

### Exception

Activates/deactivates the sending of an exception response in case of a protocol violation or if the plausibility check identifies errors.

Possible values:

- **marked**
  The sending of an exception response is active.
  If the device identifies a protocol violation or a plausibility check error, then the device sends an exception response to the end points and terminates the Modbus TCP connection.
- **unmarked** (default setting)
  The sending of an exception response is inactive. The Modbus TCP connection remains established.
Reset

Activates/deactivates the resetting of the TCP connection in case of a protocol violation or if the plausibility check identifies errors.

Possible values:
- **marked** (default setting)
  The resetting of the TCP connection is active.
  If the device identifies a protocol violation or a plausibility check error, then the device terminates the TCP connection.
- **unmarked**
  The resetting of the TCP connection is inactive. The TCP connection remains established.

Profile active

Activates/deactivates the rules.

Possible values:
- **marked**
  The rule is active.
  The device applies the Modbus Enforcer rules specified in this table entry to the data packets.
- **unmarked**
  The rule is inactive.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the *Create* window to add a new entry to the table.
- In the *Index* field, you specify the number of the rule.
  Possible values:
  - 1..32
  When you click the *Ok* button, the device creates the new table entry and assigns the number specified in the *Index* field to the entry.

Removes the highlighted rule from the table. To save the changes in the non-volatile memory (NVM), perform the following steps:

- Open the *Basic Settings > Load/Save* dialog.
- In the table highlight the desired configuration profile.
- When in the *Selected* column the checkbox is unmarked, click the button and then the *Select* item.
- Click the *Save* button.

If you mark the *Profile active* checkbox for the rule, then the device stops you from removing the rule.
Copy

Opens the **Create** dialog to copy an existing table entry. The prerequisite is that the table entry for the rule to be copied is marked.

- In the **Index** field, you specify the new number of the copied rule.
  Possible values:
  - 1..32
    The device creates the new table entry and assigns the number specified in the **Index** field to the entry.

Edit

Opens the **Edit** window for specifying the function code list. The prerequisite is that a table entry is marked.

When a value other than **advanced** is specified in the **Function type** column, the **Modbus Enforcer** function changes the value to **advanced**.

Commit changes

The device applies the specified rules to the data stream.

If you changed the value in the **Function type** field, then the device applies the change to the **Function code** list and refreshes the display in the **Function code** column.

**[Edit]**

To assign the function codes to the rule, click the **Ok** button.

Function type

Specifies the function type for the **Modbus Enforcer** rule.

Possible values:

- **readOnly** (default setting)
  Assigns the function codes for the read function of the **Modbus TCP** protocol. The **Function code** column in the field on the right side displays the related values.

- **readWrite**
  Assigns the function codes for the read/write functions of the **Modbus TCP** protocol. The **Function code** column in the field on the right side displays the related values.

- **programming**
  Assigns the function codes for the programming functions of the **Modbus TCP** protocol. The **Function code** column in the field on the right side displays the related values.

- **all**
  Assigns the function codes for every function of the **Modbus TCP** protocol. The **Function code** column in the field on the right side displays the values 1,2,…,254,255.

- **advanced**
  Lets you specify user-defined values. You can select arbitrary values in the fields on the left or right side.

  If you change the value to **advanced**, then for your own security the device does not allow any subsequent changes to be made to the value. Before you can select the value **advanced**, perform the following steps:
  - Close the **Edit** window.
  - Create a new rule. To do this, click the **Add** button.
In the Function type column, specify the value advanced for the new rule.

- Click the button.
- Highlight the row for the relevant rule.
- Continue to specify the function codes. To do this, click the button and then the Edit item.

---

Moves every entry from the field on the left side to the field on the right side.

> Moves the entries highlighted in the field on the left side to the field on the right side.

< Moves the entries highlighted in the field on the right side to the field on the left side.

<< Moves every entry from the field on the right side to the field on the left side.

Function code

Displays the number and the meaning of the available function codes for the Modbus Enforcer rule.

You find the meaning of the Function code numbers in section “Meaning of the Function code values” on page 144.

Range

Specifies the Register or Coil address range for certain function codes. See section “Meaning of the Function code values” on page 144.

Possible values:

- 0..65535
- 0..65535 | 0..65535 (for Function code = 23)

---

**Meaning of the Function code values**

<table>
<thead>
<tr>
<th>#</th>
<th>Meaning</th>
<th>Address range (read)</th>
<th>Address range (write)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Read Coils</td>
<td>&lt;0..65535&gt;</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Read Discrete Inputs</td>
<td>&lt;0..65535&gt;</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>Read Holding Registers</td>
<td>&lt;0..65535&gt;</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>Read Input Registers</td>
<td>&lt;0..65535&gt;</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>Write Single Coil</td>
<td>&lt;0..65535&gt;</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Write Single Register</td>
<td>&lt;0..65535&gt;</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>Read Exception Status</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>Diagnostic</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>#</td>
<td>Meaning</td>
<td>Address range (read)</td>
<td>Address range (write)</td>
</tr>
<tr>
<td>-----</td>
<td>--------------------------------------------------------------</td>
<td>----------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>11</td>
<td>Get Comm Event Counter</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>12</td>
<td>Get Comm Event Log</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>13</td>
<td>Program (584/984)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>14</td>
<td>Poll (584/984)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>15</td>
<td>Write Multiple Coils</td>
<td>&lt;0..65535&gt;</td>
<td>-</td>
</tr>
<tr>
<td>16</td>
<td>Write Multiple Registers</td>
<td>&lt;0..65535&gt;</td>
<td>-</td>
</tr>
<tr>
<td>17</td>
<td>Report Slave ID</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>20</td>
<td>Read File Record</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>21</td>
<td>Write File Record</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>22</td>
<td>Mask Write Register</td>
<td>&lt;0..65535&gt;</td>
<td>-</td>
</tr>
<tr>
<td>23</td>
<td>Read/Write Multiple Registers</td>
<td>&lt;0..65535&gt;</td>
<td>&lt;0..65535&gt;</td>
</tr>
<tr>
<td>24</td>
<td>Read FIFO Queue</td>
<td>&lt;0..65535&gt;</td>
<td>-</td>
</tr>
<tr>
<td>40</td>
<td>Program (Concept)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>42</td>
<td>Concept Symbol Table</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>43</td>
<td>Encapsulated Interface Transport</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>48</td>
<td>Advantech Co. Ltd. - Management Functions</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>66</td>
<td>Scan Data Inc. - Expanded Read Holding Registers</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>67</td>
<td>Scan Data Inc. - Expanded Write Holding Registers</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>90</td>
<td>Unity Programming/OFS</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>100</td>
<td>Scattered Register Read</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>125</td>
<td>Schneider Electric - Firmware</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
4.4.2 Deep Packet Inspection - OPC Enforcer

This dialog lets you specify the OPC Enforcer (OLE for Process Control Enforcer) settings and define the OPC Enforcer specific rules.

The OPC is an integration protocol for industrial environments. The OPC Enforcer is a function that supports the network security. The device blocks the data packets that violate the specified rules. Upon user request, the device verifies the data packets for their plausibility and their fragment characteristics. The device verifies and observes OPC data connections and helps protect against invalid or fake data packets. The function dynamically activates TCP ports for each data connection. When requested by an OPC server, the device sets up the data connection only between the OPC server and the related OPC client.

The device removes the state information from the packet filter on the following events:
- When applying the rules saved in the device to the data stream.
- When activating/deactivating the Routing function on a router interface.

This includes potential DCE RPC information of the OPC Enforcer. In the process, the device interrupts open communication connections.

**Operation**

Uncommitted changes present

Displays if the OPC Enforcer rules applied to the data stream differ from the rules saved in the device.

Possible values:
- **marked**
  - At least one of the active OPC Enforcer rules saved in the device contains modified settings.
  - When you click the button and then the Commit changes item, the device applies the specified OPC Enforcer rules.
- **unmarked**
  - The device applies the saved OPC Enforcer rules to the data stream.

**Table**

Index

Displays the sequential number of the rule to which the table entry relates.

Description

Specifies the name for the rule.

Possible values:
- Alphanumeric ASCII character string with 0..64 characters
  - (default setting: opc)
  - The device differentiates between upper and lower case.
Sanity check

Activates/deactivates the plausibility verification for the data packets.

Possible values:

- **marked**  (default setting)
  The plausibility check is active.  
  The device checks the plausibility of the data packets as regards format and specification.

- **unmarked**
  The plausibility verification is inactive.

Fragment check

Activates/deactivates the fragment verification for the data packets.

Possible values:

- **marked**  (default setting)
  The fragment verification is active.  
  The device checks the data packets for fragment characteristics.

- **unmarked**
  The fragment verification is inactive.

Timeout at connect

Specifies the period in seconds after which the device terminates the OPC data connection.

Possible values:

- **1..60**  (default setting: 5)
- **0**
  The value 0 deactivates the function. The OPC data connection remains set up without a time limit.

Profile active

Activates/deactivates the rules.

Possible values:

- **marked**
  The rule is active.  
  The device applies the OPC Enforcer rules specified in this table entry to the data packets.

- **unmarked**
  The rule is inactive.
Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.
- In the Index field, you specify the number of the rule.
  Possible values:
  - 1..32
    When you click the Ok button, the device creates the new table entry and assigns the number specified in the Index field to the entry.

Removes the highlighted rule from the table.

To save the changes in the non-volatile memory (NVM), perform the following steps:
- Open the Basic Settings > Load/Save dialog.
- In the table highlight the desired configuration profile.
- When in the Selected column the checkbox is unmarked, click the Select button.
- Click the Save button.

If you mark the Profile active checkbox for the rule, then the device stops you from removing the rule.

Copy

Opens the Create dialog to copy an existing table entry. The prerequisite is that the table entry for the rule to be copied is marked.
- In the Index field, you specify the number of the rule.
  Possible values:
  - 1..32
    The device creates the new table entry and assigns the number specified in the Index field to the entry.

Commit changes

The device applies the specified rules to the data stream.
4.4.3 Deep Packet Inspection - DNP3 Enforcer

This dialog lets you specify the DNP3 Enforcer (Distributed Network Protocol v3 Enforcer) settings and define the DNP3 Enforcer specific rules.

The DNP3 protocol is designed to help ensure reliable communication between components in process automation systems. The protocol provides multiplexing, error checking, link control, prioritization, and layer 2 addressing services for user data. The DNP3 Enforcer function activates the Deep Pack Inspection (DPI) firewall capabilities for the DNP3 data stream. The device blocks the data packets that violate the specified rules. Upon user request, the device verifies the data packets for their plausibility and their fragment characteristics. The device verifies and monitors DNP3 data connections and helps protect against invalid or falsified data packets.

When the DNP3 Enforcer rule is active (checkbox in the Profile active column is marked), the device applies the rules to the data stream.

- The device permits data packets containing only the function codes specified in the Function code list column.
- The device rejects the data packets containing any other function codes that are not specified in the Function code list column.

Operation

Uncommitted changes present

Displays if the DNP3 Enforcer rules applied to the data stream differ from the rules saved in the device.

Possible values:

- marked
  At least one of the active DNP3 Enforcer rules saved in the device contains modified settings.
  When you click the button and then the Commit changes item, the device applies the specified DNP3 Enforcer rules.
- unmarked
  The device applies the saved DNP3 Enforcer rules to the data stream.

Table

Index

Displays the sequential number of the rule to which the table entry relates.

Description

Specifies the name for the rule.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters (default setting: dnp3)
  The device differentiates between upper and lower case.
Function code list

Displays the function codes for the DNP3 Enforcer rule. The device permits data packets with the specified properties.

The device lets you specify multiple function codes. To do this, perform the following steps:

- Highlight the row for the relevant rule.
- Click the button and then the Edit item.
  The dialog displays the Edit window.
- In the Available function codes field, highlight the desired function codes.
- Click the > button to move the highlighted entries to the Selected function codes field.
- Click the Ok button.

Possible values:

- 0..255
  You find the meaning of the Function code list numbers in section “Meaning of the Function code values” on page 153.

- <FC>, <FC>, ...
  The device lets you specify multiple function codes. You find the meaning of the values in section “Meaning of the Function code values” on page 144.
  Function code <FC> = 1..255
  You separate each function code with a comma, for example 1,2,3.

CRC check

Activates/deactivates the CRC check for the data packets to validate the checksum contained in the DNP3 data packets.

Possible values:

- marked (default setting)
  The CRC check is active.
  The device calculates the checksum and compares it with the checksum field in the DNP3 data packets.

- unmarked
  The CRC check is inactive.

Sanity check

Activates/deactivates the plausibility check for the data packets.

Possible values:

- marked (default setting)
  The plausibility check is active.
  The device checks the plausibility of the data packets in regards to format and specification.

- unmarked
  The plausibility verification is inactive.
Check outstation traffic

Activates/deactivates the checking of the data packets that originate at an outstation.

Possible values:
- **marked**
  - The checking of data packets from an outstation is active.
- **unmarked**
  - The checking of data packets from an outstation is inactive.

TCP reset

Activates/deactivates the resetting of the TCP connection in case of a protocol violation or if the plausibility check identifies errors.

Possible values:
- **marked** (default setting)
  - The resetting of the TCP connection is active.
  - If the device identifies a protocol violation or a plausibility check error, then the device terminates the TCP connection.
- **unmarked**
  - The resetting of the TCP connection is inactive. The TCP connection remains established.

Profile active

Activates/deactivates the rules.

Possible values:
- **marked**
  - The rule is active.
  - The device applies the DNP3 Enforcer rules specified in this table entry to the data packets.
- **unmarked**
  - The rule is inactive.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.
- In the Index field, you specify the number of the rule.
  - Possible values:
    - **1..32**
    - When you click the Ok button, the device creates the new table entry and assigns the number specified in the Index field to the entry.
Copy

Opens the Create dialog to copy an existing table entry. The prerequisite is that the table entry for the rule to be copied is marked.

- In the Index field, you specify the new number of the copied rule.
  Possible values:
  - 1..32
    The device creates the new table entry and assigns the number specified in the Index field to the entry.

Edit

Opens the Edit window for specifying the function code list. The prerequisite is that a table entry is marked.

Commit changes

The device applies the specified rules to the data stream.

[Edit]

Available function codes

Displays the number and the meaning of the available function codes for the DNP3 Enforcer rule.

You find the meaning of the Function code numbers in section “Meaning of the Function code values” on page 153.

>>

Moves every entry from the Available function codes field to the Selected function codes field.

>]

Moves the entries highlighted in the Available function codes field to the Selected function codes field.

<

Moves the entries highlighted in the Selected function codes field to the Available function codes field.

<<

Moves every entry from the Selected function codes field to the Available function codes field.

Selected function codes

Displays the number and the meaning of the selected function codes for the DNP3 Enforcer rule.

You find the meaning of the Function code list numbers in section “Meaning of the Function code values” on page 153.
### Meaning of the Function code values

<table>
<thead>
<tr>
<th>#</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Confirm</td>
</tr>
<tr>
<td>1</td>
<td>Read</td>
</tr>
<tr>
<td>2</td>
<td>Write</td>
</tr>
<tr>
<td>3</td>
<td>Select</td>
</tr>
<tr>
<td>4</td>
<td>Operate</td>
</tr>
<tr>
<td>5</td>
<td>Direct Operate</td>
</tr>
<tr>
<td>6</td>
<td>Direct Operate-No Response Required</td>
</tr>
<tr>
<td>7</td>
<td>Freeze</td>
</tr>
<tr>
<td>8</td>
<td>Freeze-No Response Required</td>
</tr>
<tr>
<td>9</td>
<td>Freeze Clear</td>
</tr>
<tr>
<td>10</td>
<td>Freeze Clear-No Response Required</td>
</tr>
<tr>
<td>11</td>
<td>Freeze at Time</td>
</tr>
<tr>
<td>12</td>
<td>Freeze at Time-No Response Required</td>
</tr>
<tr>
<td>13</td>
<td>Cold Restart</td>
</tr>
<tr>
<td>14</td>
<td>Warm Restart</td>
</tr>
<tr>
<td>15</td>
<td>Initialize Data</td>
</tr>
<tr>
<td>16</td>
<td>Initialize Application</td>
</tr>
<tr>
<td>17</td>
<td>Start Application</td>
</tr>
<tr>
<td>18</td>
<td>Stop Application</td>
</tr>
<tr>
<td>19</td>
<td>Save Configuration</td>
</tr>
<tr>
<td>20</td>
<td>Enable Unsolicited Messages</td>
</tr>
<tr>
<td>21</td>
<td>Disable Unsolicited Messages</td>
</tr>
<tr>
<td>22</td>
<td>Assign Class</td>
</tr>
<tr>
<td>23</td>
<td>Delay Measurement</td>
</tr>
<tr>
<td>24</td>
<td>Record Current Time</td>
</tr>
<tr>
<td>25</td>
<td>Open File</td>
</tr>
<tr>
<td>26</td>
<td>Close File</td>
</tr>
<tr>
<td>27</td>
<td>Delete File</td>
</tr>
<tr>
<td>28</td>
<td>Get File Information</td>
</tr>
<tr>
<td>29</td>
<td>Authenticate File</td>
</tr>
<tr>
<td>30</td>
<td>Abort File Transfer</td>
</tr>
<tr>
<td>31</td>
<td>Active Configuration</td>
</tr>
<tr>
<td>32</td>
<td>Authentication Request</td>
</tr>
<tr>
<td>33</td>
<td>Authenticate Request-No Acknowledgment</td>
</tr>
<tr>
<td>129</td>
<td>Response</td>
</tr>
<tr>
<td>130</td>
<td>Unsolicited Response</td>
</tr>
<tr>
<td>131</td>
<td>Authentication Response</td>
</tr>
</tbody>
</table>

[DNP3 Enforcer - Object wizard]

The wizard lets you select a DNP3 rule and create a user-defined object list for the selected DNP3 rule. The wizard also lets you modify the Index of Default Object List for the selected DNP3 rule.
**Select DNP3 rule**

**Index**

Displays the number of the rule to which the table entry relates.

**Description**

Displays the name of the rule.

**Profile active**

Displays if the rule is active or inactive.

Possible values:

- **marked**
  - The rule is active.
  - If the selected rule is active and you want to modify the selected rule, then the device displays a *Warning* dialog. You can only view the object list.

- **unmarked**
  - The rule is inactive.
  - You can update the object list when the selected rule is inactive.

**Edit object code for DNP3 rule**

The *DNP3* function uses objects to transmit values and information between devices. The *DNP3* function uses group numbers to categorize the data type and variation numbers to specify how the data within the group is encoded. Each instance of an encoded information element that defines a unique group and variation in the message, is a *DNP3* object.

This window lets you create custom *DNP3* objects and also lets you view the previously created custom *DNP3* objects. To verify that a created *DNP3* object is valid in a particular request message/response message, check the following parameters:

- **Object type**
- **Group no.**
- **Variation no.**
- **Function code**
- **Function name**
- **Length**
- **Qualifier code**

Based on the IEEE 1815-2012 standard, the *DNP3 Enforcer* function permits by default the data stream containing *DNP3* objects which are available in the *default object list*.

**Note:** The table on the top displays the parameters already set up. In the fields below the table you specify the parameters.
Index of Default Object List

Specifies the *index numbers* used in the *default object list*.

Possible values:

- **all** (default setting)
  The device applies the *DNP3 Enforcer* rule to the every data packet regardless of the *index number*.

- **1..317**
  The device applies the *DNP3 Enforcer* rule only to data packets containing the specified *index number*.
  The field lets you specify the following options:
  - A single *index number* with a single numerical value, for example *1*.
  - Multiple *index numbers* with numerical values separated by a comma, for example *1,2,3*.
  - A range with numerical values joined by a dash, for example *7-25*.
  - You can also combine single numerical values and ranges, for example *2,7-25,56*.

- **none**
  The device does not apply the *index number* to the *DNP3 Enforcer* rule.

**Index**

Specifies the number of the rule to which the table entry relates.

Possible values:

- **1..256**

**Object type**

Specifies the type of the message.

Possible values:

- **1 - Request**
  Creates a *request message* object in the object list.

- **2 - Response**
  Creates a *response message* object in the object list.

**Group no.**

Specifies a means of classifying the type or the types of data packets in a message. The prerequisite is that you have specified a valid value in the *Object type* field.

Possible values:

- **0..255**
  Each group number shares a common *point type* and *method of data packet creation*. The *point type* defines the machine in an *outstation*.

**Variation no.**

Specifies the *variation number*. The prerequisite is that you have specified a valid value in the *Group no.* field. The device applies the *DNP3 Enforcer* rule only to data packets containing the specified value.

The *DNP3* function provides the choice of encoding formats for the type of data packets known as *variation number*. Every value in the *Group no.* field has a set of *variation numbers*.
Possible values:

▶ 0..255
   The field lets you specify the following options:
   – You specify a single variation number with a single numerical value, for example 1.
   – You specify a range with numerical values connected by a dash, for example 0-55.

**Function code**

The function code identifies the purpose of the message. The prerequisite is that you have specified a valid value in the Variation no. field. The device applies the DNP3 Enforcer rule only to data packets containing the specified value.

Possible values:

▶ 0..128
   Request messages from masters. Specify a single numerical value, for example 1.
▶ 129..255
   Response messages from outstations. Specify a single numerical value, for example 254.

**Function name**

Specifies the optional name for the function code. The prerequisite is that you have specified a valid value in the Function code field.

Possible values:

▶ Alphanumeric ASCII character string with 0..32 characters
   For example, the device permits data packets with the following function names:
   – READ
   – WRITE
   – SELECT

**Length**

Specifies the optional length for the object. The prerequisite is that you have specified a valid value in the Function code field. The device applies the DNP3 Enforcer rule only to data packets containing the specified value.

Possible values:

▶ 0..255
   Specify a single numerical value, for example 1.
▶ byte_2
   The second byte of the object data contains the length of the remaining portion of the data.
▶ single_bit_packed
   The packed, single-bit values are padded out to the next byte boundary if the count of values is not a multiple of 8.
▶ double_bit_packed
   The packed, double-bit values are padded out to the next byte boundary if the count of values is not a multiple of 4.
▶ variation
   Encodes the length of the object.
Qualifier code

Specifies the qualifier code for a pair of each Group no., Variation no., and Function code fields. The qualifier code is an 8-bit value that defines the prefix code and the range specifier code for the object in a DNP3 message. The prerequisite is that you have specified a valid value in the Function code field. The device applies the DNP3 Enforcer rule only to data packets containing the specified value.

Possible values:

- 0x00..0xff
  - You specify multiple individual qualifier codes using hexadecimal values separated by a comma for a set of each Group no., Variation no., and Function code fields.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Index of Default Object List

Table 1: Request messages

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>209-239</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>240</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>240</td>
<td>2</td>
<td>WRITE</td>
<td>byte_2</td>
<td>0x00</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>241-243</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>245-247</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>245-247</td>
<td>2</td>
<td>WRITE</td>
<td>byte_2</td>
<td>0x00</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>248-250</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>252</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>254</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06</td>
</tr>
</tbody>
</table>
### Table 1: Request messages (cont.)

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0</td>
<td>255</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x06</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>0-2</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>12</td>
<td>1</td>
<td>0</td>
<td>22</td>
<td>ASSIGN CLASS</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>13</td>
<td>2</td>
<td>0-3</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06 0x07 0x08</td>
</tr>
<tr>
<td>14</td>
<td>3</td>
<td>0-2</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>15</td>
<td>3</td>
<td>0</td>
<td>22</td>
<td>ASSIGN CLASS</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>16</td>
<td>4</td>
<td>0-3</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06 0x07 0x08</td>
</tr>
<tr>
<td>17</td>
<td>10</td>
<td>0</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>18</td>
<td>10</td>
<td>0</td>
<td>22</td>
<td>ASSIGN CLASS</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>19</td>
<td>10</td>
<td>1</td>
<td>2</td>
<td>WRITE</td>
<td>single_bit_packed</td>
<td>0x00 0x01</td>
</tr>
<tr>
<td>20</td>
<td>10</td>
<td>2</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>21</td>
<td>11</td>
<td>0-2</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06 0x07 0x08</td>
</tr>
</tbody>
</table>
### Table 1: Request messages (cont.)

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>12</td>
<td>0</td>
<td>22</td>
<td>ASSIGN_CLASS</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>23</td>
<td>12</td>
<td>1</td>
<td>3</td>
<td>SELECT</td>
<td>11</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>24</td>
<td>12</td>
<td>1</td>
<td>4</td>
<td>OPERATE</td>
<td>11</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>25</td>
<td>12</td>
<td>1</td>
<td>5</td>
<td>DIRECT_OPERATE</td>
<td>11</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>26</td>
<td>12</td>
<td>1</td>
<td>6</td>
<td>DIRECT_OPERATE_NR</td>
<td>11</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>27</td>
<td>12</td>
<td>2</td>
<td>3</td>
<td>SELECT</td>
<td>11</td>
<td>0x07 0x08</td>
</tr>
<tr>
<td>28</td>
<td>12</td>
<td>2</td>
<td>4</td>
<td>OPERATE</td>
<td>11</td>
<td>0x07 0x08</td>
</tr>
<tr>
<td>29</td>
<td>12</td>
<td>2</td>
<td>5</td>
<td>DIRECT_OPERATE</td>
<td>11</td>
<td>0x07 0x08</td>
</tr>
<tr>
<td>30</td>
<td>12</td>
<td>2</td>
<td>6</td>
<td>DIRECT_OPERATE_NR</td>
<td>11</td>
<td>0x07 0x08</td>
</tr>
<tr>
<td>31</td>
<td>12</td>
<td>3</td>
<td>3</td>
<td>SELECT</td>
<td>single_bit_packed</td>
<td>0x00 0x01</td>
</tr>
<tr>
<td>32</td>
<td>12</td>
<td>3</td>
<td>4</td>
<td>OPERATE</td>
<td>single_bit_packed</td>
<td>0x00 0x01</td>
</tr>
<tr>
<td>33</td>
<td>12</td>
<td>3</td>
<td>5</td>
<td>DIRECT_OPERATE</td>
<td>single_bit_packed</td>
<td>0x00 0x01</td>
</tr>
<tr>
<td>34</td>
<td>12</td>
<td>3</td>
<td>6</td>
<td>DIRECT_OPERATE_NR</td>
<td>single_bit_packed</td>
<td>0x00 0x01</td>
</tr>
<tr>
<td>35</td>
<td>13</td>
<td>0-2</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06 0x07 0x08</td>
</tr>
<tr>
<td>36</td>
<td>20</td>
<td>0-2</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>37</td>
<td>20</td>
<td>5-6</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
</tbody>
</table>
### Table 1: Request messages (cont.)

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td>20</td>
<td>0</td>
<td>7</td>
<td>IMMEDIATE_FREEZE</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>39</td>
<td>20</td>
<td>0</td>
<td>8</td>
<td>IMMEDIATE_FREEZE_NR</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>40</td>
<td>20</td>
<td>0</td>
<td>9</td>
<td>FREEZE_CLEAR</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>41</td>
<td>20</td>
<td>0</td>
<td>10</td>
<td>FREEZE_CLEAR_NR</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>42</td>
<td>20</td>
<td>0</td>
<td>11</td>
<td>FREEZE_AT_TIME</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>43</td>
<td>20</td>
<td>0</td>
<td>12</td>
<td>FREEZE_AT_TIME_NR</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>44</td>
<td>20</td>
<td>0</td>
<td>22</td>
<td>ASSIGN_CLASS</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>45</td>
<td>21</td>
<td>0-2</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>46</td>
<td>21</td>
<td>5-6</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>47</td>
<td>21</td>
<td>9-10</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
</tbody>
</table>
### Table 1: Request messages (cont.)

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>48</td>
<td>21</td>
<td>0</td>
<td>22</td>
<td>ASSIGN_CLASS</td>
<td>-</td>
<td>0x00, 0x01, 0x06, 0x17, 0x28</td>
</tr>
<tr>
<td>49</td>
<td>22</td>
<td>0-2</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06, 0x07, 0x08</td>
</tr>
<tr>
<td>50</td>
<td>22</td>
<td>5-6</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06, 0x07, 0x08</td>
</tr>
<tr>
<td>51</td>
<td>23</td>
<td>0-2</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06, 0x07, 0x08</td>
</tr>
<tr>
<td>52</td>
<td>23</td>
<td>5-6</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06, 0x07, 0x08</td>
</tr>
<tr>
<td>53</td>
<td>30</td>
<td>0-6</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00, 0x01, 0x06, 0x17, 0x28</td>
</tr>
<tr>
<td>54</td>
<td>30</td>
<td>0</td>
<td>7</td>
<td>IMMEDIATE_FREEZE</td>
<td>-</td>
<td>0x00, 0x01, 0x06, 0x17, 0x28</td>
</tr>
<tr>
<td>55</td>
<td>30</td>
<td>0</td>
<td>0</td>
<td>IMMEDIATE_FREEZE_NR</td>
<td>-</td>
<td>0x00, 0x01, 0x06, 0x17, 0x28</td>
</tr>
<tr>
<td>56</td>
<td>30</td>
<td>0</td>
<td>11</td>
<td>FREEZE_AT_TIME</td>
<td>-</td>
<td>0x00, 0x01, 0x06, 0x17, 0x28</td>
</tr>
<tr>
<td>57</td>
<td>30</td>
<td>0</td>
<td>12</td>
<td>FREEZE_AT_TIME_NR</td>
<td>-</td>
<td>0x00, 0x01, 0x06, 0x17, 0x28</td>
</tr>
<tr>
<td>58</td>
<td>30</td>
<td>0</td>
<td>22</td>
<td>ASSIGN_CLASS</td>
<td>-</td>
<td>0x00, 0x01, 0x06, 0x17, 0x28</td>
</tr>
</tbody>
</table>
### Table 1: Request messages (cont.)

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>59</td>
<td>31</td>
<td>0-8</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>60</td>
<td>31</td>
<td>0</td>
<td>22</td>
<td>ASSIGN_CLASS</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>61</td>
<td>32</td>
<td>0-8</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06 0x07 0x08</td>
</tr>
<tr>
<td>62</td>
<td>33</td>
<td>0-8</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06 0x07 0x08</td>
</tr>
<tr>
<td>63</td>
<td>34</td>
<td>0-3</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06</td>
</tr>
<tr>
<td>64</td>
<td>34</td>
<td>1</td>
<td>2</td>
<td>WRITE</td>
<td>2</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>65</td>
<td>34</td>
<td>2</td>
<td>2</td>
<td>WRITE</td>
<td>4</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>66</td>
<td>34</td>
<td>3</td>
<td>2</td>
<td>WRITE</td>
<td>4</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>67</td>
<td>40</td>
<td>0</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06</td>
</tr>
<tr>
<td>68</td>
<td>40</td>
<td>0</td>
<td>22</td>
<td>ASSIGN_CLASS</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>69</td>
<td>40</td>
<td>1-4</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>70</td>
<td>41</td>
<td>0</td>
<td>22</td>
<td>ASSIGN_CLASS</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
</tbody>
</table>
Table 1: Request messages (cont.)

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>71</td>
<td>41</td>
<td>1</td>
<td>3</td>
<td>SELECT</td>
<td>5</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>72</td>
<td>41</td>
<td>2</td>
<td>3</td>
<td>SELECT</td>
<td>3</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>73</td>
<td>41</td>
<td>3</td>
<td>3</td>
<td>SELECT</td>
<td>5</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>74</td>
<td>41</td>
<td>1</td>
<td>4</td>
<td>OPERATE</td>
<td>5</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>75</td>
<td>41</td>
<td>2</td>
<td>4</td>
<td>OPERATE</td>
<td>3</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>76</td>
<td>41</td>
<td>3</td>
<td>4</td>
<td>OPERATE</td>
<td>5</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>77</td>
<td>41</td>
<td>1</td>
<td>5</td>
<td>DIRECT_OPERATE</td>
<td>5</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>78</td>
<td>41</td>
<td>2</td>
<td>5</td>
<td>DIRECT_OPERATE</td>
<td>3</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>79</td>
<td>41</td>
<td>3</td>
<td>5</td>
<td>DIRECT_OPERATE</td>
<td>5</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>41</td>
<td>1</td>
<td>6</td>
<td>DIRECT_OPERATE_NR</td>
<td>5</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>41</td>
<td>2</td>
<td>6</td>
<td>DIRECT_OPERATE_NR</td>
<td>3</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>41</td>
<td>3</td>
<td>6</td>
<td>DIRECT_OPERATE_NR</td>
<td>5</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>83</td>
<td>42</td>
<td>0-8</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06 0x07 0x08</td>
</tr>
<tr>
<td>Index</td>
<td>Group no.</td>
<td>Variation no.</td>
<td>Function code</td>
<td>Function name</td>
<td>Length</td>
<td>Qualifier code</td>
</tr>
<tr>
<td>-------</td>
<td>-----------</td>
<td>---------------</td>
<td>---------------</td>
<td>-----------------------------------</td>
<td>--------</td>
<td>----------------</td>
</tr>
<tr>
<td>84</td>
<td>43</td>
<td>0-8</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06 0x07 0x08</td>
</tr>
<tr>
<td>85</td>
<td>50</td>
<td>1</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x07</td>
</tr>
<tr>
<td>86</td>
<td>50</td>
<td>1</td>
<td>2</td>
<td>WRITE</td>
<td>6</td>
<td>0x07</td>
</tr>
<tr>
<td>87</td>
<td>50</td>
<td>2</td>
<td>11</td>
<td>FREEZE_AT_TIME</td>
<td>10</td>
<td>0x07</td>
</tr>
<tr>
<td>88</td>
<td>50</td>
<td>2</td>
<td>12</td>
<td>FREEZE_AT_TIME_NR</td>
<td>10</td>
<td>0x07</td>
</tr>
<tr>
<td>89</td>
<td>50</td>
<td>3</td>
<td>2</td>
<td>WRITE</td>
<td>10</td>
<td>0x07</td>
</tr>
<tr>
<td>90</td>
<td>50</td>
<td>4</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>91</td>
<td>50</td>
<td>4</td>
<td>2</td>
<td>WRITE</td>
<td>11</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>92</td>
<td>60</td>
<td>1</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06</td>
</tr>
<tr>
<td>93</td>
<td>60</td>
<td>2-4</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06 0x07 0x08</td>
</tr>
<tr>
<td>94</td>
<td>60</td>
<td>1-4</td>
<td>22</td>
<td>ASSIGN_CLASS</td>
<td>-</td>
<td>0x06</td>
</tr>
<tr>
<td>95</td>
<td>60</td>
<td>2-4</td>
<td>20</td>
<td>ENABLE_UNSOLICITED</td>
<td>-</td>
<td>0x06</td>
</tr>
<tr>
<td>96</td>
<td>60</td>
<td>2-4</td>
<td>21</td>
<td>DISABLE_UNSOLICITED</td>
<td>-</td>
<td>0x06</td>
</tr>
<tr>
<td>97</td>
<td>70</td>
<td>2</td>
<td>29</td>
<td>FILE_AUTHENTICATE</td>
<td>QC_5B_count_1</td>
<td>0x5B</td>
</tr>
<tr>
<td>98</td>
<td>70</td>
<td>3</td>
<td>25</td>
<td>OPEN_FILE</td>
<td>QC_5B_count_1</td>
<td>0x5B</td>
</tr>
<tr>
<td>99</td>
<td>70</td>
<td>3</td>
<td>27</td>
<td>DELETE_FILE</td>
<td>QC_5B_count_1</td>
<td>0x5B</td>
</tr>
<tr>
<td>100</td>
<td>70</td>
<td>4</td>
<td>26</td>
<td>CLOSE_FILE</td>
<td>QC_5B_count_1</td>
<td>0x5B</td>
</tr>
<tr>
<td>101</td>
<td>70</td>
<td>4</td>
<td>30</td>
<td>FILE_ABORT</td>
<td>QC_5B_count_1</td>
<td>0x5B</td>
</tr>
<tr>
<td>102</td>
<td>70</td>
<td>5-6</td>
<td>1</td>
<td>READ</td>
<td>QC_5B_count_1</td>
<td>0x5B</td>
</tr>
<tr>
<td>103</td>
<td>70</td>
<td>5</td>
<td>2</td>
<td>WRITE</td>
<td>QC_5B_count_1</td>
<td>0x5B</td>
</tr>
<tr>
<td>104</td>
<td>70</td>
<td>7</td>
<td>28</td>
<td>GET_FILE_INFORMATION</td>
<td>QC_5B_count_1</td>
<td>0x5B</td>
</tr>
<tr>
<td>105</td>
<td>70</td>
<td>8</td>
<td>31</td>
<td>ACTIVATE_CONFIGURATION</td>
<td>QC_5B_count_1</td>
<td>0x5B</td>
</tr>
<tr>
<td>106</td>
<td>80</td>
<td>1</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01</td>
</tr>
<tr>
<td>107</td>
<td>80</td>
<td>1</td>
<td>2</td>
<td>WRITE</td>
<td>single_bit_packed</td>
<td>0x00 0x01</td>
</tr>
<tr>
<td>108</td>
<td>81</td>
<td>1</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01</td>
</tr>
<tr>
<td>109</td>
<td>82</td>
<td>1</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01</td>
</tr>
<tr>
<td>110</td>
<td>83</td>
<td>1</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01</td>
</tr>
<tr>
<td>111</td>
<td>85</td>
<td>0</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06</td>
</tr>
</tbody>
</table>
### Table 1: Request messages (cont.)

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>112</td>
<td>85</td>
<td>1</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>113</td>
<td>85</td>
<td>1</td>
<td>2</td>
<td>WRITE QC_5B</td>
<td>0x5B</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>114</td>
<td>86</td>
<td>0</td>
<td>22</td>
<td>ASSIGN_CLASS</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>115</td>
<td>86</td>
<td>1-3</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>116</td>
<td>86</td>
<td>1</td>
<td>2</td>
<td>WRITE QC_5B</td>
<td>0x5B</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>117</td>
<td>86</td>
<td>3</td>
<td>2</td>
<td>WRITE QC_5B</td>
<td>0x5B</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>118</td>
<td>87</td>
<td>0</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>119</td>
<td>87</td>
<td>1</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>120</td>
<td>87</td>
<td>1</td>
<td>2</td>
<td>WRITE QC_5B</td>
<td>0x5B</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>121</td>
<td>87</td>
<td>1</td>
<td>3</td>
<td>SELECT QC_5B</td>
<td>0x5B</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>122</td>
<td>87</td>
<td>1</td>
<td>4</td>
<td>OPERATE QC_5B</td>
<td>0x5B</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>123</td>
<td>87</td>
<td>1</td>
<td>5</td>
<td>DIRECT_OPERATE QC_5B</td>
<td>0x5B</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>124</td>
<td>87</td>
<td>1</td>
<td>6</td>
<td>DIRECT_OPERATE_NR QC_5B</td>
<td>0x5B</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>125</td>
<td>88</td>
<td>0-1</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>126</td>
<td>90</td>
<td>1</td>
<td>16</td>
<td>INITIALIZE_APPLICATION QC_5B</td>
<td>0x5B</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>127</td>
<td>90</td>
<td>1</td>
<td>17</td>
<td>START_APPLICATION QC_5B</td>
<td>0x5B</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>128</td>
<td>90</td>
<td>1</td>
<td>18</td>
<td>STOP_APPLICATION QC_5B</td>
<td>0x5B</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>129</td>
<td>101</td>
<td>1-3</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
<tr>
<td>130</td>
<td>102</td>
<td>1</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00 0x01 0x06 0x17 0x28</td>
</tr>
</tbody>
</table>
Table 1: Request messages (cont.)

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>131</td>
<td>102</td>
<td>1</td>
<td>2</td>
<td>WRITE</td>
<td>1</td>
<td>0x00, 0x01, 0x03, 0x04, 0x05, 0x17, 0x28</td>
</tr>
<tr>
<td>132</td>
<td>110</td>
<td>128</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00, 0x01, 0x03, 0x04, 0x05, 0x17, 0x28</td>
</tr>
<tr>
<td>133</td>
<td>110</td>
<td>128</td>
<td>2</td>
<td>WRITE</td>
<td>variation</td>
<td>0x00, 0x01, 0x03, 0x04, 0x05, 0x17, 0x28</td>
</tr>
<tr>
<td>134</td>
<td>110</td>
<td>128</td>
<td>31</td>
<td>ACTIVATE_CONFIGURATION</td>
<td>variation</td>
<td>0x5B</td>
</tr>
<tr>
<td>135</td>
<td>111</td>
<td>128</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x06</td>
</tr>
<tr>
<td>136</td>
<td>112</td>
<td>128</td>
<td>2</td>
<td>WRITE</td>
<td>variation</td>
<td>0x00, 0x01, 0x17, 0x28</td>
</tr>
<tr>
<td>137</td>
<td>113</td>
<td>0</td>
<td>1</td>
<td>READ</td>
<td>-</td>
<td>0x00, 0x01, 0x17, 0x28</td>
</tr>
<tr>
<td>138</td>
<td>113</td>
<td>0</td>
<td>22</td>
<td>ASSIGN_CLASS</td>
<td>-</td>
<td>0x00, 0x01, 0x06, 0x17, 0x28</td>
</tr>
</tbody>
</table>

Table 2: Response messages

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>139</td>
<td>0</td>
<td>209-239</td>
<td>129</td>
<td>RESPONSE</td>
<td>byte_2</td>
<td>0x00, 0x17</td>
</tr>
<tr>
<td>140</td>
<td>0</td>
<td>240</td>
<td>129</td>
<td>RESPONSE</td>
<td>byte_2</td>
<td>0x00, 0x17</td>
</tr>
<tr>
<td>141</td>
<td>0</td>
<td>241-243</td>
<td>129</td>
<td>RESPONSE</td>
<td>byte_2</td>
<td>0x00, 0x17</td>
</tr>
<tr>
<td>142</td>
<td>0</td>
<td>245-247</td>
<td>129</td>
<td>RESPONSE</td>
<td>byte_2</td>
<td>0x00, 0x17</td>
</tr>
</tbody>
</table>
Table 2: Response messages (cont.)

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>143</td>
<td>0</td>
<td>248–250</td>
<td>129</td>
<td>RESPONSE</td>
<td>byte_2</td>
<td>0x00 0x17</td>
</tr>
<tr>
<td>144</td>
<td>0</td>
<td>252</td>
<td>129</td>
<td>RESPONSE</td>
<td>byte_2</td>
<td>0x00 0x17</td>
</tr>
<tr>
<td>145</td>
<td>0</td>
<td>255</td>
<td>129</td>
<td>RESPONSE</td>
<td>byte_2</td>
<td>0x00 0x17</td>
</tr>
<tr>
<td>146</td>
<td>1</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>single_bit_packed</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>147</td>
<td>1</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>1</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>148</td>
<td>2</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>1</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>149</td>
<td>2</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>7</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>150</td>
<td>2</td>
<td>3</td>
<td>129</td>
<td>RESPONSE</td>
<td>3</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>151</td>
<td>2</td>
<td>1</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>1</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>152</td>
<td>2</td>
<td>2</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>7</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>153</td>
<td>2</td>
<td>3</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>3</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>154</td>
<td>3</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>double_bit_packed</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>155</td>
<td>3</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>1</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>156</td>
<td>4</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>1</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>157</td>
<td>4</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>7</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>158</td>
<td>4</td>
<td>3</td>
<td>129</td>
<td>RESPONSE</td>
<td>3</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>159</td>
<td>4</td>
<td>1</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>1</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>160</td>
<td>4</td>
<td>2</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>7</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>161</td>
<td>4</td>
<td>3</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>3</td>
<td>0x17 0x28</td>
</tr>
</tbody>
</table>
Table 2: Response messages (cont.)

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>162</td>
<td>10</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>1</td>
<td>0x00, 0x01, 0x17, 0x28</td>
</tr>
<tr>
<td>163</td>
<td>11</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>1</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>164</td>
<td>11</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>7</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>165</td>
<td>11</td>
<td>1</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>1</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>166</td>
<td>11</td>
<td>2</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>7</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>167</td>
<td>12</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>11</td>
<td>0x00, 0x01, 0x17, 0x28</td>
</tr>
<tr>
<td>168</td>
<td>12</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>11</td>
<td>0x07, 0x08</td>
</tr>
<tr>
<td>169</td>
<td>12</td>
<td>3</td>
<td>129</td>
<td>RESPONSE</td>
<td>Single_bit_packed, 0x00, 0x01</td>
<td></td>
</tr>
<tr>
<td>170</td>
<td>13</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>1</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>171</td>
<td>13</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>7</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>172</td>
<td>13</td>
<td>1</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>1</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>173</td>
<td>13</td>
<td>2</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>7</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>174</td>
<td>20</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x00, 0x01, 0x17, 0x28</td>
</tr>
<tr>
<td>175</td>
<td>20</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>3</td>
<td>0x00, 0x01, 0x17, 0x28</td>
</tr>
<tr>
<td>176</td>
<td>20</td>
<td>5</td>
<td>129</td>
<td>RESPONSE</td>
<td>4</td>
<td>0x00, 0x01, 0x17, 0x28</td>
</tr>
<tr>
<td>177</td>
<td>20</td>
<td>6</td>
<td>129</td>
<td>RESPONSE</td>
<td>2</td>
<td>0x00, 0x01, 0x17, 0x28</td>
</tr>
<tr>
<td>178</td>
<td>21</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x00, 0x01, 0x17, 0x28</td>
</tr>
</tbody>
</table>
### Table 2: Response messages (cont.)

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>179</td>
<td>21</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>3</td>
<td>0x00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>180</td>
<td>21</td>
<td>5</td>
<td>129</td>
<td>RESPONSE</td>
<td>4</td>
<td>0x00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>181</td>
<td>21</td>
<td>6</td>
<td>129</td>
<td>RESPONSE</td>
<td>2</td>
<td>0x00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>182</td>
<td>21</td>
<td>9</td>
<td>129</td>
<td>RESPONSE</td>
<td>4</td>
<td>0x00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>183</td>
<td>21</td>
<td>10</td>
<td>129</td>
<td>RESPONSE</td>
<td>2</td>
<td>0x00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>184</td>
<td>22</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>185</td>
<td>22</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>3</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>186</td>
<td>22</td>
<td>1</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>5</td>
<td>0x17</td>
</tr>
<tr>
<td>187</td>
<td>22</td>
<td>2</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>3</td>
<td>0x17</td>
</tr>
<tr>
<td>188</td>
<td>22</td>
<td>5</td>
<td>129</td>
<td>RESPONSE</td>
<td>11</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>189</td>
<td>22</td>
<td>6</td>
<td>129</td>
<td>RESPONSE</td>
<td>9</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>190</td>
<td>22</td>
<td>5</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>11</td>
<td>0x17</td>
</tr>
<tr>
<td>191</td>
<td>22</td>
<td>6</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>9</td>
<td>0x17</td>
</tr>
<tr>
<td>192</td>
<td>23</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>193</td>
<td>23</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>3</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>194</td>
<td>23</td>
<td>1</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>5</td>
<td>0x17</td>
</tr>
<tr>
<td>195</td>
<td>23</td>
<td>2</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>3</td>
<td>0x17</td>
</tr>
<tr>
<td>196</td>
<td>23</td>
<td>5</td>
<td>129</td>
<td>RESPONSE</td>
<td>11</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>197</td>
<td>23</td>
<td>6</td>
<td>129</td>
<td>RESPONSE</td>
<td>9</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
</tbody>
</table>
Table 2: Response messages (cont.)

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>198</td>
<td>23</td>
<td>5</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>11</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>199</td>
<td>23</td>
<td>6</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>9</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>200</td>
<td>30</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>201</td>
<td>30</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>3</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>202</td>
<td>30</td>
<td>3</td>
<td>129</td>
<td>RESPONSE</td>
<td>4</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>203</td>
<td>30</td>
<td>4</td>
<td>129</td>
<td>RESPONSE</td>
<td>2</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>204</td>
<td>30</td>
<td>5</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>205</td>
<td>30</td>
<td>6</td>
<td>129</td>
<td>RESPONSE</td>
<td>9</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>206</td>
<td>31</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>207</td>
<td>31</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>3</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>208</td>
<td>31</td>
<td>3</td>
<td>129</td>
<td>RESPONSE</td>
<td>11</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>209</td>
<td>31</td>
<td>4</td>
<td>129</td>
<td>RESPONSE</td>
<td>9</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>210</td>
<td>31</td>
<td>5</td>
<td>129</td>
<td>RESPONSE</td>
<td>4</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>Index</td>
<td>Group no.</td>
<td>Variation no.</td>
<td>Function code</td>
<td>Function name</td>
<td>Length</td>
<td>Qualifier code</td>
</tr>
<tr>
<td>-------</td>
<td>-----------</td>
<td>---------------</td>
<td>---------------</td>
<td>-------------------</td>
<td>--------</td>
<td>----------------</td>
</tr>
<tr>
<td>211</td>
<td>31</td>
<td>6</td>
<td>129</td>
<td>RESPONSE</td>
<td>2</td>
<td>0x00, 0x01, 0x17, 0x28</td>
</tr>
<tr>
<td>212</td>
<td>31</td>
<td>7</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x00, 0x01, 0x17, 0x28</td>
</tr>
<tr>
<td>213</td>
<td>31</td>
<td>8</td>
<td>129</td>
<td>RESPONSE</td>
<td>9</td>
<td>0x00, 0x01, 0x17, 0x28</td>
</tr>
<tr>
<td>214</td>
<td>32</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>215</td>
<td>32</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>3</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>216</td>
<td>32</td>
<td>3</td>
<td>129</td>
<td>RESPONSE</td>
<td>11</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>217</td>
<td>32</td>
<td>4</td>
<td>129</td>
<td>RESPONSE</td>
<td>9</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>218</td>
<td>32</td>
<td>5</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>219</td>
<td>32</td>
<td>6</td>
<td>129</td>
<td>RESPONSE</td>
<td>9</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>220</td>
<td>32</td>
<td>7</td>
<td>129</td>
<td>RESPONSE</td>
<td>11</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>221</td>
<td>32</td>
<td>8</td>
<td>129</td>
<td>RESPONSE</td>
<td>15</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>222</td>
<td>32</td>
<td>1</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>5</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>223</td>
<td>32</td>
<td>2</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>3</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>224</td>
<td>32</td>
<td>3</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>11</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>225</td>
<td>32</td>
<td>4</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>9</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>226</td>
<td>32</td>
<td>5</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>5</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>227</td>
<td>32</td>
<td>6</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>9</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>228</td>
<td>32</td>
<td>7</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>11</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>229</td>
<td>32</td>
<td>8</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>15</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>230</td>
<td>33</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x17, 0x18</td>
</tr>
<tr>
<td>231</td>
<td>33</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>3</td>
<td>0x17, 0x28</td>
</tr>
<tr>
<td>Index</td>
<td>Group no.</td>
<td>Variation no.</td>
<td>Function code</td>
<td>Function name</td>
<td>Length</td>
<td>Qualifier code</td>
</tr>
<tr>
<td>-------</td>
<td>-----------</td>
<td>---------------</td>
<td>---------------</td>
<td>----------------------</td>
<td>--------</td>
<td>----------------</td>
</tr>
<tr>
<td>232</td>
<td>33</td>
<td>3</td>
<td>129</td>
<td>RESPONSE</td>
<td>11</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>233</td>
<td>33</td>
<td>4</td>
<td>129</td>
<td>RESPONSE</td>
<td>9</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>234</td>
<td>33</td>
<td>5</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>235</td>
<td>33</td>
<td>6</td>
<td>129</td>
<td>RESPONSE</td>
<td>9</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>236</td>
<td>33</td>
<td>7</td>
<td>129</td>
<td>RESPONSE</td>
<td>11</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>237</td>
<td>33</td>
<td>8</td>
<td>129</td>
<td>RESPONSE</td>
<td>15</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>238</td>
<td>33</td>
<td>1</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>5</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>239</td>
<td>33</td>
<td>2</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>3</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>240</td>
<td>33</td>
<td>3</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>11</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>241</td>
<td>33</td>
<td>4</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>9</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>242</td>
<td>33</td>
<td>5</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>5</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>243</td>
<td>33</td>
<td>6</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>9</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>244</td>
<td>33</td>
<td>7</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>11</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>245</td>
<td>33</td>
<td>8</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>15</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>246</td>
<td>34</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>2</td>
<td>0x00 0x01</td>
</tr>
<tr>
<td>247</td>
<td>34</td>
<td>2-3</td>
<td>129</td>
<td>RESPONSE</td>
<td>4</td>
<td>0x00 0x01</td>
</tr>
<tr>
<td>248</td>
<td>40</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x00 0x01</td>
</tr>
<tr>
<td>249</td>
<td>40</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>3</td>
<td>0x00 0x01</td>
</tr>
<tr>
<td>250</td>
<td>40</td>
<td>3</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x00 0x01</td>
</tr>
<tr>
<td>251</td>
<td>40</td>
<td>4</td>
<td>129</td>
<td>RESPONSE</td>
<td>9</td>
<td>0x00 0x01</td>
</tr>
</tbody>
</table>
Table 2: Response messages (cont.)

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>252</td>
<td>41</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>253</td>
<td>41</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>3</td>
<td>0x00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>254</td>
<td>41</td>
<td>3</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>255</td>
<td>42</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>256</td>
<td>42</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>3</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>257</td>
<td>42</td>
<td>3</td>
<td>129</td>
<td>RESPONSE</td>
<td>11</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>258</td>
<td>42</td>
<td>4</td>
<td>129</td>
<td>RESPONSE</td>
<td>9</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>259</td>
<td>42</td>
<td>5</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>260</td>
<td>42</td>
<td>6</td>
<td>129</td>
<td>RESPONSE</td>
<td>9</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>261</td>
<td>42</td>
<td>7</td>
<td>129</td>
<td>RESPONSE</td>
<td>11</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>262</td>
<td>42</td>
<td>8</td>
<td>129</td>
<td>RESPONSE</td>
<td>15</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>263</td>
<td>42</td>
<td>1</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>5</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>264</td>
<td>42</td>
<td>2</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>3</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>265</td>
<td>42</td>
<td>3</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>11</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>266</td>
<td>42</td>
<td>4</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>9</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>267</td>
<td>42</td>
<td>5</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>5</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>268</td>
<td>42</td>
<td>6</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>9</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>269</td>
<td>42</td>
<td>7</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>11</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>270</td>
<td>42</td>
<td>8</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>15</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>271</td>
<td>43</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
<tr>
<td>272</td>
<td>43</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>3</td>
<td>0x17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x28</td>
</tr>
</tbody>
</table>
### Table 2: Response messages (cont.)

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>273</td>
<td>43</td>
<td>3</td>
<td>129</td>
<td>RESPONSE</td>
<td>11</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>274</td>
<td>43</td>
<td>4</td>
<td>129</td>
<td>RESPONSE</td>
<td>9</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>275</td>
<td>43</td>
<td>5</td>
<td>129</td>
<td>RESPONSE</td>
<td>5</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>276</td>
<td>43</td>
<td>6</td>
<td>129</td>
<td>RESPONSE</td>
<td>9</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>277</td>
<td>43</td>
<td>7</td>
<td>129</td>
<td>RESPONSE</td>
<td>11</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>278</td>
<td>43</td>
<td>8</td>
<td>129</td>
<td>RESPONSE</td>
<td>15</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>279</td>
<td>43</td>
<td>1</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>5</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>280</td>
<td>43</td>
<td>2</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>3</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>281</td>
<td>43</td>
<td>3</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>11</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>282</td>
<td>43</td>
<td>4</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>9</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>283</td>
<td>43</td>
<td>5</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>5</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>284</td>
<td>43</td>
<td>6</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>9</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>285</td>
<td>43</td>
<td>7</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>11</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>286</td>
<td>43</td>
<td>8</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>15</td>
<td>0x17 0x28</td>
</tr>
<tr>
<td>287</td>
<td>50</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>6</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>288</td>
<td>50</td>
<td>4</td>
<td>129</td>
<td>RESPONSE</td>
<td>11</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>289</td>
<td>51</td>
<td>1-2</td>
<td>129</td>
<td>RESPONSE</td>
<td>6</td>
<td>0x07</td>
</tr>
<tr>
<td>290</td>
<td>51</td>
<td>1-2</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>6</td>
<td>0x07</td>
</tr>
<tr>
<td>291</td>
<td>52</td>
<td>1-2</td>
<td>129</td>
<td>RESPONSE</td>
<td>2</td>
<td>0x07</td>
</tr>
<tr>
<td>292</td>
<td>70</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>QC_5B_count_1</td>
<td>0x5B</td>
</tr>
<tr>
<td>293</td>
<td>70</td>
<td>4-7</td>
<td>129</td>
<td>RESPONSE</td>
<td>QC_5B_count_1</td>
<td>0x5B</td>
</tr>
<tr>
<td>294</td>
<td>70</td>
<td>4-7</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>QC_5B_count_1</td>
<td>0x5B</td>
</tr>
<tr>
<td>295</td>
<td>80</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>2</td>
<td>0x00 0x01</td>
</tr>
<tr>
<td>296</td>
<td>81</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>3</td>
<td>0x07</td>
</tr>
<tr>
<td>297</td>
<td>82</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>QC_5B_count_1</td>
<td>0x5B</td>
</tr>
<tr>
<td>298</td>
<td>82</td>
<td>1</td>
<td>130</td>
<td>RESPONSE</td>
<td>QC_5B_count_1</td>
<td>0x5B</td>
</tr>
<tr>
<td>299</td>
<td>83</td>
<td>1-2</td>
<td>129</td>
<td>RESPONSE</td>
<td>QC_5B</td>
<td>0x5B</td>
</tr>
<tr>
<td>300</td>
<td>83</td>
<td>1</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>QC_5B</td>
<td>0x5B</td>
</tr>
</tbody>
</table>
### Table 2: Response messages (cont.)

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>301</td>
<td>85</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>0x5B</td>
<td>0x5B</td>
</tr>
<tr>
<td>302</td>
<td>86</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>0x5B</td>
<td>0x5B</td>
</tr>
<tr>
<td>303</td>
<td>86</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>1</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>304</td>
<td>86</td>
<td>3</td>
<td>129</td>
<td>RESPONSE</td>
<td>0x5B</td>
<td>0x5B</td>
</tr>
<tr>
<td>305</td>
<td>87</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>0x5B</td>
<td>0x5B</td>
</tr>
<tr>
<td>306</td>
<td>88</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>0x5B</td>
<td>0x5B</td>
</tr>
<tr>
<td>307</td>
<td>88</td>
<td>1</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>QC_5B</td>
<td>0x5B</td>
</tr>
<tr>
<td>308</td>
<td>91</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>QC_5B</td>
<td>0x5B</td>
</tr>
<tr>
<td>309</td>
<td>101</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>2</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>310</td>
<td>101</td>
<td>2</td>
<td>129</td>
<td>RESPONSE</td>
<td>4</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>311</td>
<td>101</td>
<td>3</td>
<td>129</td>
<td>RESPONSE</td>
<td>8</td>
<td>0x00 0x01 0x17 0x28</td>
</tr>
<tr>
<td>312</td>
<td>102</td>
<td>1</td>
<td>129</td>
<td>RESPONSE</td>
<td>1</td>
<td>0x00 0x01 0x03 0x04 0x05 0x17 0x28</td>
</tr>
<tr>
<td>313</td>
<td>110</td>
<td>128</td>
<td>129</td>
<td>RESPONSE</td>
<td>variation</td>
<td>0x00 0x01 0x03 0x04 0x05 0x17 0x28</td>
</tr>
<tr>
<td>314</td>
<td>111</td>
<td>128</td>
<td>129</td>
<td>RESPONSE</td>
<td>variation</td>
<td>0x00 0x01 0x03 0x04 0x05 0x17 0x28</td>
</tr>
</tbody>
</table>
Table 2:  Response messages (cont.)

<table>
<thead>
<tr>
<th>Index</th>
<th>Group no.</th>
<th>Variation no.</th>
<th>Function code</th>
<th>Function name</th>
<th>Length</th>
<th>Qualifier code</th>
</tr>
</thead>
<tbody>
<tr>
<td>315</td>
<td>111</td>
<td>128</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>variation</td>
<td>0x00, 0x01, 0x17, 0x28</td>
</tr>
<tr>
<td>316</td>
<td>113</td>
<td>128</td>
<td>129</td>
<td>RESPONSE</td>
<td>variation</td>
<td>0x00, 0x01, 0x17, 0x28</td>
</tr>
<tr>
<td>317</td>
<td>113</td>
<td>128</td>
<td>130</td>
<td>UNSOLICITED_RESPONSE</td>
<td>variation</td>
<td>0x00, 0x01, 0x17, 0x28</td>
</tr>
</tbody>
</table>

4.5 DoS

Denial of Service (DoS) is a cyber-attack that aims to bring down specific services or devices. In this dialog you can set up several filters to help protect the device itself and other devices in the network from DoS attacks.

The menu contains the following dialogs:

- DoS Global
4.5.1 DoS Global

In this dialog you specify the DoS settings for the TCP/UDP, IP and ICMP protocols.

TCP/UDP

A scanner uses port scans to prepare network attacks. The scanner uses different techniques to determine running devices and open ports. This frame lets you activate filters for specific scanning techniques.

The device supports the detection of the following scan types:
- Null scans
- Xmas scans
- SYN/FIN scans
- TCP Offset attacks
- TCP SYN attacks
- L4 Port attacks
- Minimal Header scans

Null Scan filter

Activates/deactivates the Null Scan filter.

The Null Scan filter detects incoming data packets with no TCP flags set and discards them.

Possible values:
- marked
  The filter is active.
- unmarked (default setting)
  The filter is inactive.

Xmas filter

Activates/deactivates the Xmas filter.

The Xmas filter detects incoming data packets with the TCP flags FIN, URG and PUSH set simultaneously and discards them.

Possible values:
- marked
  The filter is active.
- unmarked (default setting)
  The filter is inactive.

SYN/FIN filter

Activates/deactivates the SYN/FIN filter.

The SYN/FIN filter detects incoming data packets with the TCP flags SYN and FIN set simultaneously and discards them.
Possible values:

▶ **marked**
  The filter is active.

▶ **unmarked** (default setting)
  The filter is inactive.

TCP Offset protection

Activates/deactivates the TCP Offset protection.

The TCP Offset protection detects incoming TCP data packets whose fragment offset field of the IP header is equal to 1 and discards them.

The TCP Offset protection accepts UDP and ICMP packets whose fragment offset field of the IP header is equal to 1.

Possible values:

▶ **marked**
  The protection is active.

▶ **unmarked** (default setting)
  The protection is inactive.

TCP SYN protection

Activates/deactivates the TCP SYN protection.

The TCP SYN protection detects incoming data packets with the TCP flag SYN set and a L4 source port < 1024 and discards them.

Possible values:

▶ **marked**
  The protection is active.

▶ **unmarked** (default setting)
  The protection is inactive.

L4 Port protection

Activates/deactivates the L4 Port protection.

The L4 Port protection detects incoming TCP and UDP data packets whose source port number and destination port number are identical and discards them.

Possible values:

▶ **marked**
  The protection is active.

▶ **unmarked** (default setting)
  The protection is inactive.

Min. Header Size filter

Activates/deactivates the Minimal Header filter.

The Minimal Header filter compares the TCP header of incoming data packets. If the data offset value multiplied by 4 is smaller than the minimum TCP header size, then the filter discards the data packet.
Possible values:
  ▶ marked
      The filter is active.
  ▶ unmarked (default setting)
      The filter is inactive.

Min. TCP header size

Displays the minimum size of a valid TCP header.

**IP**

This frame lets you activate or deactivate the Land Attack filter. With the land attack method, the attacking station sends data packets whose source and destination addresses are identical to those of the recipient. When you activate this filter, the device detects data packets with identical source and destination addresses and discards these data packets.

**Land Attack filter**

Activates/deactivates the Land Attack filter.

The Land Attack filter detects incoming IP data packets whose source and destination IP address are identical and discards them.

Possible values:
  ▶ marked
      The filter is active.
  ▶ unmarked (default setting)
      The filter is inactive.

**ICMP**

This dialog provides you with filter options for the following ICMP parameters:
  ▶ Fragmented data packets
  ▶ ICMP packets from a specific size upwards

**Filter fragmented packets**

Activates/deactivates the filter for fragmented ICMP packets.

The filter detects fragmented ICMP packets and discards them.

Possible values:
  ▶ marked
      The filter is active.
  ▶ unmarked (default setting)
      The filter is inactive.
Filter by packet size

Activates/deactivates the filter for incoming ICMP packets.

The filter detects ICMP packets whose payload size exceeds the size specified in the **Allowed payload size [byte]** field and discards them.

Possible values:
- **marked**
  - The filter is active.
- **unmarked** (default setting)
  - The filter is inactive.

Allowed payload size [byte]

Specifies the maximum allowed payload size of ICMP packets in bytes.

Possible values:
- **0..1472** (default setting: **512**)

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

4.6 Intrusion Detection System

This dialog lets you specify the settings for the **IDS** function.

The **IDS** function monitors the network traffic and sends alerts when the function detects any unusual activity.

Prerequisites to use the **IDS** function in the device:
- **Remote dissector (sensor)**
- Tripwire Industrial Visibility (TIV) server
- A local user account with the user role **administrator**
- A minimum of one available SSH session in the device

**Note:** The prerequisite to use the **IDS** function in the device is that the operator has a license of the TIV server.

The **remote dissector** is built into the device. The device uses the **remote dissector** to intercept the data packets on the ports. You select the ports from the dashboard of the TIV server. The **remote dissector** inspects the data packets and sends the compressed data to the TIV server.

The TIV server receives the data from the **remote dissector** and analyses the data. If the TIV server detects any unusual or potentially nonsecure activity in the data stream, then the TIV server dashboard displays alerts based on the behavior pattern of the data packets. This helps to get continuous and real-time threat detection.
The following table displays the port names in the device and their counterparts in the dashboard of the TIV server. The real number of ports depends on the hardware equipment of the device:

<table>
<thead>
<tr>
<th>Port name in the device</th>
<th>Port name in the TIV server dashboard</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>port00</td>
</tr>
<tr>
<td>1/2</td>
<td>port01</td>
</tr>
<tr>
<td>1/3</td>
<td>port02</td>
</tr>
<tr>
<td>1/4</td>
<td>port03</td>
</tr>
<tr>
<td>1/5</td>
<td>port06</td>
</tr>
<tr>
<td>1/6</td>
<td>port04</td>
</tr>
<tr>
<td>1/7</td>
<td>port05</td>
</tr>
</tbody>
</table>

**Operation**

Enables/disables the *IDS* function.

Possible values:

- **On**
  - The *IDS* function is enabled. The *remote dissector* starts operating.
  - The *IDS* function operates in the device with the access rights of the user account specified in the *User details* frame.
- **Off** (default setting)
  - The *IDS* function is disabled. The *remote dissector* stops operating.

**Status**

Displays the operating state of the *remote dissector* in the device.

Possible values:

- **marked**
  - The *remote dissector* is active in the device.
- **unmarked**
  - The *remote dissector* is inactive in the device.
**User details**

**IDS user name**

Specifies the local user account associated with the **IDS** function. The **IDS** function operates with the access rights of this user account.

Possible values:

- `<name of the user account>`
  The drop-down list displays the local user accounts with the user role **administrator**. If you assign a different user role to the selected user account in the **Device Security > User Management** dialog, then this has no effect on the current operation of the **IDS** function in the device. However, you can no longer select this user account from the drop-down list.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

**Delete**

Removes the association of the **IDS** function with the local user account selected in the **User details** frame. The **IDS** function continues to operate with the access rights of this user account until you disable the **IDS** function.
Virtual Private Network

5 Virtual Private Network

The menu contains the following dialogs:

- VPN Overview
- VPN Certificates
- VPN Connections

5.1 VPN Overview

Virtual Private Networks (VPN) provide secure communications for remote users or branch offices, allowing them to connect to servers within other branch offices, or even other companies using public networks. Even though the VPN tunnel uses a public network, it has the same behavior as a private network.

VPN tunnels provide secure communications to support the current trend of increased telecommuting and global business operations. In such cases, remote users or branch offices are able to connect to each other and central resources.

To provide secure communications, VPNs use IP Security (IPSec). IPSec has 2 functions for providing confidentiality namely, data encryption and data integrity. To provide authentication and integrity of the source with encryption, the device uses the IPSec Encapsulating Security Payload (ESP). Only the sender and receiver know the security key.

The device also uses the Negotiated Security Association method. The first packet received initiates a negotiation, between the sender and receiver, for which security association (SA) parameters the devices are going to use. The devices use the Internet Key Exchange (IKE) for the negotiation process. When negotiating the parameters, the sending and receiving devices agree on the authentication and data-security methods. The devices also perform mutual authentication, and then generate a shared key. The devices use the shared key to encrypt the data contained in each packet.

The VPN LED is green if at least one VPN tunnel is active and established. The LED is a separate LED for VPN and as such is non-configurable for this device. The VPN LED only displays the status of the VPN tunnels.

The dialog contains tabs which display the current VPN tunnels and statuses.

The Connection errors tab displays detected errors that are helpful when troubleshooting a VPN tunnel.

The dialog contains the following tabs:

- [Overview]
- [Diagnostics]
- [Connection errors]
### Connection

Connections (max.)

Displays the maximum number of VPN tunnels supported. The device limits the maximum number of active VPN tunnels to the amount set in Max. active connections.

Max. active connections

Displays the maximum number of active VPN tunnels supported.

---

### [Overview]

#### Table

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN index</td>
<td>Displays the row index for unique identification of a VPN tunnel.</td>
</tr>
<tr>
<td>VPN description</td>
<td>Displays the user-defined name for the VPN tunnel.</td>
</tr>
<tr>
<td>VPN active</td>
<td>Displays if the VPN tunnel is active/inactive.</td>
</tr>
<tr>
<td></td>
<td>The device limits the maximum number of configured VPN tunnels to the value displayed in Connections (max.). The device also limits the maximum number of active VPN tunnels to the value specified in the Max. active connections column.</td>
</tr>
<tr>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>▶ marked</td>
</tr>
<tr>
<td></td>
<td>The VPN tunnel is active.</td>
</tr>
<tr>
<td></td>
<td>▶ unmarked</td>
</tr>
<tr>
<td></td>
<td>The VPN tunnel is inactive.</td>
</tr>
<tr>
<td>Used IKE version</td>
<td>Displays the version of the IKE protocol that the VPN tunnel uses.</td>
</tr>
<tr>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>▶ ikev1</td>
</tr>
<tr>
<td></td>
<td>The device uses the IKE version 1 (ISAKMP) protocol.</td>
</tr>
<tr>
<td></td>
<td>▶ ikev2</td>
</tr>
<tr>
<td></td>
<td>The device uses the IKE version 2 protocol.</td>
</tr>
</tbody>
</table>
Startup

Displays the starting role for mediating the key exchange for VPN tunnel.

Possible values:

- **initiator**
  If you specify the role of the device as an initiator for the VPN tunnel, then the device actively initiates the Internet Key Exchange (IKE) and parameter negotiation.

- **responder**
  If you specify the role of the device as a responder for the VPN tunnel, then the device waits for the initiator to begin a key exchange (IKE) and connection parameter negotiation.

Operational status

Displays the current status of the VPN tunnel.

Possible values:

- **up**
  The Internet Key Exchange-Security Association (IKE-SA) and every Internet Protocol Security-Security Association (IPsec-SA) is up.

- **down**
  The IKE-SA and IPsec-SAs are down.

- **negotiation**
  If you specify the VPN tunnel for this device as the initiator, then the value indicates that the key exchange and negotiation algorithm is in progress. If the VPN tunnel for this device is the responder, then the value indicates that the VPN tunnel is waiting for the process to begin.

- **constructing**
  The IKE-SA is up. However, the device has detected at least one unestablished IPsec-SA for this instance.

- **dormant**
  The device is waiting for you to complete the configuration before starting the VPN tunnel setup. For example, the device has an unsuccessful hostname resolution.

- **re-keying**
  The key exchange is in progress. The device displays the value after the expiration of either the IKE or the IPSEC lifetime timer.

Connection established [s]

Displays the time, in seconds, since the device established the VPN tunnel for this device. The device updates the value after every IKE re-authentication.
Local host
Displays the name and/or IP address of the local host that the device detected using IKE.
Possible values:
► Alphanumeric ASCII character string with 1..128 characters

Remote host
Displays the name and/or IP address of the remote host that the device detected using IKE.
Possible values:
► Alphanumeric ASCII character string with 1..128 characters

IKE proposal
Displays the algorithms that IKE uses for the key exchange.
The device displays a combination of the IKE key agreement, IKE integrity (MAC) and IKE encryption parameters.
If you configure an IKE algorithm for the device in the VPN Connections dialog, and the remote endpoint has a more secure algorithm configured, then it is possible that both the local and remote devices use the remote algorithm.
The device displays the current cipher suite used for the connection.

IPsec proposal
Displays the algorithms that IPsec uses for data communication.
The device displays a combination of the IPsec key agreement, IPsec integrity (MAC) and IPsec encryption parameters.
If you configure an IPsec algorithm for the instance in the VPN Connections dialog, and the remote endpoint has a better, more secure algorithm configured, then it is possible that both the local and remote devices use the better algorithm.
The device displays the current cipher suite used for the connection.

Tunnels
Displays the number of IPsec tunnels within the VPN network.

**Buttons**
You find the description of the standard buttons in section "Buttons" on page 14.
[Diagnostics]

**Table**

| VPN index | Displays the row index for unique identification of a VPN tunnel. |
| VPN description | Displays the user-defined name for the VPN tunnel. |
| VPN active | Displays if the VPN tunnel is active/inactive. |

The device limits the maximum number of configured VPN tunnels to the value displayed in `Connections (max.)`. The device also limits the maximum number of active VPN tunnels to the value specified in the `Max. active connections` column.

Possible values:

- **marked**
  - The VPN tunnel is active.
- **unmarked**
  - The VPN tunnel is inactive.

| Tunnel index | Displays the index value that, together with the value in the `VPN index` column, identifies the entry in the connection tunnel info table. |
| Traffic selector index | Displays the index value that, together with the value in the `VPN index` column, identifies the entry in the traffic selector table which is mapped into the IPsec tunnel. |

Possible values:

- **0**
  - The traffic selector index is unknown.
- **1..16**

| Operational status | Displays the current status of the VPN tunnel. |

Possible values:

- **up**
  - The Internet Key Exchange-Security Association (IKE-SA) and every Internet Protocol Security-Security Association (IPsec-SA) is up.
- **down**
  - The IKE-SA and IPsec-SAs are down.
Virtual Private Network

[Virtual Private Network > Overview]

- **negotiation**
  If you specify the VPN tunnel for this instance as the initiator, then the value indicates that the key exchange and negotiation algorithm is in progress. If the VPN tunnel for this instance is the responder, then the value indicates that the VPN tunnel is waiting for the process to begin.

- **constructing**
  The IKE-SA is up. However, the device has detected at least one unestablished IPsec-SA for this instance.

- **dormant**
  The device is waiting for you to complete the configuration before starting the VPN tunnel setup. For example, the device has an unsuccessful hostname resolution.

- **re-keying**
  The key exchange is in progress. The device displays the value after the expiration of either the IKE or the IPSEC lifetime timer.

**IKE re-authentication [s]**

Displays the remaining time, in seconds, before the next IKE re-authentication. The value 0 indicates that re-authentication is unconfigured.

**Next IKE re-keying [s]**

Displays the remaining time, in seconds, before the next IKE re-key. The value 0 indicates that re-keying is unconfigured.

**IKE initiator SPI**

Displays the Security Parameter Index (SPI) of the IKE initiator, depending which device you specify as the initiator. For example, when you specify this device as the initiator, then this value is the SPI of the local device.

**IKE responder SPI**

Displays the SPI of the IKE responder, depending which device you specify as the initiator. For example, when you specify this device as the initiator, then this value is the SPI of the remote device.

**Local traffic selector**

Displays the local traffic selector for this IPsec tunnel. As a result of the negotiation process between the peers, the local traffic selector can be different from the configured traffic selector.

**Remote traffic selector**

Displays the remote traffic selector for this IPsec tunnel. As a result of the negotiation process between the peers, the traffic selector can be different from the configured traffic selector.

**Tunnel status**

Displays the current operational status of the IPsec tunnel.

Possible values:

- **unknown**
  The IPsec proposal is in progress. No traffic selectors or security parameters have been negotiated for this IPsec-SA.
Virtual Private Network

Virtual Private Network > Overview

- **created**
  The key exchange and the negotiation algorithm is finished for this IPsec-SA, but the tunnel is inactive.

- **routed**
  The encryption policies for the data stream are established, but the negotiation process has not started.

- **installing**
  The peer authentication is established, but the IPsec proposal for this tunnel is still in progress.

- **installed**
  The IPsec-SA is installed.

- **updating**
  The device updates the security associations.

- **re-keying**
  The key exchange is in progress for this IPsec-SA. The device displays the value after the expiration of the IPsec lifetime timer.

- **re-keyed**
  The key exchange for this IPsec-SA is finished and the device creates a new tunnel. The tunnel is active after the expiration of the previous IPsec proposal.

- **re-trying**
  The key exchange for this IPsec-SA failed. The device will automatically try to initiate a new key exchange.

- **deleting**
  The device replaces the IPsec tunnel during re-keying. The device keeps the tunnel open till the processing of delayed packets, which is default set to 5 seconds. After the IPsec lifetime timer has expired, the device deletes the tunnel.

- **destroying**
  The IPsec lifetime timer has expired. The device deletes the tunnel.

**IPsec input SPI**

Displays IPsec Security Parameter Index (SPI) that the device applies to the data it receives from the VPN tunnel. The SPI lets the device select the SA under which it processes a received packet.

**IPsec output SPI**

Displays IPsec Security Parameter Index (SPI) that the device applies to the data it transmits to the VPN tunnel.

**Next IPsec re-keying [s]**

Displays the remaining time, in seconds, before the next re-keying starts for this IPsec tunnel.

**IPsec tunnel input [byte]**

Displays the number of bytes received into this VPN tunnel.

**IPsec-tunnel input [packets]**

Displays the number of packets received into this VPN tunnel.

**Last IPsec data received [s]**

Displays the time, in seconds, since the VPN tunnel has received the last time data.
IPsec tunnel output [byte]

Displays the number of bytes sent into this VPN tunnel.

IPsec tunnel output [packets]

Displays the number of packets sent into this VPN tunnel.

Last IPsec data transmitted [s]

Displays the time, in seconds, since the VPN tunnel has sent the last time data.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

### [Connection errors]

**Table**

| VPN index | Displays the row index for unique identification of a VPN tunnel. |
| VPN description | Displays the user-defined name for the VPN tunnel. |
| VPN active | Displays if the VPN tunnel is active/inactive. The device limits the maximum number of configured VPN tunnels to the value displayed in **Connections (max)**. The device also limits the maximum number of active VPN tunnels to the value specified in the **Max. active connections** column. Possible values: |
| [marked] | The VPN tunnel is active. |
| [unmarked] | The VPN tunnel is inactive. |
| Last connection error | Displays the last error notification that occurred for this VPN tunnel. When the connection remains in the down state, this value is useful to help you isolate detected errors. This value helps you determine if a detected error occurred in the proposal exchange or during tunnel establishment. |
Possible values:
- Alphanumeric ASCII character string with 1..512 characters

**Buttons**

You find the description of the standard buttons in section "Buttons" on page 14.
5.2 VPN Certificates

A Certificate Authority (CA) issues certificates to authenticate the identity of devices requesting a VPN tunnel. You configure the devices that form a VPN tunnel to trust the CA that signed the certificate. When a trusted CA issues a certificate, the device considers it to be valid. Using a trusted CA, lets you add, renew, and change the certificates loaded in the device without affecting the VPN. The prerequisite is, that the actual identity information is correct.

Using certificates also lets you reduce the required maintenance work. The reason for this is because you change certificates less often as you change pre-shared keys. The CA creates certificates with commence and expiration date. The certificate is only valid during this time. When a certificate expires, the device requires a new certificate.

You create a self signed certificate using the strongSwan application in conjunction with the Linux Operating System.

**Note:** RC2 certificate encryption algorithms are unsupported, for example PKCS12 containers with RC2 encryption or passphrase protection.

### Table

<table>
<thead>
<tr>
<th>Index</th>
<th>Displays the row index of the certificate entry.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>▶ 1..100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>File name</th>
<th>Displays the name of the file uploaded to the device.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>▶ Alphanumeric ASCII character string with 1..64 characters</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subject</th>
<th>Displays the subject field of certificate.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The subject field of the certificate is a combination of the following items the country (C), state (ST), organization (O), organizational unit (OU), common name (CN), and email address of the recipient (emailAddress).</td>
</tr>
</tbody>
</table>
Possible values:
- Alphanumeric ASCII character string with 0..64 characters

**Issuer**
Displays the issuer of the certificate.
Possible values:
- Alphanumeric ASCII character string with 0..64 characters

**Valid from**
Displays the certificate commencement time and date.
Possible values:
- Date and time stamp

**Valid until**
Displays the certificate expiration time and date.
Possible values:
- Date and time stamp

**Type**
Displays the type of the container file used.
Possible values:
- **ca**
  The value indicates that the uploaded file is a certificate authority.
- **peer**
  The value indicates that the uploaded file is a peer certificate.
- **pkcs12**
  The value indicates that the uploaded file is a p12 bundle.
- **encrypted key**
  The value indicates that the uploaded file is a key file with password encryption.
- **encrypted pkcs12**
  The value indicates that the uploaded file is a p12 bundle with password encryption.
Upload date

Displays the time and date of the last certificate upload.

Possible values:
- Date and time stamp

Private key status

Displays the status of the private key in the peer certificate. A peer certificate is unusable without a private key.

Possible values:
- none
  The peer certificate does not contain a private key.
- present
  The device has located and extracted the private key from the peer certificate.
- notFound
  The device has located a private key. However, the key is missing the passphrase and the device has suspended the transfer.

Private key file

Displays the name of the private key file.

The device lets you enter alphanumeric characters plus hyphens, underscores and dots.

Possible values:
- Alphanumeric ASCII character string with 0..64 characters

Active connections

Displays the number of active connections that are using this certificate.

The device lets you delete the certificate only when the value is 0.

Possible values:
- 0..256

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Upload

Opens the Upload certificate window to add another certificate to the table.

- In the Pass Phrase (Private Key) field, you enter the passphrase used with this certificate.
  Possible values:
  - Alphanumeric ASCII character string with 0..128 characters
- In the File field, you enter the certificate file path.
  When the certificate is located on your PC or on a network drive, click the area to select the file that contains the certificate.
5.3 VPN Connections

This dialog lets you create, delete and edit VPN tunnels.

Note: The device uses software for des and AES-Galois/Counter Mode (GCM) encryption.

Table

VPN description

Specifies the user-defined name for the VPN tunnel.

Possible values:
- Alphanumeric ASCII character string with 1..128 characters

Traffic selector index

Displays the index value that, together with the value in the VPN index column, identifies the entry in the traffic selector table.

Possible values:
- 1..16
  - The device lets you specify any available value within the given range.

VPN active

Activates/deactivates the VPN tunnel.

The device limits the maximum number of configured VPN tunnels to the value displayed in Connections (max.). The device also limits the maximum number of active VPN tunnels to the value displayed in Max. active connections.

Possible values:
- marked
  - The VPN tunnel is active.
  - The device does not let you change any value, including active traffic selectors.
- unmarked (default setting)
  - The VPN tunnel is inactive.
  - The device lets you change values.

Traffic selector active

Activates/deactivates the table entry.
Possible values:

- **marked**
  - The table entry is active.
  - The device filters the data stream according to the parameters specified in the traffic selector only when the table entry is active.

- **unmarked** (default setting)
  - The table entry is inactive.
  - The device lets you edit the traffic selector parameters only when the table entry is inactive.

**Traffic selector description**

Specifies the name of the traffic selector.

Possible values:

- Alphanumeric ASCII character string with 0..128 characters

**Source address (CIDR)**

Specifies the IP address and netmask of the source host. When the device forwards packets containing this source IP address over a VPN tunnel, the device applies the settings specified in this row. Furthermore, the device applies the associated IPsec and IKE-SA settings, to every IP packet it forwards containing this address.

Possible values:

- Valid IPv4 address and netmask in CIDR notation
- **any** (default setting)
  - The device applies the settings in this row to every packet it forwards.

**Source restrictions**

Specifies the optional source restrictions using names or numbers entered as `<protocol/port>`. The device sends only the type of data specified through the VPN tunnel.

Examples:

- `tcp/http` is equal to `6/80`
- `udp` is equal to `udp/any`
- `/53` is equal to `any/53`

Possible values:

- **<empty>** (default setting)
  - The device uses `any/any` as the restriction.
- Alphanumeric ASCII character string with 0..32 characters
Virtual Private Network
[Virtual Private Network > Connections]

Destination address (CIDR)

Specifies the IP address and netmask of the destination. When the device forwards packets containing this destination IP address over a VPN tunnel, the device applies the settings specified in this row. Furthermore, for every IP packet the device forwards containing this address, it applies the associated IPsec and IKE-SA settings.

Possible values:

- Valid IPv4 address and netmask in CIDR notation
- any (default setting)
  The device applies the settings in this row to every packet it forwards.

Destination restrictions

Specifies the optional destination restrictions using names or numbers entered as <protocol/port>. The device accepts only the type of data specified from the VPN tunnel.

Examples:

tcp/http is equal to 6/80
udp is equal to udp/any
/53 is equal to any/53

Possible values:

- <empty> (default setting)
  The device uses any/any as the restriction.
- Alphanumeric ASCII character string with 0..32 characters

Version

Specifies the version of the IKE protocol for the VPN connection.

Possible values:

- auto (default setting)
  The VPN starts with protocol IKEv2 as the initiator and accepts IKEv1/v2 as the responder.
- ikev1
  The VPN starts with the IKEv1 (ISAKMP) protocol.
- ikev2
  The VPN starts with the IKEv2 protocol.

Startup

Specifies if the device starts this instance as a responder or initiator.

If you specify the local peer as the responder, and the remote peer sends traffic to a specific selector, then the device attempts to establish the connection as the responder. Establishing a connection as a responder depends upon other settings for this connection. For example, if you specify the Remote endpoint as any, then it is not possible to initiate the connection.
Possible values:

- **initiator**
  
  If you specify that the device starts as an initiator, then the device begins an IKE with the responder.

- **responder**
  
  If you specify that the device starts as a responder, then the device waits for the initiator to start the IKE and parameter negotiation.

**DPD timeout [s]**

Specifies the timeout, in seconds, before the local peer declares the remote peer dead, if the remote peer is unresponsive.

Possible values:

- **0..86400** (default setting: 120)
  
  The value 0 disables this feature. The default setting is 2 minutes. The maximum setting is 24 hours.

**IKE lifetime [s]**

Specifies the lifetime, in seconds, of the IKE security association between two network devices to support secure communication. The devices establish a security association after exchanging a set of pre-defined keys.

Possible values:

- **300..86400** (default setting: 28800)
  
  The default setting is 8 hours. The maximum setting is 24 hours.

**IKE exchange mode**

Specifies the use of the phase 1 exchange mode for IKEv1.

The purpose of IKE phase 1 is to establish a secure authenticated communication channel. The device uses the Diffie-Hellman key exchange algorithm to generate a shared secret key. The device then uses the shared secret key to further encrypt IKE communications.

Possible values:

- **main** (default setting)
  
  The main mode for phase 1 provides identity protection.

- **aggressive**
  
  You use the aggressive mode to reduce round trips.

**Authentication type**

Specifies the type of authentication that the device uses.

Possible values:

- **psk** (default setting)
  
  Select this value for the device to use a key that was previously created and saved on both the remote and local devices.
- **individualx509**
  - Select this value for the device to use an X509 certificate.
  - Use a separate certificate for CA and local identification.

- **pkcs12**
  - Select this value for the device to use a PKCS12 container with the needed certificates, which also includes the CA.

### Pre-shared key

Specifies the pre-shared key.

The device also lets you create pre-shared secrets as hexadecimal or Base64 encoded binary values. The device interprets a character sequence beginning with `0x` as sequence with hexadecimal digits. Similarly, the device also interprets a character sequence beginning with multiple `0`s as Base64 encoded binary data.

The prerequisite for using this parameter is that you specify in the *Authentication type* column the value **psk**.

Possible values:
- Alphanumeric ASCII character string with 0..128 characters excluding new line and double-quote characters

### IKE auth. cert. CA

Specifies the Certificate Authority certificate file names. The device uses this certificate for signature verification of the local and remote certificates.

The prerequisite for using this parameter is that you specify in the *Authentication type* column the value **individualx509**.

Possible values:
- Alphanumeric ASCII character string with 0..128 characters

### IKE auth. cert. local

Specifies the file name of the certificate the local device uses. The device uses this certificate for authentication of the local peer on the remote side.

If you specify in the *Authentication type* column the value **individualx509**, then the certificate binds the identity of local peer to the specified public key, that the certification authority (CA) signed in IKE auth. cert. CA.

If you specify in the *Authentication type* column the value **pkcs12**, then the certificate in the pkcs bundle binds the identity of local peer to the specified public key. This is done independently of the certificate displayed in the IKE auth. cert. CA column.
Possible values:
▶ Alphanumeric ASCII character string with 0..128 characters

IKE auth. cert. remote

Specifies the file name of the certificate the remote device uses. The device uses this certificate authentication of the remote peer on the local side. This certificate binds the identity of remote peer to the specified public key.

The value is optional, because the remote peer typically sends the certificate and the device only checks the validity of the certificate.

The prerequisite for using this parameter is that you specify in the Authentication type column the value individualx509.

Possible values:
▶ Alphanumeric ASCII character string with 0..128 characters

Encrypted private key

Specifies the private key file name. This value is only the file name of the private key. Enter the passphrase in Encrypted key/PKCS12 passphrase.

Prerequisites:
▶ In the Authentication type column, specify the individualx509 value.
▶ Encrypt the key saved in the device with a passphrase.

If you encrypt the key saved in the device, then the key and the certificate remain unmatched.

Possible values:
▶ Alphanumeric ASCII character string with 0..128 characters

Encrypted key/PKCS12 passphrase

Specifies the passphrase to use for the decryption of the private key in Encrypted private key or pkcs12 certificate container.

Possible values:
▶ Alphanumeric ASCII character string with 0..128 characters

IKE local identifier type

Specifies the type of local peer identifier that the device uses for the IKE local ID parameter.

Possible values:
▶ default (default setting)
  If in the Authentication type column the value psk is specified, then the device uses the IP address specified in the Local endpoint column as the local identifier.
  If in the Authentication type column the value individualx509 or pkcs12 is specified, then the device uses the distinguished name (DN) contained in the local IKE auth. cert. local certificate.
▶ address
  Use the local IP address or DNS name from the Local endpoint column as the IKE local ID.
▶ id
  The device identifies the value specified in the IKE local ID column as one of the following types:
  ▶ An IPv4 address or DNS host name
A key identifier specifying data that the device uses to pass vendor-specific information. The device uses the information to identify which pre-shared key it uses for aggressive mode authentication during negotiations.

- A Fully Qualified Domain Name web address, for example, foo.bar.com
- An email address
- The ASN.1 X.500 Distinguished Name (DN) contained within the IKE auth. cert. remote column. The local and remote devices exchange their certificates to establish the SA.

**IKE local ID**

Specifies the local peer identifier that the device sends to the remote device in the ID payload during phase 1 negotiations. The devices use the ID payload to identify the initiator of the security association (SA). The responder uses the identity to determine the correct host system policy requirement for the security association.

The formats for this parameter depend on the type specified in the IKE local identifier type column.

Possible values:

- `<empty>` (default setting)
- When you specify the value `id` in the IKE local identifier type column, the following values are possible:
  - An IPv4 address or DNS host name
  - A previously specified key identifier, specifying data that the device uses to pass vendor-specific information.
  - A Fully Qualified Domain Name web address, for example, foo.bar.com
  - An email address
  - A typical X.500 distinguished name

**Remote identifier type**

Specifies the type of remote peer identifier that the device uses for the Remote ID parameter.

Possible values:

- `any` (default setting)
  - The device accepts every received remote identifier as unverified.
- `address`
  - In the Remote ID column, use the IP address or the DNS name from the Remote endpoint column.
- `id`
  - The device identifies the value specified in the Remote ID column as one of the following types:
    - An IPv4 address or DNS host name
    - A key identifier specifying data that the device uses to pass vendor-specific information. The device uses the information to identify which pre-shared key it uses for aggressive mode authentication during negotiations.
    - A Fully Qualified Domain Name web address, for example, foo.bar.com
    - An email address
    - The ASN.1 X.500 Distinguished Name (DN) contained within the IKE auth. cert. remote column. The local and remote devices exchange their certificates to establish the SA.

**Remote ID**

Specifies the remote peer identifier which the device compares with the value in the ID payload during phase 1 negotiations. The device uses the ID payload to identify the initiator of the security association. The responder uses the identity to determine the correct host system policy requirement for the security association.

The formats for this parameter depend on the type specified in the Remote identifier type column.
Possible values:

- `<empty>`
- When you specify the value `id` in the `Remote identifier type` column, the following values are possible:
  - An IPv4 address or DNS host name
  - A previously specified key identifier, specifying data that the device uses to pass vendor-specific information.
  - A Fully Qualified Domain Name web address, for example, `foo.bar.com`
  - An email address
  - A typical X.500 distinguished name

IKE key agreement

Specifies which Diffie-Hellman key agreement algorithm the device uses for establishing the IKE-SA session key establishment.

Possible values:

- `any`
  - The device accepts every algorithm when specified as the responder.
- `modp1024` (default setting)
  - 1024 bits modulus which is DH Group 2.
- `modp1536`
  - 1536 bits modulus which is DH Group 5.
- `modp2048`
  - 2048 bits modulus which is DH Group 14.
- `modp3072`
  - 3072 bits modulus which is DH Group 15.
- `modp4096`
  - 4096 bits modulus which is DH Group 16.

IKE integrity (MAC)

Specifies which IKEv2 Integrity (MAC) algorithm the device uses.

In order to help keep the information on the VPN secure, the Hash-based Message Authentication Code (HMAC) process mixes (hashes) a shared secret key with the message data. The device mixes the results (hash value) with the secret key again, and then applies the hash function a second time.

Possible values:

- `any`
  - When you specify the device as the responder, the device accepts every algorithm. When you specify the device as the initiator, the device uses various pre-defined algorithms.
- `hmacmd5`
  - The device uses the Message Digest Algorithm 5 (MD5) for the hash function calculation.
- `hmacsha1` (default setting)
  - The device uses the Secure Hash Algorithm version 1 (SHA-1) for the hash function calculation.
- `hmacsha256`
  - The device uses SHA-256, part of the version 2 family, for the hash function calculation which the device computes with 32-bit words.
hmacsha384
The device uses SHA-384, part of the version 2 family, for hash function calculation which the device computes using a shorter version of SHA-512.

hmacsha512
The device uses SHA-512, part of the version 2 family, for hash function calculation which the device computes with 64 bit words.

IKE encryption

Specifies the encryption algorithm that the device uses for IKE.

Possible values:
- **any**
  - When you specify the device as the responder, the device accepts every algorithm. When you specify the device as the initiator, the device uses various pre-defined algorithms.
- **des**
  - The device uses the Data Encryption Standard (DES) block cipher for encryption of message data with a 56-bit key.
- **des3**
  - The device uses the Triple DES block cipher for encryption of message data which applies the 56-bit key, from DES, 3 times to each block.
- **aes128** (default setting)
  - The device uses the Advanced Encryption Standard (AES) with a block size of 128 bits, and a key length of 128 key bits.
- **aes192**
  - The device uses the Advanced Encryption Standard (AES) with a block size of 128 bits, and a key length of 192 key bits.
- **aes256**
  - The device uses the Advanced Encryption Standard (AES) with a block size of 128 bits, and a key length of 256 key bits.

Local endpoint

Specifies the hostname or IP address of the local security gateway.

Possible values:
- **any** (default setting)
  - The device uses the IP address of the interface the device uses to forward data to the remote endpoint.
- **Valid IPv4 address and netmask**
- **hostname**
  - Alphanumeric ASCII character string with 0..128 characters
    - If you specify a hostname, then the device delays the VPN tunnel until it receives an IP address for the hostname.

Remote endpoint

Specifies the hostname or IP address of the remote security gateway.

Possible values:
- **any** (default setting)
  - The device accepts any IP address when establishing an IKE-SA as a VPN responder.
Valid IPv4 address and netmask
If you specify that the device is a responder for this VPN tunnel, then the device accepts a network in CIDR notation, during IKE-SA establishment.

hostname
Alphanumeric ASCII character string with 0..128 characters
If you specify a hostname, then the device delays the VPN tunnel until it receives an IP address for the hostname.

Re-authentication

Activates/deactivates peer re-authentication after an IKE-SA re-key.

If you specify in the Version column the value IKEv1, then the device constantly re-authenticates the VPN tunnel, even when you unmark the checkbox.

Possible values:
► marked
The device creates a new IKE-SA and attempts to recreate the IPsec SAs.
► unmarked (default setting)
When using IKEv2, the device re-keys the VPN tunnel and retains the IPsec SAs.

IPsec key agreement

Specifies which Diffie-Hellman key agreement algorithm the device uses for establishing the IPsec-SA session key establishment.

Possible values:
► any
When you specify the device as the responder, the device accepts every algorithm. When you specify the device as the initiator, the device uses various pre-defined algorithms.
► modp1024 (default setting)
The value represents a Rivest, Shamir, and Adleman (RSA) algorithm with 1024 bits modulus which is Diffie-Hellman Group 2.
► modp1536
The value represents an RSA with 1536 bits modulus which is Diffie-Hellman Group 5.
► modp2048
The value represents an RSA with 2048 bits modulus which is Diffie-Hellman Group 14.
► modp3072
The value represents an RSA with 3072 bits modulus which is Diffie-Hellman Group 15.
► modp4096
The value represents an RSA with 4096 bits modulus which is Diffie-Hellman Group 16.
► none
The value disables Perfect Forward Secrecy (PFS). With PFS enabled, if a compromise of a single key occurs, then the integrity remains for subsequently generated keys.

IPsec integrity (MAC)

Specifies what the device uses for the IPsec Integrity (MAC) algorithm.

In order to help keep the information on the VPN secure, the Hash-based Message Authentication Code (HMAC) process mixes (hashes) a shared secret key with the message data. The device mixes the results (hash value) with the secret key again, and then applies the hash function a second time.
Possible values:

- **any**
  When you specify the device as the responder, the device accepts every algorithm. When you specify the device as the initiator, the device uses various pre-defined algorithms.

- **hmacmd5**
  The device uses the Message Digest Algorithm 5 (MD5) for the hash function calculation.

- **hmacsha1** (default setting)
  The device uses the Secure Hash Algorithm version 1 (SHA-1) for the hash function calculation.

- **hmacsha256**
  The device uses SHA-256, part of the version 2 family, for the hash function calculation which the device computes with 32-bit words.

- **hmacsha384**
  The device uses SHA-384, part of the version 2 family, for hash function calculation which the device computes using a shorter version of SHA-512.

- **hmacsha512**
  The device uses SHA-512, part of the version 2 family, for hash function calculation which the device computes with 64 bit words.

### IPsec encryption

Specifies the algorithm that the device uses for IPsec encryption.

Possible values:

- **any**
  When you specify the device as the responder, the device accepts every algorithm. When you specify the device as the initiator, the device uses various pre-defined algorithms.

- **des**
  The device uses the Data Encryption Standard (DES) block cipher for encryption of message data with a 56-bit key.

- **des3**
  The device uses the Triple DES block cipher for encryption of message data which applies the 56-bit key, from DES, 3 times to each block.

- **aes128** (default setting)
  The device uses the Advanced Encryption Standard (AES) with a block size of 128 bits, and a key length of 128 key bits.

- **aes192**
  The device uses the AES with a block size of 128 bits, and a key length of 192 key bits.

- **aes256**
  The device uses the AES with a block size of 128 bits, and a key length of 256 key bits.

- **aes128gcm64**
  The device uses the AES-Galois/Counter Mode (GCM) with a 64 bit Integrity Check Value (ICV) and 128 key bits.

- **aes128gcm96**
  AES-GCM with a 96 bit ICV and 128 key bits.

- **aes128gcm128**
  AES-GCM with a 128 bit ICV and 128 key bits.

- **aes192gcm64**
  AES-GCM with a 64 bit ICV and 192 key bits.

- **aes192gcm96**
  AES-GCM with a 96 bit ICV and 192 key bits.

- **aes192gcm128**
  AES-GCM with a 128 bit ICV and 192 key bits.

- **aes256gcm64**
  AES-GCM with a 64 bit ICV and 256 key bits.
Virtual Private Network
[Virtual Private Network > Connections]

- **aes256gcm96**
  AES-GCM with a 96 bit ICV and 256 key bits.

- **aes256gcm128**
  AES-GCM with a 128 bit ICV and 256 key bits.

**IPsec lifetime [s]**

Specifies the lifetime, in seconds, of the IPsec security association between two network devices to support secure communication. The devices establish a security association after exchanging a set of pre-defined keys.

Possible values:

- **300..28800** *(default setting: 3600)*
  The default setting is 1 hour. The maximum setting is 8 hours.

**Margin time [s]**

Specifies the period in seconds, before IKE lifetime [s] and IPsec lifetime [s] expire, in which the device attempts to negotiate a new key.

Possible values:

- **1..1800** *(default setting: 150)*
  The default setting is equal to 2.5 minutes. The maximum value is half an hour.

**Log informational entries**

Activates/deactivates event log entries for debugging proposes only.

Possible values:

- **marked**
  The device receives and processes the informational messages for this VPN tunnel, and enters the message in the event log.

- **unmarked** *(default setting)*
  The device receives and processes the informational messages for this connection, without an event log entry.

**Log unhandled messages**

Activates/deactivates message handling for messages unknown to strongSwan for debugging proposes only.

Possible values:

- **marked**
  The device enters the non-strongSwan messages received for this connection, in the event log.

- **unmarked** *(default setting)*
  The device ignores the non-strongSwan messages received for this connection.
Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Create entry

Opens the Create entry window to add a entry for VPN description and traffic selector index.

- In the **VPN description** field, you specify the user-defined description.
  Possible values:
  - Alphanumeric ASCII character string with 0..128 characters

- In the **Traffic selector index** field, you specify the index of the VPN tunnel traffic selector.
  Possible values:
  - 1..16

[VPN configuration (Wizard)]

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

The device also lets you create or change a VPN tunnel directly in the dialog.

[VPN configuration (Wizard) – Create or select entry]

Create or select entry – Table

**VPN index**

Displays the row index for unique identification of a VPN tunnel.

**VPN description**

Displays the user-defined name for the VPN tunnel.

**Remote host**

Displays the name and/or IP address of the remote host that the device detected using IKE.

Possible values:

- Alphanumeric ASCII character string with 1..128 characters

**Operational status**

Displays the current status of the VPN tunnel.

Possible values:

- **up**
  The Internet Key Exchange-Security Association (IKE-SA) and every Internet Protocol Security-Security Association (IPsec-SA) is up.
- **down**
  The IKE-SA and IPsec-SAs are down.

- **negotiation**
  If you specify the VPN tunnel for this device as the initiator, then the value indicates that the key exchange and negotiation algorithm is in progress. If the VPN tunnel for this device is the responder, then the value indicates that the VPN tunnel is waiting for the process to begin.

- **constructing**
  The IKE-SA is up. However, the device has detected at least one unestablished IPsec-SA for this instance.

- **dormant**
  The device is waiting for you to complete the configuration before starting the VPN tunnel setup. For example, the device has an unsuccessful hostname resolution.

- **re-keying**
  The key exchange is in progress. The device displays the value after the expiration of either the IKE or the IPSEC lifetime timer.

### Startup
Displays the starting role for mediating the key exchange for VPN tunnel.

Possible values:

- **initiator**
  If you specify the role of the device as the initiator for the VPN tunnel, then the device actively initiates the Internet Key Exchange (IKE) and parameter negotiation.

- **responder**
  If you specify the role of the device as a responder for the VPN tunnel, then the device waits for the initiator to begin a key exchange (IKE) and connection parameter negotiation.

### Authentication type
Displays the type of authentication that the device uses.

Possible values:

- **psk** *(default setting)*
  Select this value for the device to use a key that was previously created and saved on both the remote and local devices.

- **individualx509**
  Select this value for the device to use an X509 certificate. Use a separate certificate for CA and local identification.

- **pkcs12**
  Select this value for the device to use a PKCS12 container with the needed certificates, which also includes the CA.

### VPN active
Displays if the VPN tunnel is active/inactive.

The device limits the maximum number of configured VPN tunnels to the value displayed in `Connections (max.)`. The device also limits the maximum number of active VPN tunnels to the value specified in the `Max. active connections` column.
Possible values:
- **marked**
  The VPN tunnel is active.
- **unmarked**
  The VPN tunnel is inactive.

**Create or select entry – Text fields**

**VPN index**

Specifies the index of the VPN tunnel.

Possible values:
- **0..256**
  The value 0 indicates that only assigned entries are available.

**VPN description**

Specifies the user-defined description for the VPN tunnel.

Possible values:
- Alphanumeric ASCII character string with 1..128 characters

**[VPN configuration (Wizard) – Authentication]**

**Authentication type**

Specifies the type of authentication that the device uses.

Possible values:
- **psk** (default setting)
  Select this value for the device to use a key that was previously created and saved on both the remote and local devices.
- **individualx509**
  Select this value for the device to use an X509 certificate.
  Use a separate certificate for CA and local identification.
- **pkcs12**
  Select this value for the device to use a PKCS12 container with the needed certificates, which also includes the CA.
**Pre-shared key (PSK)**

Pre-shared key (PSK)

Specifies the pre-shared key.

The device also lets you create pre-shared secrets as hexadecimal or Base64 encoded binary values. The device interprets a character sequence beginning with `0x` as sequence with hexadecimal digits. Similarly, the device also interprets a character sequence beginning with multiple `0`s as Base64 encoded binary data.

The prerequisite for using this parameter is that you specify in the *Authentication type* column the value *psk*.

Possible values:
- Alphanumeric ASCII character string with 0..128 characters excluding new line and double-quote characters

**Confirm**

Specify the same key you specified in the *Pre-shared key* field for confirmation. If the key is different from the value you entered in the *Pre-shared key* field, then the *Next* button remains gray.

Prerequisites:
- In the *Authentication type* drop-down list, select the *Pre-shared key (PSK)* item.
- Mark the *Change* checkbox.

Possible values:
- Alphanumeric ASCII character string with 1..128 characters

**Change**

Activates/deactivates the *Pre-shared key* and *Confirm* fields, allowing you to enter and confirm the pre-shared key.

Possible values:
- marked (default setting for new entries)
  - Activates the *Pre-shared key* and *Confirm* fields which lets you enter and confirm a new key.
- unmarked (default setting for pre-existing entries)
  - The *Pre-shared key* and *Confirm* fields are inactive.

**Certificate**

Local Certificate

Displays the name of the local peer identified in the certificate.

The device uses this certificate for authentication of the local peer on the remote side. The certificate binds the identity of the local peer to its public key, which the CA signed. You select the file using the *Choose...* button.

The prerequisite for activating the *Choose...* button is that you select the *individualx509* or *pkcs12* item in the *Authentication type* drop-down list.
Possible values:
- Alphanumeric ASCII character string with 1..128 characters

**Encrypted Private Key**

Specifies the private key file name.

This value is only the file name of the private key. The key requires that you specify the passphrase in the **Pass Phrase (Private Key)** field.

Prerequisites:
- In the **Authentication type** drop-down list, select the **individualx509** item.
- Encrypt the key saved in the device with a passphrase.

If you encrypt the key saved in the device, then the key and the certificate remain unmatched. You select the file using the **Choose...** button.

The prerequisite for activating the **Choose...** button is that you select the **individualx509** item in the **Authentication type** drop-down list.

Possible values:
- Alphanumeric ASCII character string with 0..128 characters

**Certificate Authority**

Displays the name of the certificate authority (CA) which issued the certificate.

The device uses this certificate for signature verification of the local and remote certificates. You select the file using the **Choose...** button.

The prerequisite for activating the **Choose...** button is that you select the **individualx509** item in the **Authentication type** drop-down list.

Possible values:
- Alphanumeric ASCII character string with 1..128 characters

**Pass Phrase (Private Key)**

Specifies the passphrase that the device uses for decryption of the private key from **Encrypted Private Key**.

Prerequisites:
- In the **Authentication type** drop-down list, select the **individualx509** or **pkcs12** item.
- Mark the **Change** checkbox.

Possible values:
- Alphanumeric ASCII character string with 0..128 characters

**Confirm**

Enter the same key you entered in the **Pass Phrase (Private Key)** field for confirmation.

Prerequisites:
- In the **Authentication type** drop-down list, select the **individualx509** or **pkcs12** item.
- Mark the **Change** checkbox.
Possible values:
- Alphanumeric ASCII character string with 1..128 characters

**Change**

Activates/deactivates the *Pass Phrase (Private Key)* and *Confirm* fields.

The prerequisite for using this parameter is that you select the *individualx509* or *pkcs12* item in the *Authentication type* drop-down list.

Possible values:
- **marked** (default setting)
  - Activates the *Pass Phrase (Private Key)* and *Confirm* fields allowing you to enter and confirm a passphrase.
- **unmarked**
  - The *Pass Phrase (Private Key)* and *Confirm* fields are inactive.

[**VPN configuration (Wizard) – Endpoint and traffic selectors**]

**Endpoints**

**Remote endpoint**

Specifies the hostname or IP address of the remote IPsec VPN tunnel endpoint.

Possible values:
- **any** (default setting)
  - The device accepts any IP address when establishing an IKE-SA as a VPN responder.
- **Valid IPv4 address and netmask**
  - If you specify that the device is a responder for this VPN tunnel, then the device accepts a network in CIDR notation, during IKE-SA establishment.
- **hostname**
  - Alphanumeric ASCII character string with 0..128 characters
    - When you enter a hostname, the device lets you use `CR LF` or `CR NULL` in the character string.
    - If you specify a hostname, then the device delays the creation of the VPN tunnel until it receives an IP address for the hostname.

**Local endpoint**

Specifies the hostname or IP address of the local IPsec VPN tunnel endpoint.

Possible values:
- **any** (default setting)
  - The device uses the IP address of the interface the device uses to forward data to the remote endpoint.
- **Valid IPv4 address and netmask**
- **hostname**
  - Alphanumeric ASCII character string with 0..128 characters
    - When you enter a hostname, the device lets you use `CR LF` or `CR NULL` in the character string.
    - If you specify a hostname, then the device delays the creation of the VPN tunnel until it receives an IP address for the hostname.
Add traffic selector

Traffic selector index

Displays the traffic selector index of the VPN tunnel. The device lets you specify any available number within the given range.

Possible values:
- 1..16

Traffic selector description

Displays the user-defined description for the traffic selector.

Possible values:
- Alphanumeric ASCII character string with 1..128 characters

Source address (CIDR)

Displays the IP address and netmask of the source host. When the device forwards packets containing this source IP address over a VPN tunnel, the device applies the settings specified in this row. Furthermore, the device applies the associated IPsec and IKE-SA settings, to every IP packet it forwards containing this address.

Possible values:
- Valid IPv4 address and netmask in CIDR notation
- any (default setting)
  - The device applies the settings in this row to every packet it forwards.

Source restrictions

Displays the optional source restrictions using names or numbers entered as <protocol/port>. The device sends only the type of data specified through the VPN tunnel.

Examples:
- tcp/http is equal to 6/80
- udp is equal to udp/any
- /53 is equal to any/53

Possible values:
- <empty> (default setting)
  - The device uses any/any as the restriction.
- Alphanumeric ASCII character string with 0..32 characters
Destination address (CIDR)

Displays the IP address and netmask of the destination. When the device forwards packets containing this destination IP address over a VPN tunnel, the device applies the settings specified in this row. Furthermore, for every IP packet the device forwards containing this address, it applies the associated IPsec and IKE-SA settings.

Possible values:
- Valid IPv4 address and netmask in CIDR notation
- any (default setting)
  - The device applies the settings in this row to every packet it forwards.

Destination restrictions

Displays the optional destination restrictions using names or numbers entered as `<protocol/port>`. The device accepts only the type of data specified from the VPN tunnel.

Example:

tcp/http is equal to 6/80
udp is equal to udp/any
/53 is equal to any/53

Possible values:
- <empty> (default setting)
  - The device uses any/any as the restriction.
- Alphanumeric ASCII character string with 0..32 characters

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Add

Opens the Add traffic selector dialog to add another selector to the VPN connection.
- In the Traffic selector index field, you specify the traffic selector index.
  - Possible values:
    - 1..16
- In the Traffic selector description field, you specify the user-defined description.
  - Possible values:
    - Alphanumeric ASCII character string with 0..128 characters
- In the Source address (CIDR) field, you specify the IP address of the source host.
  - Possible values:
    - Valid IPv4 address and netmask in CIDR notation
- In the Source restrictions field, you specify the optional source restrictions.
  - Possible values:
    - Alphanumeric ASCII character string with 0..32 characters
In the **Destination address (CIDR)** field, you specify the IP address of the destination. Possible values:
- Valid IPv4 address and netmask in CIDR notation

In the **Destination restrictions** field, you specify the optional destination restrictions. Possible values:
- Alphanumeric ASCII character string with 0..32 characters

**Remove**

Removes the highlighted entry from the table.

**[VPN configuration (Wizard) – Advanced configuration]**

**General**

**Margin time [s]**

Specifies the time, in seconds, remaining before the connection or the keying channel expires. Afterwards, the device attempts to negotiate a replacement.

Possible values:
- **1..1800** (default setting: 540)
  - The default setting is equal to 9 minutes. The maximum value is half an hour.

**IKE/Key-exchange**

**Version**

Specifies the version of the IKE protocol for the VPN connection.

Possible values:
- **auto** (default setting)
  - The VPN starts with protocol IKEv2 as the initiator and accepts IKEv1/v2 as the responder.
- **ikev1**
  - The VPN starts with the IKEv1 (ISAKMP) protocol.
- **ikev2**
  - The VPN starts with the IKEv2 protocol.

**Startup**

Specifies if the device starts this instance as a responder or initiator.

If you specify the local peer as the responder, and the remote peer sends traffic to a specific selector, then the device attempts to establish the connection as the responder. Establishing a connection as a responder depends upon other settings for this connection. For example, if you specify the **Remote endpoint** as **any**, then it is not possible to initiate the connection.
Possible values:

- **initiator**
  If you specify that the device starts as an initiator, then the device begins an IKE with the responder.

- **responder**
  If you specify that the device starts as a responder, then the device waits for the initiator to start the IKE and parameter negotiation.

### IKE local identifier type

Specifies the type of local peer identifier that the device uses for the `IKE local ID` parameter.

Possible values:

- **default** (default setting)
  If in the `Authentication type` column the value `psk` is specified, then the device uses the IP address specified in the `Local endpoint` field as the local identifier.
  If in the `Authentication type` column the value `individualx509` or `pkcs12` is specified, then the device uses the distinguished name (DN) contained in the local `IKE auth. cert. local` certificate.

- **address**
  In the `IKE local ID` column, use the IP address or the DNS name from the `Local endpoint` field.

- **id**
  The device identifies the value specified in the `IKE local ID` column as one of the following types:
  - An IPv4 address or DNS host name
  - A key identifier specifying data that the device uses to pass vendor-specific information. The device uses the information to identify which pre-shared key it uses for aggressive mode authentication during negotiations.
  - A Fully Qualified Domain Name web address, for example, `foo.bar.com`
  - An email address
  - The ASN.1 X.500 Distinguished Name (DN) contained within the `IKE auth. cert. remote` column. The local and remote devices exchange their certificates to establish the SA.

### IKE local ID

Specifies the local peer identifier that the device sends to the remote device in the ID payload during phase 1 negotiations. The devices use the ID payload to identify the initiator of the security association (SA). The responder uses the identity to determine the correct host system policy requirement for the security association.

The formats for this parameter depend on the type specified in the `IKE local identifier type` column.

Possible values:

- **<empty>** (default setting)

- When you specify the value `id` in the `IKE local identifier type` column, the following values are possible:
  - An IPv4 address or DNS host name
  - A previously specified key identifier, specifying data that the device uses to pass vendor-specific information.
  - A Fully Qualified Domain Name web address, for example, `foo.bar.com`
  - An email address
  - A typical X.500 distinguished name
Remote identifier type

Specifies the type of remote peer identifier that the device uses for the Remote ID parameter.

Possible values:
- **any** (default setting)
  The device accepts every received remote identifier as unverified.
- **address**
  In the Remote ID column, use the IP address or the DNS name from the Remote endpoint field.
- **id**
  The device identifies the value specified in the Remote ID column as one of the following types:
  - An IPv4 address or DNS host name
  - A key identifier specifying data that the device uses to pass vendor-specific information. The device uses the information to identify which pre-shared key it uses for aggressive mode authentication during negotiations.
  - A Fully Qualified Domain Name web address, for example, `foo.bar.com`
  - An email address
  - The ASN.1 X.500 Distinguished Name (DN) contained within the `IKE auth. cert. remote` column. The local and remote devices exchange their certificates to establish the SA.

Remote ID

Specifies the remote peer identifier which the device compares with the value in the ID payload during phase 1 negotiations. The device uses the ID payload to identify the initiator of the security association. The responder uses the identity to determine the correct host system policy requirement for the security association.

The formats for this parameter depend on the type specified in the Remote identifier type column.

Possible values:
- **<empty>**
- When you specify the value **id** in the Remote identifier type column, the following values are possible:
  - An IPv4 address or DNS host name
  - A previously specified key identifier, specifying data that the device uses to pass vendor-specific information.
  - A Fully Qualified Domain Name web address, for example, `foo.bar.com`
  - An email address
  - A typical X.500 distinguished name

IKE exchange mode

Specifies the use of the phase 1 exchange mode for IKEv1.

The purpose of IKE phase 1 is to establish a secure authenticated communication channel. The device uses the Diffie-Hellman key exchange algorithm to generate a shared secret key. The device then uses the shared secret key to further encrypt IKE communications.

Possible values:
- **main** (default setting)
  The main mode for phase 1 provides identity protection.
- **aggressive**
  You use the aggressive mode to reduce round trips.
Virtual Private Network
[Virtual Private Network > Connections]

IKE key agreement

Specifies which Diffie-Hellman key agreement algorithm the device uses for establishing the IKE-SA session key establishment.

Possible values:

- **any**
  With this value selected the device accepts every algorithm when specified as the responder.

- **modp1024** (default setting)
  The value represents an RSA with 1024 bits modulus which is DH Group 2.

- **modp1536**
  The value represents an RSA with 1536 bits modulus which is DH Group 5.

- **modp2048**
  The value represents an RSA with 2048 bits modulus which is DH Group 14.

- **modp3072**
  The value represents an RSA with 3072 bits modulus which is DH Group 15.

- **modp4096**
  The value represents an RSA with 4096 bits modulus which is DH Group 16.

IKE integrity (MAC)

Specifies which IKE Integrity (MAC) algorithm the device uses.

In order to help keep the information on the VPN secure, the Hash-based Message Authentication Code (HMAC) process mixes (hashes) a shared secret key with the message data. The device mixes the results (hash value) with the secret key again, and then applies the hash function a second time.

Possible values:

- **any**
  When you specify the device as the responder, the device accepts every algorithm. When you specify the device as the initiator, the device uses various pre-defined algorithms.

- **hmacmd5**
  The device uses the Message Digest Algorithm 5 (MD5) for the hash function calculation.

- **hmacsha1** (default setting)
  The device uses the Secure Hash Algorithm version 1 (SHA-1) for the hash function calculation.

- **hmacsha256**
  The device uses SHA-256, part of the version 2 family, for the hash function calculation which the device computes with 32-bit words.

- **hmacsha384**
  The device uses SHA-384, part of the version 2 family, for hash function calculation which the device computes using a shorter version of SHA-512.

- **hmacsha512**
  The device uses SHA-512, part of the version 2 family, for hash function calculation which the device computes with 64 bit words.

IKE encryption

Specifies the IKE encryption algorithm that the device uses.

Possible values:

- **any**
  When you specify the device as the responder, the device accepts every algorithm. When you specify the device as the initiator, the device uses various pre-defined algorithms.
The device uses the Data Encryption Standard (DES) block cipher for encryption of message data with a 56-bit key.

The device uses the Triple DES block cipher for encryption of message data which applies the 56-bit key, from DES, 3 times to each block.

The device uses the Advanced Encryption Standard (AES) with a block size of 128 bits, and a key length of 128 key bits.

The device uses the Advanced Encryption Standard (AES) with a block size of 128 bits, and a key length of 192 key bits.

The device uses the Advanced Encryption Standard (AES) with a block size of 128 bits, and a key length of 256 key bits.

DPD timeout [s]

Specifies the timeout, in seconds, before the local peer declares the remote peer dead, if the remote peer is unresponsive.

Possible values:

- 0..86400 (default setting: 120)
  The value 0 disables this feature. The default setting is 2 minutes. The maximum setting is 24 hours.

IKE lifetime [s]

Specifies the lifetime, in seconds, of the IKE security association between two network devices to support secure communication. The device establishes a security association after exchanging a set of pre-defined keys.

Possible values:

- 300..86400 (default setting: 28800)
  The default setting is 8 hours. The maximum setting is 24 hours.

IPSec/Data-exchange

IPsec key agreement

Specifies which Diffie-Hellman key agreement algorithm the device uses for establishing the IPsec-SA session key establishment.

Possible values:

- any
  When you specify the device as the responder, the device accepts every algorithm. When you specify the device as the initiator, the device uses various pre-defined algorithms.

- modp1024 (default setting)
  The value represents an Rivest, Shamir, and Adleman (RSA) algorithm with 1024 bits modulus. This value is Diffie-Hellman Group 2.

- modp1536
  The value represents an RSA with 1536 bits modulus which is Diffie-Hellman Group 5.
Virtual Private Network
[Virtual Private Network > Connections]

- **modp2048**
  The value represents an RSA with 2048 bits modulus which is Diffie-Hellman Group 14.

- **modp3072**
  The value represents an RSA with 3072 bits modulus which is Diffie-Hellman Group 15.

- **modp4096**
  The value represents an RSA with 4096 bits modulus which is Diffie-Hellman Group 16.

- **none**
  The value disables Perfect Forward Secrecy (PFS). With PFS enabled, if a compromise of a single key occurs, then the integrity remains for subsequently generated keys.

**IPsec lifetime [s]**

Specifies the lifetime, in seconds, of the IPsec security association between two network devices to support secure communication. The device establishes a security association after exchanging a set of pre-defined keys.

Possible values:

- **300..28800** (default setting: 3600)
  The default setting is 1 hour. The maximum setting is 8 hours.

**IPsec integrity (MAC)**

Specifies which IPsec Integrity (MAC) algorithm the device uses for the instance.

In order to help keep the information on the VPN secure, the Hash-based Message Authentication Code (HMAC) process mixes (hashes) a shared secret key with the message data. The device mixes the results (hash value) with the secret key again, and then applies the hash function a second time.

Possible values:

- **any**
  When you specify the device as the responder, the device accepts every algorithm. When you specify the device as the initiator, the device uses various pre-defined algorithms.

- **hmacmd5**
  The device uses the Message Digest Algorithm 5 (MD5) for the hash function calculation.

- **hmacsha1** (default setting)
  The device uses the Secure Hash Algorithm version 1 (SHA-1) for the hash function calculation.

- **hmacsha256**
  The device uses SHA-256, part of the version 2 family, for the hash function calculation which the device computes with 32-bit words.

- **hmacsha384**
  The device uses SHA-384, part of the version 2 family, for hash function calculation which the device computes using a shorter version of SHA-512.

- **hmacsha512**
  The device uses SHA-512, part of the version 2 family, for hash function calculation which the device computes with 64 bit words.

**IPsec encryption**

Specifies the IPsec encryption algorithm that the device uses.

Possible values:

- **any**
  When you specify the device as the responder, the device accepts every algorithm. When you specify the device as the initiator, the device uses various pre-defined algorithms.
Virtual Private Network
[Virtual Private Network > Connections]

- **des**
  The device uses the Data Encryption Standard (DES) block cipher for encryption of message data with a 56-bit key.

- **des3**
  The device uses the Triple DES block cipher for encryption of message data which applies the 56-bit key, from DES, 3 times to each block.

- **aes128** (default setting)
  The device uses the Advanced Encryption Standard (AES) with a block size of 128 bits, and a key length of 128 key bits.

- **aes192**
  The device uses the AES with a block size of 128 bits, and a key length of 192 key bits.

- **aes256**
  The device uses the AES with a block size of 128 bits, and a key length of 256 key bits.

- **aes128gcm64**
  The device uses the AES-Galois/Counter Mode (GCM) with a 64 bit Integrity Check Value (ICV) and 128 key bits.

- **aes128gcm96**
  AES-GCM with a 96 bit ICV and 128 key bits.

- **aes128gcm128**
  AES-GCM with a 128 bit ICV and 128 key bits.

- **aes192gcm64**
  AES-GCM with a 64 bit ICV and 192 key bits.

- **aes192gcm96**
  AES-GCM with a 96 bit ICV and 192 key bits.

- **aes192gcm128**
  AES-GCM with a 128 bit ICV and 192 key bits.

- **aes256gcm64**
  AES-GCM with a 64 bit ICV and 256 key bits.

- **aes256gcm96**
  AES-GCM with a 96 bit ICV and 256 key bits.

- **aes256gcm128**
  AES-GCM with a 128 bit ICV and 256 key bits.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

- **Back**
  Displays the previous page. Changes are lost.

- **Next**
  Saves the changes and displays the next page.

- **Finish**
  Saves the changes and closes the wizard.
Cancel

Closes the Wizard. Changes are lost.
6 Switching

The menu contains the following dialogs:
- Switching Global
- Rate Limiter
- Filter for MAC Addresses
- QoS/Priority
- VLAN

6.1 Switching Global

This dialog lets you specify the following settings:
- Change the Aging time of the address table
- Enable the flow control in the device

If a large number of data packets are received in the priority queue of a port at the same time, then this can cause the port memory to overflow. This happens, for example, when the device receives data on a Gigabit port and forwards it to a port with a lower bandwidth. The device discards surplus data packets.

The flow control mechanism described in standard IEEE 802.3 helps ensure that no data packets are lost due to a port memory overflowing. Shortly before a port memory is completely full, the device signals to the connected devices that it is not accepting any more data packets from them.

- In full-duplex mode, the device sends a pause data packet.
- In half-duplex mode, the device simulates a collision.

Then the connected devices do not send any more data packets for as long as the signaling takes. On uplink ports, this can possibly cause undesired sending breaks in the higher-level network segment ("wandering backpressure").

Configuration

MAC address

Displays the MAC address of the device.

Aging time [s]

Specifies the aging time in seconds.

Possible values:
- 10..500000 (default setting: 30)

The device monitors the age of the learned unicast MAC addresses. The device deletes address entries that exceed a particular age (aging time) from its address table.

You find the address table in the Switching > Filter for MAC Addresses dialog.

In connection with the router redundancy, specify a time ≥ 30 s.
Flow control

Activates/deactivates the flow control in the device.

Possible values:

- **marked**
  The flow control is active in the device.
  Additionally activate the flow control on the required ports. See the Basic Settings > Port dialog, Configuration tab, checkbox in the Flow control column.

- **unmarked** (default setting)
  The flow control is inactive in the device.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.
6.2 Rate Limiter

The device lets you limit the traffic on the ports in order to help provide stable operation even with a large traffic volume. If the traffic on a port exceeds the traffic value entered, then the device discards the excess traffic on this port.

The rate limiter function operates only on Layer 2, and is used to limit the effects of storms of data packets that flood the device (typically Broadcasts).

The rate limiter function ignores protocol information on higher layers, such as IP or TCP.

The dialog contains the following tabs:

- [Ingress]

**Ingress**

In this tab you enable the *Rate Limiter* function. The threshold value specifies the maximum amount of traffic the port receives. If the traffic on this port exceeds the threshold value, then the device discards the excess traffic on this port.

**Table**

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
</table>

**Threshold unit**

Specifies the unit for the threshold value:

Possible values:

- **percent** (default setting)
  - Specifies the threshold value as a percentage of the data rate of the port.
- **pps**
  - Specifies the threshold value in data packets per second.

**Broadcast mode**

Activates/deactivates the rate limiter function for received broadcast data packets.

Possible values:

- **marked**
- **unmarked** (default setting)

If the threshold value is exceeded, then the device discards the excess broadcast data packets on this port.
Broadcast threshold

Specifies the threshold value for received broadcasts on this port.

Possible values:
- \[0..14880000\] (default setting: 0)
  - The value 0 deactivates the rate limiter function on this port.
  - If you select the value \textit{percent} in the \textit{Threshold unit} column, then enter a percentage value from 1 to 100.
  - If you select the value \textit{pps} in the \textit{Threshold unit} column, then enter an absolute value for the data rate.

Multicast mode

Activates/deactivates the rate limiter function for received multicast data packets.

Possible values:
- \textit{marked}
- \textit{unmarked} (default setting)

If the threshold value is exceeded, then the device discards the excess multicast data packets on this port.

Multicast threshold

Specifies the threshold value for received multicasts on this port.

Possible values:
- \[0..14880000\] (default setting: 0)
  - The value 0 deactivates the rate limiter function on this port.
  - If you select the value \textit{percent} in the \textit{Threshold unit} column, then enter a percentage value from 0 to 100.
  - If you select the value \textit{pps} in the \textit{Threshold unit} column, then enter an absolute value for the data rate.

Unknown unicast mode

Activates/deactivates the rate limiter function for received unicast data packets with an unknown destination address.

Possible values:
- \textit{marked}
- \textit{unmarked} (default setting)

If the threshold value is exceeded, then the device discards the excess unicast data packets on this port.

Unicast threshold

Specifies the threshold value for received unicasts with an unknown destination address on this port.

Possible values:
- \[0..14880000\] (default setting: 0)
  - The value 0 deactivates the rate limiter function on this port.
If you select the value **percent** in the **Threshold unit**, then enter a percentage value from *0* to *100*.

If you select the value **pps** in the **Threshold unit** column, then enter an absolute value for the data rate.

**Buttons**

You find the description of the standard buttons in section “**Buttons**” on page 14.
6.3 Filter for MAC Addresses

This dialog lets you display and edit address filters for the address table. Address filters specify the way the data packets are forwarded in the device based on the destination MAC address.

Each row in the table represents one filter. The device automatically sets up the filters. The device lets you set up additional filters manually.

The device transmits the data packets as follows:
- When the table contains an entry for the destination address of a data packet, the device transmits the data packet from the receiving port to the port specified in the table entry.
- When there is no table entry for the destination address, the device transmits the data packet from the receiving port to every other port.

Table

To delete the learned MAC addresses from the address table, click in the Basic Settings > Restart dialog the Reset MAC address table button.

Address

Displays the destination MAC address to which the table entry applies.

VLAN ID

Displays the ID of the VLAN to which the table entry applies.

The device learns the MAC addresses for every VLAN separately (independent VLAN learning).

Status

Displays how the device has set up the address filter.

Possible values:
- learned
  Address filter set up automatically by the device based on received data packets.
- permanent
  Address filter set up manually. The address filter stays set up permanently.
- mgmt
  MAC address of the device. The address filter is protected against changes.

<Port number>

Displays how the corresponding port transmits data packets which it directs to the adjacent destination address.

Possible values:
- –
  The port does not transmit any data packets to the destination address.
- learned
  The port transmits data packets to the destination address. The device created the filter automatically based on received data packets.
### 6.4 QoS/Priority

Communication networks transmit a number of applications at the same time that have different requirements as regards availability, bandwidth and latency periods.

QoS (Quality of Service) is a procedure defined in IEEE 802.1D. It is used to distribute resources in the network. You therefore have the possibility of providing minimum bandwidth for necessary applications. The prerequisite is that the end devices and the devices in the network support prioritized data transmission. Data packets with high priority are given preference when transmitted by devices in the network. You transfer data packets with lower priority when there are no data packets with a higher priority to be transmitted.

The device provides the following setting options:

- You specify how the device evaluates QoS/prioritization information for inbound data packets.
- For outbound packets, you specify which QoS/prioritization information the device writes in the data packet (for example priority for management packets, port priority).

**Note:** If you use the functions in this menu, then disable the flow control. The flow control is inactive if in the Switching > Global dialog, Configuration frame the Flow control checkbox is unmarked.
Switching
[Switching > QoS/Priority]

The menu contains the following dialogs:
- QoS/Priority Global
- QoS/Priority Port Configuration
- 802.1D/p Mapping
6.4.1 QoS/Priority Global

The device lets you maintain access to the device management, even in situations with heavy utilization. In this dialog you specify the required QoS/priority settings.

**Configuration**

VLAN priority for management packets

Specifies the VLAN priority for sending management data packets. Depending on the VLAN priority, the device assigns the data packet to a specific traffic class and thus to a specific priority queue of the port.

Possible values:

- 0..7 (default setting: 0)

In the Switching > QoS/Priority > 802.1D/p Mapping dialog, you assign a traffic class to every VLAN priority.

IP DSCP value for management packets

Specifies the IP DSCP value for sending management data packets. Depending on the IP DSCP value, the device assigns the data packet to a specific traffic class and thus to a specific priority queue of the port.

Possible values:

- 0 (be/cs0)..63 (default setting: 0 (be/cs0))

Some values in the list also have a DSCP keyword, for example 0 (be/cs0), 10 (af11) and 46 (ef). These values are compatible with the IP precedence model.

Queues per port

Displays the number of priority queues per port.

The device has 8 priority queues per port. You assign every priority queue to a specific traffic class (traffic class according to IEEE 802.1D).

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.
6.4.2 QoS/Priority Port Configuration

In this dialog you specify for every port how the device processes received data packets based on their QoS/priority information.

**Table**

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
</table>

| Port priority | Specifies what VLAN priority information the device writes into a data packet if the data packet contains no priority information. After this, the device transmits the data packet depending on the value specified in the *Trust mode* column. |

Possible values:

- 0..7  (default setting: 0)

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.
6.4.3 **802.1D/p Mapping**

The device transmits data packets with a VLAN tag according to the contained QoS/priority information with a higher or lower priority.

In this dialog you see which VLAN priority is assigned to which traffic class. You assign the traffic classes to the priority queues of the ports.

**Table**

<table>
<thead>
<tr>
<th>VLAN priority</th>
<th>Traffic class</th>
<th>Content description according to IEEE 802.1D</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
<td>Best Effort Normal data without prioritizing</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Background Non-time-sensitive data and background services</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>Standard Normal data</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>Excellent Effort Crucial data</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>Controlled Load Time-sensitive data with a high priority</td>
</tr>
</tbody>
</table>

Note: Among other things redundancy mechanisms use the highest traffic class. Therefore, select another traffic class for application data.

**Buttons**

You find the description of the standard buttons in section "Buttons" on page 14.
With VLAN (Virtual Local Area Network) you distribute the data traffic in the physical network to logical subnetworks. This provides you with the following advantages:

- **High flexibility**
  - With VLAN you distribute the data traffic to logical networks in the existing infrastructure. Without VLAN, it would be necessary to have additional devices and complicated cabling.
  - With VLAN you specify network segments independently of the location of the individual end devices.

- **Improved throughput**
  - In VLANs data packets can be transferred by priority. When the priority is high, the device transfers the data of a VLAN preferentially, for example for time-sensitive applications such as VoIP phone calls.
  - When the data packets and Broadcasts are distributed in small network segments instead of in the entire network, the network load is considerably reduced.

- **Increased security**
  The distribution of the data traffic among individual logical networks makes unwanted accessing more difficult and strengthens the system against attacks such as MAC Flooding or MAC Spoofing.

The device supports packet-based “tagged” VLANs according to the IEEE 802.1Q standard. The VLAN tagging in the data packet indicates the VLAN to which the data packet belongs.

The device transmits the tagged data packets of a VLAN only on ports that are assigned to the same VLAN. This reduces the network load.

The device learns the MAC addresses for every VLAN separately (independent VLAN learning).

The menu contains the following dialogs:

- VLAN Global
- VLAN Configuration
- VLAN Port

<table>
<thead>
<tr>
<th>VLAN Priority</th>
<th>Traffic class</th>
<th>Content description according to IEEE 802.1D</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5</td>
<td><strong>Video</strong> Video transmission with delays and jitter &lt; 100 ms</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td><strong>Voice</strong> Voice transmission with delays and jitter &lt; 10 ms</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td><strong>Network Control</strong> Data for network management and redundancy mechanisms</td>
</tr>
</tbody>
</table>
6.5.1 VLAN Global

This dialog lets you view general VLAN parameters for the device.

**Configuration**

Max. VLAN ID

Highest ID assignable to a VLAN.

See the Switching > VLAN > Configuration dialog.

VLANs (max.)

Displays the maximum number of VLANs possible.

See the Switching > VLAN > Configuration dialog.

VLANs

Number of VLANs currently configured in the device.

See the Switching > VLAN > Configuration dialog.

The VLAN ID 1 is constantly present in the device.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

Clear...

 Resets the VLAN settings of the device to the default setting.

Note that you lose your connection to the device if you have changed the VLAN ID for the device management in the Basic Settings > Network dialog.
6.5.2 VLAN Configuration

In this dialog you manage the VLANs. To set up a VLAN, create a further row in the table. There you specify for each port if it transmits data packets of the respective VLAN and if the data packets contain a VLAN tag.

You distinguish between the following VLANs:
- The user sets up static VLANs.
- The device sets up dynamic VLANs automatically and removes them if the prerequisites cease to apply.
  For the following functions the device creates dynamic VLANs:
  - **Routing**: The device creates a VLAN for every router interface.

**Table**

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>ID of the VLAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The device supports up to 64 VLANs simultaneously set up.</td>
</tr>
<tr>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>- 1..4042</td>
</tr>
</tbody>
</table>

**Status**

Displays how the VLAN is set up.

Possible values:
- **other**
  - **VLAN** 1
- **permanent**
  - VLAN set up by the user.
  - If you save the changes in the non-volatile memory, then the VLANs with this setting remain set up after a restart.

**Creation time**

Displays the time of VLAN creation.

The field displays the time stamp for the operating time (system uptime).
Name

Specifies the name of the VLAN.

Possible values:
- Alphanumeric ASCII character string with 1..32 characters

<Port number>

Specifies if the respective port transmits data packets of the VLAN and if the data packets contain a VLAN tag.

Possible values:
- - (default setting)
  The port is not a member of the VLAN and does not transmit data packets of the VLAN.
- T = Tagged
  The port is a member of the VLAN and transmits the data packets with a VLAN tag. You use this setting for uplink ports, for example.
- LT = Tagged Learned
  The port is a member of the VLAN and transmits the data packets with a VLAN tag. The device created the entry automatically based on the GVRP or MVRP function.
- F = Forbidden
  The port is not a member of the VLAN and does not transmit data packets of this VLAN.
- U = Untagged (default setting for VLAN 1)
  The port is a member of the VLAN and transmits the data packets without a VLAN tag. Use this setting if the connected device does not evaluate any VLAN tags, for example on end ports.
- LU = Untagged Learned
  The port is a member of the VLAN and transmits the data packets without a VLAN tag. The device created the entry automatically based on the GVRP or MVRP function.

Note: Verify that the port on which the network management station is connected is a member of the VLAN in which the device transmits the management data. In the default setting, the device transmits the management data on VLAN 1. Otherwise, the connection to the device terminates when you transfer the changes to the device. The access to the device management is possible only using the Command Line Interface through the serial interface.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.

In the VLAN ID field, you specify the ID of the VLAN.
6.5.3 VLAN Port

In this dialog you specify how the device handles received data packets that have no VLAN tag, or whose VLAN tag differs from the VLAN ID of the port.

This dialog lets you assign a VLAN to the ports and thus specify the port VLAN ID.

Additionally, you also specify for each port how the device transmits data packets and one of the following situations occurs:

- The port receives data packets without a VLAN tagging.
- The port receives data packets with VLAN priority information (VLAN ID 0, priority tagged).
- The VLAN tagging of the data packet differs from the VLAN ID of the port.

### Table

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Port-VLAN ID</th>
<th>Specifies the ID of the VLAN which the device assigns to data packets without a VLAN tag.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites:</td>
<td>In the Acceptable packet types column, you specify the value admitAll.</td>
</tr>
<tr>
<td>Possible values:</td>
<td>▶ ID of a VLAN you set up (default setting: 1)</td>
</tr>
<tr>
<td></td>
<td>▶ 4043..</td>
</tr>
<tr>
<td></td>
<td>The device assigns values &gt; 4042 for internal functions for example, for port based router interfaces.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acceptable packet types</th>
<th>Specifies if the port transmits or discards received data packets without a VLAN tag.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possible values:</td>
<td>▶ admitAll (default setting)</td>
</tr>
<tr>
<td></td>
<td>The port accepts data packets both with and without a VLAN tag.</td>
</tr>
<tr>
<td></td>
<td>▶ admitOnlyVlanTagged</td>
</tr>
<tr>
<td></td>
<td>The port accepts only data packets tagged with a VLAN ID ≥ 1.</td>
</tr>
</tbody>
</table>
Ingress filtering

Activates/deactivates the ingress filtering.

Possible values:
- **marked** (default setting)
  The ingress filtering is active.
  The device compares the VLAN ID in the data packet with the VLANs of which the device is a member. See the *Switching > VLAN > Configuration* dialog. If the VLAN ID in the data packet matches one of these VLANs, then the port transmits the data packet. Otherwise, the device discards the data packet.
- **unmarked**
  The ingress filtering is inactive.
  The device transmits received data packets without comparing the VLAN ID. Thus the port also transmits data packets with a VLAN ID of which the port is not a member.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.
7 Routing

The menu contains the following dialogs:

- Routing Global
- Routing Interfaces
- ARP
- Open Shortest Path First
- Routing Table
- Tracking
- L3 Relay
- Loopback Interface
- L3-Redundancy
- NAT

7.1 Routing Global

The Routing menu lets you specify the Routing functions settings for transmitting data on Layer 3 of the ISO/OSI layer model.

For security reasons, the following functions are permanently disabled in the device:
- Source Routing
  With source routing, the data packet contains the routing information and overwrites the settings in the router with it.
- ICMP Redirects
  ICMP redirect data packets are able to modify the routing table. The device generally ignores received ICMP redirect data packets. The settings in the Routing > Interfaces > Configuration dialog, column ICMP redirects, have an effect only on the sending of ICMP redirect data packets.

In accordance with RFC 2644, the device does not exchange any broadcast data packets from external networks in a local network. This behavior supports you in protecting the devices in the local network against overloading, for example due to so-called smurf attacks.

This dialog lets you enable the routing function in the device and to specify further settings.

Operation

Enable disables the Routing function in the device.

Possible values:

- **On**
  The Routing function is enabled.
  Also activate the routing function on the router interfaces. See the Routing > Interfaces > Configuration dialog.

- **Off** (default setting)
  The Routing function is disabled.
ICMP filter

In the ICMP filter frame, you have the option of limiting the transmission of ICMP messages on the set up router interfaces. A limitation is meaningful for several reasons:

- A large number of “ICMP Error” messages influences the router performance and reduces the available network bandwidth.
- Malicious senders use “ICMP Redirect” messages to perform man-in-the-middle attacks or to divert data packets through “black hole” for the purpose of supervision or denial-of-service (DoS).
- “ICMP Echo Reply” messages are ping responses which can be misused to discover vulnerable devices and routers in the network.

Send echo reply

Activates/deactivates the responding to pings on the router interfaces.

Possible values:

- **marked** (default setting)
  - Responding to pings is active.
  - The device reacts to received “IPv4 Echo Requests” and responds with an “ICMP Echo Reply” message.

- **unmarked**
  - Responding to pings is inactive.

Send redirects

Activates/deactivates the sending of “ICMP Redirect” messages on the router interfaces.

Possible values:

- **marked** (default setting)
  - The sending of “ICMP Redirect” messages is active.
  - In the Routing > Interfaces > Configuration dialog, you have the option of individually activating the sending on every router interface. See the ICMP redirects function.

- **unmarked**
  - The sending of “ICMP Redirect” messages is inactive.
  - This setting helps prevent the multiplication of data packets, if both hardware and software functions of the device forward a copy of the same data packet.

Rate limit interval [ms]

Specifies the average minimum time in milliseconds between sending ICMP packets. The device sends existing ICMP packets to each receiver using a token bucket algorithm.

- In periods without sending ICMP packets, the device accumulates tokens to allow bursts.
- In the case of bursts, the interval is shorter than specified here.
Possible values:

- $0..2147483647$ (default setting: 1000)

**Rate limit burst size**

Displays the maximum number of ICMP packets, the device sends during a burst to each receiver.

Possible values:

- 6

**Information**

**Default TTL**

Displays the fixed TTL value 64 which the device adds to IP packets that the device management sends.

TTL (Time To Live, also known as “Hop Count”) identifies the maximum number of steps an IP packet is allowed to perform on the way from the sender to the receiver. Every router on the transmission path reduces the value in the IP packet by 1. If a router receives a data packet with the TTL value 1, then the router discards the IP packet. The router reports to the source that it has discarded the IP packet.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

**7.2 Routing Interfaces**

This menu lets you specify the settings for the router interfaces.

The menu contains the following dialogs:

- Routing Interfaces Configuration
- Routing Interfaces Secondary Interface Addresses
7.2.1 Routing Interfaces Configuration

This dialog lets you specify the settings for the router interfaces.

To set up a port-based router interface, edit the table entries. To set up a VLAN-based router interface, use the *Wizard* window.

**Table**

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the number of the port or VLAN belonging to the router interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the port.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Alphanumeric ASCII character string with 0..64 characters" /> The following characters are allowed:</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="&lt;space&gt;" /></td>
</tr>
<tr>
<td>Port on</td>
<td>Activates/deactivates the port.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="marked" /> (default setting) The port is active.</td>
</tr>
<tr>
<td>Port status</td>
<td>Displays the operating state of the port.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="marked" /> The port is enabled.</td>
</tr>
</tbody>
</table>
IP address

Specifies the IP address for the router interface.

Possible values:
- Valid IPv4 address (default setting: 0.0.0.0)

Verify that the IP subnet of the router interface is not overlapping with any subnet connected to another interface of the device:
- management port
- router interface
- loopback interface

Netmask

Specifies the netmask for the router interface.

Possible values:
- Valid IPv4 netmask (default setting: 0.0.0.0)

Routing

Activates/deactivates the Routing function on the router interface.

In the process, the device removes the state information from the packet filter. This includes potential DCE RPC information of the OPC enforcer. In the process, the device interrupts open communication connections.

Possible values:
- marked
  The Routing function is active.
  - With port-based routing, the device transforms the port into a router interface.
    Enabling the Routing function removes the port from the VLANs in which it was previously a member. Disabling the Routing function does NOT reestablish the assignment; the port is not a member of any VLAN.
  - With VLAN-based routing, the device forwards the data packets in the related VLAN.
- unmarked (default setting)
  The Routing function is inactive.
  With VLAN-based routing, the device is still reachable through the router interface if the IP address and netmask have been configured for the router interface.

Proxy ARP

Activates/deactivates the Proxy ARP function on the router interface. This feature lets you connect devices from other networks as if these devices could be reached in the same network.

Possible values:
- marked
  The Proxy ARP function is active.
  The device responds to ARP requests from end devices that are located in other networks.
- unmarked (default setting)
  The Proxy ARP function is inactive.
Routing
[Routing > Interfaces > Configuration]

MTU value

Specifies the maximum allowed size of IP packets on the router interface in bytes.

Possible values:
- 0
  Restores the default value (1500).
- 68..1500 (default setting: 1500)
  The prerequisite is that on the ports belonging to the router interface you specify the maximum allowed size of Ethernet packets at least 18 bytes larger than specified here. See the Basic Settings > Port dialog, MTU column.

ICMP unreachable

Displays if the sending of ICMP Destination Unreachable messages is activated on the router interface.

Possible values:
- marked
  The router interface sends ICMP Destination Unreachable messages.

ICMP redirects

Displays if the sending of “ICMP Redirect” messages is activated on the router interface.

Possible values:
- marked
  The router interface sends “ICMP Redirect” messages.
- unmarked (default setting)
  The router interface does not send “ICMP Redirect” messages.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.
In the VLAN ID field, you specify the ID of the VLAN.

[Configure VLAN router interface (Wizard)]

This Wizard window lets you set up a VLAN-based router interface.
- To set up a router interface from a VLAN already set up, highlight a VLAN in the table.
- To set up a router interface from a new VLAN, specify at the bottom of the VLAN ID field the ID of the new VLAN.
[Configure VLAN router interface (Wizard) – Create or select VLAN]

Table

VLAN ID
Displays the ID of the VLANs set up in the device.

Name
Displays the name of the VLANs set up in the device.

Area under the table

VLAN ID
Specifies the ID of a VLAN that the Wizard window specifies for you.
Possible values:
► 1..4042

[Configure VLAN router interface (Wizard) – Setup VLAN]

Area above the table

VLAN ID
Displays the ID of the VLAN that you have marked or specified in the Create or select VLAN dialog.

Name
Specifies the name of the VLAN.
Possible values:
► Alphanumeric ASCII character string with 1..32 characters (0x20..0x7E) including space characters

This setting overwrites the setting specified for the port in the Switching > VLAN > Configuration dialog.

Table

Port
Displays the port number.
Member
Activates/deactivates the VLAN membership of the port.
As a VLAN member the port belongs to the router interface to be set up. This setting overwrites the setting for the port specified in the Switching > VLAN > Configuration dialog.
Possible values:
- marked
  The port is a member of the VLAN.
- unmarked
  The port is not a member of the VLAN.

Untagged
Activates/deactivates the transmission of data packets with a VLAN tag on the port. This setting overwrites the setting for the port specified in the Switching > VLAN > Configuration dialog.
Possible values:
- marked
  The port transmits the data packets without a VLAN tag.
  Use this setting if the connected device does not evaluate any VLAN tags, for example on end ports.
- unmarked
  The port transmits the data packets with a VLAN tag.

Port-VLAN ID
Specifies the ID of the VLAN which the device assigns to data packets without a VLAN tag. This setting overwrites the setting for the port specified in the Switching > VLAN > Port dialog, column Port-VLAN ID.
Possible values:
- ID of a VLAN you set up  (default setting: 1)

Configure VLAN router interface (Wizard) – Setup virtual router port
The device lets you specify up to 2 IP addresses (1 primary, 1 secondary) for a router interface and a total of up to 64 IP addresses.
When you assign ports to the router interface that already transmit data packets in other VLANs, the device displays a message upon closing the Wizard window:
- If you click the Yes button, then the related ports transmit the data packets from now on only in the router VLAN.
  In the Switching > VLAN > Configuration dialog, the related ports in the row of the router VLAN have the value U or T, in the rows of other VLANs the value –.
- If you click the No button, then the related ports transmit the data packets in the router VLAN and in other VLANs. This setting possibly causes undesired behavior.
**Primary address**

Address

Specifies the primary IP address for the router interface.

Possible values:
- Valid IPv4 address (default setting: 0.0.0.0)

Netmask

Specifies the primary netmask for the router interface.

Possible values:
- Valid IPv4 netmask (default setting: 0.0.0.0)

**Secondary addresses**

Address

Specifies a further IP address for the router interface (Multinetting).

Possible values:
- Valid IPv4 address (default setting: 0.0.0.0)

Specify an IP address which is different from the primary IP address of the router interface.

Netmask

Specifies the netmask for the belonging further IP address.

Possible values:
- Valid IPv4 netmask (default setting: 0.0.0.0)
7.2.2 Routing Interfaces Secondary Interface Addresses

This dialog lets you assign further IP addresses to the router interfaces. You use this function to connect a router interface to several subnets.

The device lets you specify up to 2 IP addresses (1 primary, 1 secondary) for a router interface and a total of up to 64 IP addresses.

Table

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the number of the port or VLAN belonging to the router interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>Displays the primary IP address of the router interface. See the Routing &gt; Interfaces &gt; Configuration dialog.</td>
</tr>
<tr>
<td>Netmask</td>
<td>Displays the primary netmask of the router interface. See the Routing &gt; Interfaces &gt; Configuration dialog.</td>
</tr>
<tr>
<td>Additional IP address</td>
<td>Displays further IP addresses assigned to the router interface.</td>
</tr>
<tr>
<td>Additional netmask</td>
<td>Displays further netmasks assigned to the router interface.</td>
</tr>
</tbody>
</table>

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add another IP address to the router interface highlighted in the table.

- In the Port drop-down list, you select the port number or VLAN ID belonging to the router interface.
- In the Additional IP address field, you specify the IP address.
  Possible values:
  - Valid IPv4 address
- In the Additional netmask field, you specify the netmask.
  Possible values:
  - Valid IPv4 netmask
Verify that the IP subnet of the router interface is not overlapping with any subnet connected to another interface of the device:

- management port
- router interface
- loopback interface

7.3 ARP

The Address Resolution Protocol (ARP) learns the MAC address that belongs to an IP address.

The menu contains the following dialogs:
- ARP Global
- ARP Current
- ARP Static
7.3.1 ARP Global

This dialog lets you set the ARP parameters and view statistical values.

**Configuration**

**Aging time [s]**

Specifies the average time in seconds, after which the device removes an entry from the ARP table. The device actually removes an entry after a randomly determined time in the range \((0.5 \text{ to } 1.5) \times\) of the value defined here.

When there is data exchange with the associated device within this time period, the time measuring begins from the start again.

Possible values:
- \(15..21600\) (default setting: 1200)

**Response timeout [s]**

Specifies the time in seconds, that the device waits for a response before the query is seen as a failure.

Possible values:
- \(1..10\) (default setting: 1)

**Retries**

Specifies how many times the device repeats a failed query before it discards the query to this address.

Possible values:
- \(0..10\) (default setting: 4)

**Information**

**Current entries total**

Displays the number of entries that the ARP table currently contains.

This includes:
- Addresses of the devices which are connected to the router interfaces. See the [Routing > ARP > Current](#) dialog.
- Addresses of the devices which are connected to the device management. See the [Diagnostics > System > ARP](#) dialog.

**Entries (max.)**

Displays how many entries the ARP table can contain at a maximum.
Total entry peaks

Displays how many entries the ARP table has already contained at a maximum.

When you reset the ARP table, the counter is reset to the value 0. See the Reset ARP table button in the Routing > ARP > Current dialog.

Current static entries

Displays the number of statically configured entries the ARP table currently contains. See the Routing > ARP > Static dialog.

Static entries (max.)

Displays the number of statically configured entries the ARP table can contain at a maximum.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
7.3.2 ARP Current

This dialog lets you view the ARP table and delete the dynamically configured entries.

**Table**

**Port**
Displays the router interface on which the device has learned the IP/MAC address assignment.

**IP address**
Displays the IP address of the device that responded to an ARP query on this router interface.

**MAC address**
Displays the MAC address of the device that responded to an ARP query on this router interface.

**Last updated**
Displays the time in seconds since the current settings of the entry were registered in the ARP table.

**Type**
Displays the way in which the ARP entry was set up.

Possible values:

- **dynamic**
  Dynamically configured entry.
  When no traffic with the associated device takes place by the end of the aging time, the device removes this entry from the ARP table.
  You specify the aging time in the Routing > ARP > Global dialog, field Aging time [s].

- **static**
  Statically configured entry.
  When you remove the dynamically configured addresses from the ARP table using the Reset ARP table button, the entry remains.

- **local**
  Identifies the IP/MAC address assignment of the router interface.

- **invalid**
  Invalid entry.

**Buttons**

You find the description of the standard buttons in section "Buttons" on page 14.

**Reset ARP table**
Removes the dynamically set up addresses from the ARP table.
7.3.3 ARP Static

This dialog lets you add to the ARP table IP/MAC address assignments that you have specified yourself.

**Table**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>Displays the IP address that the device assigns to the adjacent MAC address.</td>
</tr>
<tr>
<td>MAC address</td>
<td>Displays the MAC address that the device assigns to the adjacent IP address.</td>
</tr>
</tbody>
</table>
| Port           | Displays the router interface to which the device applies the IP/MAC address assignment. Possible values:  
|                | <Router interface>  
|                | The device applies the IP/MAC address assignment to this router interface.  
|                | no port  
|                | The IP/MAC address assignment is currently not assigned to a router interface. |
| Active         | Displays if the IP/MAC address assignment is active or inactive.  
|                | Possible values:  
|                | marked  
|                | The IP/MAC address assignment is active. The ARP table of the device contains the IP/MAC address assignment as a static entry.  
|                | unmarked (default setting)  
|                | The IP/MAC address assignment is inactive. |

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.

In the IP address field, you specify the IP address that the device assigns to the adjacent MAC address.
Routing

[Routing > OSPF]

[ARP (Wizard)]

The Wizard window lets you add to the ARP table IP/MAC address assignments that you have specified yourself. The prerequisite is that at least one router interface is set up.

[ARP (Wizard) – Edit ARP table]

Perform the following steps:
- In the fields under the table, specify the IP address and the associated MAC address.
- To insert the IP/MAC address assignment into the table on the top, click the Add button.
- After closing the Wizard window, specify in the Port column the router interface. Then enable in the Active column the IP/MAC address assignment.

Table

<table>
<thead>
<tr>
<th>IP address</th>
<th>Specifies the IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possible values:</td>
<td>Valid IPv4 address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC address</th>
<th>Specifies the MAC address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possible values:</td>
<td>Valid MAC address</td>
</tr>
</tbody>
</table>

7.4 Open Shortest Path First

Open Shortest Path First (OSPF) version 2, is a routing protocol described in RFC 2328, which is applicable to networks with many routers.

In contrast to the hop count based distance-vector routing protocols such as RIP, OSPF provides a link state algorithm. OSPF bases its link state algorithm on link cost meaning that the criteria for the routing decisions are the path costs instead of hop counts. The path cost is calculated as \((100 \, \text{Mbit/s}) / (\text{bandwidth in Mbit/s})\). OSPF also supports Variable Length Subnet Masking (VLSM) or Classless Inter-Domain Routing (CIDR) networks.

OSPF convergence of the entire network is slow. However, after initialization the protocol is quick in reacting to topology changes. The convergence time for OSPF is 5 to 15 seconds, depending on the size of the network.
OSPF supports networks grouped to "Areas" and thus reduces the administrative effort when maintaining the overall network (OSPF domain). The routers participating in the network know and only manage their own "Area" by flooding Link State Advertisements (LSAs) into the area. Using the LSAs each router builds its own topology database.

- The Area Border Routers (ABR) flood LSAs in an "Area" informing the local networks about destinations in other areas within the OSPF domain. The Designated Routers (DR) transmit LSAs informing about destinations in other areas.
- With Hello packets, neighboring routers periodically identify themselves and signal their availability. If a router misses the Hello packets of another router, then after the expiration of the dead-interval timer, the router considers this router as unreachable.

The device lets you use the md5 algorithm for data transmission. If you use the md5 mode, then specify the same values in the devices in the same area. Specify the area relevant values connected to the ABRs and ASBRs.

OSPF divides routers into the following roles:
- Designated Router (DR)
- Backup Designated Router (BDR)
- Area Border Router (ABR)
- Autonomous System Boundary Router (ASBR)

The menu contains the following dialogs:
- OSPF Global
- OSPF Areas
- OSPF Stub Areas
- OSPF Not So Stubby Areas
- OSPF Interfaces
- OSPF Virtual Links
- OSPF Ranges
- OSPF Diagnostics
This dialog lets you specify the basic OSPF settings.

The menu contains the following dialogs:

- [General]
- [Configuration]
- [Redistribution]

[General]

This tab lets you enable OSPF in the device and to specify network parameters.

Operation

Enables/disables the OSPF function in the device.

Possible values:

- On: The OSPF function is enabled.
- Off (default setting): The OSPF function is disabled.

Configuration

Router ID

Specifies the unique identifier for the router in the Autonomous System (AS). It influences the election of the Designated Router (DR) and the Backup Designated Router (BDR). Ideally, you use the IP address of a router interface in the device.

Possible values:

- <IP address of an interface> (default setting: 0.0.0.0)

External LSDB limit

Specifies the maximum number of entries, non-default AS-external-LSAs, that the device saves in the link state database. When this limit is reached, the router enters the overflow state.

Possible values:

- -1 (default setting)
  - The router continues to save entries until the memory is full.
- 0..2147483647
  - The device saves up to the specified number of entries.
  - Specify the same value in the routers on the OSPF backbone and in any regular OSPF area.
External LSAs

Displays the current number of entries, non-default AS-external-LSAs, that the device currently holds in the link state database.

Autocost reference bandwidth

Specifies a reference for router interface bandwidth calculations, in Mbps. You use this value for metric calculations.

Possible values:

- \texttt{1..4294967} (default setting: \texttt{100})

Paths (max.)

Specifies the maximum number of ECMP routes that OSPF adds to the routing table when multiple routes exist for a subnet with same path costs, but different next hops.

Possible values:

- \texttt{1..4} (default setting: \texttt{4})
- \texttt{5..16}
  - Available when the ipv4DataCenter routing profile is currently applied. See the Routing profile frame in the Routing > Global dialog.

Default metric

Specifies the default metric value for OSPF.

Possible values:

- \texttt{0} (default setting)
  - OSPF automatically assigns a cost of 20 for routes learned from external sources (static or directly connected).
- \texttt{1..16777214}

Send trap

Activates/deactivates the sending of SNMP traps when the device detects a OSPF parameter change.

Possible values:

- \texttt{marked}
  - The sending of SNMP traps is active.
  - If the device detects changes in the OSPF parameters, then the device sends an SNMP trap.
- \texttt{unmarked} (default setting)
  - The sending of SNMP traps is inactive.

The prerequisite for sending SNMP traps is that you enable the function in the Diagnostics > Status Configuration > Alarms (Traps) dialog and specify at least one trap destination.
**Routing**

[Routing > OSPF > Global]

**Shortest path first**

**Delay time [s]**

Specifies the delay time, in seconds, between when the router receives a topology change and when it starts an SPF calculation.

Possible values:
- 0..65535  (default setting: 5)
  - The value 0 means that the router immediately begins the SPF calculation after receiving the topology change.

**Hold time [s]**

Specifies the minimum time, in seconds, between consecutive SPF calculations.

Possible values:
- 0..65535  (default setting: 10)
  - The value 0 means that after the router completes an SPF calculation it immediately begins the next consecutive SPF calculation.

**Exit overflow interval [s]**

Specifies the number of seconds, after entering the overflow state, that a router attempts to leave the overflow state. When the router leaves the overflow state, the router transmits new non-default AS-external-LSAs.

Possible values:
- 0..2147483647  (default setting: 0)
  - The value 0 means that the router remains in the Overflow-State until restarted.

**Information**

**ASBR status**

Displays if the device operates as an Autonomous System Boundary Router (ASBR).

Possible values:
- marked
  - The router is an ASBR.
- unmarked
  - The router functions in a role other than the role of an ASBR.

**ABR status**

Displays if the device operates as an Area Border Router (ABR).

Possible values:
- marked
  - The router is an ABR.
- unmarked
  - The router functions in a role other than the role of an ABR.
External LSA checksum

Displays the link state checksums of the external LSAs contained in the link state database. This value helps to determine when changes occur in a link state database of the router, and to compare the link state database to other routers.

New LSA originated

Displays the number of new link state advertisements originated on this router. The router increments this number each time it originates a new Link State Advertisement (LSA).

LSAs received

Displays the number of LSAs received that the router determined to be new instances. This number also excludes newer instances of self-originated LSAs.

Buttons

You find the description of the standard buttons in section "Buttons" on page 14.

[Configuration]

This dialog lets you specify the following settings:
- the manner in which the device calculates the path costs
- how OSPF handles default routes
- the type of route OSPF uses for the path-cost calculation

RFC 1583 compatibility

The Network Working Group is continually developing the OSPF function improving and adding parameters. This router provides parameters in accordance with RFC 2328. With parameters in this dialog, you make the router compatible with routers developed under RFC 1583. Activating the compatibility function lets you install this device in a network containing routers developed under RFC 1583.

RFC 1583 compatibility

Enables/disabled the device to be compatible with routers developed under RFC 1583.

In order to minimize the chance of routing loops, set this function to the same value on the OSPF enabled routers in an OSPF domain.

Possible values:
-  On (default setting)
  Enable the function when routers are present in the domain without software containing the external path preference functionality described in RFC 2328.
-  Off
  Disable the function when every router present in the domain has software containing the external path preference functionality described in RFC 2328.
Preferences

The preferences in this dialog are metrics values which the device uses as a tie breaker between identical routes with different distance types. For example, when a route is inside the local area (intra-area) and the other is outside the local area (inter-area or external). If the metric values are the same for intra, inter and external, then the order of preference is intra, inter then external.

OSPF considers routes specified with a preference value of 255 as unreachable.

Preference (intra)

Specifies the "administrative distance" between routers within the same area (intra-area OSPF routes).

Possible values:
- 1..255 (default setting: 110)

Preference (inter)

Specifies the "administrative distance" between routers in different areas (inter-area OSPF routes).

Possible values:
- 1..255 (default setting: 110)

Preference (external)

Specifies the "administrative distance" between routers external to the areas (external OSPF routes).

Possible values:
- 1..255 (default setting: 110)

Default route

Advertise

Activates/deactivates OSPF advertisements of default routes learned from other protocols.

For example, area border routers of stub areas advertise a default route into the stub area through summary link advertisements. When you configure the router as an AS boundary router, it advertises the default route in AS external link advertisements.

Possible values:
- marked
  - The router advertises default routes.
- unmarked (default setting)
  - The router suppresses advertisements of default routes.
Advertise always

Displays if the router constantly advertises 0.0.0.0 as the default route.

When routers forward an IP packet, the router constantly forwards the packet to the best matching destination address. A default route with a destination address of 0.0.0.0 and a mask of 0.0.0.0 is a match for every IP destination address. Matching every IP destination address lets an AS boundary router operate as a gateway for destinations outside of the AS.

Possible values:
- **marked**
  - The router constantly advertises 0.0.0.0 as the default route.
- **unmarked** (default setting)
  - The device uses the settings specified in the Advertise parameter.

Metric

Specifies the metric of the default route, which OSPF advertises when learned from other protocols.

Possible values:
- **0**
  - The device uses the value specified in the Default metric field.
- **1..16777214**

Metric type

Displays the metric type of the default route which OSPF advertises when learned from another protocol.

Possible values:
- **externalType1**
  - Includes both the external path cost from the ABR to the ASBR that originated the route plus the internal path cost to the ABR that advertised the route in the local area.
- **externalType2** (default setting)
  - Includes only the external path cost.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Redistribution

A router with a disabled OSPF function on a routed interface does not propagate the network of this interface on its other interfaces. Thus, the network cannot be reached. To propagate such networks, enable the Redistribution for "connected" networks.

Redistribution is helpful in cases where multiple network administrators manage different departments, or in multi-vendor networks with multiple protocols. OSPF redistribution lets you convert route information such as cost and distance to a destination from other protocols into OSPF.
To help prevent routes from double redistribution and thus preventing a possible loop, use the *Tag* function. This function marks the routes redistributed from other protocols into OSPF. Then on the other routers in the network, create an *ACL active* to deny the tagged number. To specify exactly which routes the device distributes in OSPF, create *ACL permit* rules.

The number of routes that the device learns through OSPF is limited to the size of the routing table.

**Table**

**Source**

Displays the source protocol, from which OSPF redistributes routes. This object also acts as the identifier for the table entry.

Activating a row lets the device redistribute routes from the specific source protocol into OSPF.

Possible values:
- `connected`
  - The router is directly connected to the route.
- `static`
  - A network administrator has specified the route in the router.

**Active**

Activates/deactivates route redistribution from the source protocol into OSPF.

Possible values:
- `marked`
  - Redistribution of routes learned from the source protocol is active.
- `unmarked` (default setting)
  - OSPF route redistribution is inactive.

**Metric**

Specifies the metric value for routes redistributed from this protocol.

Possible values:
- `0` (default setting)
  - The device uses the value specified in the *Default metric* field.
- `1..16777214`

**Metric type**

Specifies the route metric type which OSPF redistributes from other source protocols.

Possible values:
- `externalType1`
  - This metric type includes both the external path cost from the ABR to the ASBR that originated the route plus the internal path cost to the ABR that advertised the route in the local area.
- `externalType2` (default setting)
  - This metric type is only that of the external path cost.
Tag

Specifies a tag for routes redistributed into OSPF.

When you set a route tag, OSPF assigns the value to every redistributed route from this source protocol. This function is useful when 2 or more border routers connect an autonomous system to an external network. To help prevent double redistribution, specify the same value in every border router when redistributing the same protocol.

Possible values:
- 0..4294967295 (default setting: 0)

Subnets

Activates/deactivates subnet route redistribution into OSPF.

OSPF only redistributes classful routes into the OSPF domain. In order to redistribute subnet routes into OSPF activate the subnet parameter.

Possible values:
- marked (default setting)
  The router redistributes classful and subnet routes into OSPF.
- unmarked
  The router redistributes only classful routes into OSPF.

ACL group name

Specifies the name of the Access Control List created to filter routes received from the specified source protocol.

To help prevent double redistribution and eventual loops, create an access list denying redistribution of routes originating in another protocol. Specify the access list ID, then activate the function in the ACL active column. When filtering redistributed routes, the device uses the source address.

Possible values:
- - (default setting)
  No Access Control List assigned.
- <Group name> (IPv4)
  You specify the Access Control Lists in the Network Security > ACL > IPv4 Rule dialog.

ACL active

Activates/deactivates Access Control List filtering for this source protocol.

Possible values:
- marked
  The router filters redistribution of routes according to the specified Access Control List.
- unmarked (default setting)
  The router ignores Access Control List filtering for this source protocol.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
**7.4.2 OSPF Areas**

OSPF supports networks divided into "Areas" and thus reduces the administrative effort when maintaining the network. The routers participating in the network know and only manage their own "Area" by flooding Link State Advertisements (LSAs) into the area. Using the LSAs each router builds its own topology database.

The device lets you specify up to a total of 64 OSPF Areas.

**Table**

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Displays the area ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area type</td>
<td>Specifies the import policy of AS external LSAs for the area which determines the Area Type. OSPF import policies apply to external routes only. An external route is a route that is outside the OSPF autonomous system. Possible values:</td>
</tr>
<tr>
<td>area</td>
<td>(default setting) The router imports type 5 AS external LSAs into the area.</td>
</tr>
<tr>
<td>stub area</td>
<td>The router ignores type 5 AS external LSAs.</td>
</tr>
<tr>
<td>nssa</td>
<td>The router translates type 7AS external LSAs into type 5 NSSA summary LSAs and imports them into the area.</td>
</tr>
<tr>
<td>SPF runs</td>
<td>Displays the number of times that the router calculated the intra-area routing table using the link state database of this area. The router uses Dijkstra's algorithm for route calculation.</td>
</tr>
<tr>
<td>Area border router</td>
<td>Displays the total number of ABRs reachable within this area. The number of reachable routers is initially 0. OSPF calculates the number in each SPF Pass.</td>
</tr>
<tr>
<td>AS boundary router</td>
<td>Displays the total number of ASBRs reachable within this area. The number of reachable ASBRs is initially 0. OSPF calculates the number in each SPF Pass.</td>
</tr>
<tr>
<td>Area LSAs</td>
<td>Displays the total number of link state advertisements in the link state database of this area, excluding AS External LSAs.</td>
</tr>
</tbody>
</table>
Area LSA checksum

Displays the total number of LS checksums contained in the LS database of this area. This sum excludes type 5 external LSAs. You use the sum to determine if there has been a change in an LS database of a router, and to compare the LS database to other routers.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.

- In the Area ID field you specify the area ID for the new table entry.
  Possible values:
  - Octet value displayed like an IPv4 address
7.4.3 OSPF Stub Areas

OSPF lets you specify certain areas as stub areas. The Area Border Router (ABR) of a stub area enters the information learned from AS external LSAs in its database without flooding the AS external LSAs across the stub area. The ABR instead sends a summary LSA into the stub area advertising a default route. The default route advertised in the summary LSA pertains only to the particular stub area. When forwarding data to AS external destinations, the routers in a stub area use the default ABR only. Sending a summary LSA containing the default route instead of AS external LSAs reduces the link state database size, and therefore the memory requirements for an internal router of a stub area.

The device gives you the following options for creating a Stub Area:

- Convert an Area into a Stub Area. To do this, perform the following step:
  - In the Routing > OSPF > Areas dialog, change the value in the Area type column to Stub Area.
- Create a new Stub Area. To do this, perform the following steps:
  - In the Routing > OSPF > Areas dialog, create an entry in the table.
  - Change the value in the Area type column to stub area.

**Table**

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Displays the area ID for the stub area.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default cost</td>
<td>Specifies the external metric value for the metric type.</td>
</tr>
<tr>
<td>Possible values:</td>
<td></td>
</tr>
<tr>
<td>0..16777215</td>
<td>The router sets the default value to equal the lower cost within the area for the metric type.</td>
</tr>
<tr>
<td>Metric type</td>
<td>Specifies the type of metric used for the default route advertised into the area.</td>
</tr>
<tr>
<td>Possible values:</td>
<td></td>
</tr>
<tr>
<td>OSPF metric (default setting)</td>
<td>The ABR advertises the metric as OSPF internal, which is the cost of an intra-area route to the ABR.</td>
</tr>
<tr>
<td>External type 1</td>
<td>The ABR advertises the metric as External type 1, which is the cost of the OSPF internal metric plus external metric to the ASBR.</td>
</tr>
<tr>
<td>External type 2</td>
<td>The ABR advertises the metric as External type 2, which is the cost of the external metric to the ASBR. You use this value for NSSAs.</td>
</tr>
</tbody>
</table>
Totally stub

Activates/deactivates the import of summary LSAs into stub areas.

Possible values:

- **marked**
  - The router does not import area summaries. The stub area relies entirely on the default route. This makes the default route a Totally Stub Area.

- **unmarked** (default setting)
  - The router both summarizes and propagates summary LSAs into the stub area.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.
### 7.4.4 OSPF Not So Stubby Areas

NSSAs are similar to the OSPF stub area. However, NSSAs have the additional capability of importing limited AS external routes. The ABR sends external routes out of the NSSA by converting type 7 AS external LSAs into type 5 AS external LSAs. The ASBR in an NSSA originates type 7 LSAs. The only difference between the type 5 and type 7 LSAs is that the router sets the "N" bit for NSSAs. Both NSSA neighbors have the "N" bit set. This forms the OSPF neighbor adjacency.

Beside the internal data traffic, NSSAs act like transit areas by transport data coming from external sources to other areas within the OSPF domain.

The device gives you the following options for creating an NSSA:

- Convert an Area into an NSSA. To do this, perform the following step:
  - In the **Routing > OSPF > Areas** dialog, change the value in the **Area type** column to **nssa**.

- Create a new NSSA. To do this, perform the following steps:
  - In the **Routing > OSPF > Areas** dialog, create an entry in the table.
  - Change the value in the **Area type** column to **nssa**.

#### Table

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Displays the area ID to which the table entries apply.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribute</td>
<td>Activates/deactivates external route redistribution into the NSSA.</td>
</tr>
<tr>
<td>Possible values:</td>
<td></td>
</tr>
<tr>
<td>mark</td>
<td>(default setting)</td>
</tr>
<tr>
<td>The NSSA ASBRs suppress external route redistribution into the NSSA. Furthermore, the ASBR stops to create type 7 external LSAs for external routes.</td>
<td></td>
</tr>
<tr>
<td>unmark</td>
<td>The NSSA ASBRs redistribute external routes into the NSSA.</td>
</tr>
<tr>
<td>Originate default info</td>
<td>Activates/deactivates the creation of type 7 default LSAs.</td>
</tr>
<tr>
<td>The prerequisite for the creation of type 7 default LSAs is that the router is an NSSA ABR or ASBR.</td>
<td></td>
</tr>
<tr>
<td>Possible values:</td>
<td></td>
</tr>
<tr>
<td>mark</td>
<td>(default setting)</td>
</tr>
<tr>
<td>The router creates type 7 default LSAs and sends them into the NSSA.</td>
<td></td>
</tr>
<tr>
<td>unmark</td>
<td>The router suppresses type 7 default LSAs.</td>
</tr>
</tbody>
</table>

Routing

[Routing > OSPF > NSSA]

Default metric

Specifies the metric value advertised in the type 7 default LSA.

Possible values:
- **1..16777214** (default setting: 10)

Default metric type

Specifies the metric type advertised in the type 7 default LSA.

Possible values:
- **ospfMetric**
  - The router advertises the metric as OSPF internal, which is the cost of an intra-area route to the ABR.
- **comparable**
  - The router advertises the metric as external type 1, which is the cost of the OSPF internal metric plus external metric to the ASBR.
- **nonComparable**
  - The router advertises the metric as external type 2, which is the cost of the external metric to the ASBR.

Translator role

Specifies the ability of an NSSA border router to perform translation of type-7 LSAs into type-5 LSAs.

NSSA Area Border Routers receive type-5 LSAs containing information about external routes. The NSSA border routers block the type-5 LSAs from entering into the NSSA. However, using type-7 LSAs the border routers inform each other about external routes. The ABRs then translate the type-7 LSAs to type-5 external LSAs and flood the information to the rest of the OSPF network.

Possible values:
- **always**
  - The router translates type-7 LSAs to type-5 LSAs. When the router receives a type-5 LSAs from another router with a router ID higher then its own, it flushes its type-5 LSAs.
- **candidate** (default setting)
  - The router translates type-7 LSAs to type-5 LSAs. To help prevent routing loops, OSPF performs a translator election. When multiple candidates exist, OSPF elects the router with the higher router ID as the translator.

Translator status

Displays if and how the router is translating type-7 LSAs into type-5 LSAs.

Possible values:
- **enabled**
  - The Translator role of the router is set to always.
- **elected**
  - As a candidate, the NSSA Border router is translating type-7 LSAs into type-5.
- **disabled**
  - Another NSSA border router is translating type-7 LSAs into type-5 LSAs.
Translator stability interval [s]

Specifies the number of seconds after the router loses a translation election that it continues to translate type-7 LSAs into type-5 LSAs.

Possible values:
- 0..65535 (default setting: 40)

Translator events

Displays the number of translator status changes that have occurred since the last boot-up.

Discontinuities in the value of this counter occur while OSPF is disabled and can occur during re-initialization of the management system.

Totally NSSA

Activates/deactivates importation of summary routes into the NSSA as type 3 summary LSAs.

Possible values:
- marked: The router suppresses summary route importation making the area a Totally NSSA.
- unmarked (default setting): The router imports summary routes into the NSSA as type 3 summary LSAs.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
### 7.4.5 OSPF Interfaces

This dialog lets you specify, activate, and display OSPF parameters on the router interfaces.

The device lets you activate up to 64 OSPF router interfaces.

The device uses the OSPF routing protocol to exchange reachability information between the routers. The device uses routing information learned from peers to determine the next hop towards the destination. To route traffic correctly, the router authenticates OSPF protocol exchanges to help prevent malicious or incorrect routing information from getting introduced into the routing table.

OSPF supports multiple types of authentication. You configure the type of authentication in use on a per interface basis. The cryptographic authentication option `md5`, helps protect your network against passive attacks and helps provide significant protection against active attacks. When using the cryptographic authentication option, each router appends a "message digest" to its transmitted OSPF packets. Receivers then use the shared secret key and received digest to verify that each received OSPF packet is authentic.

<table>
<thead>
<tr>
<th>Table</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Displays the interface to which the table entry applies.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Displays the IP address of this OSPF interface.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Activates/deactivates the OSPF administrative status of the interface.</td>
</tr>
</tbody>
</table>

**Possible values:**

- `marked`
  - The router advertises the values specified on the interface, and the interface as an OSPF internal route.

- `unmarked` (default setting)
  - The interface is external to OSPF.

<table>
<thead>
<tr>
<th>Table</th>
<th>Area ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specifies the area ID of the domain to which the interface connects.</td>
</tr>
</tbody>
</table>

**Possible values:**

- `<Area ID>`
  - You specify the area IDs in the `Routing > OSPF > Areas` dialog.
Priority

Specifies the priority of this interface.

In multi-access networks, the router uses the value in the Designated Router election algorithm. When a tie occurs, the routers use their router ID as a tie breaker. The highest router ID wins.

Possible values:
- **0**
  - The router is unable to become the Designated Router on this particular network.
- **1..255** (default setting: **1**)

Transmit delay [s]

Specifies the estimated number of seconds it takes to transmit a link state update packet over this interface.

This setting is useful for low speed links. The timer increases the age of the LS updates to compensate for estimated delays on the interface. Increasing the packet age too much results in a reply that is younger than the original packet.

Possible values:
- **0..3600** (default setting: **1**)

Retrans interval [s]

Specifies the number of seconds between link state advertisement retransmissions for adjacencies belonging to this interface.

You also use this value when retransmitting database description and link state request packets.

Possible values:
- **0..3600** (default setting: **5**)

Hello interval [s]

Specifies the number of seconds between Hello packet transmissions on the interface.

Set this value the same for the routers attached to a common network. Verify that every router in an area has the same value.

Possible values:
- **1..65535** (default setting: **10**)

Dead interval [s]

Specifies the number of seconds between received Hello packets before a router declares the neighbor router down.

Specify the value to a multiple of the `Hello interval [s]`. Specify the same value for the router interfaces within the same area.

Possible values:
- **1..65535** (default setting: **40**)
  - Specify a lower value to get a faster detection of a neighbor in a down state.

**Note:** Lower values are prone to interoperability issues.
Status

Displays the OSPF interface state.

Possible values:

- **down** *(default setting)*
  The interface is in the initial state and is blocking traffic.

- **loopback**
  The interface is a loopback interface of the device. Although packets are not sent out on the loopback interface, the router LSAs continue to advertise the interface address.

- **waiting**
  Applies only to interfaces connected to broadcast and Non-broadcast Multi-access (NBMA) network types. While in this state, the router attempts to identify the state of the network DR and BDR by sending and receiving Hello packets. The wait timer causes the interface to exit the waiting state and select a DR. The period of this timer is the same as the value in the *Dead interval [s]* field.

- **pointToPoint**
  Applies only to interfaces connected to point-to-point, point-to-multipoint, and virtual link network types. While in this state the interface sends Hello packets every *Hello interval [s]* and establishes an adjacency with its neighbor.

- **designatedRouter**
  The router is the DR for the multi-access network and establishes adjacencies with the other network routers.

- **backupDesignatedRouter**
  The router is the BDR for the multi-access network and establishes adjacencies with the other network routers.

- **otherDesignatedRouter**
  The router is only a network participant. The router establishes adjacencies only with the DR and BDR and tracks its network neighbors.

Designated router

Displays the IP address of the Designated Router.

Possible values:

- **Valid IPv4 address** *(default setting: 0.0.0.0)*

Backup designated router

Displays the IP address of the Backup Designated Router.

Possible values:

- **Valid IPv4 address** *(default setting: 0.0.0.0)*

Events

Displays the number of times this OSPF interface changed its state, or the router detected an error.

Network type

Specifies the OSPF network type of the autonomous system.

Possible values:

- **broadcast**
  Use this value for broadcast networks, such as Ethernet and IEEE 802.5. OSPF performs a DR and BDR election with which the non-designated routers form an adjacency.
Routing

[Routing > OSPF > Interfaces]

- **nbma**
  Use this value for non-broadcast multi-access networks such as X.25 and similar technologies. OSPF performs a DR and BDR election to limit the number of adjacencies formed.

- **pointToPoint**
  Use this value for networks that link only 2 interfaces.

- **pointToMultipoint**
  Use this value when you collect several point-to-point links into a non-broadcast network. Every router in the network transmits Hello packets to other routers in the network, but without having a DR and BDR election.

**Auth type**

Specifies the authentication type for an interface.

If you specify **simple** or **MD5**, then this router requires other routers to pass an authentication process before this router accepts the other routers as neighbors.

If you use authentication to help protect your network, then use the same type and key for every router in your autonomous system.

Possible values:

- **none** (default setting)
  Network authentication is inactive.

- **simple**
  The router uses clear text authentication. In this case, routers transmit the passwords as clear text.

- **MD5**
  The router uses the message-digest algorithm MD5 authentication. This type of authentication helps make your network more secure.

**Auth key**

Specifies the authentication key.

After entering the field displays ***** (asterisk) instead of the authentication key.

Possible values:

- Alphanumeric ASCII character string with 16 characters
  - with 8 characters if in the **Auth type** drop-down list the **simple** item is selected
  - with 16 characters if in the **Auth type** drop-down list the **MD5** item is selected
  If you specify a shorter authentication key, then the device fills in the remaining characters with 0.

**Auth key ID**

Specifies the **MD5** authentication key ID value.

The cryptographic authentication option **MD5**, helps protect your network against passive attacks and helps provide significant protection against active attacks.

The prerequisite for changing the value is that, in the **Auth type** column, you specify the value **MD5**.
Routing

[Routing > OSPF > Interfaces]

Possible values:
- 0 .. 255 (default setting: 0)

Cost

Specifies the internal metric.

OSPF uses link cost as the metric. OSPF also uses the cost of a link to calculate the SPF routes. OSPF prefers the route with the smaller value.

The formula to calculate cost is reference bandwidth divided by interface bandwidth. Reference bandwidth is specified in the Autocost reference bandwidth field and is set to 100 Mbit/s by default. See the Routing > OSPF > Global dialog, General tab.

Example:

The interface bandwidth is 10 Mbit/s.

The metric is 100 Mbit/s divided by 10 Mbit/s = 10.

Possible values:
- auto (default setting)
  - OSPF calculates the metric and automatically adjusts the value when the interface bandwidth changes.
- 1 .. 65535
  - OSPF uses the value specified here as metric.

Calculated cost

Displays the metric value which OSPF currently uses for this interface.

MTU ignore

Activates/deactivates the IP MTU (Maximum Transmission Unit) mismatch detection on this OSPF interface.

Possible values:
- marked
  - Disables the IP MTU check and makes adjacencies possible when the MTU value differs on the interfaces.
- unmarked (default setting)
  - The router checks if neighbors are using the same MTU value on the interfaces.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
OSPF Virtual Links

OSPF requires that you link every area to the backbone area. The physical location of routers often prohibits a direct link to the backbone. Virtual links allow you to connect physically separated areas to the backbone through a transit area. You specify both routers on the endpoints of a virtual link as ABRs on a point-to-point link. To enter a virtual link in the table, perform the following steps:

1. Click the button.

### Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area ID</td>
<td>Displays the area ID for the transit area that the virtual link traverses.</td>
</tr>
<tr>
<td>Neighbor ID</td>
<td>Displays the router ID of the virtual neighbor.</td>
</tr>
<tr>
<td></td>
<td>The router learns this value from Hello packets received from the virtual</td>
</tr>
<tr>
<td></td>
<td>neighbor. The value is a static value for virtual adjacencies.</td>
</tr>
<tr>
<td>Transmit delay [s]</td>
<td>Specifies the estimated number of seconds it takes to transmit an LS</td>
</tr>
<tr>
<td></td>
<td>update packet over this interface.</td>
</tr>
<tr>
<td></td>
<td>This setting is useful for low speed links. The timer increases the age of</td>
</tr>
<tr>
<td></td>
<td>the LS updates to compensate for estimated delays on the interface.</td>
</tr>
<tr>
<td></td>
<td>Increasing the packet age too much results in a reply that is younger than</td>
</tr>
<tr>
<td></td>
<td>the original packet.</td>
</tr>
<tr>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>▶ 0..3600 (default setting: 1)</td>
</tr>
<tr>
<td>Retrans interval [s]</td>
<td>Specifies the number of seconds between the LS advertisement</td>
</tr>
<tr>
<td></td>
<td>retransmissions for adjacencies belonging to this interface.</td>
</tr>
<tr>
<td></td>
<td>You also use this value when retransmitting Database Description (DD) and</td>
</tr>
<tr>
<td></td>
<td>LS Request packets.</td>
</tr>
<tr>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>▶ 0..3600 (default setting: 5)</td>
</tr>
<tr>
<td>Dead interval [s]</td>
<td>Specifies the number of seconds between received Hello packets before a</td>
</tr>
<tr>
<td></td>
<td>router declares the neighbor router down.</td>
</tr>
<tr>
<td></td>
<td>Specify the value to a multiple of the Hello interval [s]. Specify the same</td>
</tr>
<tr>
<td></td>
<td>value for the router interfaces within the same area.</td>
</tr>
</tbody>
</table>
Possible values:
- \textbf{1..65535} (default setting: 40)
  Specify a lower value to get a faster detection of a neighbor in a down state.

\textbf{Note:} Lower values are prone to interoperability issues.

**Hello interval [s]**

Specifies the number of seconds between Hello packet transmissions on the interface.

Set this value the same for the routers attached to a common network.

Possible values:
- \textbf{1..65535} (default setting: 10)

**Status**

Displays the OSPF virtual interface state.

Possible values:
- \textbf{down} (default setting)
  The interface is in the initial state and is blocking traffic.
- \textbf{pointToPoint}
  Applies only to interfaces connected to point-to-point, point-to-multipoint, and virtual link network types. While in this state the interface sends Hello packets every \textit{Hello interval [s]} and establishes an adjacency with its neighbor.

**Events**

Displays the number of times this interface changed its state due to a received event.

**Auth type**

Specifies the authentication type for a virtual link.

If you specify \textit{simple} or \textit{MD5}, then this router requires other routers to pass an authentication process before this router accepts the other routers as neighbors.

If you use authentication to help protect your network, then use the same type and key for every router in your autonomous system.

Possible values:
- \textbf{none} (default setting)
  Network authentication is inactive.
- \textbf{simple}
  The router uses clear text authentication. In this case, routers transmit the passwords as clear text.
- \textbf{MD5}
  The router uses the message-digest algorithm MD5 authentication. This type of authentication helps make your network more secure.

**Auth key**

Specifies the authentication key.

After entering the field displays ***** (asterisk) instead of the authentication key.
Possible values:
- Alphanumeric ASCII character string with 16 characters
  - with 8 characters if in the Auth type drop-down list the simple item is selected
  - with 16 characters if in the Auth type drop-down list the MD5 item is selected
If you specify a shorter authentication key, then the device fills in the remaining characters with 0.

Auth key ID

Specifies the MD5 authentication key ID value.

The cryptographic authentication option md5, helps protect your network against passive attacks and helps provide significant protection against active attacks.

The prerequisite for specifying this value is that you specify in the Auth type column the value MD5.

Possible values:
- 0..255 (default setting: 0)

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.
- In the Area ID drop-down list you select the area ID for the new table entry.
- In the Neighbor ID field you specify the router ID of the virtual neighbor.
7.4.7 OSPF Ranges

In large areas, OSPF messages flooded across the network reduce available bandwidth and increase the size of the routing table. A large routing table increases the amount of CPU processing that the router requires to enter the information into the routing table. A large routing table also reduces available memory. To decrease the number of OSPF messages flooded across the network, OSPF lets you create several smaller subnets within a large area.

In order to summarize routing information into and out of a subnet, the Area Border Router (ABR) specifies the subnet as a single address range. The ABR advertises each address range as a single route to the external area. The IP address that the ABR advertises for the subnet is an address and mask pair. Unadvertised ranges allow you to hide the existence of subnets from other areas.

The router specifies cost of the advertised route as the greater cost in the set component subnets. To enter an address range into the table, perform the following step:

□ Click the button.

Table

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Displays the area ID of the address range.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSDB type</td>
<td>Displays the route information aggregated by the address range.</td>
</tr>
<tr>
<td>Possible values:</td>
<td></td>
</tr>
<tr>
<td>summaryLink</td>
<td>The area range aggregates type 5 route information.</td>
</tr>
<tr>
<td>nssaExternalLink</td>
<td>The area range aggregates type 7 route information.</td>
</tr>
<tr>
<td>Network</td>
<td>Displays the IP address of the subnet of the range.</td>
</tr>
<tr>
<td>Netmask</td>
<td>Displays the netmask of the subnet of the range.</td>
</tr>
<tr>
<td>Effect</td>
<td>Specifies the external advertisement of the subnet ranges.</td>
</tr>
<tr>
<td>Possible values:</td>
<td></td>
</tr>
<tr>
<td>advertiseMatching (default setting)</td>
<td>The router advertises the range in other areas.</td>
</tr>
<tr>
<td>doNotAdvertiseMatching</td>
<td>The router withholds range advertisement to other external areas.</td>
</tr>
</tbody>
</table>
Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.

- In the Area ID drop-down list you select the area ID of the address range.
- In the LSDB type drop-down list you select the route information aggregated by the address range.
  Possible values:
  - summaryLink
    The area range aggregates type 5 route information.
  - nssaExternalLink
    The area range aggregates type 7 route information.
- In the Network field you specify the IP address for the area subnet.
- In the Netmask field you specify the netmask for the area subnet.
7.4.8 OSPF Diagnostics

To function properly, OSPF relies on 2 basic processes.
  - forming adjacencies
  - after forming adjacencies, the neighboring routers exchange information and update their routing table

The statistics displayed in the tabs help you to analyze the OSPF processes.

The dialog contains the following tabs:
  - [Statistics]
  - [Link state database]
  - [Neighbors]
  - [Virtual neighbors]
  - [External link state database]
  - [Route]

[Statistics]

In order to accomplish the 2 basic processes, OSPF routers send and receive various messages containing information to form adjacencies, and update routing tables. The counters in the tab indicate the amount of message traffic transmitted and received on the OSPF interfaces.
  - Link State Acknowledgments (LSAcks) provide a response to a Link State Update (LS update) request as part of the link state exchange process.
  - The Hello messages allow a router to discover other OSPF routers in the area and to establish adjacencies between the neighboring devices. After establishing adjacencies, the routers advertise their credentials for establishing a role as either a Designated Router (DR), a Backup Designated Router (BDR), or only as a participant in the OSPF network. The routers then use the Hello messages to exchange information about the OSPF configuration in the Autonomous System (AS).
  - Database Description (DD) messages contain descriptions of the AS or area topology. The messages also propagate the contents of the link state database for the AS or area from a router to other routers in the area.
  - Link State Requests (LS Request) messages provide a means of requesting updated information about a portion of the Link State Database (LSDB). The message specifies the link or links for which the requesting router requires current information.
  - LS Update messages contain updated information about the state of certain links on the LSDB. The router sends the updates as a response to an LS Request message. The router also broadcast or multicast messages periodically. The router uses the message contents to update the information in the LSDBs of routers that receive them.
  - LSAs contain the local routing information for the OSPF area. The router transmits the LSAs to other routers in an OSPF area and only on interfaces connecting the router to the specific OSPF area.
  - Type 1 LSAs are router LSAs. Each router in an area originates a router-LSA. A single router LSA describes the state and cost of every link in the area. The router floods type 1 LSAs only across its own area.
  - Type 2 LSAs are network LSAs. The DR creates a network LSA from information received in the type 1 LSAs. The DR originates in its own area a network LSA for each broadcast and NBMA network it is connected to. The LSA describes every router attached to the network, including the DR itself. The router floods type 2 LSAs only across its own area.
Type 3 LSAs are network summary LSAs. An Area Border Router (ABR) creates a single network summary LSA from information contained in the type 1 and type 2 LSAs received from the DRs. The ABR transmits network summary LSAs describing inter-area destinations. The router floods type 3 LSAs across every area connected to it. Except this is the area for which it generated the Type 3 LSA.

Type 4 LSAs are Autonomous System Boundary Router (ASBR) summary LSAs. An ABR creates a single ASBR summary LSA from information contained in the type 1 and type 2 LSAs received from the DRs. The ABR transmits type 4 LSAs to areas different than the area it resides in, to describe the ASBRs from which the ABR received type 5 LSAs. The router floods type 4 LSAs across every area connected to it. Except this is the area for which it generated the Type 4 LSA.

Type 5 LSAs are AS external LSAs. The AS boundary routers create the AS external LSAs describing destinations external to the AS. The type 5 LSAs contain information redistributed into OSPF from other routing processes. The router floods type 5 LSAs to every area except stub and NSSA areas.

**Function**

**LSA retransmitted**
 Displays the total number of LSAs retransmitted since resetting the counters. When the router transmits the same LSA to multiple neighbors, the router increments the count for each neighbor.

**Hello packets received**
 Displays the total number of OSPFv2 Hello packets received since resetting the counters.

**Hello packets transmitted**
 Displays the total number of OSPFv2 Hello packets transmitted since resetting the counters.

**DB description packets received**
 Displays the total number of OSPFv2 Database Description packets received since resetting the counters.

**DB description packets transmitted**
 Displays the total number of OSPFv2 Database Description packets transmitted since resetting the counters.

**LS request packets received**
 Displays the total number of OSPFv2 Link State Request packets received since resetting the counters.

**LS request packets transmitted**
 Displays the total number of OSPFv2 Link State Request packets transmitted since resetting the counters.

**LS update packets received**
 Displays the total number of OSPFv2 LS Update packets received since resetting the counters.
LS update packets transmitted

Displays the total number of OSPFv2 LS Update packets transmitted since resetting the counters.

LS ack update packets received

Displays the total number of OSPFv2 LS Acknowledgement packets received since resetting the counters.

LS ack update packets transmitted

Displays the total number of OSPFv2 LS Acknowledgement packets transmitted since resetting the counters.

Max. rate of LSU received in any 5sec

Displays the maximum rate of OSPFv2 LS Update packets received over any 5-second interval since resetting the counters. The field displays the rate in packets per second. For example, the number of packets received during the 5-second interval, divided by 5.

Max. rate of LSU transmitted in any 5sec

Displays the maximum rate of OSPFv2 LS Update packets transmitted over any 5-second interval since resetting the counters. The field displays the rate in packets per second. For example, the number of packets transmitted during the 5-second interval, divided by 5.

Type-1 (Router) LSAs received

Displays the number of type 1 router LSAs received since resetting the counters.

Type-2 (Network) LSAs received

Displays the number of type 2 network LSAs received since resetting the counters.

Type-3 (Summary) LSAs received

Displays the number of type 3 network summary LSAs received since resetting the counters.

Type-4 (ASBR) LSAs received

Displays the number of type 4 ASBR summary LSAs received since resetting the counters.

Type-5 (External) LSAs received

Displays the number of type 5 external LSAs received since resetting the counters.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
A router maintains a separate link state database for every area to which it belongs.

The router adds LSAs to the database in the following cases:
- When the router receives an LSA, for example during the flooding process.
- When the router originates the LSA.

When a router deletes an LSA from the database, it also removes the LSA from the link state retransmission lists of the other routers in the network. A router deletes an LSA from its database in the following cases:
- A newer instance overwrites the LSA during the flooding process.
- The router originates a newer instance of a self-originated LSA.
- The LSA ages out and the router flushes the LSA from the routing domain.

### Table

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Displays the area ID from which router received the LSA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Displays the type of the LSAs received. Each LSA type has a separate advertisement format. Possible values:</td>
</tr>
<tr>
<td></td>
<td>- <code>routerLink</code> The router received the information from another router in the same area. Routers announce their existence and list the links to other routers within the same area using a type 1 LSA. The link state ID is the originating router ID.</td>
</tr>
<tr>
<td></td>
<td>- <code>networkLink</code> The router received the information from a DR on a broadcast segment using a type 2 LSA. The DR compiles the information received in type 1 LSAs and lists the routers linked together by the segment. The link state ID is the IP interface address of the DR.</td>
</tr>
<tr>
<td></td>
<td>- <code>summaryLink</code> The router received the information from an ABR using a type 3 LSA describing routes to networks. ABRs compile information learned from type 1 and type 2 LSAs received from the attached areas before sending the routing information to the other areas. The link state ID is the destination network number which is the results of the summarization process.</td>
</tr>
<tr>
<td></td>
<td>- <code>asSummaryLink</code> The router received the information from an ABR using a type 4 LSA describing routes to ASBRs. ABRs compile information learned from type 1 and type 2 LSAs received from the attached areas before sending the routing information to the other areas. The link state ID is the destination network number.</td>
</tr>
<tr>
<td></td>
<td>- <code>asExternalLink</code> The router received the information from an ASBR using a type 5 LSA describing routes to another AS. The link state ID is the router id of the ASBR.</td>
</tr>
<tr>
<td></td>
<td>- <code>nssaExternalLink</code> The router received the information from a router in a NSSA using a type 7 LSA.</td>
</tr>
</tbody>
</table>
Routing

[Routing > OSPF > Diagnostics]

LSID
Displays the Link State ID (LSID) value received in the LSA.

The LSID is a field located in the LSA header. The field contains either a router ID or an IP address according to the LSA type.

Possible values:
- <Router ID>
- Valid IPv4 address

Router ID
Displays the router ID uniquely identifying the originating router.

Sequence
Displays the value of the sequence field in an LSA.

The router examines the contents or the LS checksum field whenever the LS sequence number field indicates that 2 instances of an LSA are the same. When there is a difference, the router considers the instance with the larger LS checksum to be most recent.

Age
Displays the age of the link state advertisement in seconds.

When the router creates the LSA, the router sets the LS age to the value 0. As the routers transmit the LSA across the network they increment the value by the value specified in the Transmit delay [s] column.

If a router receives 2 LSAs for the same segment having identical LS sequence numbers and LS checksums, then the router examines the age of the LSAs.
- The router immediately discards LSA with MaxAge.
- Otherwise, the router discards the LSA with the smaller age.

Checksum
Displays the contents of the checksum.

The field is a checksum of the complete contents of the LSA, except for the age field. The age field of the advertisement increases as the routers transmit the message across the network. Excluding the age field lets routers transmit the message without needing to update the checksum field.

Buttons
You find the description of the standard buttons in section “Buttons” on page 14.
The Hello Protocol is responsible for neighbor acquisition, maintenance, and for 2-way communication between neighbors.

During the acquisition process, the routers on a segment compare their configurations for compatibility. If the routers are compatible, then the routers form adjacencies. The routers discover their master or slave status using information provided in the Hello packets.

After the routers discover their roles, they exchange routing information to synchronize their routing databases. When the routers finish updating their databases, the neighbors are fully adjacent and the LSA lists the adjacency.

### Table

**Neighbor ID**

Displays the router ID of the neighboring router.

The router learns this value from Hello packets received from the neighbor. The value is a static value for virtual adjacencies.

**IP address**

Displays the IP address of the neighboring router interface attached to the port.

When sending unicast protocol packets on this adjacency, the router uses the value as the destination IP address. When the neighboring router is the DR, the router is also used in router LSAs as the link ID for the attached network. The router learns the neighbor IP address when it receives Hello packets from the neighbor. For virtual links, the router learns the neighbor IP address while building the routing table.

**Interface**

Displays the interface to which the entries in this row refer.

**Status**

Displays the state of the relationship with the neighbor listed in this instance.

An event invokes each state change, such as a received Hello packet. This event produces different effects, depending on the current state of the neighbor. Also, depending on the state of neighbor change, the routers initiate a DR election.

Possible values:

- **down** (default setting)
  - The initial state of a neighbor conversation or a router terminated the conversation due to expiration of the *Dead interval [s]* timer.

- **attempt**
  - The state is only valid for neighbors attached to NBMA networks. The information from the neighbor remains unresolved. The router actively attempts to contact the neighbor by sending the neighbor Hello packets in the interval specified in *Hello interval [s]*.
The router has recently seen a Hello packet from the neighbor. However, the router has only established uni-directional communication with the neighbor. For example, the router ID of this router is missing from the Hello packet of the neighbor. When sending Hello packets, the associated interface lists neighbors in this state or higher.

Communication between the 2 routers is bidirectional. The router verifies the operation by examining the contents of the Hello packet. The routers elect a DR and BDR from the set of neighbors while in or after the 2-way state.

The first step in creating an adjacency between the 2 neighboring routers. The goal of this step is to decide which router is the master and to decide upon the initial Sequence number.

The router is announcing its entire link state database by sending Database Description (DD) packets to the neighbor. The router explicitly acknowledges each DD packet. Each packet has a sequence number. The adjacencies only allow one DD packet to be outstanding at any time. In this state, the router sends LS Request packets asking for up-to-date database information. The adjacencies are fully capable of transmitting and receiving OSPF routing protocol packets.

The router sends LS Request packets to the neighbor inquiring about the outstanding database updates sent in the exchange state.

The neighboring routers are fully adjacent. The adjacencies now appear in router LSAs and network LSAs.

Displays the amount of time remaining before the router declares the neighbor status as down. The timer initiates the count down after the router receives a Hello packet.

You find the description of the standard buttons in section “Buttons” on page 14.

OSPF requires a continuous connection of the Autonomous System backbone area. OSPF also requires that every area has a connection to the backbone area. The physical location of routers often prohibits an area from directly connecting to the backbone area. Virtual links allow you to connect physically separated areas to the backbone area.

The ABRs of the backbone area and the physically separated area form a point-to-point link through a transit area. When the ABRs establish an adjacency, the backbone router LSAs include the link and OSPF packets flow over the virtual link. Furthermore, the routing database of each endpoint router includes the link state information of the other endpoint router.

Note: The OSPF lets you specify virtual links through every type of area except for stub areas.
Table

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area ID</td>
<td>Displays the transit area ID of the virtual link.</td>
</tr>
<tr>
<td>Router ID</td>
<td>Displays the router ID of the other virtual endpoint ABR.</td>
</tr>
<tr>
<td>IP address</td>
<td>Displays the IP address of the virtual neighbor.</td>
</tr>
<tr>
<td>Options</td>
<td>Displays the information contained in the options field of the LSA. This</td>
</tr>
<tr>
<td></td>
<td>value indicates the capabilities of the virtual neighbor.</td>
</tr>
</tbody>
</table>

After virtual adjacencies form, the virtual link carries OSPF packets such as Hello packets and LS update packets containing database information. The prerequisite is that the LSAs of the neighbor router contain the router ID of the local router.

The options field used in the Hello packets allow routers to identify their optional capabilities, and to communicate the capabilities to other routers. This mechanism lets you mix routers of different capabilities within a routing domain.

The router supports 4 options by setting the following bits in the options field either high or low depending on the capabilities of the router. The field displays the value by adding the following option bits together. You read the fields from least significant bit to most significant bit.

- The routers advertise the ability to process TOS 0 in AS external routes when it sets the E-bit high. The E-bit is the second bit in the options field and represents the value $2^1$ or 2.
- The routers advertise the ability to process multicast routes when it sets the MC-bit high. The MC-bit is the third bit in the options field and represents the value $2^2$ or 4.
- The routers advertise the ability to process AS external routes in an NSSA summary with type 7 LSAs when it sets the N/P-bit high. The N/P-bit is the fourth bit in the options field and represents the value $2^3$ or 8.
- The routers advertise the ability to process demand circuits when it sets the DC-bit high. The DC-bit is the sixth bit in the options field and represents the value $2^5$ or 32.

In a special case, the router sets the E-bit low.

- The routers advertise the ability to process TOS metrics other than TOS 0 when it sets the E-bit low. The E-bit is the second bit in the options field and when set low, the bit represents the value 0.

Possible values:

- $2, 6, 10, 14, 34, 38, 42, 46$
  The values indicate that the virtual neighbor supports Type of Service metric (TOS) 0 in AS external LSAs.
- $0, 4, 8, 12, 32, 36, 40, 44$
  The values indicate that the virtual neighbor supports TOS metrics other than TOS 0.
The values indicate that the virtual neighbor supports multicast routing.

The values indicate that the virtual neighbor supports Type 7 LSAs.

The values indicate that the virtual neighbor supports demand circuits.

Displays the state of the relationship with the neighbor listed in this instance.

Possible values:

- **down** (default setting)
  The initial state of a neighbor conversation or a router terminated the conversation due to expiration of the Dead interval [s] timer.

- **attempt**
  The state is only valid for neighbors attached to NBMA networks. Information from the neighbor remains unresolved. The router actively attempts to contact the neighbor by sending the neighbor Hello packets in the interval specified in Hello interval [s].

- **init**
  The router has recently seen a Hello packet from the neighbor. However, the router has only established uni-directional communication with the neighbor. For example, the router ID of this router is missing from the Hello packet of the neighbor. When sending Hello packets, the associated interface lists neighbors in this state or higher.

- **twoWay**
  Communication between the 2 routers is bidirectional. The router verifies the operation by examining the contents of the Hello packet. The routers elect a DR and BDR from the set of neighbors while in or after the 2-way state.

- **exchangeStart**
  The first step in creating an adjacency between the 2 neighboring routers. The goal of this step is to decide which router is the master and to decide upon the initial Sequence number.

- **exchange**
  The router is announcing its entire link state database by sending Database Description (DD) packets to the neighbor. The router explicitly acknowledges each DD packet. Each packet has a sequence number. The adjacencies only allow one DD packet to be outstanding at any time. In this state, the router sends LS Request packets asking for up-to-date database information. The adjacencies are fully capable of transmitting and receiving OSPF routing protocol packets.

- **loading**
  The router sends LS Request packets to the neighbor inquiring about the outstanding database updates sent in the exchange state.

- **full**
  The neighboring routers are fully adjacent. The adjacencies now appear in router LSAs and network LSAs.

Displays the number of times this interface changed its state due to a received event such as HelloReceived or 2-way.
Length of retransmission queue

Displays the length of the retransmission list.

In order to flood LSAs out of an interface to the neighbor, the router places the LSAs on the link state retransmission list of the adjacency. To validate LSA flooding, the router retransmits the LSAs until the neighbor acknowledges the LSA reception. You configure the length of time between retransmissions in the *Routing > OSPF > Interfaces* dialog in the *Retrans interval [s]* column.

Suppressed Hellos

Displays if the router is suppressing Hello packets to the neighbor.

Suppressing Hello packet transmission to the neighbor lets demand circuits close, on point-to-point links, during periods of inactivity. In NBMA networks, the periodic transmission of LSAs causes the circuit to remain open.

Possible values:
- **marked**
  - The router suppresses Hello packets.
- **unmarked**
  - The router transmits Hello packets.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

[External link state database]

The table displays the contents of the external link state database, with an entry for each unique link state ID. External links allow the area to connect to destinations outside of the autonomous system. Routers pass information about the external links throughout the network as link state updates.

Table

**Type**

Displays the type of the link state advertisement. When the router detects an external link state advertisement, the router enters the information in the table.

Possible values:
- **asExternalLink**

**LSID**

Displays the Link State ID is an LS type-specific field containing either a router ID or an IP address. The value identifies the routing domain described in the advertisement.
Router ID

Displays the router ID uniquely identifying the originating router.

Sequence

Displays the value of the sequence field in an LSA.

The router examines the contents or the LS checksum field whenever the LS sequence number field indicates that 2 instances of an LSA are the same. When there is a difference, the router considers the instance with the larger LS checksum to be most recent.

Age

Displays the age of the link state advertisement in seconds.

When the router creates the LSA, the router sets the LS age to the value 0. As the routers transmit the LSA across the network they increment the value by the value specified in the Transmit delay [s] column.

If a router receives 2 LSAs for the same segment having identical LS sequence numbers and LS checksums, then the router examines the age of the LSAs.

- The router immediately discards LSA with MaxAge.
- Otherwise, the router discards the LSA with the smaller age.

Checksum

Displays the contents of the checksum.

The field is a checksum of the complete contents of the LSA, except for the age field. The age field of the advertisement increases as the routers transmit the message across the network. Excluding the age field lets routers transmit the message without needing to update the checksum field.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

[Route]

The dialog displays the OSPF route information learned from the Link State Advertisements (LSA).

Table

IP address

Displays the IP address of the network or subnet for the route.

Netmask

Displays the netmask for the network or subnet.
Metric
Displays the route cost, calculated in the SPF algorithm, to reach the network.

Type
Displays the type of route that was learned from OSPF.
Possible values:
- **intra**
  Entry for routes from the OSPF protocol within an area.
- **inter**
  Entry for routes from the OSPF protocol between areas.
- **ext-type1**
  These routes were imported from an Autonomous System Boundary Router (ASBR) into the OSPF area. These routes use the costs relating to the connection between the ASBR and the route costs includes this device.
- **ext-type2**
  These routes were imported from an Autonomous System Boundary Router (ASBR) into the OSPF area. These routes do not use the costs relating to the connection between the ASBR and the route costs includes this device.
- **nssa-type1**
  These routes were imported from an Autonomous System Boundary Router (ASBR) into the Not-So-Stub Area. These routes use the costs relating to the connection between the ASBR and the route costs includes this device.
- **nssa-type2**
  These routes were imported from an Autonomous System Boundary Router (ASBR) into the Not-So-Stub Area. These routes do not use the costs relating to the connection between the ASBR and the route costs includes this device.

Buttons
You find the description of the standard buttons in section “Buttons” on page 14.

7.5 Routing Table
[Routing > Routing Table]

This dialog displays the routing table with the routes configured in the device. Using the routing table, the device learns the router interface through which it transfers IP packets that are addressed to recipients in a different network.
**Configuration**

### Preference

Specifies the preference number that the device assigns by default to the newly configured, static routes.

Possible values:

- **1..255** (default setting: 1)

  Routes with a value of 255 will be ignored by the device in the routing decision.

**Table**

### Port

Displays the router interface through which the device is currently transmitting IP packets addressed to the destination network.

Possible values:

- `<Router interface>`
  
  The device uses this router interface to transfer IP packets addressed to the destination network.

- **no port**
  
  The static route is currently not assigned to a router interface.

### Network address

Displays the address of the destination network.

### Netmask

Displays the netmask.

### Next hop IP address

Displays the IP address of the next router on the path to the destination network.

### Type

Displays the type of the route.

Possible values:

- **local**
  
  The router interface is directly connected to the destination network.

- **remote**
  
  The router interface is connected to the destination network through a router (**Next hop IP address**).

- **reject**
  
  The device discards IP packets addressed to the destination network and informs the sender.

- **other**
  
  The route is inactive. See the **Active** checkbox.
Routing

Displays the origin of this route.

Possible values:

▶ **local**
  The device created this route when setting up the router interface. See the *Routing > Interfaces > Configuration* dialog.

▶ **netmgmt**
  A user created this static route with the button.

**Note:** You can make static routes with the same destination and preference, but with different next hops. The device uses Equal Cost Multi Path (ECMP) forwarding mechanism to help ensure load sharing and redundancy over the network. Depending on the selected routing profile in the *Routing > Global* dialog, ECMP can use up to 4 routes. If you select the *ipv4DataCenter* routing profile, then ECMP can use up to 16 routes.

▶ **ospf**
  The **OSPF** function created this route. See the *Routing > OSPF* dialog.

**Preference**

Specifies the "administrative distance" of the route.

The device uses this value instead of the metric, when the metric of the routes is incomparable.

Possible values:

▶ **0**
  Reserved for routes that the device creates when setting up the router interfaces. These routes have the value **local** in the **Protocol** column.

▶ **1..254**
  In routing decisions, the device gives preference to the route with the smallest value.

▶ **255**
  In routing decisions, the device ignores the route.

The "administrative distance" can be set for static routes created using the button.

**Metric**

Displays the metric of the route.

The device transmits the data packets using the route with the smallest value.

**Last update [s]**

Displays the time in seconds, since the current settings of the route were entered in the routing table.

**Track name**

Specifies the tracking object with which the device links the route.

The device automatically activates or deactivates static routes – depending on the link status of an interface or the reachability of a remote router or end device.

You set up tracking objects in the *Routing > Tracking > Configuration* dialog.
Routing

Routing Table

Possible values:
- Name of the tracking object, made up of Type and Track ID.
- – No tracking object selected.

This function is used only for static routes. (Column Protocol = netmgmt)

Active

Displays if the route is active or inactive.

Possible values:
- marked
  The route is active; the device uses the route.
- unmarked
  The route is inactive.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create dialog to create a static route.

- In the Network address field, you specify the address of the destination network.
  Possible values:
  - Valid IPv4 address
    If you specify a default route (0.0.0.0), then you specify a default gateway in the Next hop IP address field. This setting takes precedence over the setting in the following dialog:
    - Basic Settings > Network dialog, Gateway address field
  - In the Netmask field, you specify the netmask that identifies the network prefix in the address of the destination network.
    Possible values:
    - Valid IPv4 netmask
  - In the Next hop IP address field, you specify the IP address of the next router on the path to the destination network.
    Possible values:
    - Valid IPv4 address
      To make a reject type route, specify the value 0.0.0.0 in this field. With this route, the device discards IP packets addressed to the destination network and informs the sender.
  - In the Preference field, you specify the preference number that the device uses to decide which of several existing routes to the destination network it will use.
    Possible values:
    - 1..255
      In routing decisions, the device gives preference to the route with the smallest value. The default setting is the value specified in the Configuration frame, field Preference.
  - In the Track name field, you specify the tracking object with which the device links the route.
    Possible values:
    - – No tracking object selected.
    - Name of the tracking object, made up of Type and Track ID.
The tracking function lets you monitor what are known as tracking objects. Examples of monitored tracking objects are the link status of an interface or the reachability of a remote router or end device.

The device forwards status changes of the tracking objects to the registered applications, for example to the routing table or to a VRRP instance. The applications then react to the status changes:
- In the routing table, the device activates/deactivates the route linked to the tracking object.
- The VRRP instance linked to the tracking object reduces the priority of the virtual router so that a backup router takes over the role of the master.

If you set up the tracking objects in the Tracking Configuration dialog, then you can link applications with the tracking objects:
- You link static routes with a tracking object in the Routing > Routing Table dialog, Track name column.
- You link virtual routers with a tracking object in the Routing > L3-Redundancy > VRRP > Tracking dialog. Click the button to open the Create window and select the tracking object in the Track name drop-down list.

The menu contains the following dialogs:
- Tracking Configuration
- Tracking Applications
7.6.1 Tracking Configuration

In this dialog you set up the tracking objects.

Table

Type

Specifies the type of the tracking object.

Possible values:
- **interface**
  The device monitors the link status of its physical ports or of its link aggregation, LRE or VLAN router interface.
- **ping**
  The device monitors the route to a remote router or end device by means of periodic ping requests.
- **logical**
  The device monitors tracking objects logically linked to each other and thus enables complex monitoring tasks.

Track ID

Specifies the identification number of the tracking object.

Possible values:
- **1..256**
  This range is available to every type (interface, ping and logical).

Track name

Displays the name of the tracking object made up of Type and Track ID.

Active

Activates/deactivates the monitoring of the tracking object.

Possible values:
- **marked**
  Monitoring is active. The device monitors the tracking object.
- **unmarked** (default setting)
  Monitoring is inactive.

Description

Specifies the description.

Here you describe what the device uses the tracking object for.
Possible values:

- Alphanumeric ASCII character string with 0..255 characters

Status

Displays the monitoring result of the tracking object.

Possible values:

- **up**
  The monitoring result is positive:
  - The link status is active.
  - The remote router or end device is reachable.
  - The result of the logical link is TRUE.

- **down**
  The monitoring result is negative:
  - The link status is inactive.
  - The remote router or end device is not reachable.
  - The result of the logical link is FALSE.

- **notReady**
  The monitoring of the tracking object is inactive. You activate the monitoring in the **Active** column.

Changes

Displays the number of status changes since the tracking object has been activated.

Last changed

Displays the time of the last status change.

Send trap

Activates/deactivates the sending of an SNMP trap when someone activates or deactivates the tracking object.

Possible values:

- **marked**
  If someone activates or deactivates the tracking object in the **Active** column, then the device sends an SNMP trap.

- **unmarked** (default setting)
  The device does not send an SNMP trap.

Port

Specifies the interface to be monitored for tracking objects of the **interface** type.

Possible values:

- **<Interface number>**
  Number of the physical ports or of the link aggregation, LRE or VLAN router interface.

- **no Port**
  No tracking object of the **interface** type.
Link up delay [s]

Specifies the period in seconds after which the device evaluates the monitoring result as positive. If the link has been active on the interface for longer than the period specified here, then the Status column displays the value *up*.

Possible values:

- 0..255
- –
  
  No tracking object of the *logical* type.

Link down delay [s]

Specifies the period in seconds after which the device evaluates the monitoring result as negative. If the link has been inactive on the interface for longer than the period specified here, then the Status column displays the value *down*.

Possible values:

- 0..255
- –
  
  No tracking object of the *interface* type.

If the link to every aggregated port is interrupted, then Link aggregation, LRE and VLAN router interfaces have a negative monitoring result.

If the link to every physical port and link-aggregation interface which is a member of the VLAN is interrupted, then a VLAN router interface has a negative monitoring result.

Ping port

Specifies the router interface for tracking objects of the *ping* type through which the device sends the ping request packets.

Possible values:

- `<Interface number>`
  
  Number of the router interface.
- noName
  
  No router interface assigned.
- –
  
  No tracking object of the *ping* type.

IP address

Specifies the IP address of the remote router or end device to be monitored.

Possible values:

- Valid IPv4 address
- –
  
  No tracking object of the *ping* type.
Ping interval [ms]

Specifies the interval in milliseconds at which the device periodically sends ping request packets.

Possible values:
- 100..20000 (default setting: 1000)
  - If you specify a value <1000, then you can set up a maximum of 16 tracking objects of the ping type.
  - No tracking object of the ping type.

Ping replies to lose

Specifies the number of missed responses from the device after which the device evaluates the monitoring result as negative. If the device does not receive a response to its sent ping request packets for the number of times specified here in a row, then the Status column displays the value down.

Possible values:
- 1..10 (default setting: 3)
  - No tracking object of the ping type.

Ping replies to receive

Specifies the number of received responses from the device after which the device evaluates the monitoring result as positive. If the device receives a response to its sent ping request packets for the number of times specified here in a row, then the Status column displays the value up.

Possible values:
- 1..10 (default setting: 2)
  - No tracking object of the ping type.

Ping timeout [ms]

Specifies the period in milliseconds for which the device waits for a response. If the device does not receive a response within this period, then the device evaluates this as a missed response. See the Ping replies to lose column.

Possible values:
- 10..10000 (default setting: 100)
  - If a large number of ping tracking objects is set up in the device, then specify a sufficiently large value. If more than 100 instances are present, then specify at least 200 ms.
  - No tracking object of the ping type.

Ping TTL

Specifies the TTL value in the IP header with which the device sends the ping request packets.

TTL (Time To Live, also known as “Hop Count”) identifies the maximum number of steps an IP packet is allowed to perform on the way from the sender to the receiver.
Possible values:

- No tracking object of the *ping* type.
- `1..255` (default setting: `128`)

**Best route**

Displays the number of the router interface through which the best route leads to the monitoring router or end device.

Possible values:

- `<Port number>`
  Number of the router interface.
- `no Port`
  No route exists.
- `-`
  No tracking object of the *ping* type.

**Logical operand A**

Specifies the first operand of the logical link for tracking objects of the *logical* type.

Possible values:

- Tracking objects set up
- `-`
  No tracking object of the *logical* type.

**Logical operand B**

Specifies the second operand of the logical link for tracking objects of the *logical* type.

Possible values:

- Tracking objects set up
- `-`
  No tracking object of the *logical* type.

**Operator**

Links the tracking objects specified in the *Logical operand A* and *Logical operand B* fields.

Possible values:

- `and`
  Logical AND link
- `or`
  Logical OR link
- `-`
  No tracking object of the *logical* type.
Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.

► In the Type field, you specify the type of the tracking object.
   Possible values:
   – interface
     The device monitors the link status of its physical ports or of its link aggregation, LRE or VLAN router interface.
   – ping
     The device monitors the route to a remote router or end device by means of periodic ping requests.
   – logical
     The device monitors tracking objects logically linked to each other and thus enables complex monitoring tasks.

► In the Track ID field, you specify the identification number of the tracking object.
   Possible values:
   – 1..2147483647
### 7.6.2 Tracking Applications

In this dialog you see which applications are linked with the tracking objects.

The following applications can be linked with tracking objects:

- You link static routes with a tracking object in the Routing > Routing Table dialog, Track name column.
- You link virtual routers with a tracking object in the Routing > L3-Redundancy > VRRP > Tracking dialog. Click the Create button to open the Create window and select the tracking object in the Track name drop-down list.

<table>
<thead>
<tr>
<th>Table</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Displays the type of the tracking object.</td>
</tr>
<tr>
<td>Track ID</td>
<td>Displays the identification number of the tracking object.</td>
</tr>
<tr>
<td>Application</td>
<td>Displays the name of the application that is linked with the tracking object.</td>
</tr>
<tr>
<td>Possible values:</td>
<td></td>
</tr>
<tr>
<td>▶ Tracking objects of the logical type</td>
<td></td>
</tr>
<tr>
<td>▶ Static routes</td>
<td></td>
</tr>
<tr>
<td>▶ Virtual router of a VRRP instance</td>
<td></td>
</tr>
<tr>
<td>Track name</td>
<td>Displays the name of the tracking object made up of Type and Track ID.</td>
</tr>
</tbody>
</table>

### Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
7.7 L3 Relay

Clients in a subnet send BOOTP/DHCP broadcasts messages to DHCP servers requesting configuration information such as IP addresses. Routers provide a border for broadcast domains so that BOOTP/DHCP requests remain in the local subnet. The Layer 3 Relay (L3 Relay) function acts as a proxy for clients that require information from a BOOTP/DHCP server in another network.

When you configure this device to retrieve IP addresses from a DHCP server located in another subnet, the L3 Relay function lets you forward requests across multiple hops to a server located in another network.

Using IP helper addresses and UDP helper ports the L3 Relay forwards DHCP packets between the clients and servers. The IP helper address is the DHCP server IP address. Clients use the UDP helper port to request a type of information such as DNS information on UDP port 53, or DHCP information on UDP port 67.

The L3 Relay function provides you the follow advantages over the standard BOOTP/DHCP function:
- redundancy, when you specify multiple servers to process client requests.
- load balancing, when you specify multiple interfaces to relay broadcast packets from the client to the servers.
- central management, useful in large networks. The administrator saves the device configurations on a centrally located server which responds to client requests in multiple subnets.
- diversity, this function lets you specify up to 512 entries.

Operation

Enables/disables the L3 Relay function.

Possible values:
- **On**
  The L3 Relay function is globally enabled.
- **off** (default setting)
  The L3 Relay function is globally disabled.

Configuration

Circuit ID

Activates/deactivates the BOOTP/DHCP Circuit ID Option Mode.

The device sends circuit ID suboption information, identifying the local agent, to the DHCP server. The DHCP server uses the suboption information to send responses back to the proper agent.
Possible values:

- **marked**
  The device adds the circuit ID of the DHCP relay agent to the suboptions for client requests.

- **unmarked** *(default setting)*
  The device removes the DHCP relay agent circuit ID suboptions from client requests.

**BOOTP/DHCP wait time (min.)**

Specifies the minimum amount of time that the device delays forwarding the BOOTP/DHCP request.

The end devices send broadcast request on the local network. This setting lets a local server respond to the client request before the router forwards the client request through the interfaces.

Possible values:

- **0..100** *(default setting: 0)*
  If a local server is absent from the network, then set the value to 0.

**BOOTP/DHCP hops (max.)**

Specifies the maximum number of cascaded devices allowed to forward the BOOTP/DHCP request.

If the hop count exceeds the maximum number of hops specified in this field, then the device drops BOOTP requests.

Possible values:

- **0..16** *(default setting: 4)*

**Information**

- **DHCP client messages received**
  Displays the number of DHCP requests received from the clients.

- **DHCP client messages relayed**
  Displays the number of DHCP requests forwarded to the servers specified in the table.

- **DHCP server messages received**
  Displays the number of DHCP offers received from the servers specified in the table.

- **DHCP server messages relayed**
  Displays the number of DHCP offers forwarded to the clients from the servers specified in the table.

- **UDP messages received**
  Displays the number of UDP requests received from the clients.
Routing
[Routing > L3 Relay]

UDP messages relayed

Displays the number of UDP requests forwarded to the servers specified in the table.

Packets with expired TTL

Displays the number of UDP packets received with an expired TTL value.

Discarded packets

Displays the number of UDP packets that device discarded, because the packet matched an active table entry.

Table

Port

Displays the interface to which the table entry applies.

UDP port

Displays the UDP port for client messages received on this interface for this table entry. The device forwards client DHCP messages matching the UDP port criteria to the IP helper address specified in this table entry.

IP address

Displays the IP helper address associated with this table entry.

Hits

Displays the current number of packets that the interface forwards for the specified UDP port in this table entry.

Active

Activates/deactivates the table entry.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Reset statistics

Resets the table statistics.
Create

Port

Specifies the interface to which the entry applies.

Interface configurations take priority over global configurations. If the destination UDP port for a packet matches any entry on an ingress interface, then the device handles the packet according to the interface configuration. If none of the interface entries match the packet, then the device handles the packet according to the global configuration.

Possible values:
- **All** (default setting)
  - Relay entries with this port value specify a global configuration.
- **<available interfaces>**
  - Used to specify interface configurations.

UDP port

Specifies the helper UDP port criteria for packets received on this interface for this entry. When active, the device forwards packets received with this destination UDP port value to the IP address specified in this entry.

Possible values:
- **default** (default setting)
  - Equal to UDP port 0.
  - An entry with a UDP port specified as 0 enables the dhcp, time, nameserver, tacacs, dns, tftp, netbios-ns, and netbios-dgm entries.
- **dhcp**
  - Equal to UDP port 67.
  - The device forwards DHCP requests for IP address assignment and networking parameters.
- **domain**
  - Equal to UDP port 53.
  - The device forwards DNS requests for host name to IP address conversion.
- **isakmp**
  - Equal to UDP port 500.
  - The device forwards Internet Security Association and Key Management Protocol requests. The requests specifies procedures and packet formats which establish, negotiate, modify and delete Security Associations.
- **mobile-ip**
  - Equal to UDP port 434.
  - The device forwards Home Agent Registration requests. Use this value when you install the device in a network other than the home network.
- **nameserver**
  - Equal to UDP port 42.
  - The device forwards Windows Internet Name Service requests. You use the port to copy the NetBIOS name table from one Windows server to another.
- **netbios-dgm**
  - Equal to UDP port 138.
  - The device forwards NetBIOS Datagram Service requests. The datagram service provides the ability to send a message to a unique name or to a group name.
- **netbios-ns**
  - Equal to UDP port 137.
  - The device forwards NetBIOS Name Service requests for name registration and resolution.
Routing

[Routing > L3 Relay]

- **ntp**
  Equal to UDP port 123.
  The device forwards Network Time Protocol requests. Use this value for peer-to-peer synchronization where both peers consider the other to be a time source.

- **pim-auto-rp**
  Equal to UDP port 496.
  The device forwards Protocol Independent Multicast-Automatic-Rendezvous Point requests. The Rendezvous Point (RP) serves as the root of the shared multicast delivery tree and is responsible for gathering multicast data from different sources, then forwarding the data to the clients.

- **rip**
  Equal to UDP port 520.
  The device forwards RIP requests and RIP response messages.

- **tacacs**
  Equal to UDP port 49.
  The device forwards TACACS Login Host Protocol requests for remote authentication and related services for networked access control through a centralized server.

- **tftp**
  Equal to UDP port 69.
  The device forwards Trivial File Transfer Protocol requests and responses.

- **time**
  Equal to UDP port 37.
  The device forwards Time Protocol requests. The device forwards client requests to a server that supports the time protocol. The server then responds with a message containing an integer representing the number of seconds since 00:00 1 January, 1900 GMT, and closes the data link.

- **0..65535**
  When you know the UDP port number, the device lets you specify the port number directly.

**IP address**

Specifies the IP helper address for packets received on this interface.

Possible values:

- **Valid IP address**
  An address of 0.0.0.0 identifies the entry as a discard entry. The device drops packets that match a discard entry. You specify discard entries only on the interfaces.
A loopback interface is a virtual network interface without reference to a physical port. Loopback interfaces are constantly available while the device is in operation.

The device lets you create router interfaces on the basis of loopback interfaces. Using such a router interface, the device is constantly available, even during periods of inactivity of individual router interfaces.

Up to 8 loopback interfaces can be set up in the device.

### Table

<table>
<thead>
<tr>
<th>Index</th>
<th>Displays the number that uniquely identifies the loopback interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Displays the name of the loopback interface.</td>
</tr>
<tr>
<td>IP address</td>
<td>Specifies the IP address for the loopback interface.</td>
</tr>
<tr>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>- Valid IPv4 address (default setting: 0.0.0.0)</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Specifies the netmask for the loopback interface.</td>
</tr>
<tr>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>- Valid IPv4 netmask (default setting: 0.0.0.0)</td>
</tr>
<tr>
<td></td>
<td>Example: 255.255.255.255</td>
</tr>
<tr>
<td>Active</td>
<td>Displays if the loopback interface is active or inactive.</td>
</tr>
<tr>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>- marked (default setting)</td>
</tr>
<tr>
<td></td>
<td>The loopback interface is active.</td>
</tr>
<tr>
<td></td>
<td>When sending SNMP traps, the device uses the IP address of the first loopback interface as the sender.</td>
</tr>
<tr>
<td></td>
<td>- unmarked</td>
</tr>
<tr>
<td></td>
<td>The loopback interface is inactive.</td>
</tr>
</tbody>
</table>
Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create dialog to create a loopback interface.

- In the Index field, you specify the number that uniquely identifies the loopback interface. Possible values:
  - 1..8
7.9 **L3-Redundancy**

The menu contains the following dialogs:
- VRRP

7.9.1 **VRRP**

The Virtual Router Redundancy Protocol (VRRP) is a procedure that lets the system react to the failure of a router.

You use VRRP in networks with end devices that support one entry for the default gateway. If the default gateway fails, then VRRP helps ensure that the end devices find a redundant gateway.

**Note:** You find detailed information on VRRP in the “Configuration” user manual.

The menu contains the following dialogs:
- VRRP Configuration
- VRRP Statistics
- VRRP Tracking
7.9.1.1 VRRP Configuration

This dialog lets you specify the following settings:
- up to 8 virtual routers per router interface
- up to 2 addresses per virtual router

**Operation**

Enables/disables the VRRP redundancy in the device.

Possible values:
- **On**
  The VRRP function is enabled.
- **Off** (default setting)
  The VRRP function is disabled.

**Information + Configuration**

**Version**

Specifies the VRRP version.

**Send trap (VRRP master)**

Activates/deactivates the sending of SNMP traps when the device is the VRRP master.

Possible values:
- **marked**
  The sending of SNMP traps is active.
  If the device is the VRRP master, then the device sends an SNMP trap.
- **unmarked** (default setting)
  The sending of SNMP traps is inactive.

The prerequisite for sending SNMP traps is that you enable the function in the Diagnostics > Status Configuration > Alarms (Traps) dialog and specify at least one trap destination.

**Send trap (VRRP authentication failure)**

Activates/deactivates the sending of SNMP traps when the device receives a VRRP packet including authentication information.

**Note:** The device supports only VRRP packets without authentication information. In order for the device to operate in conjunction with other devices that support VRRP authentication, verify that on those devices the VRRP authentication is not applied.
Possible values:

- **marked**
  The sending of SNMP traps is active.
  If the device receives a VRRP packet including authentication information, then the device
  sends an SNMP trap.

- **unmarked** (default setting)
  The sending of SNMP traps is inactive.

The prerequisite for sending SNMP traps is that you enable the function in the Diagnostics > Status
Configuration > Alarms (Traps) dialog and specify at least one trap destination.

**Table**

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number to which the table entry relates.</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRID</td>
<td>Displays the Virtual Router IDentifier.</td>
</tr>
<tr>
<td>Active</td>
<td>Activates/deactivates the VRRP instance specified in this row.</td>
</tr>
</tbody>
</table>
| Oper status | Specifies the row status. The operational state of the related virtual router controls the row status
of a currently active row in the table. |
| State | Displays the VRRP state. |

Possible values:

- **active**
  The instance is available for use.

- **notInService**
  The instance exists in the device, but necessary information is missing and it is unavailable for
  use.

- **notReady**
  The instance exists in the device, but necessary information is missing and it is unavailable for
  use.

- **initialize**
  VRRP is in the initialization phase, the function is inactive, or the master router is still unnamed.
Routing

[Routing > L3-Redundancy > VRRP > Configuration]

- **backup**
  The router sees the possibility of becoming the master router.

- **master**
  The router is the master router.

### Base priority

Specifies the priority of the virtual router. The value differs from `Priority` if tracked objects are down or the virtual router is the IP address owner.

Possible values:

- 1..254 (default setting: 100)

When you configure multiple VRRP routers in a single instance, distribute the priority values uniformly on the routers. For example, assign the priority value of 50 to the primary router, the value of 100 to the next router. Repeat the steps with the value 150, and so on.

### Priority

Specifies the VRRP priority value.

The router with the higher priority value takes over the master router role. If the virtual router IP address is the same as an IP address of a router interface, then the router is the “owner” of the IP address. If an IP address owner exists, then VRRP assigns the IP address owner the VRRP priority 255 and declares the router as the master router.

Possible values:

- 1..255 (default setting: 100)

When you plan to remove a master router from the network, lower the priority number to force an election, thus reducing the black hole period.

### Virtual IP address

Displays the virtual IP address in the subnet of the primary IP address on the interface. If no match is found, then the device returns an unspecified virtual address. If no virtual address is configured, then 0.0.0.0 is returned.

Possible values:

- Valid IPv4 address

### Preempt mode

Activates/deactivates the preempt mode. This setting specifies if this router, as a backup router, takes over the master router role when the master router has a lower VRRP priority.

Possible values:

- **marked** (default setting)
  When you enable the preempt mode, this router takes the master router role from a router with a lower VRRP priority without waiting for an election.

- **unmarked**
  When you disable the Preempt mode, this router assumes the role of a backup router and listens for master router advertisements. After the master down interval expires, without receiving advertisements from the master router, this router participates in the master router election process.
VRRP master candidate

Specifies the primary virtual router IP address.

When the interface has several specified IP addresses, the parameter lets you select an IP address as the Master IP address.

Possible values:

- Valid IPv4 address  (default setting: 0.0.0.0)
  - The default setting 0.0.0.0 indicates that the router is using the lower IP address as the Master IP address.

Master IP address

Displays the current master router interface IP address.

Possible values:

- Valid IPv4 address  (default setting: 0.0.0.0)

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.

- In the Port field, you specify the router interface.
- In the VRID field, you specify the Virtual Route Identifier (VRID).

Setting up the VRRP router instance

The device lets you set up to 8 virtual routers per router interface.

Before you set up a VRRP instance, verify that network routing functions properly and set the IP addresses on the router interfaces used for the VRRP instances.

Perform the following steps:

1. In the Routing > L3-Redundancy > VRRP > Configuration dialog, open the Wizard window.
2. In the Wizard window, open the Create or select entry dialog.
   - Select a router interface in the Port drop-down list.
   - Specify the Virtual Router IDentifier in the VRID column.
3. In the Wizard window, open the Edit entry dialog.
   - In the Configuration frame, specify the values for the following parameters:
     - Priority
     - Preempt mode
     - Advertisement interval [s]
     - Ping answer
     - Select the VRRP master candidate IP address in the drop-down list.
     - VRRP advert address (IP address of the partner HiVRRP router)
     - VRRP advert interval [ms]
Routing

[Routing > L3-Redundancy > VRRP > Configuration]

- **Link-down notify address** (IP address of the second router to which the device sends link-down notifications)
  
  You use this function when the virtual router consists of 2 VRRP routers.

- **Domain ID**

- **Domain role**

  □ To transfer the settings to the VRRP router interface table, click the **Finish** button.

  □ In the **Routing > L3-Redundancy > VRRP > Configuration** dialog, select the **on** radio button in the **Operation** frame. Then click the ✔ button.

---

**Editing an existing VRRP router instance**

Perform one of the following steps:

- In the **Routing > L3-Redundancy > VRRP > Configuration** dialog, highlight a row in the table and click the ✖ button to edit it.

  Or

  □ Double-click a field in the table and edit the entry directly.

  Or

  □ Right-click a field and select a value.

---

**Deleting a VRRP router instance**

Perform the following step:

- In the **Routing > L3-Redundancy > VRRP > Configuration** dialog, highlight a row and click the ✖ button.

---

[VRRP configuration (Wizard)]

The **Wizard** window helps you to create a VRRP router instance.

**Prerequisites:**

- Network routing is functioning correctly.
- On the interfaces used in the VRRP instance the IP addresses are specified.

---

[VRRP configuration (Wizard) – Create or select entry]

**Table**

**Port**

Displays the router interface number to which the table entry relates.

**VRID**

Displays the Virtual Router IDentifier.
IP address

Displays the primary IP address of the router interface.
You specify this address in the Routing > Interfaces > Configuration dialog.

Netmask

Displays the netmask of primary IP address.
You specify this subnet mask in the Routing > Interfaces > Configuration dialog.

Area below the table

Port

Specifies the router interface number to which the table entry relates.
Possible values:
▶ <Available router interfaces>

VRID

Specifies the Virtual Router IDentifier.
A virtual router uses 00-00-5E-00-01-XX as its MAC address. The value specified here replaces the last octet (XX) in the MAC address. Assign a unique value to every physical router within a virtual router instance. The device changes the effective priority value to 255 for a physical router with the same IP address as the virtual router.
Possible values:
▶ 1..255

[VRRP configuration (Wizard) – Edit entry – VRRP]

Operation

Enables/disables the VRRP redundancy in the device.
Possible values:
▶ On
The VRRP function is enabled.
▶ Off (default setting)
The VRRP function is disabled.
Information

Port
Displays the router interface number to which the table entry relates.

VRID
Displays the Virtual Router IDentifier.

Configuration

Base priority
Specifies the priority of the virtual router. The value differs from Priority if tracked objects are down or the virtual router is the IP address owner.

Possible values:
- 1..254 (default setting: 100)

When you configure multiple VRRP routers in a single instance, distribute the priority values uniformly on the routers. For example, assign the priority value of 50 to the primary router, the value of 100 to the next router. Repeat the steps with the value 150, and so on.

Priority
Specifies the VRRP priority value.

The router with the higher priority value takes over the master router role. If the virtual router IP address is the same as an IP address of a router interface, then the router is the “owner” of the IP address. If an IP address owner exists, then the VRRP function assigns the IP address owner the priority value 255 and declares the router as the master router.

Possible values:
- 1..255 (default setting: 100)

Disabling or removing an VRRP router, which is in the master role, forces the instance to send an advertisement with priority value 0. This lets the other backup routers know that the master is not participating. Sending a priority value 0 forces a new election.

Preempt mode
Activates/deactivates the preempt mode. This setting specifies if this router, as a backup router, takes over the master router role when the master router has a lower VRRP priority.

Possible values:
- marked (default setting)
  - When you enable the Preempt mode, this router takes the master router role from a router with a lower VRRP priority without waiting for an election.
- unmarked
  - When you disable the Preempt mode, this router assumes the role of a backup router and listens for master router advertisements. After the master down interval expires, without receiving advertisements from the master router, this router participates in the master router election process.
Advertisement interval [s]

Specifies the interval between master router advertisements in seconds.

Possible values:
- **1..255** (default setting: **1**)

**Note:** The longer the advertisement interval, the longer the time for which backup routers wait for a message from the master router before starting a new election process (master down interval). Also, specify the same value on every participant in a given virtual router instance.

Ping answer

Activates/deactivates the ping answer function in the device. You use the VRRP ping for connectivity analyses.

The prerequisite for allowing the device to answer ping requests from the interfaces is that you activate the **Send echo reply** function globally. In the **Routing > Global** dialog, **ICMP filter** frame, mark the **Send echo reply** checkbox.

Possible values:
- **marked** (default setting)
  - The **Ping answer** function in the device is active. The device answers ICMP ping requests.
- **unmarked**
  - The **Ping answer** function in the device is inactive. The device ignores ICMP ping requests.

VRRP master candidate

Primary virtual router IP address.

Physical routers within a virtual router instance use the VRRP IP address to communicate with themselves. If the virtual router IP address is the same as an IP address of a router interface, then the router is the “owner” of the IP address and the master router.

Possible values:
- **Valid IP address** (default setting: **0.0.0.0**)

[VRRP configuration (Wizard) – Tracking]

Current track entries

**Type**

Displays the type of the tracking object.

Possible values:
- **interface**
  - The device monitors the link status of its physical ports or of its link aggregation, LRE or VLAN router interface.
Routing
[Routing > L3-Redundancy > VRRP > Configuration]

- ping
  The device monitors the route to a remote router or end device by means of periodic ping requests.

- logical
  The device monitors tracking objects logically linked to each other and thus enables complex monitoring tasks.

**Track ID**
Displays the identification number of the tracking object.

**Track name**
Displays the name of the tracking object made up of Type and Track ID.

**Assigned track entries**

**Track name**
Displays the name of the tracking object to which the virtual router is linked.

If the result for a tracking object is negative, then the VRRP instance reduces the priority of the virtual router. The tracking object is negative for example, if the monitored interface is inactive or the monitored router cannot be reached.

Possible values:
- Name of the tracking object, made up of Type and Track ID.
- Logical trackers, which combine multiple trackers
- - No tracking object selected.

You set up tracking objects in the Routing > Tracking > Configuration dialog.

**Decrement**

Specifies the value by which the VRRP instance reduces the priority of the virtual router when the monitoring result is negative.

Possible values:
- 1..253 (default setting: 20)

**Note:** If in the Routing > L3-Redundancy > VRRP > Configuration dialog the value in the Priority column is 255, then the virtual router is the owner of the IP address. In this case the priority of the virtual router remains unchanged.
[VRRP configuration (Wizard) – Virtual IP addresses]

**Information**

**IP address**

Displays the primary IP address of the router interface.

**Multinetting**

**Additional IP address**

Displays the secondary IP addresses of the router interface.

The device lets you specify one primary and one secondary multinetting addresses per router interface.

**Additional netmask**

Displays the subnet mask of the secondary IP addresses.

**Virtual IP addresses**

**IP address**

Displays the assigned IP address of the master router within a virtual router.

**Virtual IP addresses**

Specifies the virtual IP address to be assigned.

To insert the IP address in the IP address table, click the Add button.
7.9.1.2 VRRP Statistics

This dialog displays the number of counters that count events relevant to the VRRP function.

Information

Checksum errors
Displays the number of VRRP messages received with the wrong checksum.

Version errors
Displays the number of VRRP messages received with an unknown or unsupported version number.

VRID errors
Displays the number of VRRP messages received with an invalid Virtual Router Identifier for this virtual router.

Table

Port
Displays the router interface number to which the table entry relates.

VRID
Displays the Virtual Router Identifier.

Become master
Displays the number of times that the device has taken the master role. This entry helps you to analyze the network. When this number is low, your network is relatively stable.

Advertise received
Displays the number of VRRP advertisements received.

Advertise interval errors
Displays the number of VRRP advertisements received by the router outside the advertisement interval. The value lets you determine if the routers have the same advertise interval specified across the virtual router instance.

Authentication failures
Displays the number of VRRP advertisements received with authentication errors.
IP TTL errors

Displays the number of VRRP advertisements received with an IP TTL not equal to 255.

Priority zero packets received

Displays the number of VRRP advertisements received with priority 0.

Priority zero packets sent

Displays the number of VRRP advertisements that the device sent with priority 0.

Invalid type packets received

Displays the number of VRRP advertisements received with an invalid type.

Address list errors

Displays the number of VRRP advertisements received for which the address list does not match the address list configured locally for the virtual router.

Invalid authentication type

Displays the number of VRRP advertisements received with an invalid authentication type.

Authentication type mismatch

Displays the number of VRRP advertisements received with an incorrect authentication type.

Packet length errors

Displays the number of VRRP advertisements received with an incorrect packet length.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
7.9.1.3 **VRRP Tracking**

VRRP tracking lets you follow the operation of specific object and react to a change in the object status. The function is periodically notified about the tracked object and displays the changes in the table. The table displays the object statuses as either **up**, **down** or **notReady**. To enter a track object in the table, perform the following step:

- Click the button.

**Table**

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the router interface number of the virtual router.</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRID</td>
<td>Displays the virtual router ID for this virtual router.</td>
</tr>
<tr>
<td>Track name</td>
<td>Displays the name of the tracking object to which the virtual router is linked.</td>
</tr>
</tbody>
</table>

If the result for a tracking object is negative, then the VRRP instance reduces the priority of the virtual router. The tracking object is negative for example, if the monitored interface is inactive or the monitored router cannot be reached.

Possible values:
- Name of the tracking object, made up of **Type** and **Track ID**.
- Logical trackers, which combine multiple trackers
- No tracking object selected.

You set up tracking objects in the **Routing > Tracking > Configuration** dialog.

**Decrement**

Specifies the value by which the VRRP instance reduces the priority of the virtual router when the monitoring result is negative.

Possible values:
- 1..253 (default setting: 20)

**Note:** If in the **Routing > L3-Redundancy > VRRP > Configuration** dialog the value in the **Priority** column is 255, then the virtual router is the owner of the IP address. In this case the priority of the virtual router remains unchanged.
Status

Displays the monitoring result of the tracking object.

Possible values:

- **notReady**
  The tracking object is not operating.
- **up**
  The monitoring result is positive:
  - The link status is active.
  - The remote router or end device is reachable.
- **down**
  The monitoring result is negative:
  - The link status is inactive.
  - The remote router or end device is not reachable.
- A combination of the **up** and **down** trackers.

Active

Displays if the monitoring of the tracking object is active or inactive.

Possible values:

- **active**
  The monitoring of the tracking object is active.
- **notReady**
  The monitoring of the tracking object is inactive. You activate the monitoring in the **Routing > Tracking > Configuration** dialog, **Active** column.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.

- In the **Port VRID** drop-down list, you select the interface and router ID of a virtual router that has been set up.
- In the **Track name** drop-down list, you select the tracking object with which the device links the virtual router.

7.10 NAT

The menu contains the following dialogs:

- **NAT Global**
- **1:1 NAT**
- **Destination NAT**
Masquerading NAT
Double NAT
7.10.1 NAT Global

Network Address Translation (NAT) contains several procedures which automatically change the IP address information in the data packet. When configured in the device, the NAT function enables communication links between devices in different networks.

The device provides a multi-step approach to set up and apply the NAT rules:
- Create rule.
- Assign rule to a router interface.
- Apply the rule to the data stream; to do this, click in the Routing > NAT > NAT Global dialog the Commit changes button.

This dialog displays how many NAT rules can be set up for the individual NAT processes and indicates changes to the active NAT rules. By clicking the Commit changes button, you apply the NAT rules configured to the data stream.

**Information**

1:1 NAT rules (max.)
Displays how many rules can be configured in the device for the 1:1 NAT function.

Destination NAT rules (max.)
Displays how many rules can be configured in the device for the Destination NAT function.

Masquerading NAT rules (max.)
Displays how many rules can be configured in the device for the Masquerading NAT function.

Double NAT rules (max.)
Displays how many rules can be configured in the device for the Double NAT function.

1:1 NAT pending actions
Displays if the 1:1 NAT rules used in the data stream differ from the saved 1:1 NAT rules.

Possible values:
- marked
  At least one saved 1:1 NAT rule contains modified settings. To apply the changes to the data stream, click the button and then the Commit changes item.
- unmarked
  The device applies the saved 1:1 NAT rules to the data stream.
Routing

[Routing > NAT > NAT Global]

Destination NAT pending actions

Displays if the Destination NAT rules used in the data stream differ from the saved Destination NAT rules.

Possible values:

- **marked**
  At least one saved Destination NAT rule contains modified settings. To apply the changes to the data stream, click the button and then the Commit changes item.

- **unmarked**
  The device applies the saved Destination NAT rules to the data stream.

Masquerading NAT pending actions

Displays if the Masquerading NAT rules used in the data stream differ from the saved Masquerading NAT rules.

Possible values:

- **marked**
  At least one saved Masquerading NAT rule contains modified settings. To apply the changes to the data stream, click the button and then the Commit changes item.

- **unmarked**
  The device applies the saved Masquerading NAT rules to the data stream.

Double NAT pending actions

Displays if the Double NAT rules used in the data stream differ from the saved Double NAT rules.

Possible values:

- **marked**
  At least one saved Double NAT rule contains modified settings. To apply the changes to the data stream, click the button and then the Commit changes item.

- **unmarked**
  The device applies the saved Double NAT rules to the data stream.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Commit changes

Applies the rules saved in the device to the data stream.

In the process, the device also removes the state information from the packet filter. This includes potential DCE RPC information of the OPC enforcer. In the process, the device interrupts open communication connections.

**Note:** While the device is activating the saved rules, the establishment of any new communication connections is impossible.
7.10.2 1:1 NAT

The 1:1 NAT function lets you establish communication links within a local network to devices that are located in other networks. The NAT router virtually “shifts” the devices into the public network. To do this, the NAT router replaces the virtual with the actual IP address in the data packet while sending it. A typical application is connecting some identically structured production cells with the same IP address to a server farm.

The prerequisite for the 1:1 NAT process is that the NAT router itself responds to ARP requests. To make this happen, turn on the Proxy ARP function on the ingress interface.

To use the NAT function, set up a router interface for each network and turn on the routing function in the device.

The data packets go through the filter functions of the device in the following sequence:

The menu contains the following dialogs:

- 1:1 NAT Rule
7.10.2.1 1:1 NAT Rule

In this dialog you generate and edit the 1:1 NAT rules and assign router interfaces to which the device applies the 1:1 NAT rules.

**Table**

**Index**

Displays the index number to which the table entry relates.

Possible values:

- 1..255

**Rule name**

Displays the name of the 1:1 NAT rule. To change the name, click the relevant field.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters

**Priority**

Specifies the priority of the 1:1 NAT rule.

Using the priority, you specify the order in which the device applies several rules to the data stream. The device applies the rules in ascending order starting with priority 1.

Possible values:

- 1..6500 (default setting: 1)

**Ingress interface**

Assigns the 1:1 NAT rule to the router interface on which the device receives data packets. The 1:1 NAT rule makes the destination device virtually accessible in the network connected here.

Possible values:

- <Interface number>
  
  The device applies the 1:1 NAT rule to this router interface, and only to data packets addressed to the IP address specified in the Destination address column.

- no Port
  
  No router interface is assigned to the 1:1 NAT rule. Someone removed the router interface after the last edit of the 1:1 NAT rule.

You enable on the ARP proxy function on this router interface in the Routing > Interfaces > Configuration dialog.
Routing

[Routing > NAT > 1:1 NAT > Rule]

Destination address

Specifies the destination address of the data packets to which the device applies the 1:1 NAT rule. The device sends data packets with this destination address to the destination address specified in the New destination address column.

Possible values:

- Valid IPv4 address
  The device applies the 1:1 NAT rule only to data packets containing the destination address specified here.
- Valid IPv4 address and netmask in CIDR notation
  The device applies the 1:1 NAT rule only to data packets containing a destination address in the subnet specified here.

Egress interface

Assigns the 1:1 NAT rule to the router interface on which the device forwards the modified data packets. The destination device can actually be reached in the network connected here.

Possible values:

- <Interface number>
  The device forwards the modified data packets on this router interface.
- no Port
  No router interface is assigned to the 1:1 NAT rule. Someone removed the router interface after the last edit of the 1:1 NAT rule.

New destination address

Specifies the actual IP address of the destination device. The device sends data packets to the destination address specified here.

Possible values:

- Valid IPv4 address
  The device replaces the destination address in the data packet with this new destination address.
- Valid IPv4 address and netmask in CIDR notation
  The device replaces the destination address in the data packet with a destination address in the subnet specified here.

Trap

Activates/deactivates the sending of SNMP traps when the 1:1 NAT rule is applied to data packets.

Possible values:

- marked
  If the device applies the 1:1 NAT rule to a data packet, then the device sends an SNMP trap.
- unmarked (default setting)
  The sending of SNMP traps is deactivated.

The prerequisite for sending SNMP traps is that you enable the function in the Diagnostics > Status Configuration > Alarms (Traps) dialog and specify at least one trap destination.
Log

Activates/deactivates the logging in the log file. See the Diagnostics > Report > System Log dialog.

Possible values:
- **marked**
  
  Logging is activated. When the device applies the 1:1 NAT rule to a data packet, the device places an entry in the log file.

- **unmarked** (default setting)
  
  Logging is deactivated.

Active

Activates/deactivates the 1:1 NAT rule.

Possible values:
- **marked**
  
  The rule is active.

- **unmarked** (default setting)
  
  The rule is inactive.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.

- In the **Destination address** field, you specify the destination address of the data packets to which the device applies the rule. The device sends data packets with this destination address to the destination address specified in the **New destination address** column.
  
  Possible values:
  - Valid IPv4 address
    
    The device applies the 1:1 NAT rule only to data packets containing the destination address specified here.
  - Valid IPv4 address and netmask in CIDR notation
    
    The device applies the 1:1 NAT rule only to data packets containing a destination address in the subnet specified here.

- In the **New destination address** field, you specify the actual IP address of the destination device. The device sends data packets to the destination address specified here.
  
  Possible values:
  - Valid IPv4 address
    
    The device replaces the destination address in the data packet with this new destination address.
  - Valid IPv4 address and netmask in CIDR notation
    
    The device replaces the destination address in the data packet with a destination address in the subnet specified here.

When you click the **Ok** button, the device creates the new table entry. The device assigns the values specified in the **Destination address** and **New destination address** fields to this entry.
7.10.3 Destination NAT

The Destination NAT function lets you divert the data stream of outgoing communication links to or through a server in a local network.

A special form of the Destination NAT function is port forwarding. You use port forwarding to hide the structure of a network from the outside while still allowing communication links from the outside into the network. A typical application is remote control of a PC in a production cell. The maintenance station establishes the communication link to the NAT router, and the Destination NAT function takes care of the routing to the production cell.

To use the NAT function, set up a router interface for each network and turn on the routing function in the device.
The data packets go through the filter functions of the device in the following sequence:

**Figure 6: Processing sequence of the data packets in the device**

The menu contains the following dialogs:
- Destination NAT Rule
- Destination NAT Mapping
- Destination NAT Overview
7.10.3.1 Destination NAT Rule

In this dialog you create and edit the Destination NAT rules.

You assign a router interface to the affected Destination NAT rule in the Routing > NAT > Destination NAT > Mapping dialog.

An overview of which Destination NAT rule is to be assigned to which router interface can be found in the Routing > NAT > Destination NAT > Overview dialog.

Table

<table>
<thead>
<tr>
<th>Index</th>
<th>Displays the index number to which the table entry relates.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>1..255</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule name</th>
<th>Displays the name of the Destination NAT rule. To change the name, click the relevant field.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>▶ Alphanumeric ASCII character string with 0..32 characters</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source address</th>
<th>Specifies the source address of the data packets to which the device applies the Destination NAT rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>▶ any (default setting)</td>
</tr>
<tr>
<td></td>
<td>The device applies the Destination NAT rule to data packets with any source address.</td>
</tr>
<tr>
<td></td>
<td>▶ Valid IPv4 address</td>
</tr>
<tr>
<td></td>
<td>The device applies the Destination NAT rule only to data packets containing the source address specified here.</td>
</tr>
<tr>
<td></td>
<td>▶ Valid IPv4 address and netmask in CIDR notation</td>
</tr>
<tr>
<td></td>
<td>The device applies the Destination NAT rule only to data packets containing a source address in the subnet specified here.</td>
</tr>
<tr>
<td></td>
<td>▶ An exclamation mark (!) preceding the IP address reverses the expression into its opposite. The device applies the Destination NAT rule to data packets NOT containing the source address specified here.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source port</th>
<th>Specifies the source port of the data packets to which the device applies the Destination NAT rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The prerequisite for specifying a source port is that, in the Protocol field, you specify the value TCP or UDP.</td>
</tr>
</tbody>
</table>
Routing

[Routing > NAT > Destination NAT > Rule]

Possible values:

- **any** (default setting)
  The device applies the Destination NAT rule to every data packet without considering the source port.

- **1..65535**
  The device applies the Destination NAT rule only to data packets containing the specified source port.

The field lets you specify the following options:
- You specify a port with a single numerical value, for example 21.
- You specify multiple individual ports with numerical values separated by commas, for example 21,80,110.
- You specify a port range with numerical values connected by dashes, for example 2000-3000.
- You can also combine ports and port ranges, for example 21,2000-3000,65535.

The column lets you specify up to 15 numerical values. When you enter 21,2000-3000,65535, for example, you use 4 of 15 numerical values.

Destination address

Specifies the destination address of the data packets to which the device applies the Destination NAT rule. The device sends data packets with this destination address to the destination address specified in the New destination address column.

Possible values:

- **any**
  The device applies the Destination NAT rule to data packets with any destination address.

- **Valid IPv4 address**
  The device applies the Destination NAT rule only to data packets containing the destination address specified here.

- **Valid IPv4 address and netmask in CIDR notation**
  The device applies the Destination NAT rule only to data packets containing a destination address in the subnet specified here.

- **An exclamation mark (!) preceding the IP address reverses the expression into its opposite.**
  The device applies the Destination NAT rule to data packets NOT containing the destination address specified here.

Destination port

Specifies the destination port of the data packets to which the device applies the Destination NAT rule.

Possible values:

- **any** (default setting)
  The device applies the Destination NAT rule to every data packet without considering the destination port.

- **1..65535**
  The device applies the Destination NAT rule only to data packets containing the specified destination port.

The field lets you specify the following options:
- You specify a port with a single numerical value, for example 21.
- You specify multiple individual ports with numerical values separated by commas, for example 21,80,110.
You specify a port range with numerical values connected by dashes, for example 2000-3000.

You can also combine ports and port ranges, for example 21,2000-3000,65535. The column lets you specify up to 15 numerical values. When you enter 21,2000-3000,65535, for example, you use 4 of 15 numerical values.

New destination address

Specifies the actual IP address of the destination device. The device sends data packets to the destination address specified here.

Possible values:
- Valid IPv4 address
  The device replaces the destination address in the data packet with this new destination address.

New destination port

Specifies the port of the destination device. The device forwards data packets to the destination port specified here.

Possible values:
- any
  The device retains the original destination port in the data packet.
- 1..65535
  The device replaces the destination port in the packet with this new destination port.

Protocol

Restricts the Destination NAT rule to an IP protocol. The device applies the Destination NAT rule only to packets of the specified IP protocol.

Possible values:
- icmp
  Internet Control Message Protocol (RFC 792)
- igmp
  Internet Group Management Protocol
- pip
  IP in IP tunneling (RFC 1853)
- tcp
  Transmission Control Protocol (RFC 793)
- udp
  User Datagram Protocol (RFC 768)
- esp
  IPsec Encapsulated Security Payload (RFC 2406)
- ah
  IPsec Authentication Header (RFC 2402)
- icmpv6
  Internet Control Message Protocol for IPv6
- any (default setting)
  The device applies the Destination NAT rule to every data packet without considering the IP protocol.
Routing

[Routing > NAT > Destination NAT > Rule]

**Log**

Activates/deactivates the logging in the log file. See the *Diagnostics > Report > System Log* dialog.

Possible values:
- **marked**
  - Logging is activated.
  - When the device applies the *Destination NAT* rule to a data packet, the device places an entry in the log file.
- **unmarked** (default setting)
  - Logging is deactivated.

**Trap**

Activates/deactivates the sending of SNMP traps when the *Destination NAT* rule is applied to data packets.

Possible values:
- **marked**
  - If the device applies the *Destination NAT* rule to a data packet, then the device sends an SNMP trap.
- **unmarked** (default setting)
  - The sending of SNMP traps is deactivated.

The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least one trap destination.

**Active**

Activates/deactivates the *Destination NAT* rule.

Possible values:
- **marked**
  - The rule is active.
- **unmarked** (default setting)
  - The rule is inactive.

**Buttons**

You find the description of the standard buttons in section "Buttons" on page 14.

Opens the *Create* window to add a new entry to the table.

- In the *New destination address* field, you specify the actual IP address of the destination device. The device sends data packets to the destination address specified here.
  - **Valid IPv4 address**
    - The device replaces the destination address in the data packet with this new destination address.

When you click the *Ok* button, the device creates the new table entry. The device assigns the value specified in the *New destination address* field to this entry.
7.10.3.2 Destination NAT Mapping

In this dialog you assign the Destination NAT rules to a router interface. To do this, click the button and then the Assign item.

You create and edit the Destination NAT rules in the Routing > NAT > Destination NAT > Rule.

An overview of which Destination NAT rule is to be assigned to which router interface can be found in the Routing > NAT > Destination NAT > Overview dialog.

**Table**

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the number of the router interface on which the device applies the Destination NAT rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule index</td>
<td>Displays the sequential number of the Destination NAT rule. See the Index column in the Routing &gt; NAT &gt; Destination NAT &gt; Rule dialog.</td>
</tr>
<tr>
<td>Rule name</td>
<td>Displays the name of the Destination NAT rule. See the Rule name column in the Routing &gt; NAT &gt; Destination NAT &gt; Rule dialog.</td>
</tr>
<tr>
<td>Direction</td>
<td>Displays if the device applies the Destination NAT rule to data packets received or sent. Possible values:</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies the priority of the Destination NAT rule. Using the priority, you specify the order in which the device applies several rules to the data stream. The device applies the rules in ascending order starting with priority 1.</td>
</tr>
</tbody>
</table>

Possible values:

- **ingress**
  
  The device applies the Destination NAT rule to data packets received on the router interface.
Routing

[Routing > NAT > Destination NAT > Mapping]
7.10.3.3 Destination NAT Overview

In this dialog you will find an overview of which Destination NAT rule is assigned to which router interface.

You create and edit the Destination NAT rules in the Routing > NAT > Destination NAT > Rule.

You assign a router interface to the affected Destination NAT rule in the Routing > NAT > Destination NAT > Mapping dialog.

Table

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the number of the router interface on which the device applies the Destination NAT rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule index</td>
<td>Displays the sequential number of the Destination NAT rule. See the Index column in the Routing &gt; NAT &gt; Destination NAT &gt; Rule dialog.</td>
</tr>
<tr>
<td>Rule name</td>
<td>Displays the name of the Destination NAT rule. See the Rule name column in the Routing &gt; NAT &gt; Destination NAT &gt; Rule dialog.</td>
</tr>
<tr>
<td>Destination address</td>
<td>Displays the destination address of the data packets to which the device applies the Destination NAT rule. The device sends data packets with this destination address to the destination address specified in the New destination address column.</td>
</tr>
<tr>
<td>New destination address</td>
<td>Displays the actual IP address of the destination device. The device sends data packets to the destination address specified here.</td>
</tr>
<tr>
<td>Trap</td>
<td>Displays if the device sends an SNTP trap when it applies the Destination NAT rule to a data packet.</td>
</tr>
<tr>
<td>Possible values:</td>
<td></td>
</tr>
<tr>
<td>marked</td>
<td>The device sends an SNMP trap.</td>
</tr>
<tr>
<td>unmarked</td>
<td>The device does not send an SNMP trap.</td>
</tr>
</tbody>
</table>

The prerequisite for sending SNMP traps is that you enable the function in the Diagnostics > Status Configuration > Alarms (Traps) dialog and specify at least one trap destination.
Routing

[Routing > NAT > Destination NAT > Overview]

Log
Displays if the device places an entry in the log file when it applies the Destination NAT rule to a data packet.
Possible values:
▸ marked
  When the device applies the Destination NAT rule to a data packet, the device places an entry in the log file. See the Diagnostics > Report > System Log dialog.
▸ unmarked
  Logging is disabled.

Direction
Displays if the device applies the Destination NAT rule to data packets received or sent.
Possible values:
▸ ingress
  The device applies the Destination NAT rule to data packets received on the router interface.

Priority
Displays the priority of the Destination NAT rule.
The device applies rules to the data stream in ascending order starting with priority 1.

Buttons
You find the description of the standard buttons in section "Buttons" on page 14.
7.10.4 Masquerading NAT

The Masquerading NAT function hides any number of devices behind the IP address of the NAT router and thus hides the structure of a network from other networks. To do this, the NAT router replaces the sender address in the data packet with its own IP address. Also, the NAT router replaces the source port in the data packet with its own value to send the response data packets back to the original sender later on.

To use the NAT function, set up a router interface for each network and turn on the routing function in the device.

Note: If you enable the VRRP function on a router interface, then the Masquerading NAT function is ineffective on this router interface.

The data packets go through the filter functions of the device in the following sequence:

The menu contains the following dialogs:
- Masquerading NAT Rule
- Masquerading NAT Mapping
- Masquerading NAT Overview
7.10.4.1 Masquerading NAT Rule

In this dialog you create and edit the Masquerading NAT rules.

You assign a router interface to the affected Masquerading NAT rule in the Routing > NAT > Masquerading NAT > Mapping dialog.

An overview of which Masquerading NAT rule is to be assigned to which router interface can be found in the Routing > NAT > Masquerading NAT > Overview dialog.

**Table**

**Index**

Displays the index number to which the table entry relates.

Possible values:

- 1..128

**Rule name**

Displays the name of the Masquerading NAT rule. To change the name, click the relevant field.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters

**Source address**

Specifies the source address of the data packets to which the device applies the Masquerading NAT rule.

Possible values:

- *any*
  
  The device applies the Masquerading NAT rule to data packets with any source address.

- Valid IPv4 address
  
  The device applies the Masquerading NAT rule only to data packets containing the source address specified here.

- Valid IPv4 address and netmask in CIDR notation
  
  The device applies the Masquerading NAT rule only to data packets containing a source address in the subnet specified here.

- An exclamation mark (!) preceding the IP address reverses the expression into its opposite. The device applies the Masquerading NAT rule to data packets NOT containing the source address specified here.
Source port

Specifies the source port of the data packets to which the device applies the Masquerading NAT rule.

Possible values:

- **any**  (default setting)
  The device applies the Masquerading NAT rule to every data packet without considering the source port.

- **1..65535**
  The device applies the Masquerading NAT rule only to data packets containing the specified source port.

  The field lets you specify the following options:
  - You specify a port with a single numerical value, for example 21.
  - You specify multiple individual ports with numerical values separated by commas, for example 21,80,110.
  - You specify a port range with numerical values connected by dashes, for example 2000-3000.
  - You can also combine ports and port ranges, for example 21,2000-3000,65535.
  
  The column lets you specify up to 15 numerical values. When you enter 21,2000-3000,65535, for example, you use 4 of 15 numerical values.

Protocol

Restricts the Masquerading NAT rule to an IP protocol. The device applies the Masquerading NAT rule only to packets of the specified IP protocol.

Possible values:

- **tcp**
  Transmission Control Protocol (RFC 793)

- **udp**
  User Datagram Protocol (RFC 768)

- **any**  (default setting)
  The device applies the Masquerading NAT rule to every data packet without considering the IP protocol.

Log

Activates/deactivates the logging in the log file. See the Diagnostics > Report > System Log dialog.

Possible values:

- **marked**
  Logging is activated.
  When the device applies the Masquerading NAT rule to a data packet, the device places an entry in the log file.

- **unmarked**  (default setting)
  Logging is deactivated.
Trap

Activates/deactivates the sending of SNMP traps when the **Masquerading NAT** rule is applied to data packets.

Possible values:
- **marked**
  - If the device applies the **Masquerading NAT** rule to a data packet, then the device sends an SNMP trap.
- **unmarked** (default setting)
  - The sending of SNMP traps is deactivated.

The prerequisite for sending SNMP traps is that you enable the function in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog and specify at least one trap destination.

IPsec exempt

Activates/deactivates applying the **Masquerading NAT** rule to IPsec data packets.

Possible values:
- **marked**
  - The device does not apply the **Masquerading NAT** rule to the IPsec data packets. The device transmits IPsec data packets through the VPN tunnel without any modification.
- **unmarked** (default setting)
  - The device applies the **Masquerading NAT** rule to the IPsec data packets. The device transmits IPsec data packets through the VPN tunnel depending on the settings of the Traffic Selector in the **Source address (CIDR)** and **Source restrictions** columns. See the **Virtual Private Network > Connections** dialog.

Active

Activates/deactivates the **Masquerading NAT** rule.

Possible values:
- **marked**
  - The rule is active.
- **unmarked** (default setting)
  - The rule is inactive.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.
7.10.4.2 Masquerading NAT Mapping

In this dialog you assign the Masquerading NAT rules to a router interface. To do this, click the button and then the Assign item.

You create and edit the Masquerading NAT rules in the Routing > NAT > Masquerading NAT > Rule.

An overview of which Masquerading NAT rule is to be assigned to which router interface can be found in the Routing > NAT > Masquerading NAT > Overview dialog.

Table

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the number of the router interface on which the device applies the Masquerading NAT rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule index</td>
<td>Displays the sequential number of the Masquerading NAT rule. See the Index column in the Routing &gt; NAT &gt; Masquerading NAT &gt; Rule dialog.</td>
</tr>
<tr>
<td>Rule name</td>
<td>Displays the name of the Masquerading NAT rule. See the Rule name column in the Routing &gt; NAT &gt; Masquerading NAT &gt; Rule dialog.</td>
</tr>
<tr>
<td>Direction</td>
<td>Displays if the device applies the Masquerading NAT rule to data packets received or sent. Possible values: egress The device applies the Masquerading NAT rule to data packets sent on the router interface.</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies the priority of the Masquerading NAT rule. Using the priority, you specify the order in which the device applies several rules to the data stream. The device applies the rules in ascending order starting with priority 1.</td>
</tr>
</tbody>
</table>
Possible values:

- **1..6500** (default setting: 1)

**Active**

Activates/deactivates the *Masquerading NAT* rule.

Possible values:

- **marked**
  The rule is active.
- **unmarked** (default setting)
  The rule is inactive.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

**Assign**

Opens the *Assign* dialog. In this dialog you assign a configured router interface of an existing *Masquerading NAT* rule.
7.10.4.3 Masquerading NAT Overview

In this dialog you will find an overview of which Masquerading NAT rule is assigned to which router interface.

You create and edit the Masquerading NAT rules in the Routing > NAT > Masquerading NAT > Rule.

You assign a router interface to the affected Masquerading NAT rule in the Routing > NAT > Masquerading NAT > Mapping dialog.

**Table**

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the number of the router interface on which the device applies the Masquerading NAT rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule index</td>
<td>Displays the sequential number of the Masquerading NAT rule. See the Index column in the Routing &gt; NAT &gt; Masquerading NAT &gt; Rule dialog.</td>
</tr>
<tr>
<td>Rule name</td>
<td>Displays the name of the Masquerading NAT rule. See the Rule name column in the Routing &gt; NAT &gt; Masquerading NAT &gt; Rule dialog.</td>
</tr>
<tr>
<td>Trap</td>
<td>Displays if the device sends an SNTP trap when it applies the Masquerading NAT rule to a data packet. Possible values:</td>
</tr>
<tr>
<td></td>
<td>▶ marked The device sends an SNMP trap.</td>
</tr>
<tr>
<td></td>
<td>▶ unmarked The device does not send an SNMP trap.</td>
</tr>
<tr>
<td></td>
<td>The prerequisite for sending SNMP traps is that you enable the function in the Diagnostics &gt; Status Configuration &gt; Alarms (Traps) dialog and specify at least one trap destination.</td>
</tr>
<tr>
<td>Log</td>
<td>Displays if the device places an entry in the log file when it applies the Masquerading NAT rule to a data packet. Possible values:</td>
</tr>
<tr>
<td></td>
<td>▶ marked When the device applies the Masquerading NAT rule to a data packet, the device places an entry in the log file. See the Diagnostics &gt; Report &gt; System Log dialog.</td>
</tr>
<tr>
<td></td>
<td>▶ unmarked Logging is disabled.</td>
</tr>
</tbody>
</table>
Direction

Displays if the device applies the Masquerading NAT rule to data packets received or sent.

Possible values:

- egress
  The device applies the Masquerading NAT rule to data packets sent on the router interface.

Priority

Displays the priority of the Masquerading NAT rule.

The device applies rules to the data stream in ascending order starting with priority 1.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

7.10.5 Double NAT

The Double NAT function lets you establish communication links between end devices located in different IP networks, which have no way to specify a default gateway or default route. The NAT router virtually “shifts” the devices into the other network. To do this, the NAT router replaces the source address and the destination address in the data packet during sending. A typical application is the linking of controllers located in different networks.

The prerequisite for the Double NAT function is that the NAT router itself responds to ARP requests from the respective network. To make this happen, turn on the ARP proxy function on the ingress interface and on the egress interface.

Figure 9: How the Double NAT function works

To use the NAT function, set up a router interface for each network and turn on the routing function in the device.
The data packets go through the filter functions of the device in the following sequence:

![Diagram showing the processing sequence of data packets in the device]

**Figure 10: Processing sequence of the data packets in the device**

The menu contains the following dialogs:
- Double NAT Rule
- Double NAT Mapping
- Double NAT Overview
### 7.10.5.1 Double NAT Rule

In this dialog you create and edit the Double NAT rules.

You assign the router interfaces to the related Double NAT rule in the Routing > NAT > Double NAT > Mapping dialog.

An overview of which Double NAT rule is assigned to which router interfaces you find in the Routing > NAT > Double NAT > Overview dialog.

#### Table

**Index**

Displays the index number to which the table entry relates.

Possible values:

- 1..255

**Rule name**

Displays the name of the Double NAT rule. To change the name, click the relevant field.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters

**Local internal IP address**

Specifies the actual IP address for the device placed in the first network.

Possible values:

- Valid IPv4 address
  - The device applies the Double NAT rule only to data packets containing the source address specified here.

**Local external IP address**

Specifies the virtual IP address in the second network for the device placed in the first network.

Possible values:

- Valid IPv4 address
  - The device applies the Double NAT rule only to data packets containing the source address specified here.

**Remote internal IP address**

Specifies the actual IP address for the device placed in the second network.

Possible values:

- Valid IPv4 address
  - The device applies the Double NAT rule only to data packets containing the source address specified here.
Remote external IP address

Specifies the virtual IP address in the first network for the device placed in the second network.

Possible values:
- Valid IPv4 address
  - The device applies the Double NAT rule only to data packets containing the source address specified here.

Log

Activates/deactivates the logging in the log file. See the Diagnostics > Report > System Log dialog.

Possible values:
- marked
  - Logging is activated.
  - The device places an entry in the log file when it applies the Double NAT rule to a data packet.
- unmarked (default setting)
  - Logging is deactivated.

Trap

Activates/deactivates the sending of SNMP traps when the Double NAT rule is applied to data packets.

Possible values:
- marked
  - If the device applies the Double NAT rule to a data packet, then the device sends an SNMP trap.
- unmarked (default setting)
  - The sending of SNMP traps is deactivated.

The prerequisite for sending SNMP traps is that you enable the function in the Diagnostics > Status Configuration > Alarms (Traps) dialog and specify at least one trap destination.

Active

Activates/deactivates the Double NAT rule.

Possible values:
- marked
  - The rule is active.
- unmarked (default setting)
  - The rule is inactive.
Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.

- In the Local internal IP address field, you specify the actual IP address for the device placed in the first network.
  Possible values:
  - Valid IPv4 address
    The device applies the Double NAT rule only to data packets containing the source address specified here.

- In the Local external IP address field, you specify the virtual IP address in the second network for the device placed in the first network.
  Possible values:
  - Valid IPv4 address
    The device applies the Double NAT rule only to data packets containing the source address specified here.

- In the Remote internal IP address field, you specify the actual IP address for the device placed in the second network.
  Possible values:
  - Valid IPv4 address
    The device applies the Double NAT rule only to data packets containing the source address specified here.

- In the Remote external IP address field, you specify the virtual IP address in the first network for the device placed in the second network.
  Possible values:
  - Valid IPv4 address
    The device applies the Double NAT rule only to data packets containing the source address specified here.

When you click the Ok button, the device creates the new table entry. The device assigns the values specified in the Local internal IP address, Local external IP address, Remote internal IP address and Remote external IP address fields to this entry.
7.10.5.2 Double NAT Mapping

In this dialog you assign the Double NAT rules to a router interface. To do this, click the button and then the Assign item.

You create and edit the Double NAT rules in the Routing > NAT > Double NAT > Rule.

An overview of which Double NAT rule is assigned to which router interfaces you find in the Routing > NAT > Double NAT > Overview dialog.

**Table**

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the number of the router interface on which the device applies the Double NAT rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule index</td>
<td>Displays the sequential number of the Double NAT rule. See the Index column in the Routing &gt; NAT &gt; Double NAT &gt; Rule dialog.</td>
</tr>
<tr>
<td>Rule name</td>
<td>Displays the name of the Double NAT rule. See the Rule name column in the Routing &gt; NAT &gt; Double NAT &gt; Rule dialog.</td>
</tr>
<tr>
<td>Direction</td>
<td>Displays if the device applies the Double NAT rule to data packets received or sent. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• ingress The device applies the Double NAT rule to data packets received on the router interface.</td>
</tr>
<tr>
<td></td>
<td>• egress The device applies the Double NAT rule to data packets sent on the router interface.</td>
</tr>
<tr>
<td></td>
<td>• both The device applies the Double NAT rule to data packets received or sent on the router interface.</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies the priority of the Double NAT rule. Using the priority, you specify the order in which the device applies several rules to the data stream. The device applies the rules in ascending order starting with priority 1.</td>
</tr>
</tbody>
</table>
Routing
[Routing > NAT > Double NAT > Mapping]

Possible values:
- 1..6500 (default setting: 1)

Active

Activates/deactivates the Double NAT rule.

Possible values:
- marked
  The rule is active.
- unmarked (default setting)
  The rule is inactive.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Assign

Opens the Assign dialog. In this dialog you assign a configured router interface of an existing Double NAT rule.
7.10.5.3 Double NAT Overview

In this dialog you will find an overview of which Double NAT rule is assigned to which router interface.

You create and edit the Double NAT rules in the Routing > NAT > Double NAT > Rule.

You assign the router interfaces to the related Double NAT rule in the Routing > NAT > Double NAT > Mapping dialog.

**Table**

| Port | Displays the number of the router interface on which the device applies the Double NAT rule. |
| Rule index | Displays the sequential number of the Double NAT rule. See the Index column in the Routing > NAT > Double NAT > Rule dialog. |
| Rule name | Displays the name of the Double NAT rule. See the Rule name column in the Routing > NAT > Double NAT > Rule dialog. |
| Local internal IP address | Displays the actual IP address for the device placed in the first network. |
| Local external IP address | Displays the virtual IP address in the second network for the device placed in the first network. |
| Remote internal IP address | Displays the actual IP address for the device placed in the second network. |
| Remote external IP address | Displays the virtual IP address in the first network for the device placed in the second network. |
Routing
[Routing > NAT > Double NAT > Overview]

Trap
Displays if the device sends an SNTP trap when it applies the Double NAT rule to a data packet.

Possible values:
- **marked**
  The device sends an SNMP trap.
- **unmarked**
  The device does not send an SNMP trap.

The prerequisite for sending SNMP traps is that you enable the function in the Diagnostics > Status Configuration > Alarms (Traps) dialog and specify at least one trap destination.

Log
Displays if the device places an entry in the log file when it applies the Double NAT rule to a data packet.

Possible values:
- **marked**
  When the device applies the Double NAT rule to a data packet, the device places an entry in the log file. See the Diagnostics > Report > System Log dialog.
- **unmarked**
  Logging is disabled.

Direction
Displays if the device applies the Double NAT rule to data packets received or sent.

Possible values:
- **ingress**
  The device applies the Double NAT rule to data packets received on the router interface.
- **egress**
  The device applies the Double NAT rule to data packets sent on the router interface.
- **both**
  The device applies the Double NAT rule to data packets received or sent on the router interface.

Priority
Displays the priority of the Double NAT rule.

The device applies rules to the data stream in ascending order starting with priority 1.

**Buttons**

You find the description of the standard buttons in section "Buttons" on page 14.
8Diagnoses

The menu contains the following dialogs:

- Status Configuration
- System
- Syslog
- Ports
- LLDP
- Report

8.1 Status Configuration

The menu contains the following dialogs:

- Device Status
- Security Status
- Signal Contact
- Alarms (Traps)
8.1.1 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.

The device displays detected faults in the Status tab and also in the Basic Settings > System dialog, Device Status frame.

The dialog contains the following tabs:
- [Global]
- [Port]
- [Status]

[Global]

Device status

Displays the current status of the device. The device determines the status from the individual monitored parameters.

Possible values:
- error
  The device displays this value to indicate a detected error in one of the monitored parameters.
- ok

Traps

Send trap

Activates/deactivates the sending of SNMP traps when the device detects changes in the monitored functions.

Possible values:
- marked (default setting)
  The sending of SNMP traps is active.
  If the device detects a change in the monitored functions, then the device sends an SNMP trap.
- unmarked
  The sending of SNMP traps is inactive.

The prerequisite for sending SNMP traps is that you enable the function in the Diagnostics > Status Configuration > Alarms (Traps) dialog and specify at least one trap destination.
## Table

### Temperature

Activates/deactivates the monitoring of the temperature in the device.

Possible values:
- **marked** (default setting)
  - Monitoring is active.
  - If the temperature exceeds or falls below the specified limit, then in the *Device status* frame, the value changes to *error*.
- **unmarked**
  - Monitoring is inactive.

You specify the temperature thresholds in the *Basic Settings > System* dialog, *Upper temp. limit [°C]* field and *Lower temp. limit [°C]* field.

### Connection errors

Activates/deactivates the monitoring of the link status of the port/interface.

Possible values:
- **marked**
  - Monitoring is active.
  - If the link interrupts on a monitored port/interface, then in the *Device status* frame, the value changes to *error*.
  - In the *Port* tab, you have the option of selecting the ports/interfaces to be monitored individually.
- **unmarked** (default setting)
  - Monitoring is inactive.

### External memory removal

Activates/deactivates the monitoring of the active external memory.

Possible values:
- **marked**
  - Monitoring is active.
  - If you remove the active external memory from the device, then in the *Device status* frame, the value changes to *error*.
- **unmarked** (default setting)
  - Monitoring is inactive.

### External memory not in sync

Activates/deactivates the monitoring of the configuration profile in the device and in the external memory.

Possible values:
- **marked**
  - Monitoring is active.
  - In the *Device status* frame, the value changes to *error* in the following situations:
    - The configuration profile only exists in the device.
    - The configuration profile in the device differs from the configuration profile in the external memory.
- **unmarked** (default setting)
  - Monitoring is inactive.
Diagnostics
[Diagnosis > Status Configuration > Device Status]

Power supply
Activates/deactivates the monitoring of the power supply unit.

Possible values:
- **marked** (default setting)
  Monitoring is active.
  If the device has a detected power supply fault, then in the *Device status* frame, the value changes to *error*.
- **unmarked**
  Monitoring is inactive.

**Buttons**
You find the description of the standard buttons in section “Buttons” on page 14.

[Port]

**Table**

Port
Displays the port number.

Propagate connection error
Activates/deactivates the monitoring of the link on the port/interface.

Possible values:
- **marked**
  Monitoring is active.
  If the link on the selected port/interface is interrupted, then in the *Device status* frame, the value changes to *error*.
- **unmarked** (default setting)
  Monitoring is inactive.

This setting takes effect when you mark the *Connection errors* checkbox in the *Global* tab.

**Buttons**
You find the description of the standard buttons in section “Buttons” on page 14.
[Status]

Table

Timestamp

Displays the date and time of the event in the format, *Month Day, Year hh:mm:ss AM/PM*.

Cause

Displays the event which caused the SNMP trap.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
8.1.2 Security Status

This dialog gives you an overview of the status of the safety-relevant settings in the device.

The device displays its current status as **error** or **ok** in the Security status frame. The device determines this status from the individual monitoring results.

The device displays detected faults in the Status tab and also in the Basic Settings > System dialog, Security status frame.

The dialog contains the following tabs:

- [Global]
- [Port]
- [Status]

[Global]

**Security status**

Security status

Displays the current status of the security-relevant settings in the device. The device determines the status from the individual monitored parameters.

Possible values:

- **error**
  The device displays this value to indicate a detected error in one of the monitored parameters.
- **ok**

**Traps**

Send trap

Activates/deactivates the sending of SNMP traps when the device detects changes in the monitored functions.

Possible values:

- **marked**
  The sending of SNMP traps is active. If the device detects a change in the monitored functions, then the device sends an SNMP trap.
- **unmarked** (default setting)
  The sending of SNMP traps is inactive.

The prerequisite for sending SNMP traps is that you enable the function in the Diagnostics > Status Configuration > Alarms (Traps) dialog and specify at least one trap destination.
Table

Password default settings unchanged
Activates/deactivates the monitoring of the password for the locally set up user accounts user and admin.

Possible values:
- **marked** (default setting)
  Monitoring is active.
  If the password is set to the default setting for the user or admin user accounts, then in the Security status frame, the value changes to error.
- **unmarked**
  Monitoring is inactive.

You set the password in the Device Security > User Management dialog.

Min. password length < 8
Activates/deactivates the monitoring of the Min. password length policy.

Possible values:
- **marked** (default setting)
  Monitoring is active.
  If the value for the Min. password length policy is less than 8, then in the Security status frame, the value changes to error.
- **unmarked**
  Monitoring is inactive.

You specify the Min. password length policy in the Device Security > User Management dialog in the Configuration frame.

Password policy settings deactivated
Activates/deactivates the monitoring of the Password policies settings.

Possible values:
- **marked** (default setting)
  Monitoring is active.
  If the value for at least one of the following policies is less than 1, then in the Security status frame, the value changes to error.
  - Upper-case characters (min.)
  - Lower-case characters (min.)
  - Digits (min.)
  - Special characters (min.)
- **unmarked**
  Monitoring is inactive.

You specify the policy settings in the Device Security > User Management dialog in the Password policy frame.
User account password policy check deactivated

Activates/deactivates the monitoring of the *Policy check* function.

Possible values:

- **marked**
  Monitoring is active.
  If the *Policy check* function is inactive for at least one user account, then in the *Security status* frame, the value changes to *error*.

- **unmarked** (default setting)
  Monitoring is inactive.

You activate the *Policy check* function in the *Device Security > User Management* dialog.

HTTP server active

Activates/deactivates the monitoring of the HTTP server.

Possible values:

- **marked** (default setting)
  Monitoring is active.
  If you enable the HTTP server, then in the *Security status* frame, the value changes to *error*.

- **unmarked**
  Monitoring is inactive.

You enable/disable the HTTP server in the *Device Security > Management Access > Server* dialog, *HTTP* tab.

SNMP unencrypted

Activates/deactivates the monitoring of the SNMP server.

Possible values:

- **marked** (default setting)
  Monitoring is active.
  If at least one of the following conditions applies, then in the *Security status* frame, the value changes to *error*:
  - The *SNMPv1* function is enabled.
  - The *SNMPv2* function is enabled.
  - The encryption for SNMPv3 is disabled.
  You enable the encryption in the *Device Security > User Management* dialog, in the *SNMP encryption type* column.

- **unmarked**
  Monitoring is inactive.

You specify the settings for the SNMP agent in the *Device Security > Management Access > Server* dialog, *SNMP* tab.

Access to system monitor with serial interface possible

Activates/deactivates the monitoring of the system monitor.

When the system monitor is activated, you have the possibility to change to the system monitor via a serial connection.
Possible values:

- **marked**
  Monitoring is active.
  If you activate the system monitor, then in the Security status frame, the value changes to error.

- **unmarked** (default setting)
  Monitoring is inactive.

You activate/deactivate the system monitor in the Diagnostics > System > Selftest dialog.

**Saving the configuration profile on the external memory possible**

Activates/deactivates the monitoring of the configuration profile in the external memory.

Possible values:

- **marked**
  Monitoring is active.
  If you activate the saving of the configuration profile in the external memory, then in the Security status frame, the value changes to error.

- **unmarked** (default setting)
  Monitoring is inactive.

You activate/deactivate the saving of the configuration profile in the external memory in the Basic Settings > External Memory dialog.

**Link interrupted on enabled device ports**

Activates/deactivates the monitoring of the link on the active ports.

Possible values:

- **marked**
  Monitoring is active.
  If the link interrupts on an active port, then in the Security status frame, the value changes to error. In the Port tab, you have the option of selecting the ports to be monitored individually.

- **unmarked** (default setting)
  Monitoring is inactive.

**Access with HiDiscovery possible**

Activates/deactivates the monitoring of the HiDiscovery function.

Possible values:

- **marked** (default setting)
  Monitoring is active.
  If you enable the HiDiscovery function, then in the Security status frame, the value changes to error.

- **unmarked**
  Monitoring is inactive.

You enable/disable the HiDiscovery function in the Basic Settings > Network dialog.
Load unencrypted config from external memory

Activates/deactivates the monitoring of loading unencrypted configuration profiles from the external memory.

Possible values:

- **marked** (default setting)
  Monitoring is active.
  If the settings allow the device to load an unencrypted configuration profile from the external memory, then in the *Security status* frame, the value changes to *error*.
  If the following preconditions are fulfilled, then the *Security status* frame in the *Basic Settings > System* dialog, displays an alarm.
  - The configuration profile stored in the external memory is unencrypted.
  - The *Config priority* column in the *Basic Settings > External Memory* dialog has the value *first*.
- **unmarked**
  Monitoring is inactive.

Self-signed HTTPS certificate present

Activates/deactivates the monitoring of the HTTPS certificate.

Possible values:

- **marked** (default setting)
  Monitoring is active.
  If the HTTPS server uses a self-created digital certificate, then in the *Security status* frame, the value changes to *error*.
- **unmarked**
  Monitoring is inactive.

### Buttons

You find the description of the standard buttons in section "Buttons" on page 14.

**[Port]**

### Table

<table>
<thead>
<tr>
<th>Port</th>
</tr>
</thead>
</table>

Displays the port number.
Link interrupted on enabled device ports

Activates/deactivates the monitoring of the link on the active ports.

Possible values:

- **marked**
  Monitoring is active.
  If the port is enabled (Basic Settings > Port dialog, Configuration tab, Port on checkbox is marked) and the link is down on the port, then in the Security status frame, the value changes to error.

- **unmarked** (default setting)
  Monitoring is inactive.

This setting takes effect when you mark the Link interrupted on enabled device ports checkbox in the Diagnostics > Status Configuration > Security Status dialog, Global tab.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

[Status]

**Table**

**Timestamp**

Displays the date and time of the event in the format, Month Day, Year hh:mm:ss AM/PM.

**Cause**

Displays the event which caused the SNMP trap.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

8.1.3 **Signal Contact**

The signal contact is a potential-free relay contact. The device thus lets you perform remote diagnosis. The device uses the relay contact to signal the occurrence of events by opening the relay contact and interrupting the closed circuit.

**Note:** The device can contain several signal contacts. Each contact contains the same monitoring functions. Several contacts allow you to group various functions together providing flexibility in system monitoring.
The menu contains the following dialogs:

- Signal Contact 1 / Signal Contact 2
8.1.3.1 Signal Contact 1 / Signal Contact 2

In this dialog you specify the trigger conditions for the signal contact.

The signal contact gives you the following options:
- Monitoring the correct operation of the device.
- Signaling the device status of the device.
- Signaling the security status of the device.
- Controlling external devices by manually setting the signal contacts.

The device displays detected faults in the Status tab and also in the Basic Settings > System dialog, Signal contact status frame.

The dialog contains the following tabs:
- [Global]
- [Port]
- [Status]

[Global]

Configuration

Mode

Specifies which events the signal contact indicates.

Possible values:
- Manual setting  (default setting for Signal Contact 2, if present)
  You use this setting to manually open or close the signal contact, for example to turn on or off a remote device. See the Contact option list.
- Monitoring correct operation  (default setting)
  Using this setting the signal contact indicates the status of the parameters specified in the table below.
- Device status
  Using this setting the signal contact indicates the status of the parameters monitored in the Diagnostics > Status Configuration > Device Status dialog. In addition, you can read the status in the Signal contact status frame.
- Security status
  Using this setting the signal contact indicates the status of the parameters monitored in the Diagnostics > Status Configuration > Security Status dialog. In addition, you can read the status in the Signal contact status frame.
- Device/Security status
  Using this setting the signal contact indicates the status of the parameters monitored in the Diagnostics > Status Configuration > Device Status and the Diagnostics > Status Configuration > Security Status dialog. In addition, you can read the status in the Signal contact status frame.
Contact

Toggles the signal contact manually. The prerequisite is that in the *Mode* drop-down list you select the *Manual setting* item.

Possible values:

- **open**
  - The signal contact is opened.

- **close**
  - The signal contact is closed.

**Signal contact status**

Displays the current status of the signal contact.

Possible values:

- **Opened (error)**
  - The signal contact is opened. The circuit is interrupted.

- **Closed (ok)**
  - The signal contact is closed. The circuit is closed.

**Trap configuration**

Send trap

Activates/deactivates the sending of SNMP traps when the device detects changes in the monitored functions.

Possible values:

- **marked**
  - The sending of SNMP traps is active.
  - If the device detects a change in the monitored functions, then the device sends an SNMP trap.

- **unmarked** (default setting)
  - The sending of SNMP traps is inactive.

The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least one trap destination.
Monitoring correct operation

In the table you specify the parameters that the device monitors. The device signals the occurrence of an event by opening the signal contact.

Connection errors

Activates/deactivates the monitoring of the link status of the port/interface.

Possible values:

- **marked** (default setting)
  Monitoring is active.
  If the link interrupts on a monitored port/interface, then the signal contact opens.
  In the Port tab, you have the option of selecting the ports/interfaces to be monitored individually.

- **unmarked**
  Monitoring is inactive.

Temperature

Activates/deactivates the monitoring of the temperature in the device.

Possible values:

- **marked** (default setting)
  Monitoring is active.
  If the temperature exceeds / falls below the threshold values, then the signal contact opens.

- **unmarked**
  Monitoring is inactive.

You specify the temperature thresholds in the Basic Settings > System dialog, Upper temp. limit [°C] field and Lower temp. limit [°C] field.

External memory removed

Activates/deactivates the monitoring of the active external memory.

Possible values:

- **marked**
  Monitoring is active.
  If you remove the active external memory from the device, then the signal contact opens.

- **unmarked** (default setting)
  Monitoring is inactive.

External memory not in sync with NVM

Activates/deactivates the monitoring of the configuration profile in the device and in the external memory.

Possible values:

- **marked**
  Monitoring is active.
  The signal contact opens in the following situations:
    - The configuration profile only exists in the device.
    - The configuration profile in the device differs from the configuration profile in the external memory.

- **unmarked** (default setting)
  Monitoring is inactive.
Power supply

Activates/deactivates the monitoring of the power supply unit.

Possible values:

- **marked** (default setting)
  - Monitoring is active.
  - If the device has a detected power supply fault, then the signal contact opens.

- **unmarked**
  - Monitoring is inactive.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Table

Port

Displays the port number.

Propagate connection error

Activates/deactivates the monitoring of the link on the port/interface.

Possible values:

- **marked**
  - Monitoring is active.
  - If the link interrupts on the selected port/interface, then the signal contact opens.

- **unmarked** (default setting)
  - Monitoring is inactive.

This setting takes effect when you mark the Connection errors checkbox in the Global tab.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
### Status

#### Table

**Timestamp**
Displays the date and time of the event in the format, *Month Day, Year hh:mm:ss AM/PM*.

**Cause**
Displays the event which caused the SNMP trap.

#### Buttons
You find the description of the standard buttons in section “Buttons” on page 14.

### 8.1.4 Alarms (Traps)

The device lets you send an SNMP trap as a reaction to specific events. In this dialog you specify the trap destinations to which the device sends the SNMP traps.

The events for which the device triggers an SNMP trap, you specify, for example, in the following dialogs:
- in the *Diagnostics > Status Configuration > Device Status* dialog
- in the *Diagnostics > Status Configuration > Security Status* dialog

When loopback interfaces are set up, the device uses the IP address of the 1st loopback interface as the source of the SNMP traps. Otherwise, the device uses the address of the device management.

#### Operation

**Operation**
Enables/disables the sending of SNMP traps to the trap destinations.

Possible values:
- **On** *(default setting)*
  - The sending of SNMP traps is enabled.
- **Off**
  - The sending of SNMP traps is disabled.
## Table

### Name

Specifies the name of the trap destination.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters

### Address

Specifies the IP address and the port number of the trap destination.

Possible values:

- `<Valid IPv4 address>:<port number>`

### Active

Activates/deactivates the sending of SNMP traps to this trap destination.

Possible values:

- **marked** (default setting)
  - The sending of SNMP traps to this trap destination is active.
- **unmarked**
  - The sending of SNMP traps to this trap destination is inactive.

## Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Opens the Create window to add a new entry to the table.

- In the **Name** field you specify a name for the trap destination.
- In the **Address** field you specify the IP address and the port number of the trap destination.
  
  If you choose not to enter a port number, then the device automatically adds the port number 162.
8.2  **System**

The menu contains the following dialogs:
- System Information
- Configuration Check
- ARP
- Selftest
8.2.1 System Information

This dialog displays the current operating condition of individual components in the device. The displayed values are a snapshot; they represent the operating condition at the time the dialog was loaded to the page.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Save system information

Opens the HTML page in a new web browser window or tab. You can save the HTML page on your PC using the appropriate web browser command.
8.2.2 Configuration Check

The device lets you compare the settings in the device with the settings in its neighboring devices. For this purpose, the device uses the information that it received from its neighboring devices through 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 content of the table by clicking the button. When the table remains empty, the configuration check was successful and the settings in the device are compatible with the settings in the detected neighboring devices.

If you have set up more than 39 VLANs in the device, then the dialog constantly displays a warning. The reason is the limited number of possible VLAN data sets in LLDP packets with a maximum length. The device compares the first 39 VLANs automatically. If you have set up 40 or more VLANs in the device, then check the congruence of the further VLANs manually, if necessary.

Note: The dialog displays the devices detected as connected to the neighboring device as if they were directly connected to the device itself.

Summary

You also find this information when you position the mouse pointer over the button in the Toolbar in the top part of the Navigation area.

Error

Displays the number of errors that the device detected during the configuration check.

Warning

Displays the number of warnings that the device detected during the configuration check.

Information

Displays the amount of information that the device detected during the configuration check.

Table

When you highlight a row in the table, the device displays additional information in the area beneath it.

ID

Displays the rule ID of the deviations having occurred. The dialog combines several deviations with the same rule ID under one rule ID.
Diagnostics
[Diagnostics > System > Configuration Check]

Level
Displays the level of deviation between the settings in this device and the settings in the detected neighboring devices.

The device differentiates between the following access statuses:

▶ INFORMATION
  The performance of the communication between the two devices is not impaired.

▶ WARNING
  The performance of the communication between the two devices is possibly impaired.

▶ ERROR
  The communication between the two devices is impaired.

Message
Displays the information, warnings and errors having occurred more precisely.

Buttons
You find the description of the standard buttons in section “Buttons” on page 14.
8.2.3 **ARP**

This dialog displays the MAC and IP addresses of the neighboring devices connected to the device management.

**Table**

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>Displays the IPv4 address of a neighboring device.</td>
</tr>
<tr>
<td>MAC address</td>
<td>Displays the MAC address of a neighboring device.</td>
</tr>
<tr>
<td>Last updated</td>
<td>Displays the time in seconds since the current settings of the entry were registered in the ARP table.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the type of the entry. Possible values:</td>
</tr>
<tr>
<td></td>
<td>static</td>
</tr>
<tr>
<td></td>
<td>dynamic</td>
</tr>
<tr>
<td>Active</td>
<td>Displays that the ARP table contains the IP/MAC address assignment as an active entry.</td>
</tr>
</tbody>
</table>

**Buttons**

You find the description of the standard buttons in section "Buttons" on page 14.

Reset ARP table

Removes the dynamically set up addresses from the ARP table.
8.2.4 Selftest

This dialog lets you do the following:
- Enable/disable the option of entering the system monitor upon the system start.
- Specify how the device behaves in the case of an error.

Configuration

If the device does not detect any readable configuration profile when restarting, then the following settings block your access to the device permanently.
- **SysMon1 is available** checkbox is **unmarked**.
- **Load default config on error** checkbox is **unmarked**.

This is the case, for example, if the password of the configuration profile that you are loading differs from the password set in the device. To have the device unlocked again, contact your sales partner.

**SysMon1 is available**

Activates/deactivates the access to the system monitor during the restart.

Possible values:
- **marked** (default setting)
  - The device lets you open the system monitor during the restart.
- **unmarked**
  - The device starts without the option of opening to the system monitor.

Among other things, the system monitor lets you update the device software and to delete saved configuration profiles.

**Load default config on error**

Activates/deactivates the loading of the default settings if the device does not detect any readable configuration profile when restarting.

Possible values:
- **marked** (default setting)
  - The device loads the default settings.
- **unmarked**
  - The device interrupts the restart and stops. The access to the device management is possible only using the Command Line Interface through the serial interface. To regain the access to the device through the network, open the system monitor and reset the settings. Upon restart, the device loads the default settings.
Table

In this table you specify how the device behaves in the case of an error.

Cause

Error causes to which the device reacts.

Possible values:

- **task**
  The device detects errors in the applications executed, for example if a task terminates or is not available.

- **resource**
  The device detects errors in the resources available, for example if the memory is becoming scarce.

- **software**
  The device detects software errors, for example error in the consistency check.

- **hardware**
  The device detects hardware errors, for example in the chip set.

Action

Specifies how the device behaves if the adjacent event occurs.

Possible values:

- **reboot** (default setting)
  The device triggers a restart.

- **logOnly**
  The device registers the detected error in the log file. See the Diagnostics > Report > System Log dialog.

- **sendTrap**
  The device sends an SNMP trap.
  The prerequisite for sending SNMP traps is that you enable the function in the Diagnostics > Status Configuration > Alarms (Traps) dialog and specify at least one trap destination.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
8.3 Syslog

The device lets you report selected events, independent of the severity of the event, to different syslog servers. In this dialog you specify the settings for this function and manage up to 8 syslog servers.

Operation

Operation enables/disables the sending of events to the syslog servers.

Possible values:
- **On** (default setting) - The sending of events is enabled. The device sends the events specified in the table to the specified syslog servers.
- **Off** - The sending of events is disabled.

Table

Index displays the index number to which the table entry relates.

When you delete a table entry, this leaves a gap in the numbering. When you create a new table entry, the device fills the first gap.

Possible values:
- 1..8

IP address

Specifies the IP address of the syslog server.

Possible values:
- Valid IPv4 address (default setting: **0.0.0.0**)
- Hostname
Destination UDP port

Specifies the UDP port on which the syslog server expects the log entries.

Possible values:
- 1..65535 (default setting: 514)

Min. severity

Specifies the minimum severity of the events. The device sends a log entry for events with this severity and with more urgent severities to the syslog server.

Possible values:
- emergency
- alert
- critical
- error
- warning (default setting)
- notice
- informational
- debug

Type

Specifies the type of the log entry transmitted by the device.

Possible values:
- systemlog (default setting)
- audittrail

Active

Activates/deactivates the transmission of events to the syslog server:
- marked
  The device sends events to the syslog server.
- unmarked (default setting)
  The transmission of events to the syslog server is deactivated.

Buttons

You find the description of the standard buttons in section “Buttons" on page 14.
8.4 Ports

The menu contains the following dialogs:

▶ SFP
8.4.1 SFP

This dialog lets you look at the SFP transceivers currently connected to the device and their properties.

**Table**

The table displays valid values if the device is equipped with SFP transceivers.

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module type</td>
<td>Type of the SFP transceiver, for example M-SFP-SX/LC.</td>
</tr>
<tr>
<td>Serial number</td>
<td>Displays the serial number of the SFP transceiver.</td>
</tr>
<tr>
<td>Connector type</td>
<td>Displays the connector type.</td>
</tr>
<tr>
<td>Supported</td>
<td>Displays if the device supports the SFP transceiver.</td>
</tr>
<tr>
<td>Temperature [°C]</td>
<td>Operating temperature of the SFP transceiver in °Celsius.</td>
</tr>
<tr>
<td>Tx power [mW]</td>
<td>Transmission power of the SFP transceiver in mW.</td>
</tr>
<tr>
<td>Rx power [mW]</td>
<td>Receiving power of the SFP transceiver in mW.</td>
</tr>
<tr>
<td>Tx power [dBm]</td>
<td>Transmission power of the SFP transceiver in dBm.</td>
</tr>
<tr>
<td>Rx power [dBm]</td>
<td>Receiving power of the SFP transceiver in dBm.</td>
</tr>
</tbody>
</table>
Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

8.5 LLDP

The device lets you gather information about neighboring devices. For this, the device uses the Link Layer Discovery Protocol (LLDP). This information enables a network management station to map the structure of your network.

This menu lets you configure the topology discovery and to display the information received in table form.

The menu contains the following dialogs:
- LLDP Configuration
- LLDP Topology Discovery
8.5.1 LLDP Configuration

This dialog lets you configure the topology discovery for every port.

**Operation**

Enables/disables the LLDP function.

Possible values:
- **On** (default setting)
  The LLDP function is enabled.
  The topology discovery using LLDP is active in the device.
- **Off**
  The LLDP function is disabled.

**Configuration**

**Transmit interval [s]**

Specifies the interval in seconds at which the device transmits LLDP data packets.

Possible values:
- 5..32768 (default setting: 30)

**Transmit interval multiplier**

Specifies the factor for determining the time-to-live value for the LLDP data packets.

Possible values:
- 2..10 (default setting: 4)

The time-to-live value coded in the LLDP header results from multiplying this value with the value in the **Transmit interval [s]** field.

**Reinit delay [s]**

Displays the delay in seconds for the reinitialization of a port.

If in the **Operation** column the value **off** is specified, then the device tries to reinitialize the port after the time specified here has elapsed.

**Transmit delay [s]**

Displays the delay in seconds for transmitting successive LLDP data packets after configuration changes in the device occur.
Notification interval [s]

Specifies the interval in seconds for transmitting LLDP notifications.

Possible values:
- **5..3600**  (default setting: 5)

After transmitting a notification trap, the device waits for a minimum of the time specified here before transmitting the next notification trap.

**Table**

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
</table>

**Operation**

Specifies if the port transmits and receives LLDP data packets.

Possible values:
- **transmit**  The port transmits LLDP data packets but does not save any information about neighboring devices.
- **receive**  The port receives LLDP data packets but does not transmit any information to neighboring devices.
- **receive and transmit**  (default setting)  The port transmits LLDP data packets and saves information about neighboring devices.
- **disabled**  The port does not transmit LLDP data packets and does not save information about neighboring devices.

**Notification**

Activates/deactivates the LLDP notifications on the port.

Possible values:
- **marked**  LLDP notifications are active on the port.
- **unmarked**  (default setting)  LLDP notifications are inactive on the port.

**Transmit port description**

Activates/deactivates the transmitting of a TLV (Type Length Value) with the port description.

Possible values:
- **marked**  (default setting)  The transmitting of the TLV is active.
  The device transmits the TLV with the port description.
- **unmarked**  The transmitting of the TLV is inactive.
  The device does not transmit a TLV with the port description.
Transmit system name

Activates/deactivates the transmitting of a TLV (Type Length Value) with the device name.

Possible values:
- **marked** (default setting)
  - The transmitting of the TLV is active.
  - The device transmits the TLV with the device name.
- **unmarked**
  - The transmitting of the TLV is inactive.
  - The device does not transmit a TLV with the device name.

Transmit system description

Activates/deactivates the transmitting of the TLV (Type Length Value) with the system description.

Possible values:
- **marked** (default setting)
  - The transmitting of the TLV is active.
  - The device transmits the TLV with the system description.
- **unmarked**
  - The transmitting of the TLV is inactive.
  - The device does not transmit a TLV with the system description.

Transmit system capabilities

Activates/deactivates the transmitting of the TLV (Type Length Value) with the system capabilities.

Possible values:
- **marked** (default setting)
  - The transmitting of the TLV is active.
  - The device transmits the TLV with the system capabilities.
- **unmarked**
  - The transmitting of the TLV is inactive.
  - The device does not transmit a TLV with the system capabilities.

Neighbors (max.)

Limits the number of neighboring devices to be recorded for this port.

Possible values:
- **1..50** (default setting: 10)

FDB mode

Specifies which function the device uses to record neighboring devices on this port.

Possible values:
- **lldpOnly**
  - The device uses only LLDP data packets to record neighboring devices on this port.
- **macOnly**
  - The device uses learned MAC addresses to record neighboring devices on this port. The device uses the MAC address only if there is no other entry in the address table (FDB, Forwarding Database) for this port.
The device uses LLDP data packets and learned MAC addresses to record neighboring devices on this port.

**autoDetect** (default setting)
If the device receives LLDP data packets at this port, then the device operates the same as with the `lldpOnly` setting. Otherwise, the device operates the same as with the `macOnly` setting.

**Buttons**

You find the description of the standard buttons in section "Buttons" on page 14.
### 8.5.2 LLDP Topology Discovery

Devices in networks send notifications in the form of packets which are also known as "LLDPDU" (LLDP data units). The data that is sent and received via LLDPDU are useful for many reasons. Thus the device detects which devices in the network are neighbors and via which ports they are connected.

The dialog lets you display the network and to detect the connected devices along with their specific features.

This dialog displays the collected LLDP information for the neighboring devices. This information enables a network management station to map the structure of your network.

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 contains one line for this port to represent every device. This line contains the number of connected devices.

The Forwarding Database (FDB) address table contains MAC addresses of devices that the topology table hides for the sake of clarity.

When you use one port to connect several devices, for example via a hub, the table contains one line for each connected device.

#### Table

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor identifier</td>
<td>Displays the chassis ID of the neighboring device. This can be the basis MAC address of the neighboring device, for example.</td>
</tr>
<tr>
<td>FDB</td>
<td>Displays if the connected device has active LLDP support. Possible values:</td>
</tr>
<tr>
<td>- marked</td>
<td>The connected device does not have active LLDP support. The device uses information from its address table (FDB, Forwarding Database)</td>
</tr>
<tr>
<td>- unmarked (default setting)</td>
<td>The connected device has active LLDP support.</td>
</tr>
<tr>
<td>Neighbor IP address</td>
<td>Displays the IP address with which the access to the neighboring device management is possible.</td>
</tr>
</tbody>
</table>
8.6 Report

[Diagnoses > Report]

The menu contains the following dialogs:

- Report Global
- Persistent Logging
- System Log
- Audit Trail
8.6.1 Report Global

The device lets you log specific events using the following outputs:

- on the console
- on one or more syslog servers
- on a connection to the Command Line Interface set up using SSH

In this dialog you specify the required settings. By assigning the severity you specify which events the device registers.

The dialog lets you save a ZIP archive with system information on your PC.

**Console logging**

**Operation**

Enables/disables the Console logging function.

Possible values:

- **On**
  - The Console logging function is enabled.
  - The device logs the events on the console.

- **Off** (default setting)
  - The Console logging function is disabled.

**Severity**

Specifies the minimum severity for the events. The device logs events with this severity and with more urgent severities.

The device outputs the messages on the serial interface.

Possible values:

- emergency
- alert
- critical
- error
- warning (default setting)
- notice
- informational
- debug
Buffered logging

The device buffers logged events in 2 separate storage areas so that the log entries for urgent events are kept.

This dialog lets you specify the minimum severity for events that the device buffers in the storage area with a higher priority.

Severity

Specifies the minimum severity for the events. The device buffers log entries for events with this severity and with more urgent severities in the storage area with a higher priority.

Possible values:

- emergency
- alert
- critical
- error
- warning (default setting)
- notice
- informational
- debug

SNMP logging

When you enable the logging of SNMP requests, the device sends these as events with the preset severity notice to the list of syslog servers. The preset minimum severity for a syslog server entry is critical.

To send SNMP requests to a syslog server, you have a number of options to change the default settings. Select the ones that meet your requirements best.

- Set the severity for which the device creates SNMP requests as events to warning or error. Change the minimum severity for a syslog entry for one or more syslog servers to the same value.
  
  You also have the option of creating a separate syslog server entry for this.

- Set only the severity for SNMP requests to critical or higher. The device then sends SNMP requests as events with the severity critical or higher to the syslog servers.

- Set only the minimum severity for one or more syslog server entries to notice or lower. Then it is possible that the device sends many events to the syslog servers.

Log SNMP get request

Enables/disables the logging of SNMP Get requests.

Possible values:

- On
  
  The logging is enabled.
  
  The device registers SNMP Get requests as events in the syslog.
  
  In the Severity get request drop-down list, you select the severity for this event.

- Off (default setting)
  
  The logging is disabled.
Log SNMP set request

Enables/disables the logging of SNMP Set requests.

Possible values:

- **On**
  The logging is enabled. The device registers SNMP Set requests as events in the syslog.
  In the *Severity set request* drop-down list, you select the severity for this event.

- **Off** (default setting)
  The logging is disabled.

Severity get request

Specifies the severity of the event that the device registers for SNMP Get requests.

Possible values:

- emergency
- alert
- critical
- error
- warning
- notice (default setting)
- informational
- debug

Severity set request

Specifies the severity of the event that the device registers for SNMP Set requests.

Possible values:

- emergency
- alert
- critical
- error
- warning
- notice (default setting)
- informational
- debug
CLI logging

Operation

Enables/disables the **CLI logging** function.

Possible values:

- **On**
  The **CLI logging** function is enabled.
  The device logs every command received using the Command Line Interface.

- **Off** (default setting)
  The **CLI logging** function is disabled.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Download support information

Generates a ZIP archive which the web browser lets you download from the device.

The ZIP archive contains system information about the device. You will find an explanation of the files contained in the ZIP archive in the following section.

Support Information: Files contained in ZIP archive

<table>
<thead>
<tr>
<th>File name</th>
<th>Format</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>audittrail.html</td>
<td>HTML</td>
<td>Contains the chronological recording of the system events and saved user changes in the Audit Trail.</td>
</tr>
<tr>
<td>defaultconfig.xml</td>
<td>XML</td>
<td>Contains the configuration profile with the default settings.</td>
</tr>
<tr>
<td>script</td>
<td>TEXT</td>
<td>Contains the output of the command <code>show running-config script</code>.</td>
</tr>
<tr>
<td>runningconfig.xml</td>
<td>XML</td>
<td>Contains the configuration profile with the current operating settings.</td>
</tr>
<tr>
<td>supportinfo.html</td>
<td>TEXT</td>
<td>Contains device internal service information.</td>
</tr>
<tr>
<td>systeminfo.html</td>
<td>HTML</td>
<td>Contains information about the current settings and operating parameters.</td>
</tr>
<tr>
<td>systemlog.html</td>
<td>HTML</td>
<td>Contains the logged events in the Log file. See the Diagnostics &gt; Report &gt; System Log dialog.</td>
</tr>
</tbody>
</table>

Meaning of the event severities

<table>
<thead>
<tr>
<th>Severity</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>emergency</td>
<td>Device not ready for operation</td>
</tr>
<tr>
<td>alert</td>
<td>Immediate user intervention required</td>
</tr>
<tr>
<td>critical</td>
<td>Critical status</td>
</tr>
<tr>
<td>Severity</td>
<td>Meaning</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>error</td>
<td>Error status</td>
</tr>
<tr>
<td>warning</td>
<td>Warning</td>
</tr>
<tr>
<td>notice</td>
<td>Significant, normal status</td>
</tr>
<tr>
<td>informational</td>
<td>Informal message</td>
</tr>
<tr>
<td>debug</td>
<td>Debug message</td>
</tr>
</tbody>
</table>
8.6.2 Persistent Logging

The device lets you save log entries permanently in a file in the external memory. Therefore, even after the device is restarted you have access to the log entries.

In this dialog you limit the size of the log file and specify the minimum severity for the events to be saved. When the log file reaches the specified size, the device archives this file and saves the following log entries in a newly created file.

In the table the device displays you the log files held in the external memory. As soon as the specified maximum number of files has been attained, the device deletes the oldest file and renames the remaining files. This helps ensure that there is enough memory space in the external memory.

**Note:** Verify that an external memory is connected. To verify if an external memory is connected, see the **Status** column in the **Basic Settings > External Memory** dialog. We recommend to monitor the external memory connection using the **Device Status** function, see the **External memory removal** parameter in the **Diagnostics > Status Configuration > Device Status** dialog.

**Operation**

**Enables/disables the Persistent Logging function.**

Only activate this function if the external memory is available in the device.

**Possible values:**

- **On** *(default setting)*
  
  The **Persistent Logging** function is enabled.
  
  The device saves the log entries in a file in the external memory.

- **Off**
  
  The **Persistent Logging** function is disabled.

**Configuration**

**Max. file size [kbyte]**

Specifies the maximum size of the log file in KBytes. When the log file reaches the specified size, the device archives this file and saves the following log entries in a newly created file.

**Possible values:**

- **0..4096** *(default setting: 1024)*
  
  The value 0 deactivates saving of log entries in the log file.
Files (max.)

Specifies the number of log files that the device keeps in the external memory.

As soon as the specified maximum number of files has been attained, the device deletes the oldest file and renames the remaining files.

Possible values:
- 0..25 (default setting: 4)

The value 0 deactivates saving of log entries in the log file.

Severity

Specifies the minimum severity of the events. The device saves the log entry for events with this severity and with more urgent severities in the log file in the external memory.

Possible values:
- emergency
- alert
- critical
- error
- warning (default setting)
- notice
- informational
- debug

Log file target

Specifies the external memory device for logging.

Possible values:
- usb

External USB memory (ACA21/ACA22)

Table

Index

Displays the index number to which the table entry relates.

Possible values:
- 1..25

The device automatically assigns this number.
File name

Displays the file name of the log file in the external memory.

Possible values:
- messages
- messages.X

File size [byte]

Displays the size of the log file in the external memory in bytes.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

Delete persistent log file

Removes the log files from the external memory.
8.6.3 **System Log**

The device logs device-internal events in a log file (System Log).

This dialog displays the log file (System Log). The dialog lets you save the log file in HTML format on your PC.

In order to search the log file for search terms, use the search function of your web browser.

The log file is kept until a restart is performed in the device. After the restart the device creates the file again.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

- **Save log file**
  
  Opens the HTML page in a new web browser window or tab. You can save the HTML page on your PC using the appropriate web browser command.

- **Delete log file**
  
  Removes the logged events from the log file.
**8.6.4 Audit Trail**

This dialog displays the log file (Audit Trail). The dialog lets you save the log file as an HTML file on your PC.

In order to search the log file for search terms, use the search function of your web browser.

The device logs system events and writing user actions in the device. This lets you keep track of WHO changes WHAT in the device and WHEN. The prerequisite is that the user role auditor or administrator is assigned to your user account.

The device logs the following user actions, among others:
- A user logging in with the Command Line Interface (local or remote)
- A user logging off manually
- Automatic logging off of a user in the Command Line Interface after a specified period of inactivity
- Device restart
- Locking of a user account due to too many unsuccessful login attempts
- Locking of the access to the device management due to unsuccessful login attempts
- Commands executed in the Command Line Interface, apart from `show commands`
- Changes to configuration variables
- Changes to the system time
- File transfer operations, including firmware updates
- Configuration changes via HiDiscovery
- Firmware updates and automatic configuration of the device via the external memory
- Opening and closing of SNMP via an HTTPS tunnel

The device does not log passwords. The logged entries are write-protected and remain saved in the device after a restart.

**Note:** During the restart, access to the system monitor is possible using the default settings of the device. If an attacker gains physical access to the device, then he is able to reset the device settings to its default values using the system monitor. After this, the device and log file are accessible using the standard password. Take appropriate measures to restrict physical access to the device. Otherwise, deactivate access to the system monitor. See the Diagnostics > System > Selftest dialog, **SysMon1 is available** checkbox.

**Buttons**

You find the description of the standard buttons in section "Buttons" on page 14.
9 Advanced

The menu contains the following dialogs:

- DNS
- Command Line Interface

9.1 DNS

The menu contains the following dialogs:

- DNS Client
- DNS Cache

9.1.1 DNS Client

DNS (Domain Name System) is a service in the network that translates host names into IP addresses. This name resolution lets you contact other devices using their host names instead of their IP addresses.

The Client function enables the device to send requests for resolving hostnames in IP addresses to a DNS server.

The menu contains the following dialogs:

- DNS Client Global
- DNS Client Current
- DNS Client Static
9.1.1.1 DNS Client Global

In this dialog you enable the Client function.

**Operation**

Enables/disables the Client function.

Possible values:

- **On**
  The Client function is enabled.
  The device sends requests for resolving hostnames in IP addresses to a DNS server.

- **Off** (default setting)
  The Client function is disabled.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.
9.1.1.2 DNS Client Current

This dialog displays to which DNS servers the device sends requests for resolving hostnames in IP addresses.

Table

<table>
<thead>
<tr>
<th>Index</th>
<th>Displays the sequential number of the DNS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Displays the IP address of the DNS server. The device forwards requests for resolving host names in IP addresses to the DNS server with this IP address.</td>
</tr>
</tbody>
</table>

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.
9.1.1.3 DNS Client Static

In this dialog you specify the DNS servers to which the device forwards requests for resolving host names in IP addresses.

The device lets you specify up to 4 IP addresses.

Configuration

Configuration source

Specifies the source from which the device obtains the IP address of DNS servers to which the device addresses requests.

Possible values:

- user
  The device uses the IP addresses specified in the table.

Table

Index

Displays the sequential number of the DNS server.

The device lets you specify up to 4 DNS servers.

Address

Specifies the IP address of the DNS server.

Possible values:

- Valid IPv4 address (default setting: 0.0.0.0)

Active

Activates/deactivates the table entry.

The device sends requests to the DNS server configured in the first active table entry. When the device does not receive a response from this server, it sends requests to the DNS server configured in the next active table entry.

Possible values:

- marked
  The DNS client sends requests to this DNS server.
  Prerequisites:
  □ Enable the DNS-client function in the Advanced > DNS > Global dialog.
  □ Select in the Configuration frame, Configuration source drop-down-list the value user.
- unmarked (default setting)
  The device does not send requests to this DNS server.
9.1.2 DNS Cache

The Cache function enables the device to respond to requests for resolving hostnames in IP addresses.

The menu contains the following dialogs:

- DNS Cache Global
9.1.2.1 DNS Cache Global

In this dialog you enable the Cache function. When the Cache function is enabled, the device operates as a Caching DNS server.

When a downstream device requests the IP address of an unknown hostname and the Caching DNS server finds a matching entry in its cache, the Caching DNS server returns the IP address.

The cache provides memory space for up to 128 hostnames with associated IP address.

Operation

Enables/disables the Cache function.

Possible values:

- **On** (default setting)
  - The Cache function is enabled.
- **Off**
  - The Cache function is disabled.

Buttons

You find the description of the standard buttons in section “Buttons” on page 14.

Flush cache

Removes every entry from the DNS cache.

9.2 Command Line Interface

This dialog lets you access the device using the Command Line Interface.

The prerequisites are:

- In the device, enable the SSH server in the Device Security > Management Access > Server dialog, tab SSH.
- On your workstation, install a SSH-capable client application which registers a handler for URLs starting with ssh:// in your operating system.
**Buttons**

You find the description of the standard buttons in section “Buttons” on page 14.

**Open SSH connection**

Opens the SSH-capable client application.

When you click the button, the web application passes the URL of the device starting with `ssh://` and the user name of the currently logged in user.

If the web browser finds a SSH-capable client application, then the SSH-capable client establishes a connection to the device using the SSH protocol.
## A  Index

<table>
<thead>
<tr>
<th>0-9</th>
<th>1to1 NAT</th>
<th>802.1D/p mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A</th>
<th>Access restriction</th>
<th>Aging time</th>
<th>Alarms</th>
<th>ARP</th>
<th>ARP table</th>
<th>Audit trail</th>
<th>Authentication list</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C</th>
<th>Certificate</th>
<th>CLI</th>
<th>Command line interface</th>
<th>Community names</th>
<th>Configuration check</th>
<th>Configuration profile</th>
<th>Context menu</th>
<th>Counter reset</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>D</th>
<th>Deep packet inspection</th>
<th>Destination NAT</th>
<th>Device software</th>
<th>Device software backup</th>
<th>Device status</th>
<th>DNP3 enforcer</th>
<th>DNS</th>
<th>DNS cache</th>
<th>DNS client</th>
<th>Domain name system</th>
<th>DoS</th>
<th>Double NAT</th>
<th>DPI</th>
<th>DPI DNP3 enforcer</th>
<th>DPI Modbus enforcer</th>
<th>DPI OPC enforcer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E</th>
<th>Egress rate limiter</th>
<th>Encryption</th>
<th>ENVM</th>
<th>Event severity</th>
<th>External memory</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---
## Index

### F
- FAQ .......................................................... 419
- FDB ................................................................ 228
- Filter MAC addresses ........................................... 228
- Fingerprint ...................................................... 78, 82
- Firewall learning mode ........................................ 106
- Flash memory .................................................. 27
- Flow control ..................................................... 223
- Forwarding database ......................................... 228

### H
- HiDiscovery ..................................................... 22, 369, 406
- HiVRRP .......................................................... 317
- Host key ......................................................... 79
- HTML .............................................................. 380, 405
- HTTP .............................................................. 80
- HTTP server .................................................... 368
- HTTPS ............................................................ 81

### I
- ICMP redirect ................................................... 241, 246
- Industrial HiVision ............................................. 9, 75
- Ingress filtering ................................................ 239
- Ingress rate limiter ............................................ 225
- IP access restriction ......................................... 85

### L
- L3 relay .......................................................... 306
- LDAP ................................................................ 62
- LLDP ................................................................ 390
- Load/save ........................................................ 28
- Log file ............................................................. 46, 405
- Login banner .................................................... 90, 93
- Loopback interface ........................................... 311

### M
- MAC address table ............................................ 228
- Management access ......................................... 22, 85
- Management VLAN ......................................... 22
- Menu .............................................................. 12
- Modbus enforcer .............................................. 139

### N
- NAT ............................................................... 329, 331, 352
- Network address translation ............................... 329
- Network time protocol ...................................... 50
- NTP ............................................................... 50
- NVM ................................................................ 12, 13, 21, 27, 33

### O
- OPC enforcer .................................................. 146
- OSPF ............................................................. 256
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
</tr>
<tr>
<td>Password ................................................................. 58, 367</td>
</tr>
<tr>
<td>Password length .......................................................... 58, 367</td>
</tr>
<tr>
<td>Persistent logging .......................................................... 402</td>
</tr>
<tr>
<td>Port configuration .......................................................... 232</td>
</tr>
<tr>
<td>Port forwarding .............................................................. 335</td>
</tr>
<tr>
<td>Port priority ................................................................. 232</td>
</tr>
<tr>
<td>Port VLAN ................................................................... 238</td>
</tr>
<tr>
<td>Power supply ................................................................. 19, 364, 376</td>
</tr>
<tr>
<td>Pre-Login banner ............................................................. 93</td>
</tr>
<tr>
<td>Priority queue ................................................................. 231</td>
</tr>
<tr>
<td>Proxy ARP ...................................................................... 245</td>
</tr>
<tr>
<td>Q</td>
</tr>
<tr>
<td>Queues ..................................................................... 231</td>
</tr>
<tr>
<td>R</td>
</tr>
<tr>
<td>RADIUS ...................................................................... 62, 96</td>
</tr>
<tr>
<td>RAM ........................................................................... 32</td>
</tr>
<tr>
<td>RAM test ..................................................................... 384</td>
</tr>
<tr>
<td>Rate limiter ................................................................. 225</td>
</tr>
<tr>
<td>Reboot ......................................................................... 46</td>
</tr>
<tr>
<td>Relay ........................................................................ 306</td>
</tr>
<tr>
<td>Router interface ............................................................. 236, 244</td>
</tr>
<tr>
<td>Routing table ............................................................... 294</td>
</tr>
<tr>
<td>S</td>
</tr>
<tr>
<td>Secure shell ................................................................. 76</td>
</tr>
<tr>
<td>Security status .............................................................. 18, 366</td>
</tr>
<tr>
<td>Self-test ..................................................................... 384</td>
</tr>
<tr>
<td>Serial interface ............................................................. 368</td>
</tr>
<tr>
<td>Settings ...................................................................... 28</td>
</tr>
<tr>
<td>Severity ..................................................................... 400</td>
</tr>
<tr>
<td>SFP module ................................................................. 389</td>
</tr>
<tr>
<td>Signal contact .............................................................. 18, 371</td>
</tr>
<tr>
<td>SNMP server ................................................................. 75, 368</td>
</tr>
<tr>
<td>SNMP traps ................................................................. 44, 259, 300, 314, 362, 366, 374, 377</td>
</tr>
<tr>
<td>SNMPv1/v2 ................................................................. 92</td>
</tr>
<tr>
<td>Software backup ............................................................. 25</td>
</tr>
<tr>
<td>Software update ............................................................. 25</td>
</tr>
<tr>
<td>Source routing .............................................................. 241</td>
</tr>
<tr>
<td>SSH server ................................................................. 76</td>
</tr>
<tr>
<td>Stratum .................................................................... 50, 52</td>
</tr>
<tr>
<td>Switch dump ................................................................. 400</td>
</tr>
<tr>
<td>Syslog ..................................................................... 386</td>
</tr>
<tr>
<td>System information .......................................................... 380</td>
</tr>
<tr>
<td>System log ................................................................. 405</td>
</tr>
<tr>
<td>System monitor ............................................................. 384</td>
</tr>
</tbody>
</table>
Index

T
Technical questions .................................................. 419
Temperature ............................................................. 20, 363, 375
Threshold values network load ..................................... 225
Time to live .............................................................. 243
Topology discovery .................................................... 395
Tracking ................................................................. 298, 326
Training courses ....................................................... 419
Trap destination ......................................................... 377
Traps ................................................................. 44, 259, 300, 314, 362, 366, 374, 377
Trust mode .............................................................. 232
TTL ................................................................. 243

U
User administration ...................................................... 57

V
Virtual local area network ........................................... 234
Virtual router redundancy protocol ................................ 313
VLAN ................................................................. 22, 234
VLAN configuration ..................................................... 236
VLAN ports .............................................................. 238
VRRP .................................................................. 313
VRRP statistics ........................................................... 324
VRRP tracking ........................................................... 326

W
Watchdog ................................................................. 28, 32
Web server .............................................................. 80, 81

Z
ZIP archive .............................................................. 400
B  Further support

Technical questions

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

You find the addresses of our partners on the Internet at www.hirschmann.com.

A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at hirschmann-support.belden.com.

This site also includes a free of charge knowledge base and a software download section.

Technical Documents

The current manuals and operating instructions for Hirschmann products are available at doc.hirschmann.com.

Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  You find the training courses on technology and products currently available at www.hicomcenter.com.
- Support ranges from the first installation through the standby service to maintenance concepts.

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

<table>
<thead>
<tr>
<th></th>
<th>Very Good</th>
<th>Good</th>
<th>Satisfactory</th>
<th>Mediocre</th>
<th>Poor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precise description</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Readability</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Understandability</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Examples</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Structure</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Comprehensive</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Graphics</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Drawings</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Tables</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>

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

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

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
Germany
Reference Manual

Command Line Interface (CLI)
Industrial Security Router
EAGLE40-03
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.

© 2020 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.

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).

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
Contents

Safety instructions 17

First login (Password change) 18

About this Manual 19

1 Application Lists 20
  1.1 applists 20
    1.1.1 applists set-authlist 20
    1.1.2 applists enable 20
    1.1.3 applists disable 20
  1.2 show 20
    1.2.1 show applists 20

2 Authentication Lists 21
  2.1 authlists 21
    2.1.1 authlists add 21
    2.1.2 authlists delete 21
    2.1.3 authlists set-policy 21
    2.1.4 authlists enable 21
    2.1.5 authlists disable 22
  2.2 show 22
    2.2.1 show authlists 22

3 Class Of Service 23
  3.1 classofservice 23
    3.1.1 classofservice dot1p-mapping 23
  3.2 show 23
    3.2.1 show classofservice dot1p-mapping 23

4 Command Line Interface (CLI) 24
  4.1 cli 24
    4.1.1 cli serial-timeout 24
    4.1.2 cli prompt 24
    4.1.3 cli numlines 24
    4.1.4 cli banner operation 24
    4.1.5 cli banner text 24
  4.2 show 25
    4.2.1 show cli global 25
    4.2.2 show cli command-tree 25
  4.3 logging 25
    4.3.1 logging cli-command 25
  4.4 show 25
    4.4.1 show logging cli-command 25

5 Clock 26
  5.1 clock 26
    5.1.1 clock set 26
    5.1.2 clock timezone offset 26
  5.2 show 26
    5.2.1 show clock 26

6 Configuration 27
  6.1 save 27
    6.1.1 save profile 27
6.2 config
   6.2.1 config watchdog admin-state 27
   6.2.2 config watchdog timeout 27
   6.2.3 config encryption password set 27
   6.2.4 config encryption password clear 27
   6.2.5 config envm auto-update 28
   6.2.6 config envm config-save 28
   6.2.7 config envm load-priority 28
   6.2.8 config profile select 28
   6.2.9 config profile delete 28
   6.2.10 config fingerprint verify nvm profile 29
   6.2.11 config fingerprint verify nvm num 29
   6.2.12 config fingerprint verify envm profile 29
   6.2.13 config fingerprint verify envm num 29

6.3 copy
   6.3.1 copy sysinfo system envm 29
   6.3.2 copy sysinfoall system envm 29
   6.3.3 copy firmware envm 29
   6.3.4 copy firmware remote 30
   6.3.5 copy config running-config nvm 30
   6.3.6 copy config running-config remote 30
   6.3.7 copy config nvm 30
   6.3.8 copy config envm 30
   6.3.9 copy config remote 30

6.4 clear
   6.4.1 clear config 31
   6.4.2 clear factory 31

6.5 show
   6.5.1 show running-config 31

6.6 show
   6.6.1 show config envm settings 31
   6.6.2 show config envm properties 31
   6.6.3 show config watchdog 31
   6.6.4 show config encryption 31
   6.6.5 show config profiles 32
   6.6.6 show config status 32

6.7 swap
   6.7.1 swap firmware system backup 32

7 Device Monitoring
   7.1 device-status
      7.1.1 device-status monitor link-failure 33
      7.1.2 device-status monitor temperature 33
      7.1.3 device-status monitor envm-removal 33
      7.1.4 device-status monitor envm-not-in-sync 33
      7.1.5 device-status monitor power-supply 33
      7.1.6 device-status trap 34

   7.2 device-status
      7.2.1 device-status link-alarm 34

   7.3 show
      7.3.1 show device-status monitor 34
      7.3.2 show device-status state 34
      7.3.3 show device-status trap 34
      7.3.4 show device-status events 35
      7.3.5 show device-status link-alarm 35
      7.3.6 show device-status all 35

8 Device Security
   8.1 security-status
      8.1.1 security-status monitor pwd-change 36
      8.1.2 security-status monitor pwd-min-length 36
      8.1.3 security-status monitor pwd-policy-config 36
      8.1.4 security-status monitor pwd-policy-inactive 36
      8.1.5 security-status monitor http-enabled 37
8.1.6 security-status monitor snmp-unsecure 37
8.1.7 security-status monitor sysmon-enabled 37
8.1.8 security-status monitor extnvm-upd-enabled 37
8.1.9 security-status monitor no-link-enabled 37
8.1.10 security-status monitor hidisc-enabled 38
8.1.11 security-status monitor extnvm-load-unsecure 38
8.1.12 security-status monitor https-certificate 38
8.1.13 security-status trap 38

8.2 security-status 38
8.2.1 security-status no-link 38

8.3 show 39
8.3.1 show security-status monitor 39
8.3.2 show security-status state 39
8.3.3 show security-status no-link 39
8.3.4 show security-status trap 39
8.3.5 show security-status events 39
8.3.6 show security-status all 39

9 Domain Name System (DNS) 40
9.1 dns 40
9.1.1 dns client servers add 40
9.1.2 dns client servers delete 40
9.1.3 dns client servers modify 40
9.1.4 dns client servers enable 40
9.1.5 dns client servers disable 40

9.2 show 41
9.2.1 show dns client info 41
9.2.2 show dns client servers 41

10 Deep Packet Inspection (DPI) 42
10.1 dpi 42
10.1.1 dpi modbus commit 42
10.1.2 dpi modbus addprofile 42
10.1.3 dpi modbus modifyprofile 43
10.1.4 dpi modbus copyprofile 44
10.1.5 dpi modbus delprofile 44
10.1.6 dpi modbus enableprofile 45
10.1.7 dpi modbus disableprofile 45
10.1.8 dpi opc commit 45
10.1.9 dpi opc addprofile 45
10.1.10 dpi opc modifyprofile 45
10.1.11 dpi opc copyprofile 46
10.1.12 dpi opc delprofile 46
10.1.13 dpi opc enableprofile 46
10.1.14 dpi opc disableprofile 46
10.1.15 dpi dnp3 profile add 46
10.1.16 dpi dnp3 profile modify 47
10.1.17 dpi dnp3 profile delete 47
10.1.18 dpi dnp3 profile enable 48
10.1.19 dpi dnp3 profile disable 49
10.1.20 dpi dnp3 profile commit 49
10.1.21 dpi dnp3 profile copy 49
10.1.22 dpi dnp3 object add 49
10.1.23 dpi dnp3 object delete 50

10.2 show 50
10.2.1 show dpi modbus profiletable 50
10.2.2 show dpi modbus pending 50
10.2.3 show dpi opc profiletable 50
10.2.4 show dpi opc pending 50
10.2.5 show dpi dnp3 profiletable 50
10.2.6 show dpi dnp3 pending 50
10.2.7 show dpi dnp3 objectlist 50

11 Filtering Database (FDB) 51
11.1 mac-filter 51
11.1.1 mac-filter 51
11.2 bridge 51
  11.2.1 bridge aging-time 51
11.3 show 51
  11.3.1 show mac-filter-table static 51
11.4 show 51
  11.4.1 show bridge aging-time 51
11.5 show 52
  11.5.1 show mac-addr-table 52
11.6 clear 52
  11.6.1 clear mac-addr-table 52

12 Firewall Learning Mode (FLM) 53
12.1 flm 53
  12.1.1 flm operation 53
  12.1.2 flm action 53
  12.1.3 flm interface add 53
  12.1.4 flm interface delete 53
12.2 show 53
  12.2.1 show flm global 53
  12.2.2 show flm interface 54

13 HiDiscovery 55
13.1 network 55
  13.1.1 network hidiscovery operation 55
  13.1.2 network hidiscovery mode 55
13.2 show 55
  13.2.1 show network hidiscovery 55

14 Hypertext Transfer Protocol (HTTP) 56
14.1 http 56
  14.1.1 http port 56
  14.1.2 http server 56
14.2 show 56
  14.2.1 show http 56

15 HTTP Secure (HTTPS) 57
15.1 https 57
  15.1.1 https server 57
  15.1.2 https port 57
  15.1.3 https fingerprint-type 57
  15.1.4 https certificate 57
15.2 copy 57
  15.2.1 copy httpscert remote 57
  15.2.2 copy httpscert envm 58
15.3 show 58
  15.3.1 show https 58

16 Interface 59
16.1 shutdown 59
  16.1.1 shutdown 59
16.2 auto-negotiate 59
  16.2.1 auto-negotiate 59
16.3 auto-power-down 59
  16.3.1 auto-power-down 59
16.4 cable-crossing 59
  16.4.1 cable-crossing 59
16.5 linktraps
  16.5.1 linktraps
16.6 speed
  16.6.1 speed
16.7 name
  16.7.1 name
16.8 power-state
  16.8.1 power-state
16.9 show
  16.9.1 show port

17 Interface Statistics
  17.1 clear
    17.1.1 clear port-statistics
  17.2 show
    17.2.1 show interface counters
    17.2.2 show interface statistics
    17.2.3 show interface ether-stats

18 Intern
  18.1 help
  18.2 logout
  18.3 history
  18.4 serviceshell
    18.4.1 serviceshell start
    18.4.2 serviceshell deactivate
  18.5 traceroute
    18.5.1 traceroute source
  18.6 reboot
  18.7 ping
    18.7.1 ping source
  18.8 show
    18.8.1 show serviceshell

19 Intrusion Detection System (IDS)
  19.1 ids
    19.1.1 ids operation
    19.1.2 ids user
  19.2 show
    19.2.1 show ids global

20 Open Shortest Path First (OSPF)
  20.1 ip
    20.1.1 ip ospf area
    20.1.2 ip ospf trapflags all
    20.1.3 ip ospf operation
    20.1.4 ip ospf 1583compatability
    20.1.5 ip ospf default-metric
    20.1.6 ip ospf router-id
    20.1.7 ip ospf external-lsdb-limit
    20.1.8 ip ospf exit-overflow
    20.1.9 ip ospf maximum-path
    20.1.10 ip ospf spf-delay
    20.1.11 ip ospf spf-holdtime
    20.1.12 ip ospf auto-cost
    20.1.13 ip ospf distance intra
    20.1.14 ip ospf distance inter
    20.1.15 ip ospf distance external
20.1.16 ip ospf re-distribute 70
20.1.17 ip ospf distribute-list 70
20.1.18 ip ospf default-info originate 71

20.2 ip
  20.2.1 ip ospf operation 71
  20.2.2 ip ospf area-id 71
  20.2.3 ip ospf link-type 71
  20.2.4 ip ospf priority 72
  20.2.5 ip ospf transmit-delay 72
  20.2.6 ip ospf retransmit-interval 72
  20.2.7 ip ospf hello-interval 72
  20.2.8 ip ospf dead-interval 72
  20.2.9 ip ospf cost 73
  20.2.10 ip ospf mtu-ignore 73
  20.2.11 ip ospf authentication type 73
  20.2.12 ip ospf authentication key 73
  20.2.13 ip ospf authentication key-id 73

20.3 show
  20.3.1 show ip ospf global 73
  20.3.2 show ip ospf area 74
  20.3.3 show ip ospf stub 74
  20.3.4 show ip ospf database internal 74
  20.3.5 show ip ospf database external 74
  20.3.6 show ip ospf range 74
  20.3.7 show ip ospf interface 74
  20.3.8 show ip ospf virtual-link 74
  20.3.9 show ip ospf virtual-neighbor 74
  20.3.10 show ip ospf neighbor 74
  20.3.11 show ip ospf statistics 75
  20.3.12 show ip ospf re-distribute 75
  20.3.13 show ip ospf nssa 75
  20.3.14 show ip ospf route 75

21 Virtual Router Redundancy Protocol (VRRP) 76

21.1 ip
  21.1.1 ip vrrp operation 76
  21.1.2 ip vrrp trap auth-failure 76
  21.1.3 ip vrrp trap new-master 76

21.2 ip
  21.2.1 ip vrrp add 76
  21.2.2 ip vrrp modify 77
  21.2.3 ip vrrp delete 77
  21.2.4 ip vrrp enable 77
  21.2.5 ip vrrp disable 77
  21.2.6 ip vrrp virtual-address add 77
  21.2.7 ip vrrp virtual-address delete 77
  21.2.8 ip vrrp track add 77
  21.2.9 ip vrrp track modify 78
  21.2.10 ip vrrp track delete 78

21.3 show
  21.3.1 show ip vrrp interface 78
  21.3.2 show ip vrrp global 78

22 Address Resolution Protocol (IP ARP) 79

22.1 ip
  22.1.1 ip arp add 79
  22.1.2 ip arp delete 79
  22.1.3 ip arp enable 79
  22.1.4 ip arp disable 79
  22.1.5 ip arp timeout 79
  22.1.6 ip arp response-time 79
  22.1.7 ip arp retries 79

22.2 show
  22.2.1 show ip arp info 80
  22.2.2 show ip arp table 80
22.2.3 show ip arp static 80
22.2.4 show ip arp entry 80
22.3 clear 80
22.3.1 clear ip arp-cache 80

23 L3 Relay 81

23.1 ip 81
   23.1.1 ip udp-helper operation 81
   23.1.2 ip udp-helper server add 81
   23.1.3 ip udp-helper server delete 81
   23.1.4 ip udp-helper server enable 81
   23.1.5 ip udp-helper server disable 81
   23.1.6 ip udp-helper maxhopcount 82
   23.1.7 ip udp-helper minwaittime 82
   23.1.8 ip udp-helper cidoptmode 82

23.2 ip 82
   23.2.1 ip udp-helper server add 82
   23.2.2 ip udp-helper server delete 82
   23.2.3 ip udp-helper server enable 82
   23.2.4 ip udp-helper server disable 83

23.3 clear 83
   23.3.1 show ip udp-helper status 83
   23.3.2 show ip udp-helper global 83
   23.3.3 show ip udp-helper interface 83
   23.3.4 show ip udp-helper statistics 83

23.4 clear 83
   23.4.1 clear ip udp-helper 83

24 Internet Protocol Version 4 (IPv4) 84

24.1 network 84
   24.1.1 network parms 84

24.2 clear 84
   24.2.1 clear arp-table-switch 84

24.3 show 84
   24.3.1 show network parms 84

24.4 show 84
   24.4.1 show arp 84

25 Link Layer Discovery Protocol (LLDP) 85

25.1 lldp 85
   25.1.1 lldp operation 85
   25.1.2 lldp config chassis admin-state 85
   25.1.3 lldp config chassis notification-interval 85
   25.1.4 lldp config chassis tx-hold-multiplier 85
   25.1.5 lldp config chassis tx-interval 85

25.2 show 85
   25.2.1 show lldp global 86
   25.2.2 show lldp port 86
   25.2.3 show lldp remote-data 86

25.3 lldp 86
   25.3.1 lldp admin-state 86
   25.3.2 lldp fdb-mode 86
   25.3.3 lldp max-neighbors 86
   25.3.4 lldp notification 87
   25.3.5 lldp tlv port-desc 87
   25.3.6 lldp tlv sys-cap 87
   25.3.7 lldp tlv sys-desc 87
   25.3.8 lldp tlv sys-name 87

26 Logging 89

26.1 logging 89
26.1.1 logging audit-trail  
26.1.2 logging buffered severity  
26.1.3 logging host add  
26.1.4 logging host delete  
26.1.5 logging host enable  
26.1.6 logging host disable  
26.1.7 logging host modify  
26.1.8 logging syslog operation  
26.1.9 logging current-console operation  
26.1.10 logging current-console severity  
26.1.11 logging console operation  
26.1.12 logging console severity  

26.2 show  
26.2.1 show logging buffered  
26.2.2 show logging traplogs  
26.2.3 show logging console  
26.2.4 show logging persistent  
26.2.5 show logging syslog  
26.2.6 show logging host  

26.3 copy  
26.3.1 copy eventlog buffered envm  
26.3.2 copy eventlog buffered remote  
26.3.3 copy eventlog persistent  
26.3.4 copy traplog system envm  
26.3.5 copy traplog system remote  
26.3.6 copy audittrail system envm  
26.3.7 copy audittrail system remote  

26.4 clear  
26.4.1 clear logging buffered  
26.4.2 clear logging persistent  
26.4.3 clear eventlog  

27 Management Access  

27.1 network  
27.1.1 network management access web timeout  
27.1.2 network management access add  
27.1.3 network management access delete  
27.1.4 network management access modify  
27.1.5 network management access operation  
27.1.6 network management access status  

27.2 show  
27.2.1 show network management access global  
27.2.2 show network management access rules  

28 Network Address Translation (NAT)  

28.1 nat  
28.1.1 nat dnat commit  
28.1.2 nat dnat add  
28.1.3 nat dnat modify  
28.1.4 nat dnat delete  
28.1.5 nat dnat logtrap  
28.1.6 nat dnat state  
28.1.7 nat dnat if add  
28.1.8 nat dnat if delete  
28.1.9 nat 1to1nat commit  
28.1.10nat 1to1nat add  
28.1.11nat 1to1nat modify  
28.1.12nat 1to1nat delete  
28.1.13nat 1to1nat logtrap  
28.1.14nat 1to1nat state  
28.1.15nat masq commit  
28.1.16nat masq add  
28.1.17nat masq modify  
28.1.18nat masq delete  
28.1.19nat masq logtrap  
28.1.20nat masq ipsec-exempt
28.1.21 nat masq state
28.1.22 nat masq if add
28.1.23 nat masq if delete
28.1.24 nat doublenat commit
28.1.25 nat doublenat add
28.1.26 nat doublenat modify
28.1.27 nat doublenat delete
28.1.28 nat doublenat logtrap
28.1.29 nat doublenat state
28.1.30 nat doublenat if add
28.1.31 nat doublenat if delete

28.2 show
28.2.1 show nat dnat rules
28.2.2 show nat dnat if
28.2.3 show nat dnat logtrap
28.2.4 show nat masq rules
28.2.5 show nat masq logtrap
28.2.6 show nat masq if
28.2.7 show nat 1to1nat rules
28.2.8 show nat 1to1nat logtrap
28.2.9 show nat doublenat rules
28.2.10 show nat doublenat logtrap
28.2.11 show nat doublenat if

29 Network Time Protocol (NTP)
29.1 ntp
29.1.1 ntp client operation
29.1.2 ntp client operating-mode
29.1.3 ntp server operation
29.1.4 ntp server operating-mode
29.1.5 ntp server localclock-stratum
29.1.6 ntp peers add
29.1.7 ntp peers delete

29.2 show
29.2.1 show ntp client-status
29.2.2 show ntp server-status

30 Packet Filter
30.1 packet-filter
30.1.1 packet-filter l3 commit
30.1.2 packet-filter l3 defaultpolicy
30.1.3 packet-filter l3 checksum-validation
30.1.4 packet-filter l3 addrule
30.1.5 packet-filter l3 modifyrule
30.1.6 packet-filter l3 delrule
30.1.7 packet-filter l3 enablerule
30.1.8 packet-filter l3 disablerule
30.1.9 packet-filter l3 logmode
30.1.10 packet-filter l3 addif
30.1.11 packet-filter l3 delif
30.1.12 packet-filter l3 enableif
30.1.13 packet-filter l3 disableif
30.1.14 packet-filter l2 commit
30.1.15 packet-filter l2 defaultpolicy
30.1.16 packet-filter l2 fcs-validation
30.1.17 packet-filter l2 rule add
30.1.18 packet-filter l2 rule modify
30.1.19 packet-filter l2 rule delete
30.1.20 packet-filter l2 rule enable
30.1.21 packet-filter l2 rule disable
30.1.22 packet-filter l2 if add
30.1.23 packet-filter l2 if delete
30.1.24 packet-filter l2 if enable
30.1.25 packet-filter l2 if disable

30.2 clear
30.3 show
## Contents

30.3.1 show packet-filter l3 global 116  
30.3.2 show packet-filter l3 maxrules 116  
30.3.3 show packet-filter l3 defaultpolicy 116  
30.3.4 show packet-filter l3 ruletable 116  
30.3.5 show packet-filter l3 iftable 116  
30.3.6 show packet-filter l3 pending 116  
30.3.7 show packet-filter l2 global 116  
30.3.8 show packet-filter l2 rule 116  
30.3.9 show packet-filter l2 if 116  

31 Password Management 117

31.1 passwords 117  
31.1.1 passwords min-length 117  
31.1.2 passwords max-login-attempts 117  
31.1.3 passwords min-uppercase-chars 117  
31.1.4 passwords min-lowercase-chars 117  
31.1.5 passwords min-numeric-chars 117  
31.1.6 passwords min-special-chars 117  
31.1.7 passwords login-attempt-period 117  

31.2 show 118  
31.2.1 show passwords 118  

32 Radius 119

32.1 radius 119  
32.1.1 radius server attribute 4 119  
32.1.2 radius server auth add 119  
32.1.3 radius server auth delete 119  
32.1.4 radius server auth modify 119  
32.1.5 radius server retransmit 120  
32.1.6 radius server timeout 120  

32.2 show 120  
32.2.1 show radius global 120  
32.2.2 show radius auth servers 120  
32.2.3 show radius auth statistics 120  

32.3 clear 120  
32.3.1 clear radius 120  

33 Remote Authentication 121

33.1 ldap 121  
33.1.1 ldap operation 121  
33.1.2 ldap cache-timeout 121  
33.1.3 ldap flush-user-cache 121  
33.1.4 ldap role-policy 121  
33.1.5 ldap basedn 121  
33.1.6 ldap search-attr 121  
33.1.7 ldap bind-user 122  
33.1.8 ldap bind-passwd 122  
33.1.9 ldap default-domain 122  
33.1.10 ldap client server add 122  
33.1.11 ldap client server delete 122  
33.1.12 ldap client server enable 122  
33.1.13 ldap client server disable 122  
33.1.14 ldap client server modify 123  
33.1.15 ldap mapping add 123  
33.1.16 ldap mapping delete 123  
33.1.17 ldap mapping enable 123  
33.1.18 ldap mapping disable 123  

33.2 show 124  
33.2.1 show ldap global 124  
33.2.2 show ldap client server 124  
33.2.3 show ldap mapping 124  

33.3 copy 124  
33.3.1 copy ldapcacert remote 124  
33.3.2 copy ldapcacert envm 124
34 Remote Monitoring (RMON) 125
34.1 show 125
34.1.1 show rmon statistics 125

35 Script File 126
35.1 script 126
35.1.1 script apply 126
35.1.2 script validate 126
35.1.3 script list system 126
35.1.4 script list envm 126
35.1.5 script delete 126
35.2 copy 126
35.2.1 copy script envm 126
35.2.2 copy script remote 127
35.2.3 copy script nvm 127
35.3 show 127
35.3.1 show script envm 127
35.3.2 show script system 127

36 Selftest 128
36.1 selftest 128
36.1.1 selftest action 128
36.1.2 selftest ramtest 128
36.1.3 selftest system-monitor 128
36.1.4 selftest boot-default-on-error 128
36.2 show 129
36.2.1 show selftest action 129
36.2.2 show selftest settings 129

37 Small Form-factor Pluggable (SFP) 130
37.1 show 130
37.1.1 show sfp 130

38 Signal Contact 131
38.1 signal-contact 131
38.1.1 signal-contact mode 131
38.1.2 signal-contact monitor link-failure 131
38.1.3 signal-contact monitor envm-not-in-sync 131
38.1.4 signal-contact monitor envm-removal 131
38.1.5 signal-contact monitor temperature 132
38.1.6 signal-contact monitor power-supply 132
38.1.7 signal-contact state 132
38.1.8 signal-contact trap 132
38.2 signal-contact 133
38.2.1 signal-contact link-alarm 133
38.3 show 133
38.3.1 show signal-contact 133

39 Simple Network Management Protocol (SNMP) 134
39.1 snmp 134
39.1.1 snmp access version v1 134
39.1.2 snmp access version v2 134
39.1.3 snmp access version v3 134
39.1.4 snmp access port 134
39.2 show 134
39.2.1 show snmp access 135

40 SNMP Community 136
40.1 snmp
   40.1.1 snmp community ro 136
   40.1.2 snmp community rw 136

40.2 show
   40.2.1 show snmp community 136

41 SNMP Logging 137

41.1 logging
   41.1.1 logging snmp-request get operation 137
   41.1.2 logging snmp-request get severity 137
   41.1.3 logging snmp-request set operation 137
   41.1.4 logging snmp-request set severity 138

41.2 show
   41.2.1 show logging snmp 138

42 Secure Shell (SSH) 139

42.1 ssh
   42.1.1 ssh server 139
   42.1.2 ssh timeout 139
   42.1.3 ssh port 139
   42.1.4 ssh max-sessions 139
   42.1.5 ssh key rsa 139
   42.1.6 ssh key fingerprint-type 139

42.2 copy
   42.2.1 copy sshkey remote 140
   42.2.2 copy sshkey envm 140

42.3 show
   42.3.1 show ssh 140

43 System 141

43.1 system
   43.1.1 system name 141
   43.1.2 system location 141
   43.1.3 system contact 141
   43.1.4 system pre-login-banner operation 141
   43.1.5 system pre-login-banner text 141
   43.1.6 system resources operation 142

43.2 temperature
   43.2.1 temperature upper-limit 142
   43.2.2 temperature lower-limit 142

43.3 show
   43.3.1 show eventlog 142
   43.3.2 show system info 142
   43.3.3 show system pre-login-banner 142
   43.3.4 show system flash-status 143
   43.3.5 show system temperature limits 143
   43.3.6 show system temperature extremes 143
   43.3.7 show system temperature histogram 143
   43.3.8 show system temperature counters 143
   43.3.9 show system resources 143
   43.3.10 show hardware by-pass 143

44 Traps 144

44.1 snmp
   44.1.1 snmp trap operation 144
   44.1.2 snmp trap mode 144
   44.1.3 snmp trap delete 144
   44.1.4 snmp trap add 144

44.2 show
   44.2.1 show snmp traps 145
## 45 Unicast Routing

45.1 ip
   45.1.1 ip routing
   45.1.2 ip proxy-arp max-delay

45.2 show
   45.2.1 show ip global

45.3 show
   45.3.1 show ip interface
   45.3.2 show ip statistics

45.4 ip
   45.4.1 ip proxy-arp operation
   45.4.2 ip address secondary
   45.4.3 ip address primary
   45.4.4 ip mtu
   45.4.5 ip icmp redirects

45.5 ip
   45.5.1 ip route add
   45.5.2 ip route modify
   45.5.3 ip route delete
   45.5.4 ip route track add
   45.5.5 ip route track delete
   45.5.6 ip default-route add
   45.5.7 ip default-route modify
   45.5.8 ip default-route delete
   45.5.9 ip loopback add
   45.5.10 ip loopback delete
   45.5.11 ip icmp redirects
   45.5.12 ip icmp echo-reply
   45.5.13 ip icmp rate-limit interval
   45.5.14 ip icmp rate-limit burst-size

45.6 show
   45.6.1 show ip route all
   45.6.2 show ip route local
   45.6.3 show ip route static
   45.6.4 show ip route entry
   45.6.5 show ip route tracking

## 46 Tracking

46.1 track
   46.1.1 track add
   46.1.2 track delete
   46.1.3 track enable
   46.1.4 track disable
   46.1.5 track trap
   46.1.6 track description
   46.1.7 track modify interface
   46.1.8 track modify ping
   46.1.9 track modify logical

46.2 show
   46.2.1 show track overview
   46.2.2 show track interface
   46.2.3 show track ping
   46.2.4 show track logical
   46.2.5 show track application

## 47 Virtual LAN (VLAN)

47.1 name
   47.1.1 name

47.2 vlan
   47.2.1 vlan add
   47.2.2 vlan delete
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>47.3 vlan</td>
<td>155</td>
</tr>
<tr>
<td>47.3.1 vlan acceptframe</td>
<td>155</td>
</tr>
<tr>
<td>47.3.2 vlan ingressfilter</td>
<td>155</td>
</tr>
<tr>
<td>47.3.3 vlan priority</td>
<td>156</td>
</tr>
<tr>
<td>47.3.4 vlan pvid</td>
<td>156</td>
</tr>
<tr>
<td>47.3.5 vlan tagging</td>
<td>156</td>
</tr>
<tr>
<td>47.3.6 vlan participation include</td>
<td>156</td>
</tr>
<tr>
<td>47.3.7 vlan participation exclude</td>
<td>156</td>
</tr>
<tr>
<td>47.3.8 vlan participation auto</td>
<td>156</td>
</tr>
<tr>
<td>47.4 show</td>
<td>157</td>
</tr>
<tr>
<td>47.4.1 show vlan id</td>
<td>157</td>
</tr>
<tr>
<td>47.4.2 show vlan brief</td>
<td>157</td>
</tr>
<tr>
<td>47.4.3 show vlan port</td>
<td>157</td>
</tr>
<tr>
<td>47.4.4 show vlan member current</td>
<td>157</td>
</tr>
<tr>
<td>47.4.5 show vlan member static</td>
<td>157</td>
</tr>
<tr>
<td>47.5 network</td>
<td>157</td>
</tr>
<tr>
<td>47.5.1 network management vlan</td>
<td>157</td>
</tr>
<tr>
<td>47.5.2 network management priority dot1p</td>
<td>157</td>
</tr>
<tr>
<td>47.5.3 network management priority ip-dscp</td>
<td>158</td>
</tr>
<tr>
<td>48 Virtual Private Network (VPN)</td>
<td>159</td>
</tr>
<tr>
<td>48.1 ipsec</td>
<td>159</td>
</tr>
<tr>
<td>48.1.1 ipsec certificate delete</td>
<td>159</td>
</tr>
<tr>
<td>48.1.2 ipsec certificate upload passphrase</td>
<td>159</td>
</tr>
<tr>
<td>48.1.3 ipsec connection add</td>
<td>159</td>
</tr>
<tr>
<td>48.1.4 ipsec connection modify</td>
<td>160</td>
</tr>
<tr>
<td>48.1.5 ipsec connection status</td>
<td>162</td>
</tr>
<tr>
<td>48.1.6 ipsec connection delete</td>
<td>162</td>
</tr>
<tr>
<td>48.1.7 ipsec traffic-selector</td>
<td>163</td>
</tr>
<tr>
<td>48.2 show</td>
<td>163</td>
</tr>
<tr>
<td>48.2.1 show ipsec general</td>
<td>163</td>
</tr>
<tr>
<td>48.2.2 show ipsec connections summary</td>
<td>163</td>
</tr>
<tr>
<td>48.2.3 show ipsec connections access</td>
<td>164</td>
</tr>
<tr>
<td>48.2.4 show ipsec connections certificates</td>
<td>164</td>
</tr>
<tr>
<td>48.2.5 show ipsec connections key-exchange</td>
<td>164</td>
</tr>
<tr>
<td>48.2.6 show ipsec connections data-exchange</td>
<td>164</td>
</tr>
<tr>
<td>48.2.7 show ipsec connections status</td>
<td>164</td>
</tr>
<tr>
<td>48.2.8 show ipsec traffic-selectors</td>
<td>164</td>
</tr>
<tr>
<td>48.2.9 show ipsec certificate summary</td>
<td>164</td>
</tr>
<tr>
<td>48.2.10 show ipsec certificate details</td>
<td>164</td>
</tr>
<tr>
<td>49 Users</td>
<td>165</td>
</tr>
<tr>
<td>49.1 users</td>
<td>165</td>
</tr>
<tr>
<td>49.1.1 users add</td>
<td>165</td>
</tr>
<tr>
<td>49.1.2 users delete</td>
<td>165</td>
</tr>
<tr>
<td>49.1.3 users enable</td>
<td>165</td>
</tr>
<tr>
<td>49.1.4 users disable</td>
<td>165</td>
</tr>
<tr>
<td>49.1.5 users password</td>
<td>165</td>
</tr>
<tr>
<td>49.1.6 users snmpv3 authentication</td>
<td>165</td>
</tr>
<tr>
<td>49.1.7 users snmpv3 encryption</td>
<td>166</td>
</tr>
<tr>
<td>49.1.8 users access-role</td>
<td>166</td>
</tr>
<tr>
<td>49.1.9 users lock-status</td>
<td>166</td>
</tr>
<tr>
<td>49.1.10 users password-policy-check</td>
<td>166</td>
</tr>
<tr>
<td>49.2 show</td>
<td>166</td>
</tr>
<tr>
<td>49.2.1 show users</td>
<td>166</td>
</tr>
</tbody>
</table>

### A Further support

### B Readers' Comments
Safety instructions

⚠️ WARNING

UNCONTROLLED MACHINE ACTIONS
To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.
Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.

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

⚠️ WARNING

UNWANTED APPLICATION BEHAVIOR
Configuration of the Ethernet devices shall be done by an Ethernet expert.
Before you start any application based on an AFS and/or AFF network, be sure to complete the configuration of all Ethernet devices correctly.

Failure to follow these instructions can result in equipment damage, serious injury or even death.
**First login (Password change)**

To help prevent undesired access to the device, it is imperative that you change the default password during initial setup.

Perform the following steps:

- Open the Graphical User Interface, the Command Line Interface, or HiView the first time you log on to the device.
- Log on to the device with the default password. The device prompts you to type in a new password.
- Type in your new password.
  
  To help increase security, choose a password that contains at least 8 characters which includes upper-case characters, lower-case characters, numerical digits, and special characters.
- The device prompts you to confirm your new password.
- Log on to the device again with your new password.

**Note:** If you lost your password, then use the System Monitor to reset the password.

For further information see: [hirschmann-support.belden.com](http://hirschmann-support.belden.com).
About this Manual

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 “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 Industrial HiVision Network Management software provides you with additional options for smooth configuration and monitoring:

- Auto-topology discovery
- Browser interface
- Client/server structure
- Event handling
- Event log
- Simultaneous configuration of multiple devices
- Graphical user interface with network layout
- SNMP/OPC gateway
1 Application Lists

1.1 applists
Configure an application list.

1.1.1 applists set-authlist
Set an authentication list reference that shall be used by given application.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: applists set-authlist <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;application&gt; Name of an application list.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>&lt;authlist_name&gt; Name of referenced authentication list.</td>
</tr>
</tbody>
</table>

1.1.2 applists enable
Activate a login application list.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: applists enable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;application&gt; Name of an application list.</td>
</tr>
</tbody>
</table>

1.1.3 applists disable
Deactivate a login application list.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: applists disable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;application&gt; Name of an application list.</td>
</tr>
</tbody>
</table>

1.2 show
Display device options and settings.

1.2.1 show applists
Display the ordered methods for application lists.

- Mode: Command is in all modes available.
- Privilege Level: Administrator
- Format: show applists
2 Authentication Lists

2.1 authlists

Configure an authentication list.

2.1.1 authlists add

Create a new login authentication list.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** authlists add <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;authlist_name&gt; Name of an authentication list.</td>
</tr>
</tbody>
</table>

2.1.2 authlists delete

Delete an existing login authentication list.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** authlists delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;authlist_name&gt; Name of an authentication list.</td>
</tr>
</tbody>
</table>

2.1.3 authlists set-policy

Set the policies of a login authentication list.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** authlists set-policy <P-1> <P-2> [<P-3> [<P-4> [<P-5> [<P-6>]]]]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;authlist_name&gt; Name of an authentication list.</td>
</tr>
<tr>
<td>P-2</td>
<td>reject</td>
<td>Authentication is rejected / not allowed</td>
</tr>
<tr>
<td></td>
<td>local</td>
<td>Authentication by local user DB</td>
</tr>
<tr>
<td></td>
<td>radius</td>
<td>Authentication by RADIUS server</td>
</tr>
<tr>
<td></td>
<td>ldap</td>
<td>Authentication by remote server</td>
</tr>
<tr>
<td>P-3</td>
<td>reject</td>
<td>Authentication is rejected / not allowed</td>
</tr>
<tr>
<td></td>
<td>local</td>
<td>Authentication by local user DB</td>
</tr>
<tr>
<td></td>
<td>radius</td>
<td>Authentication by RADIUS server</td>
</tr>
<tr>
<td></td>
<td>ldap</td>
<td>Authentication by remote server</td>
</tr>
<tr>
<td>P-4</td>
<td>reject</td>
<td>Authentication is rejected / not allowed</td>
</tr>
<tr>
<td></td>
<td>local</td>
<td>Authentication by local user DB</td>
</tr>
<tr>
<td></td>
<td>radius</td>
<td>Authentication by RADIUS server</td>
</tr>
<tr>
<td></td>
<td>ldap</td>
<td>Authentication by remote server</td>
</tr>
<tr>
<td>P-5</td>
<td>reject</td>
<td>Authentication is rejected / not allowed</td>
</tr>
<tr>
<td></td>
<td>local</td>
<td>Authentication by local user DB</td>
</tr>
<tr>
<td></td>
<td>radius</td>
<td>Authentication by RADIUS server</td>
</tr>
<tr>
<td></td>
<td>ldap</td>
<td>Authentication by remote server</td>
</tr>
<tr>
<td>P-6</td>
<td>reject</td>
<td>Authentication is rejected / not allowed</td>
</tr>
<tr>
<td></td>
<td>local</td>
<td>Authentication by local user DB</td>
</tr>
<tr>
<td></td>
<td>radius</td>
<td>Authentication by RADIUS server</td>
</tr>
<tr>
<td></td>
<td>ldap</td>
<td>Authentication by remote server</td>
</tr>
</tbody>
</table>

2.1.4 authlists enable

Activate a login authentication list.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** authlists enable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;authlist_name&gt; Name of an authentication list.</td>
</tr>
</tbody>
</table>
2.1.5 authlists disable
Deactivate a login authentication list.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** authlists disable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;authlist_name&gt; Name of an authentication list.</td>
</tr>
</tbody>
</table>

2.2 show
Display device options and settings.

2.2.1 show authlists
Display the ordered methods for authentication lists.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** show authlists
3 Class Of Service

3.1 classofservice
Class of service configuration.

3.1.1 classofservice dot1p-mapping
Enter a VLAN priority and the traffic class it should be mapped to.
▶ Mode: Global Config Mode
▶ Privilege Level: Operator
▶ Format: classofservice dot1p-mapping <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..7</td>
<td>Enter the 802.1p priority.</td>
</tr>
<tr>
<td>P-2</td>
<td>0..7</td>
<td>Enter the Traffic Class value.</td>
</tr>
<tr>
<td>P-3</td>
<td>0..3</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

3.2 show
Display device options and settings.

3.2.1 show classofservice dot1p-mapping
Display a table containing the vlan priority to traffic class mappings.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show classofservice dot1p-mapping
4 Command Line Interface (CLI)

4.1 cli
Set the CLI preferences.

4.1.1 cli serial-timeout
Set login timeout for serial line connection to CLI. Setting to 0 will disable the timeout. The value is active after next login.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** cli serial-timeout <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0.160</td>
<td>Enter a number in the given range. Setting to 0 will disable the timeout.</td>
</tr>
</tbody>
</table>

4.1.2 cli prompt
Change the system prompt. Following wildcards are allowed: %d date, %t time, %i IP address, %m MAC address, %p product name

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** cli prompt <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters. Following wildcards are allowed: %d date, %t time, %i IP address, %m MAC address, %p product name</td>
</tr>
</tbody>
</table>

4.1.3 cli numlines
Screen size for 'more' (23 = default). Enter a 0 will disable the feature. The value is only valid for the current session.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** cli numlines <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0.250</td>
<td>Screen size for 'more' (23 = default). Enter a 0 will disable the feature. The value is only valid for the current session.</td>
</tr>
</tbody>
</table>

4.1.4 cli banner operation
Enable or disable the CLI login banner.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** cli banner operation

- no cli banner operation

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** no cli banner operation

4.1.5 cli banner text
Set the text for the CLI login banner (C printf format syntax allowed: ).

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** cli banner text <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 1024 characters (allowed characters are from ASCII 32 to 127).</td>
</tr>
</tbody>
</table>
4.2 **show**
Display device options and settings.

4.2.1 **show cli global**
Display the CLI preferences.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show cli global

4.2.2 **show cli command-tree**
Display a list of every command.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show cli command-tree

4.3 **logging**
Logging configuration.

4.3.1 **logging cli-command**
Enable or disable the CLI command logging.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** logging cli-command

**no logging cli-command**
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** no logging cli-command

4.4 **show**
Display device options and settings.

4.4.1 **show logging cli-command**
Display the CLI command logging preferences.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show logging cli-command
5 Clock

5.1 clock
Configure local and DST clock settings.

5.1.1 clock set
Edit current local time.

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: clock set <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>YYYY-MM-DD</td>
<td>Local date (range: 2004-01-01 - 2037-12-31).</td>
</tr>
<tr>
<td>P-2</td>
<td>HH:MM:SS</td>
<td>Local time.</td>
</tr>
</tbody>
</table>

5.1.2 clock timezone offset
Local time offset (in minutes) with respect to UTC (positive values for locations east of Greenwich).

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: clock timezone offset <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>-780..840</td>
<td>Edit the timezone offset (in minutes).</td>
</tr>
</tbody>
</table>

5.2 show
Display device options and settings.

5.2.1 show clock
Display the current time information.

- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: show clock
6 Configuration

6.1 save
Save the configuration to the specified destination.

6.1.1 save profile
Save the configuration to the specific profile.

- **Mode:** All Privileged Modes
- **Privilege Level:** Operator
- **Format:** `save profile <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>

6.2 config
Configure the configuration saving settings.

6.2.1 config watchdog admin-state
Enable or disable the configuration undo feature.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `config watchdog admin-state`

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `no config watchdog admin-state`

6.2.2 config watchdog timeout
Configure the configuration undo timeout (unit: seconds).

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `config watchdog timeout <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>30..600</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

6.2.3 config encryption password set
Set the configuration file password.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `config encryption password set [P-1] [P-2]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 64 characters.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 64 characters.</td>
</tr>
</tbody>
</table>

6.2.4 config encryption password clear
Clear the configuration file password.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `config encryption password clear [P-1]`
6.2.5 config envm auto-update

Allow automatic firmware updates with this memory device.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** config envm auto-update <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>usb</td>
<td>USB Storage Device</td>
</tr>
</tbody>
</table>

- **no config envm auto-update**

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** no config envm auto-update <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>usb</td>
<td>USB Storage Device</td>
</tr>
</tbody>
</table>

6.2.6 config envm config-save

Allow the configuration to be saved to this memory device.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** config envm config-save <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>usb</td>
<td>USB Storage Device</td>
</tr>
</tbody>
</table>

- **no config envm config-save**

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** no config envm config-save <P-1>

6.2.7 config envm load-priority

Configure the order of configuration load attempts from memory devices at boot time. If one load is successful, then the device discards further attempts.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** config envm load-priority <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>usb</td>
<td>USB Storage Device</td>
</tr>
<tr>
<td>P-2</td>
<td>disable</td>
<td>Config will not be loaded at all</td>
</tr>
<tr>
<td></td>
<td>first</td>
<td>Config will be loaded first. If successful, no other config will be tried.</td>
</tr>
</tbody>
</table>

6.2.8 config profile select

Select a configuration profile to be the active configuration.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** config profile select <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>nvm</td>
<td>You can only select nvm for this command.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..20</td>
<td>Index of the profile entry.</td>
</tr>
</tbody>
</table>

6.2.9 config profile delete

Delete a specific configuration profile.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** config profile delete <P-1> num <P-2> profile <P-3>

num: Select the index of a profile to delete.
profile: Select the name of a profile to delete.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>nvm</td>
<td>non-volatile memory</td>
</tr>
<tr>
<td></td>
<td>envm</td>
<td>external non-volatile memory device</td>
</tr>
<tr>
<td>P-2</td>
<td>1..20</td>
<td>Index of the profile entry.</td>
</tr>
<tr>
<td>P-3</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>
6.2.10 config fingerprint verify nvm profile
Select the name of a profile to be verified.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** config fingerprint verify nvm profile <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter hash as 40 hexa-decimal characters.</td>
</tr>
</tbody>
</table>

6.2.11 config fingerprint verify nvm num
Select the index number of a profile to be verified.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** config fingerprint verify nvm num <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..20</td>
<td>Index of the profile entry.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter hash as 40 hexa-decimal characters.</td>
</tr>
</tbody>
</table>

6.2.12 config fingerprint verify envm profile
Select the name of a profile to be verified.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** config fingerprint verify envm profile <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter hash as 40 hexa-decimal characters.</td>
</tr>
</tbody>
</table>

6.2.13 config fingerprint verify envm num
Select the index number of a profile to be verified.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** config fingerprint verify envm num <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..20</td>
<td>Index of the profile entry.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter hash as 40 hexa-decimal characters.</td>
</tr>
</tbody>
</table>

6.3 copy
Copy different kinds of items.

6.3.1 copy sysinfo system envm
Copy the system information to external non-volatile memory.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** copy sysinfo system envm [filename <P-1>]

[filename]: Enter the filename (format xyz.html) to be saved in external non-volatile memory.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>

6.3.2 copy sysinfoall system envm
Copy the system information and the event log from the device to external non-volatile memory.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** copy sysinfoall system envm

6.3.3 copy firmware envm
Copy a firmware image to the device from external non-volatile memory.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** copy firmware envm <P-1> system
system: Copy a firmware image to the device from external non-volatile memory.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
</tbody>
</table>

6.3.4 copy firmware remote
Copy a firmware image to the device from a server.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** copy firmware remote <P-1> system

system: Copy a firmware image to the device from a file server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a valid server URL.</td>
</tr>
</tbody>
</table>

6.3.5 copy config running-config nvm
Copy the running-config to non-volatile memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** copy config running-config nvm [profile <P-1>]

[profile]: Save the configuration as a specific profile name.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>

6.3.6 copy config running-config remote
Copy the running-config to a file server.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** copy config running-config remote <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a valid server URL.</td>
</tr>
</tbody>
</table>

6.3.7 copy config nvm
Load a configuration from non-volatile memory to the running-config.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** copy config nvm [profile <P-1>] running-config remote <P-2>

[profile]: Load a configuration from a specific profile name.

running-config: (Re)-load a configuration from non-volatile memory to the running-config.
remote: Copy a configuration from non-volatile memory to a server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a valid server URL.</td>
</tr>
</tbody>
</table>

6.3.8 copy config envm
Copy a configuration from external non-volatile memory to non-volatile memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** copy config envm [profile <P-1>] nvm

[profile]: Copy a specific configuration profile from external non-volatile memory to non-volatile memory.
nvm: Copy a specific profile from external non-volatile memory to non-volatile memory.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
</tbody>
</table>

6.3.9 copy config remote
Copy a configuration file to the device from a server.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** copy config remote <P-1> nvm [profile <P-2>] running-config

nvm: Copy a configuration file from a server to non-volatile memory.
[profile]: Copy a configuration from a server to a specific profile in non-volatile memory.
running-config: Copy a configuration file from a server to the running-config.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a valid server URL.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>
6.4 clear
Clear several items.

6.4.1 clear config
Clear the running configuration.
- **Mode**: Privileged Exec Mode
- **Privilege Level**: Administrator
- **Format**: clear config

6.4.2 clear factory
Set the device back to the factory settings (use with care).
- **Mode**: Privileged Exec Mode
- **Privilege Level**: Administrator
- **Format**: clear factory

6.5 show
Display device options and settings.

6.5.1 show running-config
Display the currently running configuration.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Administrator
- **Format**: show running-config

6.6 show
Display device options and settings.

6.6.1 show config envm settings
Display the settings of the external non-volatile memory.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: show config envm settings

6.6.2 show config envm properties
Display the properties of the external non-volatile memory.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: show config envm properties

6.6.3 show config watchdog
Display the Auto Configuration Undo settings.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: show config watchdog

6.6.4 show config encryption
Display the settings for configuration encryption.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: show config encryption
6.6.5 show config profiles
Display the configuration profiles.
├ Mode: Command is in all modes available.
├ Privilege Level: Administrator
├ Format: show config profiles <P-1> [<P-2>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>nvm</td>
<td>non-volatile memory</td>
</tr>
<tr>
<td></td>
<td>envm</td>
<td>external non-volatile memory device</td>
</tr>
<tr>
<td>P-2</td>
<td>1..20</td>
<td>Index of the profile entry.</td>
</tr>
</tbody>
</table>

6.6.6 show config status
Display the synchronization status of the running configuration with the non-volatile memory and the ACA.
├ Mode: Command is in all modes available.
├ Privilege Level: Guest
├ Format: show config status

6.7 swap
Swap software images.

6.7.1 swap firmware system backup
Swap the main and backup images.
├ Mode: Privileged Exec Mode
├ Privilege Level: Administrator
├ Format: swap firmware system backup
7 Device Monitoring

7.1 device-status

Configure various device conditions to be monitored.

7.1.1 device-status monitor link-failure

Enable or disable monitor state of network connection(s).

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** device-status monitor link-failure

    no device-status monitor link-failure

    Disable the option

    - **Mode:** Global Config Mode
    - **Privilege Level:** Administrator
    - **Format:** no device-status monitor link-failure

7.1.2 device-status monitor temperature

Enable or disable monitoring of the device temperature.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** device-status monitor temperature

7.1.3 device-status monitor envm-removal

Enable or disable monitoring the presence of the external non-volatile memory.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** device-status monitor envm-removal

    no device-status monitor envm-removal

    Disable the option

    - **Mode:** Global Config Mode
    - **Privilege Level:** Administrator
    - **Format:** no device-status monitor envm-removal

7.1.4 device-status monitor envm-not-in-sync

Enable or disable monitoring synchronization between the external non-volatile memory and the running configuration.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** device-status monitor envm-not-in-sync

    no device-status monitor envm-not-in-sync

    Disable the option

    - **Mode:** Global Config Mode
    - **Privilege Level:** Administrator
    - **Format:** no device-status monitor envm-not-in-sync

7.1.5 device-status monitor power-supply

Enable or disable monitoring the condition of the power supply(s).

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** device-status monitor power-supply <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..2</td>
<td>Number of power supply.</td>
</tr>
</tbody>
</table>
7.1.6 device-status trap
Configure the device to send a trap when the device status changes.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** device-status trap

7.2 device-status
Configure various device conditions to be monitored.

7.2.1 device-status link-alarm
Configure the monitor settings of the port link.
- **Mode:** Interface Range Mode
- **Privilege Level:** Administrator
- **Format:** device-status link-alarm

7.3 show
Display device options and settings.

7.3.1 show device-status monitor
Display the device monitoring configurations.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show device-status monitor

7.3.2 show device-status state
Display the current state of the device.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show device-status state

7.3.3 show device-status trap
Display the device trap information and configurations.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show device-status trap
7.3.4  **show device-status events**
Display occurred device status events.
► **Mode:** Command is in all modes available.
► **Privilege Level:** Guest
► **Format:** show device-status events

7.3.5  **show device-status link-alarm**
Display the monitor configurations of the network ports.
► **Mode:** Command is in all modes available.
► **Privilege Level:** Guest
► **Format:** show device-status link-alarm

7.3.6  **show device-status all**
Display the configurable device status settings.
► **Mode:** Command is in all modes available.
► **Privilege Level:** Guest
► **Format:** show device-status all
8 Device Security

8.1 security-status
Configure the security status settings.

8.1.1 security-status monitor pwd-change
Sets the monitoring of default password change for 'user' and 'admin'.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `security-status monitor pwd-change`

```
no security-status monitor pwd-change
```
Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `no security-status monitor pwd-change`

8.1.2 security-status monitor pwd-min-length
Sets the monitoring of minimum length of the password (smaller 8).

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `security-status monitor pwd-min-length`

```
no security-status monitor pwd-min-length
```
Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `no security-status monitor pwd-min-length`

8.1.3 security-status monitor pwd-policy-config
Sets the monitoring whether the minimum password policy is configured. The device changes the security status to the value "error" if the value for at least one of the following password rules is 0: "minimum upper cases", "minimum lower cases", "minimum numbers", "minimum special characters".

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `security-status monitor pwd-policy-config`

```
no security-status monitor pwd-policy-config
```
Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `no security-status monitor pwd-policy-config`

8.1.4 security-status monitor pwd-policy-inactive
Sets the monitoring whether at least one user is configured with inactive policy check. The device changes the security status to the value "error" if the function "policy check" is inactive for at least 1 user account.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `security-status monitor pwd-policy-inactive`

```
no security-status monitor pwd-policy-inactive
```
Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `no security-status monitor pwd-policy-inactive`
8.1.5 security-status monitor http-enabled
Sets the monitoring of the activation of http on the switch.
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: security-status monitor http-enabled

no security-status monitor http-enabled
Disable the option
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: no security-status monitor http-enabled

8.1.6 security-status monitor snmp-unsecure
Sets the monitoring of SNMP security (SNMP v1/v2 is enabled or v3 encryption is disabled).
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: security-status monitor snmp-unsecure

no security-status monitor snmp-unsecure
Disable the option
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: no security-status monitor snmp-unsecure

8.1.7 security-status monitor sysmon-enabled
Sets the monitoring of the activation of System Monitor 1 on the switch.
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: security-status monitor sysmon-enabled

no security-status monitor sysmon-enabled
Disable the option
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: no security-status monitor sysmon-enabled

8.1.8 security-status monitor extnvm-upd-enabled
Sets the monitoring of activation of the configuration saving to external non volatile memory.
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: security-status monitor extnvm-upd-enabled

no security-status monitor extnvm-upd-enabled
Disable the option
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: no security-status monitor extnvm-upd-enabled

8.1.9 security-status monitor no-link-enabled
Sets the monitoring of no link detection.
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: security-status monitor no-link-enabled

no security-status monitor no-link-enabled
Disable the option
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: no security-status monitor no-link-enabled
8.1.10 security-status monitor hidisc-enabled
Sets the monitoring of HiDiscovery.
➤ Mode: Global Config Mode
➤ Privilege Level: Administrator
➤ Format: security-status monitor hidisc-enabled

no security-status monitor hidisc-enabled
Disable the option
➤ Mode: Global Config Mode
➤ Privilege Level: Administrator
➤ Format: no security-status monitor hidisc-enabled

8.1.11 security-status monitor extnvm-load-unsecure
Sets the monitoring of security of the configuration loading from extnvm.
➤ Mode: Global Config Mode
➤ Privilege Level: Administrator
➤ Format: security-status monitor extnvm-load-unsecure

no security-status monitor extnvm-load-unsecure
Disable the option
➤ Mode: Global Config Mode
➤ Privilege Level: Administrator
➤ Format: no security-status monitor extnvm-load-unsecure

8.1.12 security-status monitor https-certificate
Sets the monitoring whether auto generated self-signed HTTPS certificate is in use.
➤ Mode: Global Config Mode
➤ Privilege Level: Administrator
➤ Format: security-status monitor https-certificate

no security-status monitor https-certificate
Disable the option
➤ Mode: Global Config Mode
➤ Privilege Level: Administrator
➤ Format: no security-status monitor https-certificate

8.1.13 security-status trap
Configure if a trap is sent when the security status changes.
➤ Mode: Global Config Mode
➤ Privilege Level: Administrator
➤ Format: security-status trap

no security-status trap
Disable the option
➤ Mode: Global Config Mode
➤ Privilege Level: Administrator
➤ Format: no security-status trap

8.2 security-status
Configure the security status interface settings.

8.2.1 security-status no-link
Configure the monitoring of the specific ports.
➤ Mode: Interface Range Mode
➤ Privilege Level: Administrator
➤ Format: security-status no-link
no security-status no-link
Disable the option
  ▶ Mode: Interface Range Mode
  ▶ Privilege Level: Administrator
  ▶ Format: no security-status no-link

8.3 show
Display device options and settings.

8.3.1 show security-status monitor
Display the security status monitoring settings.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show security-status monitor

8.3.2 show security-status state
Display the current security status.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show security-status state

8.3.3 show security-status no-link
Display the settings of the monitoring of the specific network ports.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show security-status no-link

8.3.4 show security-status trap
Display the security status trap information and settings.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show security-status trap

8.3.5 show security-status events
Display the occurred security status events.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show security-status events

8.3.6 show security-status all
Display the security status settings.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show security-status all
9  Domain Name System (DNS)

9.1  dns

Set DNS parameters.

9.1.1  dns client servers add

Add a new DNS server.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: dns client servers add <P-1> ip <P-2>
ip: Enter the DNS server address.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>DNS Client servers index.</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

9.1.2  dns client servers delete

Delete a DNS server.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: dns client servers delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>DNS Client servers index.</td>
</tr>
</tbody>
</table>

9.1.3  dns client servers modify

Modify a DNS server entry.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: dns client servers modify <P-1> ip <P-2> status <P-3> operation <P-4>
  ip: Change the DNS server address.
  status: Change the status of this DNS server.
  operation: Change the status of this DNS server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>DNS Client servers index.</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
<tr>
<td>P-4</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

9.1.4  dns client servers enable

Activate a DNS server entry.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: dns client servers enable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>DNS Client servers index.</td>
</tr>
</tbody>
</table>

9.1.5  dns client servers disable

Deactivate a DNS server entry.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: dns client servers disable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>DNS Client servers index.</td>
</tr>
</tbody>
</table>
9.2 show
Display device options and settings.

9.2.1 show dns client info
Display the DNS Client related information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show dns client info`

9.2.2 show dns client servers
Display the DNS Client servers.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show dns client servers`
10 Deep Packet Inspection (DPI)

10.1 dpi
Creation and configuration of DPI profiles.

10.1.1 dpi modbus commit
Writes all changes made in the DPI MODBUS profiles to the enforcer.
- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: `dpi modbus commit`

10.1.2 dpi modbus addprofile
Adds a profile to the DPI MODBUS profile table.
- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: `dpi modbus addprofile <P-1> [description <P-2>] [function-type <P-3>] [function-code-list <P-4>] [unit-identifier-list <P-5>] [sanity-check <P-6>] [exception <P-7>] [reset <P-8>]

- **Parameter** | **Value** | **Meaning**
- P-1       | 1..32        | Profile index 1 - 32
- P-2       | string       | Profile description/name
- P-3       | readonly      | Read only function codes for function code list
-             | readwrite     | Read write function codes for function code list
-             | programming   | Programming function codes for function code list
-             | all           | All possible function codes for function code list (allow any function code)
-             | advanced      | Keeps the function code list from the previous selection and makes it editable by the user
-             |              |
10.1.3 dpi modbus modifyprofile

Modifies a profile in the DPI MODBUS profile table.

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: `dpi modbus modifyprofile <P-1> [description <P-2>] [function-type <P-3>] [function-code-list <P-4>] [unit-identifier-list <P-5>] [sanity-check <P-6>] [exception <P-7>] [reset <P-8>]
- **description**: Profile description/name for the DPI MODBUS profile.
- **function-type**: Function type of corresponding function codes.
- **function-code-list**: Function code list. A function code has the syntax 'val'. Function codes are separated by a comma. When more than one value for an function code is specified the values are separated by the pipe symbol ('|').
- **unit-identifier-list**: Unit identifier list. A unit identifier has the syntax 'val'. To specify no options, the value 'none' must be given. Unit identifiers are separated by a comma.
- **sanity-check**: Sanity check including format and specification.
- **exception**: Device exception message.
- **reset**: Reset connection message.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Profile description/name</td>
</tr>
</tbody>
</table>
### 10.1.4 dpi modbus copyprofile

Copies a profile to another DPI MODBUS profile.

**Mode:** Global Config Mode  
**Privilege Level:** Operator  
**Format:** `dpi modbus copyprofile <P-1> <P-2>`

#### Parameter Value | Meaning
--- | ---
P-1 | 1..32  
Profile source index 1 - 32
P-2 | 1..32  
Profile destination index 1 - 32

### 10.1.5 dpi modbus delprofile

Deletes a profile from the DPI MODBUS profile table. You cannot delete an active profile or if an enforcer mappings to it.

**Mode:** Global Config Mode  
**Privilege Level:** Operator  
**Format:** `dpi modbus delprofile <P-1>`

#### Parameter Value | Meaning
--- | ---
P-1 | 1..32  
Profile index 1 - 32
10.1.6 dpi modbus enableprofile
Enables a profile in the DPI MODBUS profile table. A profile can only be activated when all required parameters are set. After activation modifications no longer possible.
➤ Mode: Global Config Mode
➤ Privilege Level: Operator
➤ Format: dpi modbus enableprofile <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
</tbody>
</table>

10.1.7 dpi modbus disableprofile
Disables a profile in the DPI MODBUS profile table. You cannot inactivate a profile if an active enforcer mappings to it.
➤ Mode: Global Config Mode
➤ Privilege Level: Operator
➤ Format: dpi modbus disableprofile <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
</tbody>
</table>

10.1.8 dpi opc commit
Writes all changes made in the DPI OPC profiles to the enforcer.
➤ Mode: Global Config Mode
➤ Privilege Level: Operator
➤ Format: dpi opc commit

10.1.9 dpi opc addprofile
Adds a profile to the DPI OPC profile table.
➤ Mode: Global Config Mode
➤ Privilege Level: Operator
➤ Format: dpi opc addprofile <P-1> [description <P-2>] [sanity-check <P-3>] [fragment-check <P-4>] [timeout-connect <P-5>]
[description]: Profile description/name for the DPI OPC profile.
[sanity-check]: Sanity check including format and specification.
[fragment-check]: Fragment check.
[timeout-connect]: Timeout at connect.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Profile description/name</td>
</tr>
<tr>
<td>P-3</td>
<td>yes</td>
<td>True</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>False</td>
</tr>
<tr>
<td>P-4</td>
<td>yes</td>
<td>True</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>False</td>
</tr>
<tr>
<td>P-5</td>
<td>0..60</td>
<td>Timeout in seconds 0 - 60</td>
</tr>
</tbody>
</table>

10.1.10 dpi opc modifyprofile
Modifies a profile in the DPI OPC profile table.
➤ Mode: Global Config Mode
➤ Privilege Level: Operator
➤ Format: dpi opc modifyprofile <P-1> [description <P-2>] [sanity-check <P-3>] [fragment-check <P-4>] [timeout-connect <P-5>]
[description]: Profile description/name for the DPI OPC profile.
[sanity-check]: Sanity check including format and specification.
[fragment-check]: Fragment check.
[timeout-connect]: Timeout at connect.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Profile description/name</td>
</tr>
<tr>
<td>P-3</td>
<td>yes</td>
<td>True</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>False</td>
</tr>
<tr>
<td>P-4</td>
<td>yes</td>
<td>True</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>False</td>
</tr>
<tr>
<td>P-5</td>
<td>0..60</td>
<td>Timeout in seconds 0 - 60</td>
</tr>
</tbody>
</table>
10.1.11 dpi opc copyprofile
Copies a profile to another DPI OPC profile.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi opc copyprofile <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile source index 1 - 32</td>
</tr>
<tr>
<td>P-2</td>
<td>1..32</td>
<td>Profile destination index 1 - 32</td>
</tr>
</tbody>
</table>

10.1.12 dpi opc delprofile
Deletes a profile from the DPI OPC profile table. You cannot delete an active profile or if an enforcer mappings to it.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi opc delprofile <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
</tbody>
</table>

10.1.13 dpi opc enableprofile
Enables a profile in the DPI OPC profile table. A profile can only be activated when all required parameters are set. After activation modifications no longer possible.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi opc enableprofile <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
</tbody>
</table>

10.1.14 dpi opc disableprofile
Disables a profile in the DPI OPC profile table. You cannot inactivate a profile if an active enforcer mappings to it.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi opc disableprofile <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
</tbody>
</table>

10.1.15 dpi dnp3 profile add
Adds a profile to the DPI DNP3 profile table.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi dnp3 profile add <P-1> [description <P-2>] [function-code-list <P-3>] [default-object-list <P-4>] [sanity-check <P-5>] [crc-check <P-6>] [outstation-packets-check <P-7>] [reset-tcp-check <P-8>]
  - **[description]:** Profile description/name for the DPI DNP3 profile.
  - **[function-code-list]:** Function code list. A function code has the syntax ‘val’. Function codes are separated by a comma.
  - **[default-object-list]:** Object entries to be included from Default white list.
  - **[sanity-check]:** Sanity check including format and specification.
  - **[crc-check]:** CRC verification for DNP3 data link layer frames.
  - **[outstation-packets-check]:** Check the DNP3 data packets originating at an outstation.
  - **[reset-tcp-check]:** Reset the TCP connection in case of a protocol violation or if the plausibility check leads to errors.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>DNP3 profile index.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Profile description/name for the DNP3 profile.</td>
</tr>
</tbody>
</table>
Modifies a profile to the DPI DNP3 profile table.

**Mode:** Global Config Mode

**Privilege Level:** Operator

**Format:**
```
dpi dnp3 profile modify <P-1> [description <P-2>] [function-code-list <P-3>] [default-object-list <P-4>] [sanity-check <P-5>] [crc-check <P-6>] [outstation-packets-check <P-7>] [reset-tcp-check <P-8>]
```

- **description**: Profile description/name for the DPI DNP3 profile.
- **function-code-list**: Function code list. A function code has the syntax 'val'. Function codes are separated by a comma.
- **default-object-list**: Object entries to be included from Default white list.
- **sanity-check**: 'enable' to enable the option.
- **crc-check**: 'enable' to enable the option.
- **outstation-packets-check**: 'enable' to enable the option.
- **reset-tcp-check**: 'enable' to enable the option.

**Function Codes**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-3</td>
<td>0..255</td>
<td>Function codes for the DNP3 profile.</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>Confirm</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Write</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Select</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Operate</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Direct Operate</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Direct Operate-No Response Required</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>Freeze</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>Freeze-No Response Required</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>Freeze Clear</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>Freeze Clear-No Response Required</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>Freeze At Time</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>Freeze At Time-No Response Required</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>Cold Restart</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>Warm Restart</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>Initialize Data</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>Initialize Application</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>Start Application</td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>Stop Application</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>Save Configuration</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>Enable Unsolicited Messages</td>
</tr>
<tr>
<td></td>
<td>21</td>
<td>Disable Unsolicited Messages</td>
</tr>
<tr>
<td></td>
<td>22</td>
<td>Assign Class</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>Delay Measurement</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>Record Current Time</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>Open File</td>
</tr>
<tr>
<td></td>
<td>26</td>
<td>Close File</td>
</tr>
<tr>
<td></td>
<td>27</td>
<td>Delete File</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>Get File Information</td>
</tr>
<tr>
<td></td>
<td>29</td>
<td>Authenticate File</td>
</tr>
<tr>
<td></td>
<td>30</td>
<td>Abort File Transfer</td>
</tr>
<tr>
<td></td>
<td>31</td>
<td>Activate Configuration</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>Authenticate Request</td>
</tr>
<tr>
<td></td>
<td>33</td>
<td>Authenticate Request-No Acknowledgement</td>
</tr>
<tr>
<td></td>
<td>34</td>
<td>Response</td>
</tr>
<tr>
<td></td>
<td>35</td>
<td>Unsolicited Response</td>
</tr>
<tr>
<td></td>
<td>36</td>
<td>Authentication Response</td>
</tr>
</tbody>
</table>

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-4</td>
<td>1..317</td>
<td>Comma separated index values e.g. 1,2,3.</td>
</tr>
<tr>
<td></td>
<td>1-317</td>
<td>Comma separated index and range of index values e.g. 1-10,120-300.</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td>'none' to exclude all default object list entries.</td>
</tr>
<tr>
<td></td>
<td>all</td>
<td>'all' to include all default object list entries.</td>
</tr>
</tbody>
</table>

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-5</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
<tr>
<td>P-6</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
<tr>
<td>P-7</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
<tr>
<td>P-8</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>
[reset-tcp-check]: Reset the TCP connection in case of a protocol violation or if the plausibility check leads to errors.

**Parameter** | **Value** | **Meaning**
--- | --- | ---
P-1 | 1..32 | DNP3 profile index.
P-2 | string | Profile description/name for the DNP3 profile.
P-3 | 0..255 | Function codes for the DNP3 profile.

- 0: Confirm
- 1: Read
- 2: Write
- 3: Select
- 4: Operate
- 5: Direct Operate
- 6: Direct Operate-No Response Required
- 7: Freeze
- 8: Freeze-No Response Required
- 9: Freeze Clear
- 10: Freeze Clear-No Response Required
- 11: Freeze At Time
- 12: Freeze At Time-No Response Required
- 13: Cold Restart
- 14: Warm Restart
- 15: Initialize Data
- 16: Initialize Application
- 17: Start Application
- 18: Stop Application
- 19: Save Configuration
- 20: Enable Unsolicited Messages
- 21: Disable Unsolicited Messages
- 22: Assign Class
- 23: Delay Measurement
- 24: Record Current Time
- 25: Open File
- 26: Close File
- 27: Delete File
- 28: Get File Information
- 29: Authenticate File
- 30: Abort File Transfer
- 31: Activate Configuration
- 32: Authenticate Request
- 33: Authenticate Request-No Acknowledgement
- 129: Response
- 130: Unsolicited Response
- 131: Authentication Response

- P-4: 1..317
  - Comma separated index values e.g. 1,2,3.
  - Comma separated index and range of index values e.g. 1-10,120-300.
- P-5: enable
t- P-5: disable
- P-6: enable
t- P-6: disable
- P-7: enable
t- P-7: disable
- P-8: enable
t- P-8: disable

**10.1.17 dpi dnp3 profile delete**

Deletes a profile from the DPI DNP3 profile table. You cannot delete an active profile or if an enforcer mappings to it.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi dnp3 profile delete <P-1>

**Parameter** | **Value** | **Meaning**
--- | --- | ---
P-1 | 1..32 | DNP3 profile index.
10.1.18 dpi dnp3 profile enable
Enables a profile in the DPI DNP3 profile table. A profile can only be activated when all required parameters are set. After activation modifications no longer possible.
- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: `dpi dnp3 profile enable <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>DNP3 profile index.</td>
</tr>
</tbody>
</table>

10.1.19 dpi dnp3 profile disable
Disables a profile in the DPI DNP3 profile table. You cannot inactivate a profile if an active enforcer mappings to it.
- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: `dpi dnp3 profile disable <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>DNP3 profile index.</td>
</tr>
</tbody>
</table>

10.1.20 dpi dnp3 profile commit
Writes all changes made in the DPI DNP3 profiles to the enforcer.
- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: `dpi dnp3 profile commit`

10.1.21 dpi dnp3 profile copy
Copies a profile to another DPI DNP3 profile.
- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: `dpi dnp3 profile copy <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Source index of DPI DNP3 profile.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..32</td>
<td>Destination index of DPI DNP3 profile.</td>
</tr>
</tbody>
</table>

10.1.22 dpi dnp3 object add
Adds an object to a DPI DNP3 rule.
- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: `dpi dnp3 object <P-1> add <P-2> object-type <P-3> group-number <P-4> variation-number <P-5> function-code <P-6> [function-name <P-7>] [function-length <P-8>] [qualifier-code-list <P-9>]`

object-type: Object type for DPI DNP3 object.
group-number: Group number for DNP3 object ranging 0-255.
variation-number: Variation number could either be any integer between 0-255 or a range from 0-255.
function-code: Function code for DNP3 object.
[function-name]: Function name for DNP3 object.
[function-length]: Function length for DNP3 Object.
[qualifier-code-list]: Qualifier code list, hexadecimal numbers separated by a comma(e.g numbers ranging between 0x00 to 0xFF).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>DNP3 profile index.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..32</td>
<td>DNP3 Object index.</td>
</tr>
<tr>
<td>P-3</td>
<td>request</td>
<td>Request</td>
</tr>
<tr>
<td></td>
<td>response</td>
<td>Response</td>
</tr>
<tr>
<td>P-4</td>
<td>0..255</td>
<td>Group number for DNP3 object.</td>
</tr>
<tr>
<td>P-5</td>
<td>string</td>
<td>Variation Number for DNP3 object.</td>
</tr>
<tr>
<td>P-6</td>
<td>0..255</td>
<td>Function code for DNP3 object.</td>
</tr>
<tr>
<td>P-7</td>
<td>string</td>
<td>Function Name for DNP3 object.</td>
</tr>
<tr>
<td>P-8</td>
<td>string</td>
<td>Function Length for DNP3 object.</td>
</tr>
<tr>
<td>P-9</td>
<td>string</td>
<td>Qualifier code list, hexadecimal numbers separated by a comma(e.g numbers ranging between 0x00 to 0xFF).</td>
</tr>
</tbody>
</table>
### 10.1.23 dpi dnp3 object delete

Deletes an object from a DPI DNP3 rule.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi dnp3 object <P-1> delete <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>DNP3 profile index.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..256</td>
<td>DNP3 Object index.</td>
</tr>
</tbody>
</table>

### 10.2 show

Display device options and settings.

#### 10.2.1 show dpi modbus profiletable

Display the DPI MODBUS profile table.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show dpi modbus profiletable

#### 10.2.2 show dpi modbus pending

Display whether uncommitted changes for DPI MODBUS enforcer exist.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show dpi modbus pending

#### 10.2.3 show dpi opc profiletable

Display the DPI OPC profile table.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show dpi opc profiletable

#### 10.2.4 show dpi opc pending

Display whether uncommitted changes for DPI OPC enforcer exist.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show dpi opc pending

#### 10.2.5 show dpi dnp3 profiletable

Display the DPI DNP3 profile table.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show dpi dnp3 profiletable

#### 10.2.6 show dpi dnp3 pending

Display whether uncommitted changes for DPI DNP3 enforcer exist.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show dpi dnp3 pending

#### 10.2.7 show dpi dnp3 objectlist

Display the DPI DNP3 object list for a profile.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show dpi dnp3 objectlist <P-1> [P-2]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>DNP3 profile index.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..256</td>
<td>DNP3 Object index.</td>
</tr>
</tbody>
</table>
11 Filtering Database (FDB)

11.1 mac-filter

11.1.1 mac-filter
Static MAC filter configuration.

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: mac-filter <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>aa:bb:cc:dd:ee:ff</td>
<td>MAC address.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

no mac-filter
Disable the option

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: no mac-filter <P-1> <P-2>

11.2 bridge
Bridge configuration.

11.2.1 bridge aging-time
Aging time configuration.

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: bridge aging-time <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>10..500000</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

11.3 show
Display device options and settings.

11.3.1 show mac-filter-table static
Display the MAC address filter table.

- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show mac-filter-table static

11.4 show
Display device options and settings.

11.4.1 show bridge aging-time
Address aging time.

- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show bridge aging-time
11.5 **show**
Display device options and settings.

11.5.1 **show mac-addr-table**
Display the MAC address table.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: `show mac-addr-table [<P-1>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>a:b:c:d:e:f</td>
<td>Enter a MAC address.</td>
</tr>
<tr>
<td></td>
<td>1..4042</td>
<td>Enter a VLAN ID.</td>
</tr>
</tbody>
</table>

11.6 **clear**
Clear several items.

11.6.1 **clear mac-addr-table**
Clears the MAC address table.
- **Mode**: Privileged Exec Mode
- **Privilege Level**: Operator
- **Format**: `clear mac-addr-table`
12 Firewall Learning Mode (FLM)

12.1 flm
Configure the firewall learning mode.

12.1.1 flm operation
Enable/disable the firewall learning mode.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: flm operation <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable the firewall learning mode.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the firewall learning mode.</td>
</tr>
</tbody>
</table>

no flm operation
Disable the option
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: no flm operation <P-1>

12.1.2 flm action
Set the action for the firewall learning mode.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: flm action <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>start</td>
<td>Start a learning phase.</td>
</tr>
<tr>
<td></td>
<td>stop</td>
<td>Stop a learning phase.</td>
</tr>
<tr>
<td></td>
<td>continue</td>
<td>Continue the previous learning phase.</td>
</tr>
<tr>
<td></td>
<td>clear</td>
<td>Clear the learned data.</td>
</tr>
</tbody>
</table>

12.1.3 flm interface add
Add an interface to the firewall learning mode.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: flm interface add <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

12.1.4 flm interface delete
Delete an interface from the firewall learning mode.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: flm interface delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

12.2 show
Display device options and settings.

12.2.1 show flm global
Display the information and settings for the firewall learning mode.
- Mode: Command is in all modes available
- Privilege Level: Guest
- Format: show flm global
12.2.2  show flm interface

Display the interfaces selected for the firewall learning mode

- **Mode:** Command is in all modes available
- **Privilege Level:** Guest
- **Format:** show flm interface
13 HiDiscovery

13.1 network
Configure the inband and outband connectivity.

13.1.1 network hidiscovery operation
Enable/disable the HiDiscovery protocol on this device.
| Mode: Privileged Exec Mode |
|Privilege Level: Operator |
|Format: network hidiscovery operation <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable the HiDiscovery protocol.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the HiDiscovery protocol.</td>
</tr>
</tbody>
</table>

no network hidiscovery operation
Disable the option
| Mode: Privileged Exec Mode |
|Privilege Level: Operator |
|Format: no network hidiscovery operation <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable the HiDiscovery protocol.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the HiDiscovery protocol.</td>
</tr>
</tbody>
</table>

13.1.2 network hidiscovery mode
Set the access level for HiDiscovery.
| Mode: Privileged Exec Mode |
|Privilege Level: Operator |
|Format: network hidiscovery mode <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>read-write</td>
<td>Allow detection and configuration.</td>
</tr>
<tr>
<td></td>
<td>read-only</td>
<td>Allow only detection, no configuration.</td>
</tr>
</tbody>
</table>

13.2 show
Display device options and settings.

13.2.1 show network hidiscovery
Display the HiDiscovery settings.
| Mode: Command is in all modes available. |
|Privilege Level: Guest |
|Format: show network hidiscovery
14 Hypertext Transfer Protocol (HTTP)

14.1 http
Set HTTP parameters.

14.1.1 http port
Set the HTTP port number.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: http port <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..65535</td>
<td>Port number of the HTTP server (default: 80).</td>
</tr>
</tbody>
</table>

14.1.2 http server
Enable or disable the HTTP server.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: http server

`no http server`
Disable the option
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: no http server

14.2 show
Display device options and settings.

14.2.1 show http
Display the HTTP server information.
- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show http
15 HTTP Secure (HTTPS)

15.1 https
Set HTTPS parameters.

15.1.1 https server
Enable or disable the HTTPS server.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: https server

no https server
Disable the option
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: no https server

15.1.2 https port
Set the HTTPS port number.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: https port <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..65535</td>
<td>Port number of the web server (default: 443).</td>
</tr>
</tbody>
</table>

15.1.3 https fingerprint-type
Configure fingerprint type.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: https fingerprint-type <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>sha1</td>
<td>Configure sha1 fingerprint</td>
</tr>
<tr>
<td></td>
<td>sha256</td>
<td>Configure sha256 fingerprint</td>
</tr>
</tbody>
</table>

15.1.4 https certificate
Generate/Delete HTTPS X509/PEM certificate.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: https certificate <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>generate</td>
<td>Generates the item</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>Deletes the item</td>
</tr>
</tbody>
</table>

15.2 copy
Copy different kinds of items.

15.2.1 copy httpscert remote
Copy X509/PEM certificate from a server to the specified destination.
- Mode: Privileged Exec Mode
- Privilege Level: Administrator
- Format: copy httpscert remote <P-1> nvm
  nvm: Copy HTTPS certificate (PEM) from a server to the device.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>
15.2.2  **copy https-cert envm**

Copy X509/PEM certificate from external non-volatile memory to the specified destination.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `copy https-cert envm <P-1> nvm`

`nvm:` Copy X509/PEM certificate from external non-volatile memory to the device.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

15.3  **show**

Display device options and settings.

15.3.1  **show https**

Display the HTTPS server information.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show https`
16 Interface

16.1 shutdown

16.1.1 shutdown
Enable or disable the interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** shutdown

**no shutdown**
Disable the option

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** no shutdown

16.2 auto-negotiate

16.2.1 auto-negotiate
Enable or disable automatic negotiation on the interface. The cable crossing settings have no effect if auto-negotiation is enabled. In this case cable crossing is always set to auto. Cable crossing is set to the value chosen by the user if auto-negotiation is disabled.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** auto-negotiate

**no auto-negotiate**
Disable the option

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** no auto-negotiate

16.3 auto-power-down

16.3.1 auto-power-down
Set the auto-power-down mode on the interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** auto-power-down <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>auto-power-save</td>
<td>The port goes in a low power mode.</td>
</tr>
<tr>
<td></td>
<td>no-power-save</td>
<td>The port does not use the automatic power save mode.</td>
</tr>
</tbody>
</table>

16.4 cable-crossing

16.4.1 cable-crossing
Cable crossing settings on the interface. The cable crossing settings have no effect if auto-negotiation is enabled. In this case cable crossing is always set to auto. Cable crossing is set to the value chosen by the user if auto-negotiation is disabled.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** cable-crossing <P-1>
16.5 linktraps

16.5.1 linktraps
Enable/disable link up/down traps on the interface.
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: linktraps

no linktraps
Disable the option
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: no linktraps

16.6 speed

16.6.1 speed
Sets the speed and duplex setting for the interface.
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: speed <P-1> [<P-2>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>mdi</td>
<td>The port does not use the crossover mode.</td>
</tr>
<tr>
<td></td>
<td>mdix</td>
<td>The port uses the crossover mode.</td>
</tr>
<tr>
<td></td>
<td>auto-mdix</td>
<td>The port uses the auto crossover mode.</td>
</tr>
<tr>
<td>P-1</td>
<td>10</td>
<td>10 MBit/s.</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>100 MBit/s.</td>
</tr>
<tr>
<td></td>
<td>1000</td>
<td>1000 MBit/s.</td>
</tr>
<tr>
<td>P-2</td>
<td>full</td>
<td>full duplex.</td>
</tr>
<tr>
<td></td>
<td>half</td>
<td>half duplex.</td>
</tr>
</tbody>
</table>

16.7 name

16.7.1 name
Set or remove a descriptive name for the interface.
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: name <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 64 characters.</td>
</tr>
</tbody>
</table>

16.8 power-state

16.8.1 power-state
Enable or disable the power state on the interface. The interface power state settings have no effect if the interface admin state is enabled.
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: power-state
no power-state

Disable the option

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** no power-state

### 16.9 show

Display device options and settings.

#### 16.9.1 show port

Display the interface parameters.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show port [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>
17 Interface Statistics

17.1 clear
Clear several items.

17.1.1 clear port-statistics
Clear all statistics counter.
- Mode: Privileged Exec Mode
- Privilege Level: Operator
- Format: clear port-statistics

17.2 show
Display device options and settings.

17.2.1 show interface counters
Display the interface counters.
- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show interface counters

17.2.2 show interface statistics
Display the summary interface statistics.
- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show interface statistics [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

17.2.3 show interface ether-stats
Display the detailed interface statistics.
- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show interface ether-stats [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>
18 Intern

18.1 help
Display the help text for various special keys.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** help

18.2 logout
Exit this session.
- **Mode:** Command is in all modes available.
- **Privilege Level:** any
- **Format:** logout

18.3 history
Display a list of previously run commands.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** history

18.4 serviceshell
Enter system mode.

18.4.1 serviceshell start
Start serviceshell prompt
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** serviceshell start

18.4.2 serviceshell deactivate
Disable the service shell access permanently (Cannot be undone).
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** serviceshell deactivate

18.5 traceroute
Trace route to a specified host.

18.5.1 traceroute source
Source address for traceroute command.
- **Mode:** Privileged Exec Mode.
- **Privilege Level:** Operator
- **Format:** traceroute <P-1> source <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Hostname or IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>
18.6 reboot
Reset the device (cold start).
- **Mode:** All Privileged Modes
- **Privilege Level:** any
- **Format:** reboot

18.7 ping
Send ICMP echo packets to a specified host or IP address.

18.7.1 ping source
Source address for ping command.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** ping \(<P-1>\) source \(<P-2>\)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Hostname or IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

18.8 show
Display device options and settings.

18.8.1 show serviceshell
Display the service shell access.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show serviceshell
19 Intrusion Detection System (IDS)

19.1 ids
Configure the Intrusion Detection System feature.

19.1.1 ids operation
Enable/disable Intrusion Detection System feature.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ids operation

- **no ids operation**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no ids operation

19.1.2 ids user
Assign/Remove an existing administrator privilege user for Intrusion Detection System feature.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ids user <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 12 characters).</td>
</tr>
</tbody>
</table>

- **no ids user**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no ids user

19.2 show
Display device options and settings.

19.2.1 show ids global
Display the information and settings for the intrusion detection system.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ids global
20 Open Shortest Path First (OSPF)

20.1 ip

Set IP parameters.

20.1.1 ip ospf area

Administer the OSPF areas. An area is a sub-division of an OSPF autonomous system. You identify an area by an area-id. OSPF networks, routers, and links that have the same area-id form a logical set.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip ospf area <P-1> range add <P-2> <P-3> <P-4> modify <P-5> <P-6> <P-7> <P-8> delete <P-9> <P-10> <P-11> add delete stub add <P-12> modify <P-13> summary lsa <P-14> default-cost <P-15> delete <P-16> virtual-link add <P-17> delete <P-18> modify <P-19> authentication type <P-20> key <P-21> key-id <P-22> hello-interval <P-23> dead-interval <P-24> transmit-delay <P-25> retransmit-interval <P-26> nssa add <P-27> delete <P-28> modify translator role <P-29> stability-interval <P-30> summary no-redistribute default-info originate [metric <P-31>] [metric-type <P-32>]

**range:** Configure the range for the area. You summarize the networks within this range into a single routing domain.
- **add:** Create an area.
- **modify:** Modify the parameters of an existing area.
- **delete:** Delete a specific area.
- **add:** Create a new area.
- **delete:** Delete an existing area.
- **stub:** Configure the preferences for a stub area. You shield stub areas from external route advertisements, but the area receives advertisements from networks that belong to other areas of the same autonomous system.
- **add:** Create a stub area. The command also allows you to convert an existing area to a stub area.
- **modify:** Modify the stub area parameters.
- **summary lsa:** Configure the summary LSA mode for a stub area. When enabled, the router both summarizes and propagates summary LSAs.
- **default-cost:** Set the default cost for the stub area.
- **delete:** Remove a stub area. After removal, the area receives external route advertisements.
- **virtual-link:** Configure a virtual link. You use the virtual link to connect the router to the backbone area (0.0.0.0) through a non-backbone area or to connect two parts of a partitioned backbone area (0.0.0.0) through a non-backbone area.
- **add:** Add a virtual neighbor.
- **delete:** Delete a virtual neighbor.
- **modify:** Modify the parameters of a virtual neighbor.
- **authentication:** Configure the authentication type. The device authenticates the OSPF protocol exchanges in the OSPF packet header which includes an authentication type field.
- **type:** Configure the authentication type. Authentication types are 0 for null authentication, 1 for simple password authentication, and 2 for cryptographic authentication.
- **key:** Configure the authentication key.
- **key-id:** Configure the authentication key-id for md5 authentication. This field identifies the algorithm and secret key used to create the message digest appended to the OSPF packet.
- **hello-interval:** Configure the OSPF hello-interval for the virtual link, in seconds. The hello timer controls the time interval between sending two consecutive hello packets. Set this value to the same hello-interval value of the virtual neighbors.
- **dead-interval:** Configure the OSPF dead-interval for the virtual link, in seconds. If the timer expires without the router receiving hello packets from a virtual neighbor, the router declares the neighbor router as down. Set the timer to at least four times the value of the hello-interval.
- **transmit-delay:** Configure the OSPF transmit-delay for the virtual link, in seconds. Transmit delay is the time that you estimate it takes to transmit a link-state update packet over the virtual link.
- **retransmit-interval:** Configure the OSPF retransmit-interval for the virtual link, in seconds. The retransmit interval is the time between two consecutive link-state advertisement transmissions. Link-state advertisements contain such information as database descriptions and link-state request packets for adjacencies belonging to virtual link.
- **nssa:** Configure a NSSA(Not-So-Stubby-Area).
- **add:** Add a NSSA.
**delete**: Delete a NSSA.

**modify**: Modify the parameters of a NSSA.

**translator**: Configure the NSSA translator related parameters.

**role**: Configure the NSSA translator role.

**stability-interval**: Configure the translator stability interval for the NSSA, in seconds.

**summary**: Configure the import summary for the specified NSSA.

**no-redistribute**: Configure route redistribution for the specified NSSA.

**default-info**: Configure the nssa default information origination parameters.

**originate**: Configuration whether a Type-7 LSA should be originated into the NSSA.

**[metric]**: Configure the metric for the NSSA.

**[metric-type]**: Configure the metric type for default information.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>
| P-2             |          | summary-link
|                 |           | Configure summary links LSDB type optional mode.                        |
|                 |           | nssa-external-link
|                 |           | Configure nssa external link LSDB type optional mode.                   |
| P-3             | A.B.C.D   | IP address.                                                             |
| P-4             | a.b.c.d   | IP subnet mask.                                                         |
| P-5             |          | summary-link
|                 |           | Configure summary links LSDB type optional mode.                        |
|                 |           | nssa-external-link
|                 |           | Configure nssa external link LSDB type optional mode.                   |
| P-6             | A.B.C.D   | IP address.                                                             |
| P-7             | a.b.c.d   | IP subnet mask.                                                         |
| P-8             | advertise | Set as advertise.                                                       |
|                 | do-not-advertise | Set as do-not-advertise.                             |
| P-9             |          | summary-link
|                 |           | Configure summary links LSDB type optional mode.                        |
|                 |           | nssa-external-link
|                 |           | Configure nssa external link LSDB type optional mode.                   |
| P-10            | A.B.C.D   | IP address.                                                             |
| P-11            | a.b.c.d   | IP subnet mask.                                                         |
| P-12            | 0         | Configure the TOS (0 is for Normal Service).                            |
| P-13            | 0         | Configure the TOS (0 is for Normal Service).                            |
| P-14            | no-area-summary | Disable the router from sending area link state advertisement summaries. |
|                 | send-area-summary | Enable the router to send area link state advertisement summaries. The router floods LSAs within the area using multicast. Every topology change starts a new flood of LSAs. |
| P-15            | 0..16777215 | Configure the default cost.                                           |
| P-16            | 0         | Configure the TOS (0 is for Normal Service).                            |
| P-17            | A.B.C.D   | IP address.                                                             |
| P-18            | A.B.C.D   | IP address.                                                             |
| P-19            | A.B.C.D   | IP address.                                                             |
| P-20            | none      | Configure the authentication type as none (Key and key ID is not required). |
|                 | simple    | Configure the authentication type as simple (Key ID is not required).    |
|                 | md5       | Configure the authentication type as md5 for the interface.             |
| P-21            | string    | <key> Configure the authentication key.                                 |
| P-22            | 0..255    | Enter a number in the given range.                                      |
| P-23            | 1..65535  | Enter a number between 1 and 65535.                                     |
| P-24            | 1..65535  | Enter a number between 1 and 65535.                                     |
| P-25            | 0..3600   | Enter a number in the given range.                                      |
| P-26            | 0..3600   | Enter a number in the given range.                                      |
| P-27            | import-nssa | Configure the area as NSSA only.                                      |
| P-28            | import-external | Change the area to support external LSAs also.                        |
| P-29            | always    | Configure the NSSA translator role as always. When used as a border router, the router translates LSAs regardless of the translator states of the other NSSA border routers. |
|                 | candidate | Configure the NSSA translator role as candidate. When used as a border router, the router participates in the translator election process. The router maintains a list of reachable NSSA border routers. |
| P-30            | 0..65535  | Enter a number between 0 and 65535.                                     |
| P-31            | 1..16777214 | Configure the metric value.                                           |
| P-32            | ospf-metric | Set the metric type as ospf Metric.                                    |
|                 | comparable-cost | Set the metric type as comparable cost.                                |
|                 | non-comparable | Set the metric type as non-comparable.                                 |
no ip ospf area
Disable the option
  Mode: Global Config Mode
  Privilege Level: Operator
  Format: no ip ospf area <P-1> range add modify delete add delete stub add modify summarylsa default-cost delete virtual-link add delete modify authentication type key key-id hello-interval dead-interval transmit-delay retransmit-interval nssa add delete modify translator role stability-interval summary no- redistribute default-info originate [metric] [metric-type]

20.1.2 ip ospf trapflags all
Set all trapflags at once.
  Mode: Global Config Mode
  Privilege Level: Operator
  Format: ip ospf trapflags all <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>[or]</td>
<td>Enable the Bit.</td>
</tr>
</tbody>
</table>

no ip ospf trapflags all
Disable the option
  Mode: Global Config Mode
  Privilege Level: Operator
  Format: no ip ospf trapflags all <P-1>

20.1.3 ip ospf operation
Enable or disable the OSPF admin mode. When enabled, the device initiates the OSPF process if the OSPF function is active on at least one interface.
  Mode: Global Config Mode
  Privilege Level: Operator
  Format: ip ospf operation

no ip ospf operation
Disable the option
  Mode: Global Config Mode
  Privilege Level: Operator
  Format: no ip ospf operation

20.1.4 ip ospf 1583compatibility
Enable or disable the 1583compatibility for calculating routes external to the autonomous system. When enabled, the router is compatible with the preference rules defined in RFC1583, section 16.4.
  Mode: Global Config Mode
  Privilege Level: Operator
  Format: ip ospf 1583compatibility

no ip ospf 1583compatibility
Disable the option
  Mode: Global Config Mode
  Privilege Level: Operator
  Format: no ip ospf 1583compatibility

20.1.5 ip ospf default-metric
Configure the default metric for re-distributed routes, when OSPF redistributes routes from other protocols.
  Mode: Global Config Mode
  Privilege Level: Operator
  Format: ip ospf default-metric <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.16777214</td>
<td>Configure the default metric for redistributed routes.</td>
</tr>
</tbody>
</table>

no ip ospf default-metric
Disable the option
  Mode: Global Config Mode
  Privilege Level: Operator
  Format: no ip ospf default-metric <P-1>
20.1.6 ip ospf router-id

Configure the router ID to uniquely identify this OSPF router in the autonomous system. If a tie occurs during the designated router election, the router with the higher router ID is the designated router.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip ospf router-id <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.16777214</td>
<td>Configure the default metric for redistributed routes.</td>
</tr>
</tbody>
</table>

20.1.7 ip ospf external-lsdb-limit

Configure the OSPF external lsdb limitation, which is the maximum number of non-default AS-external-LSA entries that the router stores in the link-state database. When the value -1 is configured, you disable the limitation.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip ospf external-lsdb-limit <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

20.1.8 ip ospf exit-overflow

Configure the OSPF exit overflow interval, in seconds. After the timer expires the router will attempt to leave the overflow-state. To disable the exit overflow interval function set the value to 0.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip ospf exit-overflow <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>-1.2147483647</td>
<td>Configure the external lsdb limit.</td>
</tr>
</tbody>
</table>

20.1.9 ip ospf maximum-path

Configure the maximum number of paths that OSPF reports.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip ospf maximum-path <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>Set the maximum path.</td>
</tr>
</tbody>
</table>

20.1.10 ip ospf spf-delay

Configure the SPF delay, in seconds. The Shortest Path First (SPF) delay is the time that the device waits for the network to stabilize before calculating the shortest path tree, after a topology change.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip ospf spf-delay <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..65535</td>
<td>Enter a number between 0 and 65535</td>
</tr>
</tbody>
</table>

20.1.11 ip ospf spf-holdtime

Configure the minimum time between two consecutive SPF calculations, in seconds.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip ospf spf-holdtime <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..65535</td>
<td>Enter a number between 0 and 65535</td>
</tr>
</tbody>
</table>

20.1.12 ip ospf auto-cost

Set the auto cost reference bandwidth of the router interfaces for ospf metric calculations. The default reference bandwidth is 100 Mbps.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip ospf auto-cost <P-1>
20.1.13 ip ospf distance intra
Enter the preference type as intra. Use intra-area routing when the device routes packets solely within an area, such as an internal router.

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip ospf distance intra <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4294967</td>
<td>Configure the auto cost for OSPF calculation.</td>
</tr>
</tbody>
</table>

20.1.14 ip ospf distance inter
Enter the preference type as inter. Use inter-area routing when the device routes packets into or out of an area, such as an area border router.

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip ospf distance inter <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter the value.</td>
</tr>
</tbody>
</table>

20.1.15 ip ospf distance external
Enter the preference type as external. Use external-area routing when the device routes packets into or out of an autonomous system, such as an autonomous system boundary router (ASBR).

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip ospf distance external <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.255</td>
<td>Enter the value.</td>
</tr>
</tbody>
</table>

20.1.16 ip ospf re-distribute
Configure the OSPF route re-distribution. An ASBR is able to translate information from other OSPF processes in separate areas and routes from other sources, such as static routes or other dynamic routing protocols, into the OSPF protocol.

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip ospf re-distribute <P-1> [metric <P-2>] [metric-type <P-3>] [tag <P-4>] [subnets <P-5>]
  - [metric]: Configure the OSPF route re-distribution metric parameters.
  - [metric-type]: Configure the OSPF route redistribution metric-type.
  - [tag]: Configure the OSPF route redistribution tag parameters.
  - [subnets]: Allow the router to redistribute subnets into OSPF.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>connected</td>
<td>Select the source protocol as connected.</td>
</tr>
<tr>
<td></td>
<td>static</td>
<td>Select the source protocol as static.</td>
</tr>
<tr>
<td>P-2</td>
<td>0..16777214</td>
<td>Configure the metric.</td>
</tr>
<tr>
<td>P-3</td>
<td>1..2</td>
<td>Configure the metric type.</td>
</tr>
<tr>
<td>P-4</td>
<td>0..4294967295</td>
<td>Configure the tag.</td>
</tr>
<tr>
<td>P-5</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

- no ip ospf re-distribute
Disable the option

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: no ip ospf re-distribute <P-1>

20.1.17 ip ospf distribute-list
Configure the distribute list for the routes from other source protocols.

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip ospf distribute-list <P-1> <P-2>
no ip ospf distribute-list
Disable the option
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: no ip ospf distribute-list <P-1> <P-2>

20.1.18 ip ospf default-info originate
Originate the OSPF default information.
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: ip ospf default-info originate [always] [metric <P-1>] [metric-type <P-2>] [always]: Always advertise the 0.0.0.0/0.0.0.0 route information.
[metric]: Configure the metric for default information.
[metric-type]: Configure the metric type for default information.

Parameter | Value | Meaning
--- | --- | ---
P-1 | 1..16777214 | Configure the metric value.
P-2 | external-type1 | Set the metric type for default information as external type-1. The type 1 value sets the metric to the sum of the internal and external OSPF metrics.
| external-type2 | Set the metric type for default information as external type-2. The type 2 value sets the metric to the sum of external OSPF metrics from the source AS to the destination AS.

no ip ospf default-info originate
Disable the option
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: no ip ospf default-info originate [always] [metric <P-1>]

20.2 ip
IP interface commands.

20.2.1 ip ospf operation
Enable or disable OSPF on port.
► Mode: Interface Range Mode
► Privilege Level: Operator
► Format: ip ospf operation

no ip ospf operation
Disable the option
► Mode: Interface Range Mode
► Privilege Level: Operator
► Format: no ip ospf operation

20.2.2 ip ospf area-id
Configure the area ID that uniquely identifies the area to which the interface is connected.
► Mode: Interface Range Mode
► Privilege Level: Operator
► Format: ip ospf area-id <P-1>

Parameter | Value | Meaning
--- | --- | ---
P-1 | A.B.C.D | IP address.

20.2.3 ip ospf link-type
Configure the OSPF link type.
► Mode: Interface Range Mode
► Privilege Level: Operator
► Format: ip ospf link-type <P-1>
20.2.4 ip ospf priority
Configure the OSPF router priority which the router uses in multi-access networks for the designated router election algorithm. The router with the higher router priority is the designated router. A value of 0 declares the router as ineligible for designated router elections.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td></td>
<td>Configure the priority.</td>
</tr>
</tbody>
</table>

20.2.5 ip ospf transmit-delay
Configure the OSPF transmit-delay for the interface, in seconds. The transmit-delay is the time that you estimate it takes to transmit a link-state update packet over the interface.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0.3600</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

20.2.6 ip ospf retransmit-interval
Configure the OSPF retransmit-interval for the interface, in seconds. The retransmit-interval is the interval after which link-state advertisements containing database description and link-state request packets, are re-transmitted for adjacencies belonging to this interface.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0.3600</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

20.2.7 ip ospf hello-interval
Configure the OSPF hello-interval for the interface, in seconds. The hello timer controls the time interval between two consecutive hello packets. Set this value to the same hello-interval value of the neighbor.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.65535</td>
<td>Enter a number between 1 and 65535</td>
</tr>
</tbody>
</table>

20.2.8 ip ospf dead-interval
Configure the OSPF dead-interval for the interface, in seconds. If the timer expires without the router receiving hello packets from the neighbor, the router declares the neighbor router as down. Set the timer to at least four times the value of the hello-interval.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.65535</td>
<td>Enter a number between 1 and 65535</td>
</tr>
</tbody>
</table>
20.2.9  ip ospf cost
Configure the OSPF cost for the interface. The cost of a specific interface indicates the overhead required to send packets across the link. If set to 0, OSPF calculates the cost from the reference bandwidth and the interface speed.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip ospf cost <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1-</td>
<td>Auto cost for OSPF calculation</td>
</tr>
<tr>
<td></td>
<td>4294967_hmcilist0</td>
<td>SPFcost</td>
</tr>
</tbody>
</table>

20.2.10  ip ospf mtu-ignore
Enable/Disable OSPF MTU mismatch on interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip ospf mtu-ignore

- **no ip ospf mtu-ignore**
  Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** no ip ospf mtu-ignore

20.2.11  ip ospf authentication type
Configure authentication type.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip ospf authentication type <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>none</td>
<td>Configure the authentication type as none (Key and key ID is not required).</td>
</tr>
<tr>
<td></td>
<td>simple</td>
<td>Configure the authentication type as simple (Key ID is not required).</td>
</tr>
<tr>
<td></td>
<td>md5</td>
<td>Configure the authentication type as md5 for the interface.</td>
</tr>
</tbody>
</table>

20.2.12  ip ospf authentication key
Configure authentication key.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip ospf authentication key <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Configure the authentication key.</td>
</tr>
</tbody>
</table>

20.2.13  ip ospf authentication key-id
Configure authentication key-id for md5 authentication.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip ospf authentication key-id <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

20.3  show
Display device options and settings.

20.3.1  show ip ospf global
Display the OSPF global configurations.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip ospf global
20.3.2  show ip ospf area
Display the OSPF area related information.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show ip ospf area [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

20.3.3  show ip ospf stub
Display the OSPF stub area related information.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show ip ospf stub

20.3.4  show ip ospf database internal
Display the internal LSA database information.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show ip ospf database internal

20.3.5  show ip ospf database external
Display the external LSA database information.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show ip ospf database external

20.3.6  show ip ospf range
Display the OSPF area range information.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show ip ospf range

20.3.7  show ip ospf interface
Display the OSPF interface related information.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show ip ospf interface [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td></td>
<td>slot no./port no.</td>
</tr>
</tbody>
</table>

20.3.8  show ip ospf virtual-link
Display the OSPF virtual-link related information.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show ip ospf virtual-link <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

20.3.9  show ip ospf virtual-neighbor
Display the OSPF Virtual-link neighbor information
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show ip ospf virtual-neighbor

20.3.10 show ip ospf neighbor
Display the OSPF neighbor related information.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show ip ospf neighbor [<P-1>]
20.3.11 show ip ospf statistics
Display the OSPF statistics.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show ip ospf statistics

20.3.12 show ip ospf re-distribute
Display the OSPF re-distribute related information
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show ip ospf re-distribute <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

20.3.13 show ip ospf nssa
Display the OSPF NSSA related information.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show ip ospf nssa <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>connected</td>
<td>Select the source protocol as connected.</td>
</tr>
<tr>
<td></td>
<td>static</td>
<td>Select the source protocol as static.</td>
</tr>
<tr>
<td></td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

20.3.14 show ip ospf route
Display the OSPF routes.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show ip ospf route
21 Virtual Router Redundancy Protocol (VRRP)

21.1 ip
Set IP parameters.

21.1.1 ip vrrp operation
Enables or disables VRRP globally on the device.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip vrrp operation

no ip vrrp operation
Disable the option
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: no ip vrrp operation

21.1.2 ip vrrp trap auth-failure
Enable or disable the sending of a trap if this router detects an authentication failure on any of its VRRP interfaces.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip vrrp trap auth-failure

no ip vrrp trap auth-failure
Disable the option
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: no ip vrrp trap auth-failure

21.1.3 ip vrrp trap new-master
Enable or disable the sending of a trap if this router becomes new master for any of its VRRP interfaces.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip vrrp trap new-master

no ip vrrp operation
Disable the option
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: no ip vrrp trap new-master

21.2 ip
IP interface commands.

21.2.1 ip vrrp add
Create a new VRRP instance.
- Mode: Interface Range Mode.
- Privilege Level: Operator
- Format: ip vrrp add <P-1> [priority <P-2>] [interval <P-3>]
  [priority]: Priority of the virtual router ..... default 100
  [interval]: Advertisement Interval in seconds .. default 1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..254</td>
<td>Enter a priority value.</td>
</tr>
<tr>
<td>P-3</td>
<td>1..255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>
21.2.2  ip vrrp modify
Modify parameters of a VRRP instance.
  ▶ Mode: Interface Range Mode.
  ▶ Privilege Level: Operator
  ▶ Format: ip vrrp modify <P-1> [priority <P-2>] [interval <P-3>]
    [priority]: Priority of the virtual router
    [interval]: Advertisement Interval in seconds

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..254</td>
<td>Enter a priority value.</td>
</tr>
<tr>
<td>P-3</td>
<td>1..255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

21.2.3  ip vrrp delete
Delete a VRRP instance.
  ▶ Mode: Interface Range Mode.
  ▶ Privilege Level: Operator
  ▶ Format: ip vrrp delete

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
</tbody>
</table>

21.2.4  ip vrrp enable
Enable a VRRP instance.
  ▶ Mode: Interface Range Mode.
  ▶ Privilege Level: Operator
  ▶ Format: ip vrrp enable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
</tbody>
</table>

21.2.5  ip vrrp disable
Enable a VRRP instance.
  ▶ Mode: Interface Range Mode.
  ▶ Privilege Level: Operator
  ▶ Format: ip vrrp disable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
</tbody>
</table>

21.2.6  ip vrrp virtual-address add
Add a virtual address.
  ▶ Mode: Interface Range Mode.
  ▶ Privilege Level: Operator
  ▶ Format: ip vrrp virtual-address add <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

21.2.7  ip vrrp virtual-address delete
Delete a virtual address.
  ▶ Mode: Interface Range Mode.
  ▶ Privilege Level: Operator
  ▶ Format: ip vrrp virtual-address add <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

21.2.8  ip vrrp track add
Add a tracking object to the vrrp instance.
  ▶ Mode: Interface Range Mode.
  ▶ Privilege Level: Operator
  ▶ Format: ip vrrp track add <P-1> <P-2> [decrement <P-3>]
    [decrement]: Configure the decrement value. Default is 20

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
</tbody>
</table>
### 21.2.9 `ip vrrp track modify`

Modify a tracking object to the vrrp instance.

- **Mode:** Interface Range Mode.
- **Privilege Level:** Operator
- **Format:** `ip vrrp track modify <P-1> <P-2> [decrement <P-3>]

  [decrement]: Configure the decrement value. Default is 20

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Track instance.</td>
</tr>
<tr>
<td>P-3</td>
<td>1..253</td>
<td>Enter the decrement value. The priority will be decremented by the configured value.</td>
</tr>
</tbody>
</table>

### 21.2.10 `ip vrrp track delete`

Delete a tracking object to the vrrp instance.

- **Mode:** Interface Range Mode.
- **Privilege Level:** Operator
- **Format:** `ip vrrp track delete <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Track instance.</td>
</tr>
</tbody>
</table>

### 21.3 `show`

Display device options and settings.

#### 21.3.1 `show ip vrrp interface`

Show parameters of one VRRP instances.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ip vrrp interface [<P-1> [<P-2>]]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
</tbody>
</table>

#### 21.3.2 `show ip vrrp global`

Show global VRRP parameters.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ip vrrp global`
22 Address Resolution Protocol (IP ARP)

22.1 ip
Set IP parameters.

22.1.1 ip arp add
Add a static arp entry.
- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: ip arp add <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

22.1.2 ip arp delete
Delete a static arp entry.
- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: ip arp delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

22.1.3 ip arp enable
Enable a static arp entry.
- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: ip arp enable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>a.b.c.d</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

22.1.4 ip arp disable
Disable a static arp entry.
- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: ip arp disable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>a.b.c.d</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

22.1.5 ip arp timeout
Configure ARP entry age-out time (in seconds).
- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: ip arp timeout <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>15..21600</td>
<td>Enter the arp response time.</td>
</tr>
</tbody>
</table>

22.1.6 ip arp response-time
Configure ARP request response timeout (in seconds).
- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: ip arp response-time <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10</td>
<td>Enter the arp response time.</td>
</tr>
</tbody>
</table>

22.1.7 ip arp retries
Configure ARP count of maximum requests for retries.
- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: ip arp retries <P-1>
### 22.2 show
Display device options and settings.

#### 22.2.1 show ip arp info
Displays ARP summary information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ip arp info`

#### 22.2.2 show ip arp table
Displays ARP cache entries.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ip arp table`

#### 22.2.3 show ip arp static
Displays static ARP entries.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ip arp static`

#### 22.2.4 show ip arp entry
Displays ARP cache entry.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ip arp entry <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10</td>
<td>Enter the arp max retries.</td>
</tr>
</tbody>
</table>

### 22.3 clear
Clear several items.

#### 22.3.1 clear ip arp-cache
Clear IP data of several items.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** `clear ip arp-cache [gateway]`
  - [gateway]: Also clear gateway ARP entries.
23 L3 Relay

23.1 ip
Set IP parameters.

23.1.1 ip udp-helper operation
Enable or disable the IP helper and DHCP relay.
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: ip udp-helper operation

no ip udp-helper operation
Disable the option
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: no ip udp-helper operation

23.1.2 ip udp-helper server add
Add a global relay agent to process DHCP client requests and UDP broadcast packets received on any interface.
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: ip udp-helper server add <P-1> <P-2>

23.1.3 ip udp-helper server delete
Delete a global relay agent.
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: ip udp-helper server delete <P-1> <P-2>

23.1.4 ip udp-helper server enable
Enable a global relay agent to process DHCP client requests and UDP broadcast packets received on any interface.
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: ip udp-helper server enable <P-1> <P-2>

23.1.5 ip udp-helper server disable
Disable a global relay agent from processing DHCP client requests and UDP broadcast packets received on any interface.
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: ip udp-helper server disable <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>67_hmcclist_ipHelp</td>
<td>DHCP server port number.</td>
</tr>
<tr>
<td></td>
<td>rUdpPorts</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>67_hmcclist_ipHelp</td>
<td>DHCP server port number.</td>
</tr>
<tr>
<td></td>
<td>rUdpPorts</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>67_hmcclist_ipHelp</td>
<td>DHCP server port number.</td>
</tr>
<tr>
<td></td>
<td>rUdpPorts</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>67_hmcclist_ipHelp</td>
<td>DHCP server port number.</td>
</tr>
<tr>
<td></td>
<td>rUdpPorts</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>
23.1.6 ip udp-helper maxhopcount
Configure the DHCP relay maximum hop count.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `ip udp-helper maxhopcount <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1-16</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

23.1.7 ip udp-helper minwaittime
Configure DHCP relay minimum wait time in seconds.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `ip udp-helper minwaittime <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0-100</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

23.1.8 ip udp-helper cidoptmode
Enable or disable DHCP relay circuit id option mode.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `ip udp-helper cidoptmode

- **no ip udp-helper cidoptmode**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Operator
  - **Format:** no ip udp-helper cidoptmode

23.2 ip
IP interface commands.

23.2.1 ip udp-helper server add
Add a relay agent to process DHCP client requests and UDP broadcast packets received on a specific interface.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip udp-helper server add <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>67_hmclList_lprUdpPorts</td>
<td>DHCP server port number.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

23.2.2 ip udp-helper server delete
Delete a relay agent from a specific interface.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip udp-helper server delete <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>67_hmclList_lprUdpPorts</td>
<td>DHCP server port number.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

23.2.3 ip udp-helper server enable
Enable a relay agent to process DHCP client requests and UDP broadcast packets received on a specific interface.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip udp-helper server enable <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>67_hmclList_lprUdpPorts</td>
<td>DHCP server port number.</td>
</tr>
</tbody>
</table>
23.2.4  **ip udp-helper server disable**
Disable a relay agent from processing DHCP client requests and UDP broadcast packets received on a specific interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip udp-helper server disable <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>67_hmccliList_IpHelper_udpPorts</td>
<td>DHCP server port number.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

23.3  **show**
Display device options and settings.

23.3.1  **show ip udp-helper status**
Display the IP helper and DHCP relay status information.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ip udp-helper status`

23.3.2  **show ip udp-helper global**
Display the DHCP and UDP relays defined globally.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ip udp-helper global`

23.3.3  **show ip udp-helper interface**
Display the DHCP and UDP relays defined for specific interfaces.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ip udp-helper interface [P-1]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

23.3.4  **show ip udp-helper statistics**
Display the IP helper and DHCP relay statistics.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ip udp-helper statistics`

23.4  **clear**
Clear several items.

23.4.1  **clear ip udp-helper**
Reset IP helper and DHCP relay statistics.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** `clear ip udp-helper`
24 Internet Protocol Version 4 (IPv4)

24.1 network
Configure the inband and outbound connectivity.

24.1.1 network parms
Set network address, netmask and gateway
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** network parms <P-1> <P-2> [<P-3>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

24.2 clear
Clear several items.

24.2.1 clear arp-table-switch
Clear the agent's ARP table (cache).
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** clear arp-table-switch

24.3 show
Display device options and settings.

24.3.1 show network parms
Display the network settings.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show network parms

24.4 show
Display device options and settings.

24.4.1 show arp
Display the ARP table.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show arp
25 Link Layer Discovery Protocol (LLDP)

25.1 lldp
Configure of Link Layer Discovery Protocol.

25.1.1 lldp operation
Enable or disable the LLDP operational state.
Mode: Global Config Mode
Privilege Level: Operator
Format: lldp operation

no lldp operation
Disable the option
Mode: Global Config Mode
Privilege Level: Operator
Format: no lldp operation

25.1.2 lldp config chassis admin-state
Enable or disable the LLDP operational state.
Mode: Global Config Mode
Privilege Level: Operator
Format: lldp config chassis admin-state <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td>P-1</td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

25.1.3 lldp config chassis notification-interval
Enter the LLDP notification interval in seconds.
Mode: Global Config Mode
Privilege Level: Operator
Format: lldp config chassis notification-interval <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>5..3600</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

25.1.4 lldp config chassis tx-hold-multiplier
Enter the LLDP transmit hold multiplier.
Mode: Global Config Mode
Privilege Level: Operator
Format: lldp config chassis tx-hold-multiplier <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>2..10</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

25.1.5 lldp config chassis tx-interval
Enter the LLDP transmit interval in seconds.
Mode: Global Config Mode
Privilege Level: Operator
Format: lldp config chassis tx-interval <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>5.32768</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

25.2 show
Display device options and settings.
25.2.1 show lldp global
Display the LLDP global configurations.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show lldp global

25.2.2 show lldp port
Display the port specific LLDP configurations.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show lldp port [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

25.2.3 show lldp remote-data
Remote information collected with LLDP.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show lldp remote-data [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

25.3 lldp
Configure of Link Layer Discovery Protocol on a port.

25.3.1 lldp admin-state
Configure how the interface processes LLDP frames.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** lldp admin-state <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>tx-only</td>
<td>Interface will only transmit LLDP frames. Received frames are not processed.</td>
</tr>
<tr>
<td></td>
<td>rx-only</td>
<td>Interface will only receive LLDP frames. Frames are not transmitted.</td>
</tr>
<tr>
<td></td>
<td>tx-and-rx</td>
<td>Interface will transmit and receive LLDP frames. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Interface will neither transmit nor process received LLDP frames.</td>
</tr>
</tbody>
</table>

25.3.2 lldp fdb-mode
Configure the LLDP FDB mode for this interface.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** lldp fdb-mode <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>lldp-only</td>
<td>Collected remote data will be based on received LLDP frames only.</td>
</tr>
<tr>
<td></td>
<td>mac-only</td>
<td>Collected remote data will be based on the switch's FDB entries only.</td>
</tr>
<tr>
<td></td>
<td>both</td>
<td>Collected remote data will be based on received LLDP frames as well as on the switch's FDB entries.</td>
</tr>
<tr>
<td></td>
<td>auto-detect</td>
<td>As long as no LLDP frames are received, the collected remote data will be based on the switch's FDB entries only. After the first LLDP frame is received, the remote data will be based on received LLDP frames only. This is the default setting.</td>
</tr>
</tbody>
</table>

25.3.3 lldp max-neighbors
Enter the LLDP max neighbors for interface.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** lldp max-neighbors <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..50</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>
25.3.4  lldp notification
Enable or disable the LLDP notification operation for interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp notification`

**no lldp notification**
Disable the option

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `no lldp notification`

25.3.5  lldp tlv port-desc
Enable or disable port description TLV transmission.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp tlv port-desc <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>[cr]</td>
<td>Enable the Bit.</td>
</tr>
</tbody>
</table>

**no lldp tlv port-desc**
Disable the option

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `no lldp tlv port-desc <P-1>`

25.3.6  lldp tlv sys-cap
Enable or disable system capabilities TLV transmission.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp tlv sys-cap <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>[cr]</td>
<td>Enable the Bit.</td>
</tr>
</tbody>
</table>

**no lldp tlv sys-cap**
Disable the option

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `no lldp tlv sys-cap <P-1>`

25.3.7  lldp tlv sys-desc
Enable or disable system description TLV transmission.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp tlv sys-desc <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>[cr]</td>
<td>Enable the Bit.</td>
</tr>
</tbody>
</table>

**no lldp tlv sys-desc**
Disable the option

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `no lldp tlv sys-desc <P-1>`

25.3.8  lldp tlv sys-name
Enable or disable system name TLV transmission.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp tlv sys-name <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>[cr]</td>
<td>Enable the Bit.</td>
</tr>
</tbody>
</table>
- **no lldp tlv sys-name**
  - Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** no lldp tlv sys-name <P-1>
# 26 Logging

## 26.1 logging

Logging configuration.

### 26.1.1 logging audit-trail

Add a comment for the audit trail.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `logging audit-trail <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 80 characters.</td>
</tr>
</tbody>
</table>

### 26.1.2 logging buffered severity

Configure the minimum severity level to be logged to the high priority buffer.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `logging buffered severity <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>emergency</td>
<td>System is unusable. System failure has occurred.</td>
</tr>
<tr>
<td></td>
<td>alert</td>
<td>Action must be taken immediately. Unrecoverable failure of a component. System failure likely.</td>
</tr>
<tr>
<td></td>
<td>critical</td>
<td>Recoverable failure of a component that may lead to system failure.</td>
</tr>
<tr>
<td></td>
<td>error</td>
<td>Error conditions. Recoverable failure of a component.</td>
</tr>
<tr>
<td></td>
<td>warning</td>
<td>Minor failure, e.g. misconfiguration of a component.</td>
</tr>
<tr>
<td></td>
<td>notice</td>
<td>Normal but significant conditions.</td>
</tr>
<tr>
<td></td>
<td>informational</td>
<td>Informational messages.</td>
</tr>
<tr>
<td></td>
<td>debug</td>
<td>Debug-level messages.</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>Same as emergency</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Same as alert</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Same as critical</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Same as error</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Same as warning</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Same as notice</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Same as informational</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>Same as debug</td>
</tr>
</tbody>
</table>

### 26.1.3 logging host add

Add a new logging host.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `logging host add <P-1> addr <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..8</td>
<td>Syslog server entry index</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

### 26.1.4 logging host delete

Delete a logging host.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `logging host delete <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..8</td>
<td>Syslog server entry index</td>
</tr>
</tbody>
</table>

### 26.1.5 logging host enable

Enable a logging host.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `logging host enable <P-1>`
26.1.6 logging host disable
Disable a logging host.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** logging host disable <P-1>

Parameter | Value | Meaning
--- | --- | ---
P-1 | 1..8 | Syslog server entry index

26.1.7 logging host modify
Modify an existing logging host.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** logging host modify <P-1> [addr <P-2>]
  [addr]: Enter the IP address of the server.

Parameter | Value | Meaning
--- | --- | ---
P-1 | 1..8 | Syslog server entry index
P-2 | a.b.c.d | IP address.

26.1.8 logging syslog operation
Enable or disable the syslog client.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** logging syslog operation

- **no logging syslog operation**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no logging syslog operation

26.1.9 logging current-console operation
Enable or disable logging messages to the current remote console.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** logging current-console operation

- **no logging current-console operation**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no logging current-console operation

26.1.10 logging current-console severity
Configure the minimum severity level to be sent to the current remote console.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** logging current-console severity <P-1>
26.1.11 logging console operation
Enable or disable logging to the local V.24 console.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** logging console operation

```plaintext
no logging console operation
```
Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** no logging console operation

26.1.12 logging console severity
Configure the minimum severity level to be logged to the V.24 console.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** logging console severity <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>emergency</td>
<td>System is unusable. System failure has occurred.</td>
</tr>
<tr>
<td></td>
<td>alert</td>
<td>Action must be taken immediately. Unrecoverable failure of a component. System failure likely.</td>
</tr>
<tr>
<td></td>
<td>critical</td>
<td>Recoverable failure of a component that may lead to system failure.</td>
</tr>
<tr>
<td></td>
<td>error</td>
<td>Error conditions. Recoverable failure of a component.</td>
</tr>
<tr>
<td></td>
<td>warning</td>
<td>Minor failure, e.g. misconfiguration of a component.</td>
</tr>
<tr>
<td></td>
<td>notice</td>
<td>Normal but significant conditions.</td>
</tr>
<tr>
<td></td>
<td>informational</td>
<td>Informational messages.</td>
</tr>
<tr>
<td></td>
<td>debug</td>
<td>Debug-level messages.</td>
</tr>
<tr>
<td>0</td>
<td>Same as emergency</td>
<td>System is unusable. System failure has occurred.</td>
</tr>
<tr>
<td>1</td>
<td>Same as alert</td>
<td>Action must be taken immediately. Unrecoverable failure of a component. System failure likely.</td>
</tr>
<tr>
<td>2</td>
<td>Same as critical</td>
<td>Recoverable failure of a component that may lead to system failure.</td>
</tr>
<tr>
<td>3</td>
<td>Same as error</td>
<td>Error conditions. Recoverable failure of a component.</td>
</tr>
<tr>
<td>4</td>
<td>Same as warning</td>
<td>Minor failure, e.g. misconfiguration of a component.</td>
</tr>
<tr>
<td>5</td>
<td>Same as notice</td>
<td>Normal but significant conditions.</td>
</tr>
<tr>
<td>6</td>
<td>Same as informational</td>
<td>Informational messages.</td>
</tr>
<tr>
<td>7</td>
<td>Same as debug</td>
<td>Debug-level messages.</td>
</tr>
</tbody>
</table>

26.2 show
Display device options and settings.
26.2.1 show logging buffered
Display the buffered (in-memory) log entries.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show logging buffered [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;P-1&gt;</td>
<td>string</td>
<td>&lt;filter&gt; Enter a comma separated list of severity ranges, numbers or enum strings are allowed. Example: 0-1, informational-debug</td>
</tr>
</tbody>
</table>

26.2.2 show logging traplogs
Display the trap log entries.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show logging traplogs

26.2.3 show logging console
Display the console logging configurations.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show logging console

26.2.4 show logging persistent
Display the persistent logging configurations.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show logging persistent [logfiles] [logfiles]: List the persistent log files.

26.2.5 show logging syslog
Display the current syslog operational setting.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show logging syslog

26.2.6 show logging host
Display a list of logging hosts currently configured.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show logging host

26.3 copy
Copy different kinds of items.

26.3.1 copy eventlog buffered envm
Copy a buffered log from the device to external non-volatile memory.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** copy eventlog buffered envm <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;P-1&gt;</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>

26.3.2 copy eventlog buffered remote
Copy a buffered log from the device to a file server.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** copy eventlog buffered remote <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;P-1&gt;</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>
26.3.3  copy eventlog persistent
Copy the persistent logs from the device to an envm or a file server.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** `copy eventlog persistent <P-1> envm <P-2> remote <P-3>
envm`: Copy the persistent log from the device to external non-volatile memory.
remote: Copy the persistent logs from the device to a file server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
<tr>
<td>P-3</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

26.3.4  copy traplog system envm
Copy the traplog from the device to external non-volatile memory.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** `copy traplog system envm <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>

26.3.5  copy traplog system remote
Copy the traplog from the device to a file server.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** `copy traplog system remote <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

26.3.6  copy audittrail system envm
Copy the audit trail from the device to external non-volatile memory.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator, Auditor
- **Format:** `copy audittrail system envm <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>

26.3.7  copy audittrail system remote
Copy the audit trail from the device to a file server.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator, Auditor
- **Format:** `copy audittrail system remote <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

26.4  clear
Clear several items.

26.4.1  clear logging buffered
Clear buffered log from memory.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `clear logging buffered`

26.4.2  clear logging persistent
Clear persistent log from memory.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `clear logging persistent`
26.4.3 clear eventlog

Clear the event log entries from memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** clear eventlog
27 Management Access

27.1 network
Configure the inband and outband connectivity.

27.1.1 network management access web timeout
Set the web interface idle timeout.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** network management access web timeout <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..160</td>
<td>Idle timeout of a session in minutes (default: 5).</td>
</tr>
</tbody>
</table>

27.1.2 network management access add
Add a new entry with index.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** network management access add <P-1> [ip <P-2>] [mask <P-3>] [http <P-4>] [https <P-5>] [snmp <P-6>]

- [ip]: Configure IP address which should have access to management.
- [mask]: Configure network mask to allow a subnet for management access.
- [http]: Configure if HTTP is allowed to have management access.
- [https]: Configure if HTTPS is allowed to have management access.
- [snmp]: Configure if SNMP is allowed to have management access.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..16</td>
<td>Pool entry index.</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>0..32</td>
<td>Prefix length netmask.</td>
</tr>
<tr>
<td>P-4</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
<tr>
<td>P-5</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
<tr>
<td>P-6</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

27.1.3 network management access delete
Delete an entry with index.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** network management access delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..16</td>
<td>Pool entry index.</td>
</tr>
</tbody>
</table>

27.1.4 network management access modify
Modify an entry with index.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** network management access modify <P-1> ip <P-2> mask <P-3> http <P-4> https <P-5> snmp <P-6> ssh <P-7>

- [ip]: Configure ip-address which should have access to management.
- [mask]: Configure network mask to allow a subnet for management access.
- [http]: Configure if HTTP is allowed to have management access.
- [https]: Configure if HTTPS is allowed to have management access.
- [snmp]: Configure if SNMP is allowed to have management access.
- [ssh]: Configure if SSH is allowed to have management access.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..16</td>
<td>Pool entry index.</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>0..32</td>
<td>Prefix length netmask.</td>
</tr>
</tbody>
</table>
27.1.5 network management access operation

Enable/Disable operation for RMA.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** network management access operation

- **no network management access operation**
  Disable the option
  - **Mode:** Privileged Exec Mode
  - **Privilege Level:** Administrator
  - **Format:** no network management access operation

27.1.6 network management access status

Activate/Deactivate an entry.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** network management access status <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..16</td>
<td>Pool entry index.</td>
</tr>
</tbody>
</table>

- **no network management access status**
  Disable the option
  - **Mode:** Privileged Exec Mode
  - **Privilege Level:** Administrator
  - **Format:** no network management access status <P-1>

27.2 show

Display device options and settings.

27.2.1 show network management access global

Display the global restricted management access preferences.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show network management access global

27.2.2 show network management access rules

Display the restricted management access rules.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show network management access rules [P-1]
28 Network Address Translation (NAT)

28.1 nat
Manage NAT rules

28.1.1 nat dnat commit
Commit pending changes for DNAT (commits all NAT changes).
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: nat dnat commit

28.1.2 nat dnat add
Add rule to DNAT
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: nat dnat add <P-1> [cfg <P-2> <P-3> <P-4> <P-5> <P-6> <P-7> <P-8> [<P-9>]]
[cfg]: Configure the rule immediately

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>Source IP address</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d/n</td>
<td>CIDR mask</td>
</tr>
<tr>
<td></td>
<td>!a.b.c.d</td>
<td>Everything BUT this address</td>
</tr>
<tr>
<td></td>
<td>!a.b.c.d/n</td>
<td>Everything BUT this CIDR mask</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any</td>
</tr>
<tr>
<td>P-3</td>
<td>number</td>
<td>number UDP/TCP Source Port</td>
</tr>
<tr>
<td></td>
<td>nu-nu</td>
<td>nu-nu Port Range</td>
</tr>
<tr>
<td></td>
<td>nu,nu-nu</td>
<td>nu,nu-nu List of ports (or port ranges)</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any Any port (or protocol without a port)</td>
</tr>
<tr>
<td>P-4</td>
<td>a.b.c.d</td>
<td>Destination IP address</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d/n</td>
<td>CIDR mask</td>
</tr>
<tr>
<td></td>
<td>!a.b.c.d</td>
<td>Everything BUT this address</td>
</tr>
<tr>
<td></td>
<td>!a.b.c.d/n</td>
<td>Everything BUT this CIDR mask</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any</td>
</tr>
<tr>
<td>P-5</td>
<td>number</td>
<td>number of the UDP/TCP Destination Port</td>
</tr>
<tr>
<td></td>
<td>nu-nu</td>
<td>nu-nu Port Range</td>
</tr>
<tr>
<td></td>
<td>number,number</td>
<td>number,number List of ports (or port ranges)</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any Any port (or protocol without a port)</td>
</tr>
<tr>
<td>P-6</td>
<td>a.b.c.d</td>
<td>New destination IP address</td>
</tr>
<tr>
<td>P-7</td>
<td>number</td>
<td>number of the UDP/TCP New Destination Port</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any Any port (or protocol without a port)</td>
</tr>
<tr>
<td>P-8</td>
<td>icmp</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td></td>
<td>igmp</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td></td>
<td>ipip</td>
<td>IP-within-IP Encapsulation Protocol</td>
</tr>
<tr>
<td></td>
<td>tcp</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td></td>
<td>udp</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td></td>
<td>esp</td>
<td>Encapsulating Security Protocol</td>
</tr>
<tr>
<td></td>
<td>ah</td>
<td>Authentication Header</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any of the above</td>
</tr>
<tr>
<td>P-9</td>
<td>string</td>
<td>Rule description/name</td>
</tr>
</tbody>
</table>

28.1.3 nat dnat modify
Configure single DNAT rule
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: nat dnat modify <P-1> <P-2> <P-3> <P-4> <P-5> <P-6> <P-7> <P-8> [P-9]}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
</tbody>
</table>
28.1.4 nat dnat delete
Delete rule from DNAT
Mode: Global Config Mode
Privilege Level: Operator
Format: nat dnat delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
</tbody>
</table>

28.1.5 nat dnat logtrap
Set log/trap for DNAT rule
Mode: Global Config Mode
Privilege Level: Operator
Format: nat dnat logtrap <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>no</td>
<td>Disable Logging</td>
</tr>
<tr>
<td></td>
<td>yes</td>
<td>Enable Logging</td>
</tr>
<tr>
<td>P-3</td>
<td>no</td>
<td>Disable SNMP Trap</td>
</tr>
<tr>
<td></td>
<td>yes</td>
<td>Enable SNMP Trap</td>
</tr>
</tbody>
</table>

28.1.6 nat dnat state
Enable/Disable specific DNAT rule
Mode: Global Config Mode
Privilege Level: Operator
Format: nat dnat state <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>
### 28.1.7 nat dnat if add

Add Interface

- **Mode:** Global Config Mode  
- **Privilege Level:** Operator  
- **Format:** `nat dnat if add <P-1> <P-2> <P-3>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
<tr>
<td>P-3</td>
<td>0..4294967295</td>
<td>Priority</td>
</tr>
</tbody>
</table>

### 28.1.8 nat dnat if delete

Delete interface

- **Mode:** Global Config Mode  
- **Privilege Level:** Operator  
- **Format:** `nat dnat if delete <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
</tbody>
</table>

### 28.1.9 nat 1to1nat commit

Commit pending changes for 1:1 NAT (commits every NAT change).

- **Mode:** Global Config Mode  
- **Privilege Level:** Operator  
- **Format:** `nat 1to1nat commit`

### 28.1.10 nat 1to1nat add

Add rule to 1:1 NAT

- **Mode:** Global Config Mode  
- **Privilege Level:** Operator  
- **Format:** `nat 1to1nat add <P-1> [cfg <P-2> <P-3> <P-4>] [ingress <P-5>] [egress <P-6> [<P-7>]]`

  - `[cfg]`: Configure the rule immediately  
  - `[ingress]`: Configure ingress interface  
  - `[egress]`: Configure egress interface

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>1:1 NAT rule number</td>
</tr>
</tbody>
</table>
| P-2       | a.b.c.d | Virtual destination IP address  
|           | a.b.c.d/n | CIDR mask |
| P-3       | a.b.c.d | Actual destination IP address  
|           | a.b.c.d/n | CIDR mask |
| P-4       | 0..4294967295 | Priority |
| P-5       | slot no./port no. |         |
| P-6       | slot no./port no. |         |
| P-7       | string | Rule description/name |

### 28.1.11 nat 1to1nat modify

Configure single 1:1 NAT rule

- **Mode:** Global Config Mode  
- **Privilege Level:** Operator  
- **Format:** `nat 1to1nat modify <P-1> <P-2> <P-3> <P-4> [ingress <P-5>] [egress <P-6> [<P-7>]]`

  - `[ingress]`: Configure ingress interface  
  - `[egress]`: Configure egress interface

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>1:1 NAT rule number</td>
</tr>
</tbody>
</table>
| P-2       | a.b.c.d | Virtual destination IP address  
|           | a.b.c.d/n | CIDR mask |
| P-3       | a.b.c.d | Actual destination IP address  
|           | a.b.c.d/n | CIDR mask |
| P-4       | 0..4294967295 | Priority |
| P-5       | slot no./port no. |         |
| P-6       | slot no./port no. |         |
| P-7       | string | Rule description/name |
28.1.12 nat 1to1nat delete
Delete the rule from 1:1 NAT
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: nat 1to1nat delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.256</td>
<td>1:1 NAT rule number</td>
</tr>
</tbody>
</table>

28.1.13 nat 1to1nat logtrap
Set log/trap for 1:1 NAT rule
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: nat 1to1nat logtrap <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.256</td>
<td>1:1 NAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>no</td>
<td>Disable Logging</td>
</tr>
<tr>
<td></td>
<td>yes</td>
<td>Enable Logging</td>
</tr>
<tr>
<td>P-3</td>
<td>no</td>
<td>Disable SNMP Trap</td>
</tr>
<tr>
<td></td>
<td>yes</td>
<td>Enable SNMP Trap</td>
</tr>
</tbody>
</table>

28.1.14 nat 1to1nat state
Enable/Disable specific 1:1 NAT rule
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: nat 1to1nat state <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.256</td>
<td>1:1 NAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

28.1.15 nat masq commit
Commit pending changes for Masquerading (commits every NAT change).
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: nat masq commit

28.1.16 nat masq add
Add rule to Masquerading
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: nat masq add <P-1> [cfg <P-2> <P-3> <P-4> [<P-5>]]
[cfg]: Configure the rule immediately

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.128</td>
<td>Masquerading rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>Source IP address</td>
</tr>
<tr>
<td></td>
<td>a.b.c/d</td>
<td>CIDR mask</td>
</tr>
<tr>
<td></td>
<td>!a.b.c.d</td>
<td>Everything BUT this address</td>
</tr>
<tr>
<td></td>
<td>!a.b.c/d/n</td>
<td>Everything BUT this CIDR mask</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any</td>
</tr>
<tr>
<td>P-3</td>
<td>number</td>
<td>number UDP/TCP Source Port</td>
</tr>
<tr>
<td></td>
<td>nu-nu</td>
<td>nu-nu Port Range</td>
</tr>
<tr>
<td></td>
<td>nu,nu</td>
<td>nu,nu List of ports (or port ranges)</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any Any port (or protocol without a port)</td>
</tr>
<tr>
<td>P-4</td>
<td>tcp</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td></td>
<td>udp</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any Any protocol at all</td>
</tr>
<tr>
<td>P-5</td>
<td>string</td>
<td>Rule description/name</td>
</tr>
</tbody>
</table>

28.1.17 nat masq modify
Configure single Masquerading rule
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: nat masq modify <P-1> <P-2> <P-3> <P-4> [<P-5>]

Parameter | Value | Meaning          |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.256</td>
<td>Masquerading rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>Source IP address</td>
</tr>
<tr>
<td></td>
<td>a.b.c/d</td>
<td>CIDR mask</td>
</tr>
<tr>
<td></td>
<td>!a.b.c.d</td>
<td>Everything BUT this address</td>
</tr>
<tr>
<td></td>
<td>!a.b.c/d/n</td>
<td>Everything BUT this CIDR mask</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any</td>
</tr>
<tr>
<td>P-3</td>
<td>number</td>
<td>number UDP/TCP Source Port</td>
</tr>
<tr>
<td></td>
<td>nu-nu</td>
<td>nu-nu Port Range</td>
</tr>
<tr>
<td></td>
<td>nu,nu</td>
<td>nu,nu List of ports (or port ranges)</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any Any port (or protocol without a port)</td>
</tr>
<tr>
<td>P-4</td>
<td>tcp</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td></td>
<td>udp</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any Any protocol at all</td>
</tr>
<tr>
<td>P-5</td>
<td>string</td>
<td>Rule description/name</td>
</tr>
</tbody>
</table>
### 28.1.18 nat masq delete

Delete rule from Masquerading

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `nat masq delete <P-1>`

#### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
</tbody>
</table>

### 28.1.19 nat masq logtrap

Set log/trap for Masquerading rule

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `nat masq logtrap <P-1> <P-2> <P-3>`

#### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>no</td>
<td>Disable Logging</td>
</tr>
<tr>
<td></td>
<td>yes</td>
<td>Enable Logging</td>
</tr>
<tr>
<td>P-3</td>
<td>no</td>
<td>Disable SNMP Trap</td>
</tr>
<tr>
<td></td>
<td>yes</td>
<td>Enable SNMP Trap</td>
</tr>
</tbody>
</table>

### 28.1.20 nat masq ipsec-exempt

Exclude IPsec traffic from Masquerading rule

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `nat masq ipsec-exempt <P-1> <P-2>`

#### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>disabled</td>
<td>Apply rule to IPsec traffic</td>
</tr>
<tr>
<td></td>
<td>enabled</td>
<td>Do not apply rule to IPsec traffic</td>
</tr>
</tbody>
</table>

### 28.1.21 nat masq state

Enable/Disable specific Masquerading rule

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `nat masq state <P-1> <P-2>`

#### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

### 28.1.22 nat masq if add

Add interface

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `nat masq if add <P-1> <P-2> <P-3>`

#### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td>Masquerading rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
</tbody>
</table>
28.1.23 nat masq if delete
Delete interface
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** nat masq if delete <P-1> <P-2>

### Parameter | Value   | Meaning
---|---|---
P-1 | slot no./port no. | Masquerading rule number
P-2 | 1..128 | Masquerading rule number

28.1.24 nat doublenat commit
Commit pending changes for Double NAT (commits all NAT changes).
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** nat doublenat commit

28.1.25 nat doublenat add
Add rule to Double NAT
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** nat doublenat add <P-1> [cfg <P-2> <P-3> <P-4> <P-5> [<P-6>]]
  - [cfg]: Configure the rule immediately

### Parameter | Value | Meaning
---|---|---
P-1 | 1..255 | Double NAT rule number
P-2 | a.b.c.d | Local internal IP address
P-3 | a.b.c.d | Local external IP address
P-4 | a.b.c.d | Remote Internal IP Address
P-5 | a.b.c.d | Remote External IP Address
P-6 | string | Rule description/name

28.1.26 nat doublenat modify
Configure single Double NAT rule
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** nat doublenat modify <P-1> <P-2> <P-3> <P-4> <P-5> [<P-6>]

### Parameter | Value | Meaning
---|---|---
P-1 | 1..255 | Double NAT rule number
P-2 | a.b.c.d | Local internal IP address
P-3 | a.b.c.d | Local external IP address
P-4 | a.b.c.d | Remote Internal IP Address
P-5 | a.b.c.d | Remote External IP Address
P-6 | string | Rule description/name

28.1.27 nat doublenat delete
Delete rule from Double NAT
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** nat doublenat delete <P-1>

### Parameter | Value | Meaning
---|---|---
P-1 | 1..255 | Double NAT rule number

28.1.28 nat doublenat logtrap
Set log/trap for Double NAT rule
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** nat doublenat logtrap <P-1> <P-2> <P-3>

### Parameter | Value | Meaning
---|---|---
P-1 | 1..255 | Double NAT rule number
P-2 | no | Disable Logging
    | yes | Enable Logging
28.1.29 nat doublenat state
Enable/Disable specific Double NAT rule
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: nat doublenat state <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1-255</td>
<td>Double NAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

28.1.30 nat doublenat if add
Add Interface
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: nat doublenat if add <P-1> <P-2> <P-3> <P-4>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>ingress</td>
<td>Ingress</td>
</tr>
<tr>
<td></td>
<td>egress</td>
<td>Egress</td>
</tr>
<tr>
<td></td>
<td>both</td>
<td>Both</td>
</tr>
<tr>
<td>P-3</td>
<td>1-255</td>
<td>Double NAT rule number</td>
</tr>
<tr>
<td>P-4</td>
<td>0-4294967295</td>
<td>Priority</td>
</tr>
</tbody>
</table>

28.1.31 nat doublenat if delete
Delete Interface
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: nat doublenat if delete <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>ingress</td>
<td>Ingress</td>
</tr>
<tr>
<td></td>
<td>egress</td>
<td>Egress</td>
</tr>
<tr>
<td></td>
<td>both</td>
<td>Both</td>
</tr>
<tr>
<td>P-3</td>
<td>1-255</td>
<td>Double NAT rule number</td>
</tr>
</tbody>
</table>

28.2 show
Display device options and settings.

28.2.1 show nat dnat rules
Show DNAT rules.
- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show nat dnat rules [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1-255</td>
<td>DNAT rule number</td>
</tr>
</tbody>
</table>

28.2.2 show nat dnat if
Show DNAT interface configuration.
- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show nat dnat if
28.2.3 show nat dnat logtrap

Show Log/Trap settings for DNAT rules.

- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show nat dnat logtrap [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
</tbody>
</table>

28.2.4 show nat masq rules

Show Masquerading rules.

- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show nat masq rules [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
</tbody>
</table>

28.2.5 show nat masq logtrap

Show Log/Trap settings for Masquerading rules.

- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show nat masq logtrap [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
</tbody>
</table>

28.2.6 show nat masq if

Show Masquerading interface configuration.

- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show nat masq if

28.2.7 show nat 1to1nat rules

Show 1:1 NAT rules.

- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show nat 1to1nat rules [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>1:1 NAT rule number</td>
</tr>
</tbody>
</table>

28.2.8 show nat 1to1nat logtrap

Show 1:1 NAT rules.

- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show nat 1to1nat logtrap [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>1:1 NAT rule number</td>
</tr>
</tbody>
</table>

28.2.9 show nat doublesnat rules

Show Double NAT rules.

- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show nat doublesnat rules [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Double NAT rule number</td>
</tr>
</tbody>
</table>

28.2.10 show nat doublesnat logtrap

Display the Log/Trap settings for Double NAT rules.

- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show nat doublesnat logtrap [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Double NAT rule number</td>
</tr>
</tbody>
</table>
28.2.11 show nat doublenat if

Show Double NAT interface configuration.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show nat doublenat if
29 Network Time Protocol (NTP)

29.1 ntp

Configure NTP settings.

29.1.1 ntp client operation

Enable or disable the NTP client.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: ntp client operation <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

29.1.2 ntp client operating-mode

Set the NTP client operating mode.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: ntp client operating-mode <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>unicast</td>
<td>Enable NTP client in unicast operating mode.</td>
</tr>
<tr>
<td></td>
<td>broadcast</td>
<td>Enable NTP client in broadcast operating mode.</td>
</tr>
</tbody>
</table>

29.1.3 ntp server operation

Enable or disable the NTP server.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: ntp server operation <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

29.1.4 ntp server operating-mode

Set the NTP server operating mode.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: ntp server operating-mode <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>symmetric</td>
<td>Enable NTP server in symmetric operating mode.</td>
</tr>
<tr>
<td></td>
<td>client-server</td>
<td>Enable NTP server in client-server operating mode.</td>
</tr>
</tbody>
</table>

29.1.5 ntp server localclock-stratum

Set the stratum of the localclock.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: ntp server localclock-stratum <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..16</td>
<td>Localclock stratum.</td>
</tr>
</tbody>
</table>

29.1.6 ntp peers add

Add a new peer.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: ntp peers add <P-1> ip <P-2> [iburst <P-3>] [burst <P-4>] [prefer <P-5>]
  ip: Set the peer address.
  [iburst]: Speed up the initial synchronization (default: disabled). Used only when operating in client-unicast mode.
  [burst]: Increase the precision on links with high jitter (default: disabled). Used only in client-unicast mode.
  [prefer]: If correctly operating, choose this peer as synchronization source (default: disabled).
29.1.7 ntp peers delete
Delete a peer.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: ntp peers delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>NTP servers index.</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
<tr>
<td>P-4</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
<tr>
<td>P-5</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

29.2 show
Display device options and settings.

29.2.1 show ntp client-status
Status of the NTP client connection.

- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show ntp client-status

29.2.2 show ntp server-status
Overall operational status of the NTP server.

- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show ntp server-status
30 Packet Filter

30.1 packet-filter
Creation and configuration of Firewall rules.

30.1.1 packet-filter l3 commit
Writes all changes made in the L3 firewall configuration to the device
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: packet-filter l3 commit

30.1.2 packet-filter l3 defaultpolicy
Sets the default policy of the L3 and DynFw rule tables
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: packet-filter l3 defaultpolicy <P-1>

30.1.3 packet-filter l3 checksum-validation
Configures the connection tracking checksum validation in Netfilter
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: packet-filter l3 checksum-validation
- no packet-filter l3 checksum-validation
  Disable the option
  - Mode: Global Config Mode
  - Privilege Level: Operator
  - Format: no packet-filter l3 checksum-validation

30.1.4 packet-filter l3 addrule
Adds a rule to the L3 firewall table
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: packet-filter l3 addrule <P-1> <P-2> <P-3> <P-4> <P-5> <P-6> <P-7> <P-8>
  [description <P-9>] [profile-index <P-10>]
  [description]: Rule description/name for the L3 firewall rule
  [profile-index]: Profile index of the DPI profile this rule is assigned to depending on enforcer action. Value
  0 no profile this rule is assigned to. You cannot assign the rule to an inactive profile if an active
  enforcer will mapping to it.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>accept</td>
<td>Accept packets</td>
</tr>
<tr>
<td></td>
<td>drop</td>
<td>Drop packets without notification</td>
</tr>
<tr>
<td></td>
<td>reject</td>
<td>Drop packets and notify source</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-2</td>
<td>string</td>
<td>Source IP address/CIDR mask/'any'</td>
</tr>
<tr>
<td>P-3</td>
<td>string</td>
<td>Source port/port list with comma/port range with hyphen/'any'</td>
</tr>
<tr>
<td>P-4</td>
<td>string</td>
<td>Target IP address/CIDR mask/'any'</td>
</tr>
<tr>
<td>P-5</td>
<td>string</td>
<td>Target port/port list with comma/port range with hyphen/'any'</td>
</tr>
<tr>
<td>P-6</td>
<td>icmp</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td></td>
<td>igmp</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td></td>
<td>ipip</td>
<td>IP-within-IP Encapsulation Protocol</td>
</tr>
<tr>
<td></td>
<td>tcp</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td></td>
<td>udp</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td></td>
<td>esp</td>
<td>Encapsulating Security Protocol</td>
</tr>
<tr>
<td></td>
<td>ah</td>
<td>Authentication Header</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any of the above</td>
</tr>
<tr>
<td>P-7</td>
<td>string</td>
<td>Parameters for rule (or 'none')</td>
</tr>
</tbody>
</table>
30.1.5 packet-filter l3 modifyrule
Modifies a rule to the L3 firewall table
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: packet-filter l3 modifyrule <P-1> <P-2> <P-3> <P-4> <P-5> <P-6> <P-7> <P-8>
[description <P-9>] [profile-index <P-10>]
[description]: Rule description/name for the L3 firewall rule
[profile-index]: Profile index of the DPI profile this rule is assigned to depending on enforcer action. Value 0 no profile this rule is assigned to. You cannot assign the rule to an inactive profile if an active enforcer will mapping to it.

Parameter | Value | Meaning
---|---|---
P-1 | 1..2048 | Rule index
P-2 | string | Source IP address/CIDR mask/'any'
P-3 | string | Source port/port list with comma/port range with hyphen/'any'
P-4 | string | Target IP address/CIDR mask/'any'
P-5 | string | Target port/port list with comma/port range with hyphen/'any'
P-6 | icmp | Internet Control Message Protocol
     | igmp | Internet Group Management Protocol
     | ipip | IP-within-IP Encapsulation Protocol
     | tcp | Transmission Control Protocol
     | udp | User Datagram Protocol
     | esp | Encapsulating Security Protocol
     | ah | Authentication Header
     | any | Any of the above
P-7 | string | Parameters for rule (or 'none')
P-8 | accept | Accept packets
     | drop | Drop packets without notification
     | reject | Drop packets and notify source
     | enforce-modbus | Accept or drop packets by Modbus TCP/IP enforcer, protocol should be tcp or udp
     | enforce-opc | Accept or drop packets by opc enforcer, protocol should be tcp
     | enforce-iec104 | Accept or drop packets by IEC104 enforcer, protocol should be tcp
     | enforce-dnp3 | Accept or drop packets by DNP3 enforcer, protocol should be tcp
P-9 | string | Rule description/name
P-10 | 0..32 | Profile index 0 - 32

30.1.6 packet-filter l3 delrule
Deletes a rule from L3 rule table
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: packet-filter l3 delrule <P-1>

Parameter | Value | Meaning
---|---|---
P-1 | 1..2048 | Rule index

30.1.7 packet-filter l3 enablerule
Enables a rule from L3 rule table. A rule can only be activated when all required parameters are set and at least one interface is mapped to the rule. You cannot activate a rule if an enforcer mappings to an inactive profile.
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: packet-filter l3 enablerule <P-1>

Parameter | Value | Meaning
---|---|---
P-1 | 1..2048 | Rule index
30.1.8 packet-filter l3 disablerule
Disables a rule from L3 rule table
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: packet-filter l3 disablerule <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..2048</td>
<td>Rule index</td>
</tr>
</tbody>
</table>

30.1.9 packet-filter l3 logmode
Set logmode for a rule from L3 rule table
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: packet-filter l3 logmode <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..2048</td>
<td>Rule index</td>
</tr>
<tr>
<td>P-2</td>
<td>log, trap, logtrap, none</td>
<td>Log when rule is applied, Send trap when rule is applied, Log and send trap when rule is applied, Disable log and trap</td>
</tr>
</tbody>
</table>

30.1.10 packet-filter l3 addif
Adds an interface to a L3 firewall rule
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: packet-filter l3 addif <P-1> <P-2> <P-3> <P-4>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>ingress, egress</td>
<td>Rule applies on ingress direction, Rule applies on egress direction</td>
</tr>
<tr>
<td>P-3</td>
<td>1..2048</td>
<td>Rule index</td>
</tr>
<tr>
<td>P-4</td>
<td>0..4294967295</td>
<td>Priority</td>
</tr>
</tbody>
</table>

30.1.11 packet-filter l3 delif
Deletes an interface of a L3 firewall rule
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: packet-filter l3 delif <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>ingress, egress</td>
<td>Rule applies on ingress direction, Rule applies on egress direction</td>
</tr>
<tr>
<td>P-3</td>
<td>1..2048</td>
<td>Rule index</td>
</tr>
</tbody>
</table>

30.1.12 packet-filter l3 enableif
Enables an interface of a L3 firewall rule
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: packet-filter l3 enableif <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>ingress, egress</td>
<td>Rule applies on ingress direction, Rule applies on egress direction</td>
</tr>
<tr>
<td>P-3</td>
<td>1..2048</td>
<td>Rule index</td>
</tr>
</tbody>
</table>

30.1.13 packet-filter l3 disableif
Disables an interface of a L3 firewall rule
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: packet-filter l3 disableif <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>ingress, egress</td>
<td>Rule applies on ingress direction, Rule applies on egress direction</td>
</tr>
</tbody>
</table>
30.1.14 packet-filter l2 commit

Writes all changes made in the L2 firewall configuration to the device.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** packet-filter l2 commit

30.1.15 packet-filter l2 defaultpolicy

Sets the default policy of the L2 rule tables.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** packet-filter l2 defaultpolicy <P-1>

### Parameter | Value | Meaning
--- | --- | ---
P-1 | accept | Accept packets.
drop | Drop packets without notification.

30.1.16 packet-filter l2 fcs-validation

Activates/Deactivates FCS validation.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** packet-filter l2 fcs-validation <P-1>

### Parameter | Value | Meaning
--- | --- | ---
P-1 | enable | Enable the option.
disable | Disable the option.

30.1.17 packet-filter l2 rule add

Adds a rule to the L2 firewall table.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** packet-filter l2 rule add <P-1> action <P-2> [src-mac <P-3>] [dst-mac <P-4>] [src-ip <P-5>] [dest-ip <P-7>] [proto <P-9>] [vlan <P-11>] [assign-queue <P-12>] [description <P-13>] [rate-limit <P-14> <P-15> <P-16>] [tos <P-17>] [log <P-18>] [trap <P-19>

**action:** Set Action
- **[src-mac]:** Specify the source MAC address.
- **[dst-mac]:** Specify the destination MAC address.
- **[src-ip]:** Specify the source IP address/mask.
- **[dest-ip]:** Specify the destination IP address/mask.
- **[destport]:** Specify the destination L4 port.
- **[ethertype]:** Specify the Ethertype.
- **[proto]:** Specify the protocol for L2 firewall rule.
- **[vlan]:** Specify the VLAN ID for L2 firewall rule.
- **[assign-queue]:** Assign a user Queue.
- **[description]:** Rule description/name for the L2 firewall rule.
- **[rate-limit]:** Specify the rate limit and burst size.
- **[tos]:** Specify TOS for L2 rule.
- **[log]:** Set logging.
- **[trap]:** Set sending SNMP traps.

### Parameter | Value | Meaning
--- | --- | ---
P-1 | 1..2048 | Rule index
P-2 | accept | Accept packets.
drop | Drop packets without notification.
P-3 | any | Enter any as a shortcut for the MAC address 00:00:00:00:00:00.
aa:bb:cc:dd:ee:ff | Enter the MAC address in hexadecimal format.
P-4 | any | Enter any as a shortcut for the MAC address 00:00:00:00:00:00.
aa:bb:cc:dd:ee:ff | Enter the MAC address in hexadecimal format.
P-5 | string | Source IP address/CIDR mask/'any'
## no packet-filter l2 rule add

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** no packet-filter l2 rule add action [src-mac] [dst-mac] [src-ip] [sourceport] [dest-ip] [destport] [ethertype] [proto] [vlan] [assign-queue] [description] [rate-limit] [tos] [log <P-18>] [trap <P-19>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-6</td>
<td>any</td>
<td>any Any port/portless protocol</td>
</tr>
<tr>
<td></td>
<td>string</td>
<td>a-b Port Range</td>
</tr>
<tr>
<td></td>
<td>string</td>
<td>a,b Port List (may be longer than two ports)</td>
</tr>
<tr>
<td></td>
<td>string</td>
<td>a-b,c-d List of Port Ranges (may be longer than two ranges)</td>
</tr>
<tr>
<td></td>
<td>string</td>
<td>1 to 65535 Port Number</td>
</tr>
<tr>
<td>P-7</td>
<td>string</td>
<td>Target IP address/CIDR mask/'any'</td>
</tr>
<tr>
<td>P-8</td>
<td>any</td>
<td>any Any port/portless protocol</td>
</tr>
<tr>
<td></td>
<td>string</td>
<td>a-b Port Range</td>
</tr>
<tr>
<td></td>
<td>string</td>
<td>a,b Port List (may be longer than two ports)</td>
</tr>
<tr>
<td></td>
<td>string</td>
<td>a-b,c-d List of Port Ranges (may be longer than two ranges)</td>
</tr>
<tr>
<td></td>
<td>string</td>
<td>1 to 65535 Port Number</td>
</tr>
<tr>
<td>P-9</td>
<td>0x0600-0xffff</td>
<td>value Ethertype</td>
</tr>
<tr>
<td></td>
<td>appletalk</td>
<td>Appletalk</td>
</tr>
<tr>
<td></td>
<td>arp</td>
<td>ARP</td>
</tr>
<tr>
<td></td>
<td>ibmsna</td>
<td>IBMSNA</td>
</tr>
<tr>
<td></td>
<td>ipv4</td>
<td>IPv4</td>
</tr>
<tr>
<td></td>
<td>ipv6</td>
<td>IPv6</td>
</tr>
<tr>
<td></td>
<td>ipx-old</td>
<td>IPX-OLD</td>
</tr>
<tr>
<td></td>
<td>mpls-mcast</td>
<td>MPLS Multicast</td>
</tr>
<tr>
<td></td>
<td>mpls-ucast</td>
<td>MPLS Unicast</td>
</tr>
<tr>
<td></td>
<td>netbios</td>
<td>NetBIOS</td>
</tr>
<tr>
<td></td>
<td>novell</td>
<td>NOVELL</td>
</tr>
<tr>
<td></td>
<td>pppoe-disc</td>
<td>PPPoE DISC</td>
</tr>
<tr>
<td></td>
<td>rarp</td>
<td>RARP</td>
</tr>
<tr>
<td></td>
<td>ppoesess</td>
<td>PPPoESESS</td>
</tr>
<tr>
<td></td>
<td>ipxnew</td>
<td>IPXNEW</td>
</tr>
<tr>
<td></td>
<td>profinet</td>
<td>PROFINET</td>
</tr>
<tr>
<td></td>
<td>powerlink</td>
<td>POWERLINK</td>
</tr>
<tr>
<td></td>
<td>ethercat</td>
<td>ETHERCAT</td>
</tr>
<tr>
<td></td>
<td>vlan8021q</td>
<td>IEEE802.1Q VLAN</td>
</tr>
<tr>
<td>P-10</td>
<td>icmp</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td></td>
<td>igmp</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td></td>
<td>ipip</td>
<td>IP-within-IP Encapsulation Protocol</td>
</tr>
<tr>
<td></td>
<td>tcp</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td></td>
<td>udp</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td></td>
<td>esp</td>
<td>Encapsulating Security Protocol</td>
</tr>
<tr>
<td></td>
<td>ah</td>
<td>Authentication Header</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any of the above</td>
</tr>
<tr>
<td>P-11</td>
<td>1..4042</td>
<td>Enter a VLAN ID in the given range.</td>
</tr>
<tr>
<td>P-12</td>
<td>0..7</td>
<td>Enter a Queue ID in the given range.</td>
</tr>
<tr>
<td>P-13</td>
<td>string</td>
<td>Rule description/name</td>
</tr>
<tr>
<td>P-14</td>
<td>0..10000000</td>
<td>Committed rate value, specified in kbps or pps.</td>
</tr>
<tr>
<td>P-15</td>
<td>0..128</td>
<td>Committed burst size value, specified in kbytes or pps.</td>
</tr>
<tr>
<td>P-16</td>
<td>pps</td>
<td>Packets per second.</td>
</tr>
<tr>
<td></td>
<td>kbps</td>
<td>kbytes per second.</td>
</tr>
<tr>
<td>P-17</td>
<td>0..255</td>
<td>Specify the IP TOS bits to match.</td>
</tr>
<tr>
<td>P-18</td>
<td>enable</td>
<td>Enable logging when applying the rule</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Do not log applying the rule</td>
</tr>
<tr>
<td>P-19</td>
<td>enable</td>
<td>Enable sending a trap when applying the rule</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Do not send a trap when applying the rule</td>
</tr>
</tbody>
</table>
30.1.18 packet-filter l2 rule modify

Modifies a rule to the L2 firewall table.

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: packet-filter l2 rule modify <P-1> action <P-2> [src-mac <P-3>] [dst-mac <P-4>] [src-ip <P-5>] [sourceport <P-6>] [dest-ip <P-7>] [destport <P-8>] [ethertype <P-9>] [proto <P-10>] [vlan <P-11>] [assign-queue <P-12>] [description <P-13>] [rate-limit <P-14> <P-15> <P-16>] [tos <P-17>] [log <P-18>] [trap <P-19>]

**Action**: Set Action

- **[src-mac]**: Specify the source MAC address.
- **[dst-mac]**: Specify the destination MAC address.
- **[src-ip]**: Specify the source IP address/mask.
- **[sourceport]**: Specify the source L4 port.
- **[dest-ip]**: Specify the destination IP address/mask.
- **[destport]**: Specify the destination L4 port.
- **[ethertype]**: Specify the Ethertype.
- **[proto]**: Specify the protocol for L2 firewall rule.
- **[vlan]**: Specify the VLAN ID for L2 firewall rule.
- **[assign-queue]**: Assign a user Queue.
- **[description]**: Rule description/name for L2 firewall rule.
- **[rate-limit]**: Specify the rate limit and burst size.
- **[tos]**: Specify TOS for L2 rule.
- **[log]**: Set logging.
- **[trap]**: Set sending SNMP traps.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1-2048</td>
<td>Rule index</td>
</tr>
<tr>
<td>P-2</td>
<td>accept drop</td>
<td>Accept packets. Drop packets without notification.</td>
</tr>
<tr>
<td>P-3</td>
<td>any aa:bb:cc:dd:ee:ff</td>
<td>Enter any as a shortcut for the MAC address 00:00:00:00:00:00. Enter the MAC address in hexadecimal format.</td>
</tr>
<tr>
<td>P-4</td>
<td>any aa:bb:cc:dd:ee:ff</td>
<td>Enter any as a shortcut for the MAC address 00:00:00:00:00:00. Enter the MAC address in hexadecimal format.</td>
</tr>
</tbody>
</table>
| P-5       | string | Source IP address/CIDR mask/'any'
| a-b Port Range |
| a,b Port List (may be longer than two ports) |
| a-b,c-d List of Port Ranges (may be longer than two ranges) |
| 1 to 65535 Port Number |
| P-7       | string | Target IP address/CIDR mask/'any'
| a-b Port Range |
| a,b Port List (may be longer than two ports) |
| a,b,c-d List of Port Ranges (may be longer than two ranges) |
| 1 to 65535 Port Number |
| P-9       | 0x0b00-0xffff | value Ethertype
| Appletalk |
| ARP |
| IBMSNA |
| IPv4 |
| IPv6 |
| IPX-OLD |
| MPLS Multicast |
| MPLS Unicast |
| NetBIOS |
| NOVELL |
| PPPoEDISC |
| RARP |
| PPPoESESS |
| IPXNEW |
| PROFINET |
| POWERLINK |
| ETHERCAT |
| IEEE802_1Q VLAN |
### no packet-filter l2 rule modify

Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** no packet-filter l2 rule modify action [src-mac] [dst-mac] [src-ip] [sourceport] [dest-ip] [destport] [ethertype] [proto] [vlan] [assign-queue] [description] [rate-limit] [tos] [log <P-18>] [trap <P-19>]

#### 30.1.19 packet-filter l2 rule delete

Deletes a rule from L2 rule table.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** packet-filter l2 rule delete <P-1>

#### 30.1.20 packet-filter l2 rule enable

Enables a rule from L2 rule table.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** packet-filter l2 rule enable <P-1>

#### 30.1.21 packet-filter l2 rule disable

Disables a rule from L2 rule table.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** packet-filter l2 rule disable <P-1>

#### 30.1.22 packet-filter l2 if add

Adds an interface to a L2 firewall rule.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** packet-filter l2 if add <P-1> <P-2> <P-3> <P-4> <P-5>

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-10</td>
<td>icmp</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td></td>
<td>igmp</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td></td>
<td>ipip</td>
<td>IP-within-IP Encapsulation Protocol</td>
</tr>
<tr>
<td></td>
<td>tcp</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td></td>
<td>udp</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td></td>
<td>esp</td>
<td>Encapsulating Security Protocol</td>
</tr>
<tr>
<td></td>
<td>ah</td>
<td>Authentication Header</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any of the above</td>
</tr>
<tr>
<td>P-11</td>
<td>1..4042</td>
<td>Enter a VLAN ID in the given range.</td>
</tr>
<tr>
<td>P-12</td>
<td>0..7</td>
<td>Enter a Queue ID in the given range.</td>
</tr>
<tr>
<td>P-13</td>
<td>string</td>
<td>Rule description/name</td>
</tr>
<tr>
<td>P-14</td>
<td>0..10000000</td>
<td>Committed rate value, specified in kbps or pps.</td>
</tr>
<tr>
<td>P-15</td>
<td>0..128</td>
<td>Committed burst size value, specified in kbytes or pps.</td>
</tr>
<tr>
<td>P-16</td>
<td>pps</td>
<td>Packets per second.</td>
</tr>
<tr>
<td></td>
<td>kbps</td>
<td>kbytes per second.</td>
</tr>
<tr>
<td>P-17</td>
<td>0.255</td>
<td>Specify the IP TOS bits to match.</td>
</tr>
<tr>
<td>P-18</td>
<td>enable</td>
<td>Enable logging when applying the rule</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Do not log applying the rule</td>
</tr>
<tr>
<td>P-19</td>
<td>enable</td>
<td>Enable sending a trap when applying the rule</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Do not send a trap when applying the rule</td>
</tr>
</tbody>
</table>

Parameter Value Meaning
---
| P-1       | 1..2048       | Rule index                         |
| P-2       | port          | Interface type to use is physical interface. |
|           | vlan          | Interface type to use is L2 VLAN.    |
| P-3       | 1.4042        | Interface ID for rule assignment.    |

---
### 30.1.23 packet-filter l2 if delete

Deletes an interface of a L2 firewall rule.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `packet-filter l2 if delete <P-1> <P-2> <P-3> <P-4>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>port</td>
<td>Interface type to use is physical interface.</td>
</tr>
<tr>
<td></td>
<td>vlan</td>
<td>Interface type to use is L2 VLAN.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..4042</td>
<td>Interface ID for rule assignment.</td>
</tr>
<tr>
<td>P-3</td>
<td>ingress</td>
<td>Rule applies on ingress direction.</td>
</tr>
<tr>
<td></td>
<td>egress</td>
<td>Rule applies on egress direction.</td>
</tr>
<tr>
<td>P-4</td>
<td>1..2048</td>
<td>Rule index</td>
</tr>
</tbody>
</table>

### 30.1.24 packet-filter l2 if enable

Enables an interface of a L2 firewall rule.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `packet-filter l2 if enable <P-1> <P-2> <P-3> <P-4>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>port</td>
<td>Interface type to use is physical interface.</td>
</tr>
<tr>
<td></td>
<td>vlan</td>
<td>Interface type to use is L2 VLAN.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..4042</td>
<td>Interface ID for rule assignment.</td>
</tr>
<tr>
<td>P-3</td>
<td>ingress</td>
<td>Rule applies on ingress direction.</td>
</tr>
<tr>
<td></td>
<td>egress</td>
<td>Rule applies on egress direction.</td>
</tr>
<tr>
<td>P-4</td>
<td>1..2048</td>
<td>Rule index</td>
</tr>
</tbody>
</table>

### 30.1.25 packet-filter l2 if disable

Disables an interface of a L2 firewall rule.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `packet-filter l2 if disable <P-1> <P-2> <P-3> <P-4>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>port</td>
<td>Interface type to use is physical interface.</td>
</tr>
<tr>
<td></td>
<td>vlan</td>
<td>Interface type to use is L2 VLAN.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..4042</td>
<td>Interface ID for rule assignment.</td>
</tr>
<tr>
<td>P-3</td>
<td>ingress</td>
<td>Rule applies on ingress direction.</td>
</tr>
<tr>
<td></td>
<td>egress</td>
<td>Rule applies on egress direction.</td>
</tr>
<tr>
<td>P-4</td>
<td>1..2048</td>
<td>Rule index</td>
</tr>
</tbody>
</table>

### 30.2 clear

Clear several items.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** `clear`
30.3.1 show packet-filter l3 global
Display the packet-filter global information and settings.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show packet-filter l3 global

30.3.2 show packet-filter l3 maxrules
Max. number of allowed rules in L3 rule table
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show packet-filter l3 maxrules

30.3.3 show packet-filter l3 defaultpolicy
Default policy (accept(1), drop(2), reject(3))
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show packet-filter l3 defaultpolicy

30.3.4 show packet-filter l3 ruletable
Display the L3 rule table.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show packet-filter l3 ruletable

30.3.5 show packet-filter l3 iftable
Display the L3 interface mapping table.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show packet-filter l3 iftable

30.3.6 show packet-filter l3 pending
Display whether uncommitted changes for L3 exist.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show packet-filter l3 pending

30.3.7 show packet-filter l2 global
Display the packet-filter global information and settings.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show packet-filter l2 global

30.3.8 show packet-filter l2 rule
Display the L2 rule table.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show packet-filter l2 rule

30.3.9 show packet-filter l2 if
Display the L2 interface mapping table.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show packet-filter l2 if
31 Password Management

31.1 passwords

Manage password policies and options.

31.1.1 passwords min-length

Set minimum password length for user passwords.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** passwords min-length <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..64</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

31.1.2 passwords max-login-attempts

Set maximum login attempts for the users.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** passwords max-login-attempts <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..5</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

31.1.3 passwords min-uppercase-chars

Set minimum upper case characters for user passwords.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** passwords min-uppercase-chars <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..16</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

31.1.4 passwords min-lowercase-chars

Set minimum lower case characters for user passwords.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** passwords min-lowercase-chars <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..16</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

31.1.5 passwords min-numeric-chars

Set minimum numeric characters for user passwords.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** passwords min-numeric-chars <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..16</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

31.1.6 passwords min-special-chars

Set minimum special characters for user passwords.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** passwords min-special-chars <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..16</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

31.1.7 passwords login-attempt-period

The time period [minutes] in which the number of failed authentication attempts is counted. Value 0 disables this functionality.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** passwords login-attempt-period <P-1>
31.2 show
Display device options and settings.

31.2.1 show passwords
Display the password policies and options.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Administrator
- **Format**: show passwords

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0</td>
<td>Disables the counting.</td>
</tr>
<tr>
<td></td>
<td>1..60</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>
32 Radius

32.1 radius

Configure RADIUS parameters.

32.1.1 radius server attribute 4

Specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: radius server attribute 4 <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

32.1.2 radius server auth add

Add a RADIUS authentication server.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: radius server auth add <P-1> ip <P-2> [name <P-3>] [port <P-4>]

- ip: RADIUS authentication server IP address.
- [name]: RADIUS authentication server name.
- [port]: RADIUS authentication server port (default: 1812).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..8</td>
<td>Next RADIUS server valid index (it can be seen with 'show radius global' command).</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Hostname or IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
<tr>
<td>P-4</td>
<td>1..65535</td>
<td>Enter port number between 1 and 65535</td>
</tr>
</tbody>
</table>

32.1.3 radius server auth delete

Delete a RADIUS authentication server.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: radius server auth delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..8</td>
<td>RADIUS server index.</td>
</tr>
</tbody>
</table>

32.1.4 radius server auth modify

Change a RADIUS authentication server parameters.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: radius server auth modify <P-1> [name <P-2>] [port <P-3>] [msgauth <P-4>] [primary <P-5>] [status <P-6>] [secret [<P-7>]] [encrypted <P-8>]

- [name]: RADIUS authentication server name.
- [port]: RADIUS authentication server port (default: 1812).
- [msgauth]: Enable or disable the message authenticator attribute for this server.
- [primary]: Configure the primary RADIUS server.
- [status]: Enable or disable a RADIUS authentication server entry.
- [secret]: Configure the shared secret for the RADIUS authentication server.
- [encrypted]: Configure the encrypted shared secret.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..8</td>
<td>RADIUS server index.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
<tr>
<td>P-3</td>
<td>1..65535</td>
<td>Enter port number between 1 and 65535</td>
</tr>
<tr>
<td>P-4</td>
<td>enable; disable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td>P-5</td>
<td>enable; disable</td>
<td>Disable the option.</td>
</tr>
<tr>
<td>P-6</td>
<td>enable; disable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td>P-7</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>
32.1.5 radius server retransmit
Configure the retransmit value for the RADIUS server.

Mode: Global Config Mode
Privilege Level: Administrator
Format: radius server retransmit <P-1>

Parameter | Value | Meaning
---|---|---
P-1 | 1..15 | Maximum number of retransmissions (default: 4).

32.1.6 radius server timeout
Configure the RADIUS server timeout value.

Mode: Global Config Mode
Privilege Level: Administrator
Format: radius server timeout <P-1>

Parameter | Value | Meaning
---|---|---
P-1 | 1..30 | Timeout in seconds (default: 5).

32.2 show
Display device options and settings.

32.2.1 show radius global
Display the global RADIUS configuration.

Mode: Command is in all modes available.
Privilege Level: Guest
Format: show radius global

32.2.2 show radius auth servers
Display the configured RADIUS authentication servers.

Mode: Command is in all modes available.
Privilege Level: Guest
Format: show radius auth servers [<P-1>]

Parameter | Value | Meaning
---|---|---
P-1 | 1..8 | RADIUS server index.

32.2.3 show radius auth statistics
Display the RADIUS authentication server statistics.

Mode: Command is in all modes available.
Privilege Level: Guest
Format: show radius auth statistics <P-1>

Parameter | Value | Meaning
---|---|---
P-1 | 1..8 | RADIUS server index.

32.3 clear
Clear several items.

32.3.1 clear radius
Clear the RADIUS statistics.

Mode: Privileged Exec Mode
Privilege Level: Administrator
Format: clear radius <P-1>

Parameter | Value | Meaning
---|---|---
P-1 | statistics | Clear the RADIUS statistics.
33 Remote Authentication

33.1 ldap
Configure LDAP settings.

33.1.1 ldap operation
Enable or disable the remote authentication operation.
   ▶ Mode: Global Config Mode
   ▶ Privilege Level: Administrator
   ▶ Format: ldap operation

   no ldap operation
   Disable the option
   ▶ Mode: Global Config Mode
   ▶ Privilege Level: Administrator
   ▶ Format: no ldap operation

33.1.2 ldap cache-timeout
Configure LDAP user cache entry timeout.
   ▶ Mode: Global Config Mode
   ▶ Privilege Level: Administrator
   ▶ Format: ldap cache-timeout <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..1440</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

33.1.3 ldap flush-user-cache
Flush LDAP user cache.
   ▶ Mode: Global Config Mode
   ▶ Privilege Level: Administrator
   ▶ Format: ldap flush-user-cache <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>action</td>
<td>Flush the LDAP user cache.</td>
</tr>
</tbody>
</table>

33.1.4 ldap role-policy
Configure LDAP user role selection policy.
   ▶ Mode: Global Config Mode
   ▶ Privilege Level: Administrator
   ▶ Format: ldap role-policy <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>highest</td>
<td>Use the role mapping with the highest user role.</td>
</tr>
<tr>
<td></td>
<td>first</td>
<td>Use the first matching role mapping table entry.</td>
</tr>
</tbody>
</table>

33.1.5 ldap basedn
Base distinguished name for LDAP query at the external AD server.
   ▶ Mode: Global Config Mode
   ▶ Privilege Level: Administrator
   ▶ Format: ldap basedn <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
</tbody>
</table>

33.1.6 ldap search-attr
Search attribute for LDAP query at the external AD server.
   ▶ Mode: Global Config Mode
   ▶ Privilege Level: Administrator
   ▶ Format: ldap search-attr <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 64 characters.</td>
</tr>
</tbody>
</table>
33.1.7 ldap bind-user
Bind-account user name for LDAP query at the external AD server.
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: ldap bind-user <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
</tbody>
</table>

33.1.8 ldap bind-passwd
Bind-account user password for LDAP query at the external AD server.
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: ldap bind-passwd <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 64 characters.</td>
</tr>
</tbody>
</table>

33.1.9 ldap default-domain
Default domain used for users without a domain name.
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: ldap default-domain <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 64 characters.</td>
</tr>
</tbody>
</table>

33.1.10 ldap client server add
Add a LDAP client server connection.
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: ldap client server add <P-1> <P-2> [port <P-3>] [security <P-4>] [description <P-5>]

[port]: Set the port number of the external LDAP server.
[security]: Set the security settings for the connection to external LDAP server.
[description]: Description of the external LDAP server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>Enter a number in the given range.</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>1..65535</td>
<td>Port number of LDAP Server.</td>
</tr>
</tbody>
</table>
| P-4       | none | ssl
|           |       | startTLS
| P-5       | string| Enter a user-defined text, max. 100 characters. |

33.1.11 ldap client server delete
Delete a LDAP client server connection.
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: ldap client server delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

33.1.12 ldap client server enable
Enable a LDAP client server connection.
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: ldap client server enable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

33.1.13 ldap client server disable
Disable a LDAP client server connection.
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: ldap client server disable <P-1>
### 33.1.14 ldap client server modify
Modify a LDAP client server connection.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `ldap client server modify <P-1> [addr <P-2>] [port <P-3>] [security <P-4>] [description <P-5>]`
  - `<addr>`: Modify the host address of the external LDAP server.
  - `<port>`: Modify the port number of the external LDAP server.
  - `<security>`: Modify the security settings for the connection to external LDAP server.
  - `<description>`: Modify the description of the external LDAP server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>Enter a number in the given range.</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>1..65535</td>
<td>Port number of LDAP Server.</td>
</tr>
<tr>
<td>P-4</td>
<td>none, ssl, startTLS</td>
<td></td>
</tr>
<tr>
<td>P-5</td>
<td>string</td>
<td>Enter a user-defined text, max. 100 characters.</td>
</tr>
</tbody>
</table>

### 33.1.15 ldap mapping add
Add a LDAP mapping entry.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `ldap mapping add <P-1> access-role <P-2> mapping-type <P-3> mapping-parameter <P-4>`
  - `<access-role>`: Access role type.
  - `<mapping-type>`: Role mapping type.
  - `<mapping-parameter>`: Role mapping parameter.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..64</td>
<td>Enter a number in the given range.</td>
</tr>
<tr>
<td>P-2</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-3</td>
<td>attribute, group</td>
<td></td>
</tr>
<tr>
<td>P-4</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
</tbody>
</table>

### 33.1.16 ldap mapping delete
Delete a LDAP role mapping entry.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `ldap mapping delete <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..64</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

### 33.1.17 ldap mapping enable
Activate a LDAP role mapping entry.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `ldap mapping enable <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..64</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

### 33.1.18 ldap mapping disable
Deactivate a LDAP role mapping entry.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `ldap mapping disable <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..64</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>
33.2 show

Display device options and settings.

33.2.1 show ldap global

Display the LDAP configuration parameters and information.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** show ldap global

33.2.2 show ldap client server

Display the LDAP client server connections.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** show ldap client server [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

33.2.3 show ldap mapping

Display the LDAP role mapping entries.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** show ldap mapping [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..64</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

33.3 copy

Copy different kinds of items.

33.3.1 copy ldapcacert remote

Copy CA certificate file (*.pem) from the remote AD server to the specified destination.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** copy ldapcacert remote <P-1> nvm [P-2]

nvm: Copy CA certificate file (*.pem) from the remote AD server to the device.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 100 characters.</td>
</tr>
</tbody>
</table>

33.3.2 copy ldapcacert envm

Copy CA certificate file (*.pem) from external non-volatile memory to the specified destination.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** copy ldapcacert envm <P-1> nvm [P-2]

envm: Copy CA certificate file (*.pem) from external non-volatile memory to the device.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 100 characters.</td>
</tr>
</tbody>
</table>
34 Remote Monitoring (RMON)

34.1 show
Display device options and settings.

34.1.1 show rmon statistics
Show RMON statistics configuration.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show rmon statistics [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>
35 Script File

35.1 script

CLI Script File.

35.1.1 script apply

Executes the CLI script file available in the device.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** script apply <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
</tbody>
</table>

35.1.2 script validate

Only validates the CLI script file available in the device.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** script validate <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
</tbody>
</table>

35.1.3 script list system

List all the script files available in the device memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** script list system

35.1.4 script list envm

List all the script files available in external non-volatile memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** script list envm

35.1.5 script delete

Delete the CLI script files.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** script delete [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
</tbody>
</table>

35.2 copy

Copy different kinds of items.

35.2.1 copy script envm

Copy script file from external non-volatile memory to specified destination.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** copy script envm <P-1> running-config nvm <P-2>

**running-config:** Copy script file from external non-volatile memory to the running-config.

**nvm:** Copy script file from external non-volatile memory to the non-volatile memory.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>
35.2.2 copy script remote
Copy script file from server to specified destination.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `copy script remote <P-1> running-config nvm <P-2>`
  - `running-config`: Copy script file from file server to running-config.
  - `nvm`: Copy script file to non-volatile memory.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>

35.2.3 copy script nvm
Copy Script file from non-volatile memory to the specified destination.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `copy script nvm <P-1> running-config envm <P-2> remote <P-3>`
  - `running-config`: Copy Script file from non-volatile system memory to running-config.
  - `envm`: Copy Script file to external non-volatile memory device.
  - `remote`: Copy Script file to file server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
<tr>
<td>P-3</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

35.3 show
Display device options and settings.

35.3.1 show script envm
Display the content of the CLI script file present in the envm.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** `show script envm <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
</tbody>
</table>

35.3.2 show script system
Display the content of the CLI script file present in the device.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** `show script system <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
</tbody>
</table>
36 Selftest

36.1 selftest
Configure the selftest settings.

36.1.1 selftest action
Configure the action that a selftest component should take.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: selftest action <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>task</td>
<td>Configure the action for task errors.</td>
</tr>
<tr>
<td></td>
<td>resource</td>
<td>Configure the action for lack of resources.</td>
</tr>
<tr>
<td></td>
<td>software</td>
<td>Configure the action for broken software integrity.</td>
</tr>
<tr>
<td></td>
<td>hardware</td>
<td>Configure the action for detected hardware errors.</td>
</tr>
<tr>
<td>P-2</td>
<td>log-only</td>
<td>Write a message to the logging file.</td>
</tr>
<tr>
<td></td>
<td>send-trap</td>
<td>Send a trap to the management station.</td>
</tr>
<tr>
<td></td>
<td>reboot</td>
<td>Reboot the device.</td>
</tr>
</tbody>
</table>

36.1.2 selftest ramtest
Enable or disable the RAM selftest on cold start of the device. When disabled the device booting time is reduced.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: selftest ramtest

no selftest ramtest
Disable the option

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: no selftest ramtest

36.1.3 selftest system-monitor
Enable or disable the System Monitor 1 access during the boot phase. Please note: If the System Monitor is disabled it is possible to loose access to the device permanently in case of loosing administrator password or misconfiguration.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: selftest system-monitor

no selftest system-monitor
Disable the option

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: no selftest system-monitor

36.1.4 selftest boot-default-on-error
Enable or disable loading of the default configuration in case there is any error loading the configuration during boot phase. If disabled the system will be halted.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: selftest boot-default-on-error

no selftest boot-default-on-error
Disable the option

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: no selftest boot-default-on-error
36.2 show
Display device options and settings.

36.2.1 show selftest action
Display the actions the device takes if an error occurs.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show selftest action

36.2.2 show selftest settings
Display the selftest settings.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show selftest settings
37 Small Form-factor Pluggable (SFP)

37.1 show
Display device options and settings.

37.1.1 show sfp
Show info about plugged in SFP modules.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show sfp [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>
38 Signal Contact

38.1 signal-contact

Configure the signal contact settings.

38.1.1 signal-contact mode

Configure the Signal Contact mode setting.

 Mode: Global Config Mode
 Privilege Level: Administrator
 Formal: signal-contact <P-1> mode <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>manual</td>
<td>The signal contact's status is determined by the associated manual setting (subcommand 'state').</td>
</tr>
<tr>
<td></td>
<td>monitor</td>
<td>The signal contact's status is determined by the associated monitor settings.</td>
</tr>
<tr>
<td></td>
<td>device-status</td>
<td>The signal contact's status is determined by the device status.</td>
</tr>
<tr>
<td></td>
<td>security-status</td>
<td>The signal contact's status is determined by the security status.</td>
</tr>
<tr>
<td></td>
<td>dev-sec-status</td>
<td>The signal contact's status is determined by the device status and security status.</td>
</tr>
</tbody>
</table>

38.1.2 signal-contact monitor link-failure

Sets the monitoring of the network connection(s).

 Mode: Global Config Mode
 Privilege Level: Administrator
 Formal: signal-contact <P-1> monitor link-failure

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
</tbody>
</table>

no signal-contact monitor link-failure

Disable the option

 Mode: Global Config Mode
 Privilege Level: Administrator
 Formal: no signal-contact <P-1> monitor link-failure

38.1.3 signal-contact monitor envm-not-in-sync

Sets the monitoring whether the external non-volatile memory device is in sync with the running configuration.

 Mode: Global Config Mode
 Privilege Level: Administrator
 Formal: signal-contact <P-1> monitor envm-not-in-sync

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
</tbody>
</table>

no signal-contact monitor envm-not-in-sync

Disable the option

 Mode: Global Config Mode
 Privilege Level: Administrator
 Formal: no signal-contact <P-1> monitor envm-not-in-sync

38.1.4 signal-contact monitor envm-removal

Sets the monitoring of the external non-volatile memory device removal.

 Mode: Global Config Mode
 Privilege Level: Administrator
 Formal: signal-contact <P-1> monitor envm-removal

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
</tbody>
</table>
### 38.1.5 signal-contact monitor temperature

Sets the monitoring of the device temperature.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `signal-contact <P-1> monitor temperature`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
</tbody>
</table>

### 38.1.6 signal-contact monitor power-supply

Sets the monitoring of the power supply(s).

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `signal-contact <P-1> monitor power-supply <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>1..2</td>
<td>Number of power supply.</td>
</tr>
</tbody>
</table>

### 38.1.7 signal-contact state

Configure the Signal Contact manual state (only takes immediate effect in manual mode).

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `signal-contact <P-1> state <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>open</td>
<td>Open the signal contact (only takes effect in the manual mode).</td>
</tr>
<tr>
<td></td>
<td>close</td>
<td>Close the signal contact (only takes effect in the manual mode).</td>
</tr>
</tbody>
</table>

### 38.1.8 signal-contact trap

Configure if a trap is sent when the Signal Contact changes state (in monitor mode).

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `signal-contact <P-1> trap`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
</tbody>
</table>

### no signal-contact monitor envm-removal

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** no signal-contact <P-1> monitor envm-removal

### no signal-contact monitor temperature

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** no signal-contact <P-1> monitor temperature

### no signal-contact monitor power-supply

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** no signal-contact <P-1> monitor power-supply <P-2>

### no signal-contact trap

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** no signal-contact <P-1> trap
38.2 signal-contact
Configure the signal contact interface settings.

38.2.1 signal-contact link-alarm
Configure the monitoring of the specific network ports.
- **Mode:** Interface Range Mode
- **Privilege Level:** Administrator
- **Format:** `signal-contact <P-1> link-alarm`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
</tbody>
</table>

- **no signal-contact link-alarm**
  Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Administrator
  - **Format:** `no signal-contact <P-1> link-alarm`

38.3 show
Display device options and settings.

38.3.1 show signal-contact
Display the signal contact settings.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show signal-contact <P-1> mode monitor state trap link-alarm events all`

  - **mode:** Display the signal contact mode.
  - **monitor:** Display the signal contact monitor settings.
  - **state:** Display the signal contact state (open/close).
  - **trap:** Display the signal contact trap information and settings.
  - **link-alarm:** Display the settings of the monitoring of the specific network ports.
  - **events:** Display the occurred device status events.
  - **all:** Display the signal contact settings for the specified signal contact.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
</tbody>
</table>
39 Simple Network Management Protocol (SNMP)

39.1 snmp
Configure of SNMP versions and traps.

39.1.1 snmp access version v1
Enable or disable SNMP version V1.

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: `snmp access version v1`
  ```
  no snmp access version v1
  ```
  Disable the option
  ```
  Mode: Global Config Mode
  Privilege Level: Administrator
  Format: no snmp access version v1
  ```

39.1.2 snmp access version v2
Enable or disable SNMP version V2.

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: `snmp access version v2`
  ```
  no snmp access version v2
  ```
  Disable the option
  ```
  Mode: Global Config Mode
  Privilege Level: Administrator
  Format: no snmp access version v2
  ```

39.1.3 snmp access version v3
Enable or disable SNMP version V3.

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: `snmp access version v3`
  ```
  no snmp access version v3
  ```
  Disable the option
  ```
  Mode: Global Config Mode
  Privilege Level: Administrator
  Format: no snmp access version v3
  ```

39.1.4 snmp access port
Configure the SNMP access port.

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: `snmp access port <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>165535</td>
<td>Port number of the SNMP server (default: 161).</td>
</tr>
</tbody>
</table>

39.2 show
Display device options and settings.
39.2.1  show snmp access
Display the SNMP access configuration settings.

► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show snmp access
40 SNMP Community

40.1 snmp
Configure of SNMP versions and traps.

40.1.1 snmp community ro
SNMP v1/v2 read-only community.
► Mode: Global Config Mode
► Privilege Level: Administrator
► Format: snmp community ro

40.1.2 snmp community rw
SNMP v1/v2 read-write community.
► Mode: Global Config Mode
► Privilege Level: Administrator
► Format: snmp community rw

40.2 show
Display device options and settings.

40.2.1 show snmp community
Display the SNMP v1/2 community.
► Mode: Command is in all modes available.
► Privilege Level: Administrator
► Format: show snmp community
41 SNMP Logging

41.1 logging
Logging configuration.

41.1.1 logging snmp-request get operation
Enable or disable logging of SNMP GET or SET requests.
▷ Mode: Global Config Mode
▷ Privilege Level: Administrator
▷ Format: logging snmp-request get operation <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable logging of SNMP GET or SET requests.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable logging of SNMP GET or SET requests.</td>
</tr>
</tbody>
</table>

no logging snmp-request get operation
Disable the option
▷ Mode: Global Config Mode
▷ Privilege Level: Administrator
▷ Format: no logging snmp-request get operation <P-1>

41.1.2 logging snmp-request get severity
Define severity level.
▷ Mode: Global Config Mode
▷ Privilege Level: Administrator
▷ Format: logging snmp-request get severity <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>emergency</td>
<td>System is unusable. System failure has occurred.</td>
</tr>
<tr>
<td></td>
<td>alert</td>
<td>Action must be taken immediately. Unrecoverable failure of a component. System failure likely.</td>
</tr>
<tr>
<td></td>
<td>critical</td>
<td>Recoverable failure of a component that may lead to system failure.</td>
</tr>
<tr>
<td></td>
<td>error</td>
<td>Error conditions. Recoverable failure of a component.</td>
</tr>
<tr>
<td></td>
<td>warning</td>
<td>Minor failure, e.g. misconfiguration of a component.</td>
</tr>
<tr>
<td></td>
<td>notice</td>
<td>Normal but significant conditions.</td>
</tr>
<tr>
<td></td>
<td>informational</td>
<td>Informational messages.</td>
</tr>
<tr>
<td></td>
<td>debug</td>
<td>Debug-level messages.</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>Same as emergency</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Same as alert</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Same as critical</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Same as error</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Same as warning</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Same as notice</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Same as informational</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>Same as debug</td>
</tr>
</tbody>
</table>

41.1.3 logging snmp-request set operation
Enable or disable logging of SNMP GET or SET requests.
▷ Mode: Global Config Mode
▷ Privilege Level: Administrator
▷ Format: logging snmp-request set operation <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable logging of SNMP GET or SET requests.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable logging of SNMP GET or SET requests.</td>
</tr>
</tbody>
</table>

no logging snmp-request set operation
Disable the option
▷ Mode: Global Config Mode
▷ Privilege Level: Administrator
▷ Format: no logging snmp-request set operation <P-1>
41.1.4 logging snmp-request set severity

Define severity level.
► Mode: Global Config Mode
► Privilege Level: Administrator
► Format: logging snmp-request set severity <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>emergency</td>
<td>P-1</td>
<td>System is unusable. System failure has occurred.</td>
</tr>
<tr>
<td>alert</td>
<td></td>
<td>Action must be taken immediately. Unrecoverable failure of a component. System failure likely.</td>
</tr>
<tr>
<td>critical</td>
<td></td>
<td>Recoverable failure of a component that may lead to system failure.</td>
</tr>
<tr>
<td>error</td>
<td></td>
<td>Error conditions. Recoverable failure of a component.</td>
</tr>
<tr>
<td>warning</td>
<td></td>
<td>Minor failure, e.g. misconfiguration of a component.</td>
</tr>
<tr>
<td>notice</td>
<td></td>
<td>Normal but significant conditions.</td>
</tr>
<tr>
<td>informational</td>
<td></td>
<td>Informational messages.</td>
</tr>
<tr>
<td>debug</td>
<td></td>
<td>Debug-level messages.</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Same as emergency</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>Same as alert</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>Same as critical</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>Same as error</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>Same as warning</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>Same as notice</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>Same as informational</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>Same as debug</td>
</tr>
</tbody>
</table>

41.2 show

Display device options and settings.

41.2.1 show logging snmp

Display the SNMP logging settings.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show logging snmp
42 Secure Shell (SSH)

42.1 ssh
Set SSH parameters.

42.1.1 ssh server
Enable or disable the SSH server.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: ssh server

**no ssh server**
Disable the option
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: no ssh server

42.1.2 ssh timeout
Set the SSH connection idle timeout in minutes (default: 5).
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: ssh timeout <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..160</td>
<td>Idle timeout of a session in minutes (default: 5).</td>
</tr>
</tbody>
</table>

42.1.3 ssh port
Set the SSH server port number (default: 22).
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: ssh port <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..65535</td>
<td>Port number of the SSH server (default: 22).</td>
</tr>
</tbody>
</table>

42.1.4 ssh max-sessions
Set the maximum number of concurrent SSH sessions (default: 5).
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: ssh max-sessions <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..5</td>
<td>Maximum number of concurrent SSH sessions.</td>
</tr>
</tbody>
</table>

42.1.5 ssh key rsa
Generate or delete RSA key
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: ssh key rsa <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>generate</td>
<td>Generates the item</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>Deletes the item</td>
</tr>
</tbody>
</table>

42.1.6 ssh key fingerprint-type
Configure fingerprint type
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: ssh key fingerprint-type <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>md5</td>
<td>Configure md5 fingerprint of the existing SSH host key</td>
</tr>
<tr>
<td></td>
<td>sha256</td>
<td>Configure sha256 fingerprint of the existing SSH host key.</td>
</tr>
</tbody>
</table>
42.2 copy

Copy different kinds of items.

42.2.1 copy sshkey remote

Copy the SSH key from a server to the specified destination.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `copy sshkey remote <P-1> nvm`
  
  **nvm:** Copy the SSH key from a server to non-volatile memory.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

42.2.2 copy sshkey envm

Copy the SSH key from external non-volatile memory to the specified destination.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `copy sshkey envm <P-1> nvm`
  
  **nvm:** Copy the SSH key from external non-volatile memory to non-volatile memory.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

42.3 show

Display device options and settings.

42.3.1 show ssh

Display the SSH server and client information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ssh`
43 System

43.1 system
Set system related values e.g. name of the device, location of the device, contact data for the person responsible for the device, and pre-login banner text.

43.1.1 system name
Edit the name of the device. The system name consists of an alphanumeric ASCII character string with 0..255 characters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
</tbody>
</table>

43.1.2 system location
Edit the location of the device. The system location consists of an alphanumeric ASCII character string with 0..255 characters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
</tbody>
</table>

43.1.3 system contact
Edit the contact information for the person responsible for the device. The contact data consists of an alphanumeric ASCII character string with 0..255 characters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
</tbody>
</table>

43.1.4 system pre-login-banner operation
Enable or disable the pre-login banner. You use the pre-login banner to display a greeting or information to users before they login to the device.

- **no system pre-login-banner operation**
  Disable the option
  - Mode: Global Config Mode
  - Privilege Level: Administrator
  - Format: no system pre-login-banner operation

43.1.5 system pre-login-banner text
Edit the text for the pre-login banner (C printf format syntax allowed: ) The device allows you to edit an alphanumeric ASCII character string with up to 512 characters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 512 characters (allowed characters are from ASCII 32 to 127).</td>
</tr>
</tbody>
</table>
43.1.6 system resources operation
Enable or disable the measurement operation.
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Administrator
  ▶ Format: system resources operation

  no system resources operation
  Disable the option
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Administrator
  ▶ Format: no system resources operation

43.2 temperature
Configure the upper and lower temperature limits of the device. The device allows you to set the threshold as an integer from -99 through 99. You configure the temperatures in degrees Celsius.

43.2.1 temperature upper-limit
Configure the upper temperature limit.
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Administrator
  ▶ Format: temperature upper-limit <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>-99..99</td>
<td>Upper temperature threshold ([C], default 70).</td>
</tr>
</tbody>
</table>

43.2.2 temperature lower-limit
Configure the lower temperature limit.
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Administrator
  ▶ Format: system location <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
</tbody>
</table>

43.3 show
Display device options and settings.

43.3.1 show eventlog
Display the event log notice and warning entries with time stamp.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show eventlog

43.3.2 show system info
Display the system related information.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show system info

43.3.3 show system pre-login-banner
Display the pre-login banner status and text.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show system pre-login-banner
43.3.4  show system flash-status
Display the flash memory statistics of the device.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show system flash-status

43.3.5  show system temperature limits
Display the temperature limits.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show system temperature limits

43.3.6  show system temperature extremes
Display the minimum and maximum recorded temperature.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show system temperature extremes

43.3.7  show system temperature histogram
Display the temperature histogram of the device.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show system temperature histogram

43.3.8  show system temperature counters
Display number of 20 centigrade C variations in maximum one hour period.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show system temperature counters

43.3.9  show system resources
Display the system resources information (CPU utilization, memory and network CPU utilization).
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show system resources

43.3.10 show hardware by-pas
Display state of hardware by-pass.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show hardware by-pass
44 Traps

44.1 snmp
Configure of SNMP versions and traps.

44.1.1 snmp trap operation
Global enable/disable SNMP trap.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: snmp trap operation

no snmp trap operation
Disable the option

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: no snmp trap operation

44.1.2 snmp trap mode
Enable/disable SNMP trap entry.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: snmp trap mode <P-1>

no snmp trap mode
Disable the option

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: no snmp trap mode <P-1>

44.1.3 snmp trap delete
Delete SNMP trap entry.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: snmp trap delete <P-1>

44.1.4 snmp trap add
Add SNMP trap entry.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: snmp trap add <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;name&gt; Trap name (1 to 32 characters)</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>Single IP address.</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d:n</td>
<td>Address with port.</td>
</tr>
</tbody>
</table>

44.2 show
Display device options and settings.
44.2.1  show snmp traps

Display the SNMP traps.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show snmp traps`
45 Unicast Routing

45.1 ip
Set IP parameters.

45.1.1 ip routing
Enables or disables Routing globally on the device.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip routing

no ip routing
Disable the option
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: no ip routing

45.1.2 ip proxy-arp max-delay
Configure the maximum time a Proxy ARP response can be delayed.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip proxy-arp max-delay <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..1000</td>
<td>Enter Proxy ARP max response delay ms</td>
</tr>
</tbody>
</table>

45.2 show
Display device options and settings.

45.2.1 show ip global
Displays all the summary information of the IP, including the ICMP rate limit configuration and the global ICMP Redirect configuration.
- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show ip global

45.3 show
Display device options and settings.

45.3.1 show ip interface
Show interface parameters.
- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show ip interface <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

45.3.2 show ip statistics
Show global IP statistics.
- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show ip statistics
45.4 ip

IP interface commands.

45.4.1 ip proxy-arp operation
Enables or disables Proxy ARP on the interface.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip proxy-arp operation

**no ip proxy-arp operation**
Disable the option
- **Mode:** Interface Config Mode
- **Privilege Level:** Operator
- **Format:** no ip proxy-arp operation

45.4.2 ip address secondary
Designates whether an IP Address is a secondary address on this interface.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip address secondary <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>IP subnet mask.</td>
</tr>
</tbody>
</table>

**no ip address secondary**
Disable the option
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** no ip address secondary <P-1>

45.4.3 ip address primary
Designates whether an IP Address is a primary address on this interface.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip proxy-arp operation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>IP subnet mask.</td>
</tr>
</tbody>
</table>

**no ip address primary**
Disable the option
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** no ip address primary

45.4.4 ip mtu
Set MTU size for IP protocol.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip mtu <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>68..12266</td>
<td>value for MTU that could be between 68 and 12266.</td>
</tr>
</tbody>
</table>

45.4.5 ip icmp redirects
Enables or disables the generation of ICMP Redirect messages.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip icmp interface
45.5  ip

Set IP parameters.

45.5.1  ip route add

Add a static route entry.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip route add <P-1> <P-2> <P-3> [preference <P-4>]
  [preference]: Change the preference value of a route.show ip entry <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-4</td>
<td>1.255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

45.5.2  ip route modify

Modify a static route entry.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip route modify <P-1> <P-2> <P-3> [preference <P-4>]
  [preference]: Change the preference value of a route.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-4</td>
<td>1.255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

45.5.3  ip route delete

Delete a static route entry.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip route delete <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

45.5.4  ip route distance

Default preference for static routes.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip route distance <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

45.5.5  ip route track add

Default preference for static routes.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip route track add <P-1> <P-2> <P-3> <P-4>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-4</td>
<td>string</td>
<td>Track instance.</td>
</tr>
</tbody>
</table>

45.5.6  ip route track delete

Remove a track-id for a static route entry.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip route track delete <P-1> <P-2> <P-3> <P-4>
45.5.7 ip default-route add
Add a static default route entry.
   ▶ Mode: Global Config Mode
   ▶ Privilege Level: Operator
   ▶ Format: ip default-route add <P-1> [preference <P-2>]
     [preference]: Change the preference value of a route.

### Parameter | Value | Meaning
---|---|---
P-1 | A.B.C.D | IP address.
P-2 | 1..255 | Enter a number in the given range.

45.5.8 ip default-route modify
Modify a static default route entry.
   ▶ Mode: Global Config Mode
   ▶ Privilege Level: Operator
   ▶ Format: ip default-route modify <P-1> [preference <P-2>]
     [preference]: Change the preference value of a route.

### Parameter | Value | Meaning
---|---|---
P-1 | A.B.C.D | IP address.
P-2 | 1..255 | Enter a number in the given range.

45.5.9 ip default-route delete
Delete a static default route entry.
   ▶ Mode: Global Config Mode
   ▶ Privilege Level: Operator
   ▶ Format: ip default-route delete <P-1>

### Parameter | Value | Meaning
---|---|---
P-1 | A.B.C.D | IP address.

45.5.10 ip loopback add
Enable a loopback interface.
   ▶ Mode: Global Config Mode
   ▶ Privilege Level: Operator
   ▶ Format: ip loopback add <P-1>

### Parameter | Value | Meaning
---|---|---
P-1 | 1..8 | Enter the loopback id in the given range.

45.5.11 ip loopback delete
Disable a loopback interface.
   ▶ Mode: Global Config Mode
   ▶ Privilege Level: Operator
   ▶ Format: ip loopback delete <P-1>

### Parameter | Value | Meaning
---|---|---
P-1 | 1..8 | Enter the loopback id in the given range.

45.5.12 ip icmp redirects
Enables or disables the generation of ICMP Redirect messages.
   ▶ Mode: Global Config Mode
   ▶ Privilege Level: Operator
   ▶ Format: ip icmp redirects

   **no ip icmp redirects**
   Disable the option
   ▶ Mode: Global Config Mode
   ▶ Privilege Level: Operator
   ▶ Format: no ip icmp redirects
45.5.13 ip icmp echo-reply
Enables or disables the generation of ICMP Echo Reply messages.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip icmp echo-reply

```
no ip icmp echo-reply
```

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** no ip icmp echo-reply

45.5.14 ip icmp rate-limit interval
Configure ICMP rate limit interval in milliseconds.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip icmp rate-limit interval <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..2147483647</td>
<td>Configure the interval.</td>
</tr>
</tbody>
</table>

45.5.15 ip icmp rate-limit burst-size
Configure ICMP rate limit burst size.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip icmp rate-limit burst-size <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..200</td>
<td>Configure the burst-size.</td>
</tr>
</tbody>
</table>

45.6 show
Display device options and settings.

45.6.1 show ip route all
Display static, dynamic and local routes.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip route all

```
45.6.2 show ip route local
Display the local routes.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip route local

45.6.3 show ip route static
Display the static routes.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip route static

45.6.4 show ip route entry
Display router route entry information.

- **Mode:** Global Config Mode
- **Privilege Level:** Guest
- **Format:** show ip route entry <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>
45.6.5  show ip route tracking

Display tracking information for static routes.

- **Mode**: Global Config Mode
- **Privilege Level**: Guest
- **Format**: `show ip route tracking`
46 Tracking

46.1 track
Configure tracking instances on the device.

46.1.1 track add
Create a tracking instance.
  ► Mode: Global Config Mode
  ► Privilege Level: Operator
  ► Format: track add <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>interface</td>
<td>interface tracking</td>
</tr>
<tr>
<td></td>
<td>ping</td>
<td>ping tracking</td>
</tr>
<tr>
<td></td>
<td>logical</td>
<td>logical tracking</td>
</tr>
<tr>
<td>P-2</td>
<td>1..256</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

46.1.2 track delete
Delete a tracking instance.
  ► Mode: Global Config Mode
  ► Privilege Level: Operator
  ► Format: track delete <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>interface</td>
<td>interface tracking</td>
</tr>
<tr>
<td></td>
<td>ping</td>
<td>ping tracking</td>
</tr>
<tr>
<td></td>
<td>logical</td>
<td>logical tracking</td>
</tr>
<tr>
<td>P-2</td>
<td>1..256</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

46.1.3 track enable
Activate a tracking instance.
  ► Mode: Global Config Mode
  ► Privilege Level: Administrator
  ► Format: track enable <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>interface</td>
<td>interface tracking</td>
</tr>
<tr>
<td></td>
<td>ping</td>
<td>ping tracking</td>
</tr>
<tr>
<td></td>
<td>logical</td>
<td>logical tracking</td>
</tr>
<tr>
<td>P-2</td>
<td>1..256</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

46.1.4 track disable
Deactivate a tracking instance.
  ► Mode: Global Config Mode
  ► Privilege Level: Operator
  ► Format: track disable <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>interface</td>
<td>interface tracking</td>
</tr>
<tr>
<td></td>
<td>ping</td>
<td>ping tracking</td>
</tr>
<tr>
<td></td>
<td>logical</td>
<td>logical tracking</td>
</tr>
<tr>
<td>P-2</td>
<td>1..256</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

46.1.5 track trap
Enable/Disable the StateChange trap for the corresponding tracking instance.
  ► Mode: Global Config Mode
  ► Privilege Level: Operator
  ► Format: users password <P-1> [<P-2>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>interface</td>
<td>interface tracking</td>
</tr>
<tr>
<td></td>
<td>ping</td>
<td>ping tracking</td>
</tr>
<tr>
<td></td>
<td>logical</td>
<td>logical tracking</td>
</tr>
<tr>
<td>P-2</td>
<td>1..256</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>
46.1.6 track description
Set the description for the corresponding tracking instance.
▶ Mode: Global Config Mode
▶ Privilege Level: Operator
▶ Format: track description <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>interface</td>
<td>interface tracking</td>
</tr>
<tr>
<td></td>
<td>ping</td>
<td>ping tracking</td>
</tr>
<tr>
<td></td>
<td>logical</td>
<td>logical tracking</td>
</tr>
<tr>
<td>P-2</td>
<td>1..256</td>
<td>Enter a number in the given range.</td>
</tr>
<tr>
<td>p-3</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
</tbody>
</table>

46.1.7 track modify interface
Modify the configuration of an interface tracking instance.
▶ Mode: Global Config Mode
▶ Privilege Level: Operator
▶ Format: track modify interface <P-1> [interface <P-2>] [linkup-delay <P-3>]
  [linkdown-delay <P-4>]
  [interface <P-2>]: Set the interface number of the tracking instance.
  [linkup-delay <P-3>]: Set the linkup-delay of the interface tracking instance
  [linkdown-delay <P-4>]: Set the linkdown-delay of the interface tracking instance

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>p-3</td>
<td>0..255</td>
<td>Enter a number in the given range.</td>
</tr>
<tr>
<td>p-4</td>
<td>0..255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

46.1.8 track modify ping
Modify the configuration of a ping tracking instance.
▶ Mode: Global Config Mode
▶ Privilege Level: Operator
▶ Format: track modify ping <P-1> <P-2> [interface <P-2>] [address <P-3>]
  [interval <P-4>] [miss <P-5>] [success <P-6>] [timeout <P-7>] [ttl <P-8>]
  [interface]: Set the source interface number of the ping tracking instance.
  [address]: Set the address of the router to be monitored.
  [interval]: Set the number of milliseconds between the pings to the target router address.
  [miss]: Set the number of consecutive ping misses until the tracked object is considered to be down.
  [success]: Set the of consecutive ping successes until the tracked object is considered to be up.
  [timeout]: Set the timeout in milliseconds for a ping reply.
  [ttl]: Set the time to live for a ping request packet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>p-3</td>
<td>a.b.c.d IP address.</td>
<td></td>
</tr>
<tr>
<td>p-4</td>
<td>100..20000</td>
<td>value for ping tracking interval range between 100 and 20000.</td>
</tr>
<tr>
<td>p-5</td>
<td>1..10</td>
<td>value for ping tracking interval range between 1 and 10.</td>
</tr>
<tr>
<td>p-6</td>
<td>1..10</td>
<td>value for ping tracking range between 1 and 10.</td>
</tr>
<tr>
<td>p-7</td>
<td>10..10000</td>
<td>value for ping tracking time range between 10 and 10000.</td>
</tr>
<tr>
<td>p-8</td>
<td>1..255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

46.1.9 track modify logical
Modify the configuration of a logical tracking instance.
▶ Mode: Global Config Mode
▶ Privilege Level: Operator
▶ Format: track modify logical <P-1> <P-2> <P-3> <P-4>
46.2 show

Display device options and settings.

46.2.1 show track overview

Display information and settings for tracking instances.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show track overview

46.2.2 show track interface

Display information and settings for interface tracking instances.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show track interface [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

46.2.3 show track ping

Display information and settings for ping tracking instances.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show track ping [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

46.2.4 show track logical

Display information and settings for logical tracking instances.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show track logical [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

46.2.5 show track application

Display information and settings for interface application registrations.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show track application

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>
47 Virtual LAN (VLAN)

47.1 name

47.1.1 name

Assign a name to a VLAN

- **Mode**: VLAN Database Mode
- **Privilege Level**: Operator
- **Format**: name <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>

47.2 vlan

Creation and configuration of VLANS.

47.2.1 vlan add

Create a VLAN

- **Mode**: VLAN Database Mode
- **Privilege Level**: Operator
- **Format**: vlan add <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

47.2.2 vlan delete

Delete a VLAN

- **Mode**: VLAN Database Mode
- **Privilege Level**: Operator
- **Format**: vlan delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>2..4042</td>
<td>Enter VLAN ID. VLAN ID 1 can not be deleted or created</td>
</tr>
</tbody>
</table>

47.3 vlan

Configure 802.1Q port parameters for VLANs.

47.3.1 vlan acceptframe

Configure how to handle tagged/untagged frames received.

- **Mode**: Interface Range Mode
- **Privilege Level**: Operator
- **Format**: vlan acceptframe <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>all</td>
<td>Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.</td>
</tr>
<tr>
<td></td>
<td>vlanonly</td>
<td>Only frames received with a VLAN tag will be forwarded. All other frames will be dropped.</td>
</tr>
</tbody>
</table>

47.3.2 vlan ingressfilter

Enable/Disable application of Ingress Filtering Rules.

- **Mode**: Interface Range Mode
- **Privilege Level**: Operator
- **Format**: vlan ingressfilter
**47.3.3 vlan priority**

Configure the priority for untagged frames.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `vlan priority <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..7</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

**47.3.4 vlan pvid**

Configure the VLAN id for a specific port.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `vlan pvid <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

**47.3.5 vlan tagging**

Enable or disable tagging for a specific VLAN port.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `vlan tagging <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

**47.3.6 vlan participation include**

Vlan participation to include
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `vlan participation include <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

**47.3.7 vlan participation exclude**

Vlan participation to exclude
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `vlan participation exclude <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

**47.3.8 vlan participation auto**

Vlan participation to auto
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `vlan participation auto <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>
47.4  show
Display device options and settings.

47.4.1  show vlan id
Display the configuration of a single specified VLAN.
➤ Mode: Command is in all modes available.
➤ Privilege Level: Guest
➤ Format: show vlan id <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

47.4.2  show vlan brief
Display the general VLAN parameters.
➤ Mode: Command is in all modes available.
➤ Privilege Level: Guest
➤ Format: show vlan brief

47.4.3  show vlan port
Display the VLAN configuration of a single port.
➤ Mode: Command is in all modes available.
➤ Privilege Level: Guest
➤ Format: show vlan port [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

47.4.4  show vlan member current
Display the membership of ports in static VLAN or dynamically created.
➤ Mode: Command is in all modes available.
➤ Privilege Level: Guest
➤ Format: show vlan member current

47.4.5  show vlan member static
Display the membership of ports in static VLAN.
➤ Mode: Command is in all modes available.
➤ Privilege Level: Guest
➤ Format: show vlan member static

47.5  network
Configure the inband and outband connectivity.

47.5.1  network management vlan
Configure the management VLAN ID of the switch.
➤ Mode: Privileged Exec Mode
➤ Privilege Level: Operator
➤ Format: network management vlan <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

47.5.2  network management priority dot1p
Configure the management VLAN priority of the switch.
➤ Mode: Privileged Exec Mode
➤ Privilege Level: Operator
➤ Format: network management priority dot1p <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..7</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>
47.5.3  network management priority ip-dscp

Configure the management VLAN ip-dscp priority of the switch.
➤ Mode: Privileged Exec Mode
➤ Privilege Level: Operator
➤ Format: network management priority ip-dscp <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..63</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>
48 Virtual Private Network (VPN)

48.1 ipsec

Configure IPsec VPN settings.

48.1.1 ipsec certificate delete

Delete a certificate uploaded to the device.

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: `ipsec certificate delete <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..100</td>
<td>Certificate Table Index.</td>
</tr>
</tbody>
</table>

48.1.2 ipsec certificate upload passphrase

Passphrase that will be used to decrypt the next uploaded file, before storing on the device (note: will not be stored after the next upload, no matter if it is used or not!)

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: `ipsec certificate upload passphrase <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

48.1.3 ipsec connection add

Add an IPsec VPN connection (use next free index if none submitted).

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: `ipsec connection add <P-1> [name <P-2>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>
48.1.4 ipsec connection modify

Modify a IPsec VPN connection (index in connection is mandatory).

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator

**Format**:

users ipsec connection modify <P-1> name <P-2> certificate ca add <P-3> clear local <P-4> [remote <P-5>] [privkey <P-6>] [passphrase <P-7>] debug informational not-handled <P-8> access [method <P-10>] [pre-shared-key <P-11>] [local-type <P-12>] [local-id <P-13>] [remote-type <P-14>] [remote-id <P-15>] keyexchange mode [protocol <P-16>] [startup <P-17>] [dpdtimeout <P-18>] [lifetime <P-19>] [exchange-mode <P-20>] [margintime <P-21>] [re-authenticate <P-22>] algorithms [key-agreement <P-23>] [integrity <P-24>] [encryption <P-25>] endpoints [local-address <P-26>] [remote-address <P-27>] data-exchange mode [lifetime <P-28>] algorithms [key-agreement <P-29>] [integrity <P-30>] [encryption <P-31>]

**name**: IPsec VPN connection name.

**certificate**: Manage certificates for this connection.

**ca**: Set the CA certificate file name(s). Also supports comma-separated chains.

**add**: Add a CA file name to the current connection.

**clear**: Remove all the CA file names added to the current connection.

**local**: Set the file name of the certificate that will identify the current device.

**[remote]**: Set the file name of the certificate that will identify the remote device.

**[privkey]**: Set the file name of the private key (if it is encrypted and cannot be automatically matched to the certificate).

**[passphrase]**: Set the passphrase to be used with an encrypted private key or PKCS12 encrypted container (warning: will be stored in the config!).

**debug**: IPsec VPN connection additional debugging information to event log.

**informational**: Enable or disable debug of informational messages.

**not-handled**: Enable or disable debug of not handled messages.

**access**: IPsec VPN access.

**[method]**: Authentication method to be used.

**[pre-shared-key]**: Preshared key (passphrase).

**[local-type]**: Type of local peer identifier.

**[local-id]**: Local peer identifier.

**[remote-type]**: Type of remote peer identifier.

**[remote-id]**: Remote peer identifier.

**key-exchange**: Key exchange parameters.

**mode**: Key exchange mode.

**[protocol]**: Version of the key exchange protocol.

**[startup]**: Key exchange at startup.

**[dpd-timeout]**: Dead peer detection timeout.

**[lifetime]**: IKE security association lifetime.

**[exchange-mode]**: IKE exchange mode.

**[margintime]**: IKE and IPsec margintime for re-keying before timeout.

**[re-authenticate]**: Re-authenticate at end of IKE lifetime (IKEv2 only).

**algorithms**: Key exchange algorithms.

**[key-agreement]**: Key agreement algorithm to be used.

**[integrity]**: Integrity (MAC) algorithm to be used in IKEv2.

**[encryption]**: Encryption algorithm to be used.

**endpoints**: IPsec VPN tunnel endpoints.

**[local-address]**: Address of local security gateway.

**[remote-address]**: Address of remote security gateway.

**data-exchange**: Data exchange parameters.

**mode**: Data exchange mode.

**[lifetime]**: Lifetime of IPsec SA.

**algorithms**: Data exchange algorithms.

**[key-agreement]**: Key agreement algorithm to be used.

**[integrity]**: Integrity (MAC) algorithm to be used in IPsec.

**[encryption]**: Algorithm to be used for IPsec payload encryption.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
<tr>
<td>P-3</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-4</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-5</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Meaning</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>P-6</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-7</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
<tr>
<td>P-8</td>
<td>debug_inform</td>
<td>debug informational</td>
</tr>
<tr>
<td>P-9</td>
<td>debug_unhandled</td>
<td>debug unhandled</td>
</tr>
<tr>
<td>P-10</td>
<td>psk</td>
<td>Pre-shared key.</td>
</tr>
<tr>
<td></td>
<td>x509rsa</td>
<td>Individual X.509 RSA certificates.</td>
</tr>
<tr>
<td></td>
<td>pkcs12</td>
<td>Single PKCS12 file with all certificates (including CA).</td>
</tr>
<tr>
<td>P-11</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
<tr>
<td>P-12</td>
<td>default</td>
<td>Local IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>address</td>
<td>IPv4 address or host name (use from address field).</td>
</tr>
<tr>
<td></td>
<td>id</td>
<td>Use identifier.</td>
</tr>
<tr>
<td>P-13</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
<tr>
<td>P-14</td>
<td>any</td>
<td>Not checked.</td>
</tr>
<tr>
<td></td>
<td>address</td>
<td>IPv4 address or host name (use from address field).</td>
</tr>
<tr>
<td></td>
<td>id</td>
<td>Use identifier.</td>
</tr>
<tr>
<td>P-15</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
<tr>
<td>P-16</td>
<td>auto</td>
<td>Accept IKEv1/v2 as responder, start with IKEv2 as initiator.</td>
</tr>
<tr>
<td></td>
<td>v1</td>
<td>IKE version 1 (ISAKMP).</td>
</tr>
<tr>
<td></td>
<td>v2</td>
<td>IKE version 2.</td>
</tr>
<tr>
<td>P-17</td>
<td>initiator</td>
<td>Initiates the IKE at startup.</td>
</tr>
<tr>
<td></td>
<td>responder</td>
<td>Peer starts the IKE initiation.</td>
</tr>
<tr>
<td>P-18</td>
<td>0..86400</td>
<td>Interval between liveness messages in seconds, 0 to disable.</td>
</tr>
<tr>
<td>P-19</td>
<td>300..86400</td>
<td>Lifetime of IKE SA in seconds (max. 24h).</td>
</tr>
<tr>
<td>P-20</td>
<td>main</td>
<td>Initiates or accepts main mode only.</td>
</tr>
<tr>
<td></td>
<td>aggressive</td>
<td>Initiates or accepts aggressive only.</td>
</tr>
<tr>
<td>P-21</td>
<td>1..1800</td>
<td>Margin time for re-keying before timeout.</td>
</tr>
<tr>
<td>P-22</td>
<td>true</td>
<td>True</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>False</td>
</tr>
<tr>
<td>P-23</td>
<td>any</td>
<td>Accept all algorithms as responder, use default as initiator.</td>
</tr>
<tr>
<td></td>
<td>modp1024</td>
<td>RSA with 1024 bits modulus.</td>
</tr>
<tr>
<td></td>
<td>modp1536</td>
<td>RSA with 1536 bits modulus.</td>
</tr>
<tr>
<td></td>
<td>modp2048</td>
<td>RSA with 2048 bits modulus.</td>
</tr>
<tr>
<td></td>
<td>modp3072</td>
<td>RSA with 3072 bits modulus.</td>
</tr>
<tr>
<td></td>
<td>modp4096</td>
<td>RSA with 4096 bits modulus.</td>
</tr>
<tr>
<td>P-24</td>
<td>any</td>
<td>Accept all algorithms as responder, use default as initiator.</td>
</tr>
<tr>
<td></td>
<td>hmacmd5</td>
<td>HMAC-MD5</td>
</tr>
<tr>
<td></td>
<td>hmacsha1</td>
<td>HMAC-SHA1</td>
</tr>
<tr>
<td></td>
<td>hmacsha256</td>
<td>HMAC-SHA256</td>
</tr>
<tr>
<td></td>
<td>hmacsha384</td>
<td>HMAC-SHA384</td>
</tr>
<tr>
<td></td>
<td>hmacsha512</td>
<td>HMAC-SHA512</td>
</tr>
<tr>
<td>P-25</td>
<td>any</td>
<td>Accept all algorithms as responder, use default as initiator.</td>
</tr>
<tr>
<td></td>
<td>des</td>
<td>DES</td>
</tr>
<tr>
<td></td>
<td>des3</td>
<td>Triple-DES</td>
</tr>
<tr>
<td></td>
<td>aes128</td>
<td>AES with 128 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes192</td>
<td>AES with 192 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes256</td>
<td>AES with 256 key bits.</td>
</tr>
<tr>
<td>P-26</td>
<td>any</td>
<td>Use the primary IP address of external interface.</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d</td>
<td>a.b.c.d IP address.</td>
</tr>
<tr>
<td></td>
<td>nu,nu-nu</td>
<td>host.name.domain FQDN</td>
</tr>
<tr>
<td>P-27</td>
<td>any</td>
<td>Use the primary IP address of external interface.</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d</td>
<td>a.b.c.d IP address.</td>
</tr>
<tr>
<td></td>
<td>nu,nu-nu</td>
<td>host.name.domain FQDN</td>
</tr>
<tr>
<td>P-28</td>
<td>300..28800</td>
<td>Lifetime of IPsec SA in seconds (Max. 8h).</td>
</tr>
<tr>
<td>P-29</td>
<td>any</td>
<td>Accept all algorithms as responder, use default as initiator.</td>
</tr>
<tr>
<td></td>
<td>modp1024</td>
<td>RSA with 1024 bits modulus.</td>
</tr>
<tr>
<td></td>
<td>modp1536</td>
<td>RSA with 1536 bits modulus.</td>
</tr>
<tr>
<td></td>
<td>modp2048</td>
<td>RSA with 2048 bits modulus.</td>
</tr>
<tr>
<td></td>
<td>modp3072</td>
<td>RSA with 3072 bits modulus.</td>
</tr>
<tr>
<td></td>
<td>modp4096</td>
<td>RSA with 4096 bits modulus.</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td>No perfect forward secrecy.</td>
</tr>
<tr>
<td>P-29</td>
<td>any</td>
<td>Accept all algorithms as responder, use default as initiator.</td>
</tr>
<tr>
<td></td>
<td>hmacmd5</td>
<td>HMAC-MD5</td>
</tr>
<tr>
<td></td>
<td>hmacsha1</td>
<td>HMAC-SHA1</td>
</tr>
<tr>
<td></td>
<td>hmacsha256</td>
<td>HMAC-SHA256</td>
</tr>
<tr>
<td></td>
<td>hmacsha384</td>
<td>HMAC-SHA384</td>
</tr>
<tr>
<td></td>
<td>hmacsha512</td>
<td>HMAC-SHA512</td>
</tr>
</tbody>
</table>
### no ipsec connection modify

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** no ipsec connection modify name certificate ca add clear local [remote] [privkey] [passphrase] debug informational <P-8> not-handled <P-9> access [method] [pre-shared-key] [local-type] [local-id] [remote-type] [remote-id] key-exchange mode [protocol] [startup] [dpd-timeout] [lifetime] [exchangemode] [margintime] [re-authenticate] algorithms [key-agreement] [integrity] [encryption] endpoints [local-address] [remote-address] data-exchange mode [lifetime] algorithms [key-agreement] [integrity] [encryption]

### 48.1.5 ipsec connection status

Enable or disable a IPsec VPN connection (index in connection is mandatory).

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ipsec connection status <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
<tr>
<td>P-2</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

### 48.1.6 ipsec connection delete

Delete a IPsec VPN connection (index in connection is mandatory).

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ipsec connection delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
</tbody>
</table>
48.1.7 ipsec traffic-selector

IPsec VPN traffic selectors.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `ipsec traffic-selector <P-1> add <P-2> [name <P-3>] delete <P-4> modify <P-5> [name <P-6>] [source-net <P-7>] [source-restriction <P-8>] [dest-net <P-9>] [dest-restriction <P-10>] status <P-11> <P-12>

  - **add:** Add new traffic selector.
    - [name]: Traffic selector ID.
  - **delete:** Delete an existing traffic selector.
    - [name]: Traffic selector ID.
  - **modify:** Modify an existing traffic selector.
    - [name]: Traffic selector ID.
    - [source-net]: Source address for the traffic selector.
    - [source-restriction]: Source restriction for the traffic selector.
    - [dest-net]: Destination address for the traffic selector.
    - [dest-restriction]: Destination restriction for the traffic selector.
  - **status:** Enable or disable an existing traffic selector.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..256</td>
<td>Index of the traffic selector (unique inside of an IPsec VPN connection).</td>
</tr>
<tr>
<td>P-3</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
<tr>
<td>P-4</td>
<td>1..256</td>
<td>Index of the traffic selector (unique inside of an IPsec connection).</td>
</tr>
<tr>
<td>P-5</td>
<td>1..256</td>
<td>Index of the traffic selector (unique inside of an IPsec VPN connection).</td>
</tr>
<tr>
<td>P-6</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
<tr>
<td>P-7</td>
<td>abc.d</td>
<td>abc.d Single IP address.</td>
</tr>
<tr>
<td></td>
<td>abc.d</td>
<td>abc.d Address range in CIDR notation.</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any IP address.</td>
</tr>
<tr>
<td>P-8</td>
<td>string</td>
<td>'protocol/port' Traffic selector restriction can be given as string, e.g. tcp/http or can be given as numbers, e.g. 6/80 (=tcp/http) or can be given as numbers, e.g. /53 (= any/53) 'protocol/port' Traffic selector restriction can be given as string, e.g. udp (= udp/any) or can be given as numbers, e.g. 17 (= 17(udp)/any) and empty restriction '' means to have no restriction (any/any)</td>
</tr>
<tr>
<td>P-9</td>
<td>abc.d</td>
<td>abc.d Single IP address.</td>
</tr>
<tr>
<td></td>
<td>abc.d</td>
<td>abc.d Address range in CIDR notation.</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any IP address.</td>
</tr>
<tr>
<td>P-10</td>
<td>string</td>
<td>'protocol/port' Traffic selector restriction can be given as string, e.g. tcp/http or can be given as numbers, e.g. 6/80 (=tcp/http) or can be given as numbers, e.g. /53 (= any/53) 'protocol/port' Traffic selector restriction can be given as string, e.g. udp (= udp/any) or can be given as numbers, e.g. 17 (= 17(udp)/any) and empty restriction '' means to have no restriction (any/any)</td>
</tr>
<tr>
<td>P-11</td>
<td>1..256</td>
<td>Index of the traffic selector (unique inside of an IPsec VPN connection).</td>
</tr>
<tr>
<td>P-12</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

48.2 show

Display device options and settings.

48.2.1 show ipsec general

General IPsec VPN settings.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ipsec general`

48.2.2 show ipsec connections summary

Overview of all configured connections.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ipsec connections summary`
48.2.3  show ipsec connections access
IPsec connection access settings.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show ipsec connections access <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
</tbody>
</table>

48.2.4  show ipsec connections certificates
IPsec connection certificates.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show ipsec connections certificates <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
</tbody>
</table>

48.2.5  show ipsec connections key-exchange
IPsec connection key exchange settings (IKE).
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show ipsec connections key-exchange <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
</tbody>
</table>

48.2.6  show ipsec connections data-exchange
IPsec connection data exchange settings.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show ipsec connections data-exchange <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
</tbody>
</table>

48.2.7  show ipsec connections status
IPsec connection status.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show ipsec connections data-exchange <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
</tbody>
</table>

48.2.8  show ipsec traffic-selectors
Traffic selectors for a IPsec VPN connection.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show ipsec traffic-selectors <P-1> [<P-2>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..256</td>
<td>Index of the traffic selector (unique inside of a IPsec VPN connection).</td>
</tr>
</tbody>
</table>

48.2.9  show ipsec certificate summary
Show a summary of all uploaded certificates and private keys.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Administrator
  ▶ Format: show ipsec certificate summary

48.2.10 show ipsec certificate details
Show details about a specific certificate or private key.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Administrator
  ▶ Format: show ipsec certificate details <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..100</td>
<td>Certificate Table Index.</td>
</tr>
</tbody>
</table>
49 Users

49.1 users
Manage Users and User Accounts.

49.1.1 users add
Add a new user.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: users add <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
</tbody>
</table>

49.1.2 users delete
Delete an existing user.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: users delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
</tbody>
</table>

49.1.3 users enable
Enable user.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: users enable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
</tbody>
</table>

49.1.4 users disable
Disable user.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: users disable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
</tbody>
</table>

49.1.5 users password
Change user password.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: users password <P-1> [<P-2>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 64 characters.</td>
</tr>
</tbody>
</table>

49.1.6 users snmpv3 authentication
Specify authentication setting for a user.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: users snmpv3 authentication <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
<tr>
<td>P-2</td>
<td>md5</td>
<td>MD5 as SNMPv3 user authentication mode.</td>
</tr>
<tr>
<td></td>
<td>sha1</td>
<td>SHA1 as SNMPv3 user authentication mode.</td>
</tr>
</tbody>
</table>
49.1.7 users snmpv3 encryption
Specify encryption settings for a user.
► Mode: Global Config Mode
► Privilege Level: Administrator
► Format: users snmpv3 encryption <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
<tr>
<td>P-2</td>
<td></td>
<td>SNMPv3 encryption method is none.</td>
</tr>
<tr>
<td></td>
<td>des</td>
<td>DES as SNMPv3 encryption method.</td>
</tr>
<tr>
<td></td>
<td>aescfb128</td>
<td>AES-128 as SNMPv3 encryption method.</td>
</tr>
</tbody>
</table>

49.1.8 users access-role
Specify snmpv3 access role for a user.
► Mode: Global Config Mode
► Privilege Level: Administrator
► Format: users access-role <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
<tr>
<td>P-2</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

49.1.9 users lock-status
Set the lockout status of a specified user.
► Mode: Global Config Mode
► Privilege Level: Administrator
► Format: users lock-status <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
<tr>
<td>P-2</td>
<td>unlock</td>
<td>Unlock specific user. User can login again.</td>
</tr>
</tbody>
</table>

49.1.10 users password-policy-check
Set password policy check option. The device checks the "minimum password length", regardless of the setting for this option.
► Mode: Global Config Mode
► Privilege Level: Administrator
► Format: users password-policy-check <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
<tr>
<td>P-2</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

49.2 show
Display device options and settings.

49.2.1 show users
Display the users and user accounts information.
► Mode: Command is in all modes available.
► Privilege Level: Administrator
► Format: show users
A  Further support

Technical questions
For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly. You find the addresses of our partners on the Internet at www.hirschmann.com. A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at hirschmann-support.belden.com. This site also includes a free of charge knowledge base and a software download section.

Technical Documents
The current manuals and operating instructions for Hirschmann products are available at doc.hirschmann.com.

Hirschmann Competence Center
The Hirschmann Competence Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification. You find the training courses on technology and products currently available at www.hicomcenter.com.
- Support ranges from the first installation through the standby service to maintenance concepts.

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

<table>
<thead>
<tr>
<th></th>
<th>Very Good</th>
<th>Good</th>
<th>Satisfactory</th>
<th>Mediocre</th>
<th>Poor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precise description</td>
<td></td>
<td>0</td>
<td>O</td>
<td>0</td>
<td>O</td>
</tr>
<tr>
<td>Readability</td>
<td></td>
<td>0</td>
<td>O</td>
<td>0</td>
<td>O</td>
</tr>
<tr>
<td>Understandability</td>
<td></td>
<td>0</td>
<td>O</td>
<td>0</td>
<td>O</td>
</tr>
<tr>
<td>Examples</td>
<td></td>
<td>0</td>
<td>O</td>
<td>0</td>
<td>O</td>
</tr>
<tr>
<td>Structure</td>
<td></td>
<td>0</td>
<td>O</td>
<td>0</td>
<td>O</td>
</tr>
<tr>
<td>Comprehensive</td>
<td></td>
<td>0</td>
<td>O</td>
<td>0</td>
<td>O</td>
</tr>
<tr>
<td>Graphics</td>
<td></td>
<td>0</td>
<td>O</td>
<td>0</td>
<td>O</td>
</tr>
<tr>
<td>Drawings</td>
<td></td>
<td>0</td>
<td>O</td>
<td>0</td>
<td>O</td>
</tr>
<tr>
<td>Tables</td>
<td></td>
<td>0</td>
<td>O</td>
<td>0</td>
<td>O</td>
</tr>
</tbody>
</table>

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

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Suggestions for improvement and additional information:

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

General comments:

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:
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
User Manual

Configuration
Industrial Security Router
EAGLE40-03
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.

© 2020 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.

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).

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety instructions</td>
<td>9</td>
</tr>
<tr>
<td>About this Manual</td>
<td>11</td>
</tr>
<tr>
<td>Key</td>
<td>12</td>
</tr>
<tr>
<td>Replacing a faulty device</td>
<td>13</td>
</tr>
<tr>
<td><strong>1 User interfaces</strong></td>
<td></td>
</tr>
<tr>
<td>1.1 Graphical User Interface</td>
<td>15</td>
</tr>
<tr>
<td>1.2 Command Line Interface</td>
<td>15</td>
</tr>
<tr>
<td>1.2.1 Preparing the data connection</td>
<td>16</td>
</tr>
<tr>
<td>1.2.2 Access to the Command Line Interface using SSH (Secure Shell)</td>
<td>17</td>
</tr>
<tr>
<td>1.2.3 Access to the Command Line Interface using the serial interface</td>
<td>19</td>
</tr>
<tr>
<td>1.2.4 Mode-based command hierarchy</td>
<td>21</td>
</tr>
<tr>
<td>1.2.5 Executing the commands</td>
<td>25</td>
</tr>
<tr>
<td>1.2.6 Structure of a command</td>
<td>25</td>
</tr>
<tr>
<td>1.2.7 Examples of commands</td>
<td>28</td>
</tr>
<tr>
<td>1.2.8 Input prompt</td>
<td>29</td>
</tr>
<tr>
<td>1.2.9 Key combinations</td>
<td>30</td>
</tr>
<tr>
<td>1.2.10 Data entry elements</td>
<td>32</td>
</tr>
<tr>
<td>1.2.11 Use cases</td>
<td>33</td>
</tr>
<tr>
<td>1.2.12 Service Shell</td>
<td>34</td>
</tr>
<tr>
<td>1.3 System monitor</td>
<td>37</td>
</tr>
<tr>
<td>1.3.1 Functional scope</td>
<td>37</td>
</tr>
<tr>
<td>1.3.2 Starting the System Monitor</td>
<td>37</td>
</tr>
<tr>
<td><strong>2 Specifying the IP parameters</strong></td>
<td></td>
</tr>
<tr>
<td>2.1 IP parameter basics</td>
<td>39</td>
</tr>
<tr>
<td>2.1.1 IPv4</td>
<td>39</td>
</tr>
<tr>
<td>2.2 Specifying the IP parameters using the Command Line Interface</td>
<td>43</td>
</tr>
<tr>
<td>2.2.1 IPv4</td>
<td>43</td>
</tr>
<tr>
<td>2.3 Specifying the IP parameters using HiDiscovery</td>
<td>45</td>
</tr>
<tr>
<td>2.4 Specifying the IP parameters using the Graphical User Interface</td>
<td>47</td>
</tr>
<tr>
<td>2.4.1 IPv4</td>
<td>47</td>
</tr>
<tr>
<td><strong>3 Access to the device</strong></td>
<td></td>
</tr>
<tr>
<td>3.1 Access roles</td>
<td>49</td>
</tr>
<tr>
<td>3.2 First login (Password change)</td>
<td>49</td>
</tr>
<tr>
<td>3.3 Authentication lists</td>
<td>50</td>
</tr>
<tr>
<td>3.3.1 Applications</td>
<td>51</td>
</tr>
<tr>
<td>3.3.2 Policies</td>
<td>51</td>
</tr>
<tr>
<td>3.3.3 Managing authentication lists</td>
<td>51</td>
</tr>
<tr>
<td>3.3.4 Adjust the settings</td>
<td>52</td>
</tr>
<tr>
<td>3.4</td>
<td>User management .................................................................................</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3.4.1</td>
<td>Access roles ...................................................................................</td>
</tr>
<tr>
<td>3.4.2</td>
<td>Managing user accounts ...................................................................</td>
</tr>
<tr>
<td>3.4.3</td>
<td>Default setting ...............................................................................</td>
</tr>
<tr>
<td>3.4.4</td>
<td>Changing default passwords ................................................................</td>
</tr>
<tr>
<td>3.4.5</td>
<td>Setting up a new user account .......................................................</td>
</tr>
<tr>
<td>3.4.6</td>
<td>Deactivating the user account .......................................................</td>
</tr>
<tr>
<td>3.4.7</td>
<td>Adjusting policies for passwords ....................................................</td>
</tr>
<tr>
<td>3.5</td>
<td>LDAP ..................................................................................................</td>
</tr>
<tr>
<td>3.5.1</td>
<td>Coordination with the server administrator .....................................</td>
</tr>
<tr>
<td>3.5.2</td>
<td>Example configuration ....................................................................</td>
</tr>
<tr>
<td>3.6</td>
<td>SNMP access .....................................................................................</td>
</tr>
<tr>
<td>3.6.1</td>
<td>SNMPv1/v2 access ...........................................................................</td>
</tr>
<tr>
<td>3.6.2</td>
<td>SNMPv3 access ................................................................................</td>
</tr>
<tr>
<td>3.6.3</td>
<td>Example configuration ....................................................................</td>
</tr>
<tr>
<td>4</td>
<td>VPN – Virtual Private Network ..........................................................</td>
</tr>
<tr>
<td>4.1</td>
<td>IPSec – Internet Protocol Security ..................................................</td>
</tr>
<tr>
<td>4.2</td>
<td>IKE – Internet Key Exchange ............................................................</td>
</tr>
<tr>
<td>4.2.1</td>
<td>Authentication ...............................................................................</td>
</tr>
<tr>
<td>4.2.2</td>
<td>Encryption .................................................................................</td>
</tr>
<tr>
<td>4.2.3</td>
<td>Creating a certificate using OpenSSL ..............................................</td>
</tr>
<tr>
<td>4.3</td>
<td>Application examples .....................................................................</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Connecting 2 subnetworks ...............................................................</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Creating a certificate using OpenSSL ..............................................</td>
</tr>
<tr>
<td>5</td>
<td>Managing configuration profiles ...........................................................</td>
</tr>
<tr>
<td>5.1</td>
<td>Detecting changed settings ...............................................................</td>
</tr>
<tr>
<td>5.1.1</td>
<td>Volatile memory (RAM) and non-volatile memory (NVM) .................</td>
</tr>
<tr>
<td>5.1.2</td>
<td>External memory (ACA) and non-volatile memory (NVM) ...............</td>
</tr>
<tr>
<td>5.2</td>
<td>Saving the settings .......................................................................</td>
</tr>
<tr>
<td>5.2.1</td>
<td>Saving the configuration profile in the device ..................................</td>
</tr>
<tr>
<td>5.2.2</td>
<td>Saving the configuration profile in the external memory .................</td>
</tr>
<tr>
<td>5.2.3</td>
<td>Exporting a configuration profile ..................................................</td>
</tr>
<tr>
<td>5.3</td>
<td>Loading settings ...........................................................................</td>
</tr>
<tr>
<td>5.3.1</td>
<td>Activating a configuration profile ..................................................</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Loading the configuration profile from the external memory ...........</td>
</tr>
<tr>
<td>5.3.3</td>
<td>Importing a configuration profile ..................................................</td>
</tr>
<tr>
<td>5.4</td>
<td>Reset the device to the factory defaults .........................................</td>
</tr>
<tr>
<td>5.4.1</td>
<td>Using the Graphical User Interface or Command Line Interface ........</td>
</tr>
<tr>
<td>5.4.2</td>
<td>Using the System Monitor .............................................................</td>
</tr>
<tr>
<td>6</td>
<td>Loading software updates ..................................................................</td>
</tr>
<tr>
<td>6.1</td>
<td>Software update from the PC .........................................................</td>
</tr>
<tr>
<td>6.2</td>
<td>Software update from a server ........................................................</td>
</tr>
<tr>
<td>6.3</td>
<td>Software update from the external memory .....................................</td>
</tr>
<tr>
<td>6.3.1</td>
<td>Manually—initiated by the administrator ..........................................</td>
</tr>
<tr>
<td>6.3.2</td>
<td>Automatically—initiated by the device .............................................</td>
</tr>
<tr>
<td>6.4</td>
<td>Loading a previous software version ...............................................</td>
</tr>
<tr>
<td>7</td>
<td>Configuring the ports .......................................................................</td>
</tr>
<tr>
<td>7.1</td>
<td>Enabling/disabling the port ..............................................................</td>
</tr>
<tr>
<td>7.2</td>
<td>Selecting the operating mode .........................................................</td>
</tr>
</tbody>
</table>
7.3 Hardware LAN bypass ................................................................. 97
7.3.1 System-off bypass ................................................................. 97
7.3.2 Run-time bypass ................................................................. 97

8 Assistance in the protection from unauthorized access .................... 99
8.1 Changing the SNMPv1/v2 community ........................................ 99
8.2 Disabling SNMPv1/v2 .............................................................. 100
8.3 Disabling HTTP ........................................................................ 101
8.4 Disabling the HiDiscovery access ............................................... 102
8.5 Activating the IP access restriction .............................................. 103
8.6 Adjusting the session timeouts................................................... 105

9 Controlling the data traffic ............................................................ 107
9.1 Packet Filter – Routed Firewall Mode ......................................... 108
9.1.1 Description ....................................................................... 108
9.1.2 Application example .......................................................... 109
9.2 Packet Filter – Transparent Firewall Mode ................................... 112
9.2.1 Description ....................................................................... 112
9.2.2 Application examples .......................................................... 113
9.3 Helping protect against unauthorized access ............................... 120
9.4 Deep Packet Inspection ............................................................ 121
9.4.1 Deep Packet Inspection - Modbus Enforcer function .................. 121
9.4.2 Application example for Modbus Enforcer ............................. 121
9.4.3 Create and edit Modbus Enforcer rules ................................... 122
9.4.4 Deep Packet Inspection - DNP3 Enforcer function ................... 123
9.4.5 Application example for DNP3 Enforcer .............................. 124
9.4.6 Create and edit a DNP3 Enforcer rule .................................... 125

10 Synchronizing the system time in the network .............................. 129
10.1 Basic settings ..................................................................... 129
10.1.1 Setting the time .................................................................. 129
10.1.2 Automatic daylight saving time changeover ............................. 130
10.2 NTP ...................................................................................... 131
10.2.1 Preparing the NTP configuration ......................................... 131
10.2.2 NTP configuration .............................................................. 132

11 Network load control ................................................................. 135
11.1 Direct packet distribution ......................................................... 135
11.1.1 Learning MAC addresses ................................................... 135
11.1.2 Aging of learned MAC addresses ........................................ 135
11.1.3 Static address entries ......................................................... 135
11.2 Rate limiter ......................................................................... 138
11.3 QoS/Priority ....................................................................... 139
11.3.1 Handling of received priority information .............................. 139
11.3.2 VLAN tagging .................................................................. 139
11.3.3 Setting prioritization ......................................................... 140
11.4 Flow control ....................................................................... 142
11.4.1 Halfduplex or fullduplex link .............................................. 142
11.4.2 Setting up the Flow Control ............................................... 143
<table>
<thead>
<tr>
<th>12</th>
<th>VLANs</th>
<th>145</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>Examples of VLANs</td>
<td>145</td>
</tr>
<tr>
<td>12.1.1</td>
<td>Example 1</td>
<td>146</td>
</tr>
<tr>
<td>12.1.2</td>
<td>Example 2</td>
<td>149</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>13</th>
<th>Routing</th>
<th>155</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.1</td>
<td>Configuration</td>
<td>155</td>
</tr>
<tr>
<td>13.2</td>
<td>Routing - Basics</td>
<td>156</td>
</tr>
<tr>
<td>13.2.1</td>
<td>ARP</td>
<td>157</td>
</tr>
<tr>
<td>13.2.2</td>
<td>CIDR</td>
<td>159</td>
</tr>
<tr>
<td>13.2.3</td>
<td>Multinetting</td>
<td>160</td>
</tr>
<tr>
<td>13.3</td>
<td>Static Routing</td>
<td>161</td>
</tr>
<tr>
<td>13.3.1</td>
<td>Port-based Router Interface</td>
<td>161</td>
</tr>
<tr>
<td>13.3.2</td>
<td>VLAN-based Router Interface</td>
<td>163</td>
</tr>
<tr>
<td>13.3.3</td>
<td>Configuration of a Static Route</td>
<td>165</td>
</tr>
<tr>
<td>13.3.4</td>
<td>Static route tracking</td>
<td>168</td>
</tr>
<tr>
<td>13.4</td>
<td>NAT – Network Address Translation</td>
<td>172</td>
</tr>
<tr>
<td>13.4.1</td>
<td>Applying the NAT Rules</td>
<td>172</td>
</tr>
<tr>
<td>13.4.2</td>
<td>1:1 NAT</td>
<td>173</td>
</tr>
<tr>
<td>13.4.3</td>
<td>Destination NAT</td>
<td>175</td>
</tr>
<tr>
<td>13.4.4</td>
<td>Masquerading NAT</td>
<td>178</td>
</tr>
<tr>
<td>13.4.5</td>
<td>Double NAT</td>
<td>179</td>
</tr>
<tr>
<td>13.5</td>
<td>Tracking</td>
<td>183</td>
</tr>
<tr>
<td>13.5.1</td>
<td>Interface tracking</td>
<td>183</td>
</tr>
<tr>
<td>13.5.2</td>
<td>Ping tracking</td>
<td>184</td>
</tr>
<tr>
<td>13.5.3</td>
<td>Logical tracking</td>
<td>185</td>
</tr>
<tr>
<td>13.5.4</td>
<td>Configuring the tracking</td>
<td>185</td>
</tr>
<tr>
<td>13.6</td>
<td>VRRP</td>
<td>192</td>
</tr>
<tr>
<td>13.6.1</td>
<td>VRRP</td>
<td>192</td>
</tr>
<tr>
<td>13.6.2</td>
<td>VRRP with load sharing</td>
<td>195</td>
</tr>
<tr>
<td>13.6.3</td>
<td>VRRP with Multinetting</td>
<td>195</td>
</tr>
<tr>
<td>13.7</td>
<td>OSPF</td>
<td>197</td>
</tr>
<tr>
<td>13.7.1</td>
<td>OSPF-Topology</td>
<td>198</td>
</tr>
<tr>
<td>13.7.2</td>
<td>General Operation of OSPF</td>
<td>202</td>
</tr>
<tr>
<td>13.7.3</td>
<td>Setting up the Adjacency</td>
<td>203</td>
</tr>
<tr>
<td>13.7.4</td>
<td>Synchronization of the LSDB</td>
<td>204</td>
</tr>
<tr>
<td>13.7.5</td>
<td>Route Calculation</td>
<td>205</td>
</tr>
<tr>
<td>13.7.6</td>
<td>Configuring OSPF</td>
<td>206</td>
</tr>
<tr>
<td>13.7.7</td>
<td>Limiting the distribution of the routes using an ACL</td>
<td>209</td>
</tr>
<tr>
<td>13.8</td>
<td>Entering the IP Parameters</td>
<td>220</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>14</th>
<th>Operation diagnosis</th>
<th>223</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Sending SNMP traps</td>
<td>223</td>
</tr>
<tr>
<td>14.1.1</td>
<td>List of SNMP traps</td>
<td>224</td>
</tr>
<tr>
<td>14.1.2</td>
<td>SNMP traps for configuration activity</td>
<td>225</td>
</tr>
<tr>
<td>14.1.3</td>
<td>SNMP trap setting</td>
<td>225</td>
</tr>
<tr>
<td>14.1.4</td>
<td>ICMP messaging</td>
<td>226</td>
</tr>
<tr>
<td>14.2</td>
<td>Monitoring the Device Status</td>
<td>227</td>
</tr>
<tr>
<td>14.2.1</td>
<td>Events which can be monitored</td>
<td>227</td>
</tr>
<tr>
<td>14.2.2</td>
<td>Configuring the Device Status</td>
<td>228</td>
</tr>
<tr>
<td>14.2.3</td>
<td>Displaying the Device Status</td>
<td>229</td>
</tr>
</tbody>
</table>
14.3 Security Status ........................................................................................................... 230
14.3.1 Events which can be monitored .............................................................................. 230
14.3.2 Configuring the Security Status .............................................................................. 231
14.3.3 Displaying the Security Status ................................................................................. 232
14.4 Out-of-Band signaling .................................................................................................. 234
14.4.1 Controlling the Signal contact ................................................................................ 234
14.4.2 Monitoring the Device and Security Statuses ......................................................... 235
14.5 Port status indication .................................................................................................... 238
14.6 Port event counter ....................................................................................................... 239
14.6.1 Detecting non-matching duplex modes ................................................................... 239
14.7 Displaying the SFP status ............................................................................................ 241
14.8 Topology discovery ..................................................................................................... 242
14.8.1 Displaying the Topology discovery results .............................................................. 242
14.9 Reports ........................................................................................................................ 244
14.9.1 Global settings ...................................................................................................... 244
14.9.2 Syslog .................................................................................................................... 246
14.9.3 System Log ........................................................................................................... 247
14.9.4 Audit Trail ............................................................................................................. 247
15 Advanced functions of the device .................................................................................. 249
15.1 Using the device as a DNS client ................................................................................ 249
15.1.1 Configuring a DNS server example ....................................................................... 249
A Setting up the configuration environment ..................................................................... 251
A.1 Preparing access via SSH ............................................................................................. 251
A.1.1 Generating a key in the device ................................................................................ 251
A.1.2 Loading your own key onto the device .................................................................. 251
A.1.3 Preparing the SSH client program ....................................................................... 252
A.2 HTTPS certificate ....................................................................................................... 254
A.2.1 HTTPS certificate management ............................................................................. 254
A.2.2 Access through HTTPS ........................................................................................ 255
B Appendix ....................................................................................................................... 257
B.1 Literature references ................................................................................................... 257
B.2 Maintenance ............................................................................................................... 258
B.3 Management Information Base (MIB) .................................................................... 259
B.4 List of RFCs ................................................................................................................. 261
B.5 Underlying IEEE Standards ...................................................................................... 263
B.6 Underlying ANSI Norms ............................................................................................ 264
B.7 Technical Data .......................................................................................................... 265
B.8 Copyright of integrated Software ............................................................................... 266
B.9 Abbreviations used ..................................................................................................... 267
C Index ............................................................................................................................... 269
D Further support .............................................................................................................. 275
E Readers’ Comments ...................................................................................................... 276
### Safety instructions

**WARNING**

**UNCONTROLLED MACHINE ACTIONS**

To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.

Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.

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

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 “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 “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 Industrial HiVision Network Management software provides you with additional options for smooth configuration and monitoring:
  ▶ Auto-topology discovery
  ▶ Browser interface
  ▶ Client/server structure
  ▶ Event handling
  ▶ Event log
  ▶ Simultaneous configuration of multiple devices
  ▶ Graphical user interface with network layout
  ▶ SNMP/OPC gateway
The designations used in this manual have the following meanings:

- **List**
- **Work step**
- **Link** Cross-reference with link
- **Note:** A note emphasizes a significant fact or draws your attention to a dependency.
- **Courier** Representation of a CLI command or field contents in the graphical user interface

- Execution in the Graphical User Interface
- Execution in the Command Line Interface
Replacing a faulty device

The device provides the following plug-and-play solutions for replacing a faulty device with a device of the same type:

- The new device loads the configuration profile of the replaced device from the external memory. See “Loading the configuration profile from the external memory” on page 83.

With each solution, upon reboot, the new device gets the same IP settings that the replaced device had.

- For accessing the device management using HTTPS, the device uses a digital certificate. You have the option to import your own certificate to the device. See “HTTPS certificate management” on page 254.

- For accessing the device management using SSH, the device uses an RSA host key. You have the option to import your own host key in PEM format to the device. See “Loading your own key onto the device” on page 251.
Replacing a faulty device
1 User interfaces

The device lets you specify the settings of the device using the following user interfaces.

Table 1: User interfaces for accessing the device management

<table>
<thead>
<tr>
<th>User interface</th>
<th>Can be reached through ...</th>
<th>Prerequisite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graphical User Interface</td>
<td>Ethernet (In-Band)</td>
<td>Web browser</td>
</tr>
<tr>
<td>Command Line Interface</td>
<td>Ethernet (In-Band)</td>
<td>Terminal emulation software</td>
</tr>
<tr>
<td></td>
<td>Serial interface (Out-of-Band)</td>
<td></td>
</tr>
</tbody>
</table>

1.1 Graphical User Interface

System requirements

To open the Graphical User Interface, you need the desktop version of a web browser with HTML5 support.

Note: Third-party software such as web browsers validate certificates based on criteria such as their expiration date and current cryptographic parameter recommendations. Old certificates can cause errors for example, when they expire or cryptographic recommendations change. To solve validation conflicts with third-party software, transfer your own up-to-date certificate onto the device or regenerate the certificate with the latest firmware.

Starting the Graphical User Interface

The prerequisite for starting the Graphical User Interface is that the IP parameters are configured in the device. See “Specifying the IP parameters” on page 39.

Perform the following steps:

- Start your web browser.
- Type 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 displays the login dialog.
- When you want to change the language of the Graphical User Interface, click the appropriate link in the top right corner of the login dialog.
- Enter the user name.
- Enter the password.
- Click the Login button.
  The web browser displays the Graphical User Interface.
1.2 **Command Line Interface**

The Command Line Interface enables you to use the functions of the device through a local or remote connection.

The Command Line Interface provides IT specialists with a familiar environment for configuring IT devices. As an experienced user or administrator, you have knowledge about the basics and about using Hirschmann devices.

1.2.1 **Preparing the data connection**

Information for assembling and starting up your device can be found in the "Installation" user manual.

- Connect the device with the network. The prerequisite for a successful data connection is the correct setting of the network parameters.

You can access the user interface of the Command Line Interface for example, with the freeware program *PuTTY*. 
This program is provided on the product CD.
- Install the **PuTTY** program on your computer.

### 1.2.2 Access to the Command Line Interface using SSH (Secure Shell)

In the following example we use the **PuTTY** program. Another option to access your device using SSH is the OpenSSH Suite.

Perform the following steps:
- Start the **PuTTY** program on your computer.

#### Figure 1: **PuTTY** input screen

- In the **Host Name (or IP address)** field you enter the IP address of your device. The IP address consists of 4 decimal numbers with values from 0 to 255. The 4 decimal numbers are separated by points.
- To specify the connection type, select the **SSH** radio button in the **Connection type** option list. After selecting and setting the required parameters, the device enables you to set up the data connection using SSH.
User interfaces

1.2 Command Line Interface

- Click the **Open** button to set up the data connection to your device. Depending on the device and the time at which SSH was configured, setting up the connection takes up to a minute.

When you first log in, towards the end of the connection setup, the **PuTTY** program displays a security alert message and lets you check the fingerprint of the key.

![PuTTY Security Alert](image)

**Figure 2:** Security alert prompt for the fingerprint

- Check the fingerprint. This helps protect yourself from unwelcome guests.
- When the fingerprint matches the fingerprint of the device key, click the **Yes** button.
- The device lets you display the finger prints of the device keys with the command `show ssh` or in the **Device Security > Management Access > Server** dialog, **SSH** tab.
- The Command Line Interface appears on the screen with a window for entering the user name. The device enables up to 5 users to have access to the Command Line Interface at the same time.
- Enter the user name. The default user name is **admin**.
- Press the <Enter> key. 
- Enter the password. The default password is **private**.
- Press the <Enter> key.

**Note:** This device is a security-relevant product. Change the password during the first startup procedure.
1.2 Command Line Interface

1.2.3 Access to the Command Line Interface using the serial interface

The serial interface is used to locally connect an external network management station (VT100 terminal or PC with terminal emulation). The interface lets you set up a data connection to the Command Line Interface and to the system monitor.

**VT 100 terminal settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>115200 bit/s</td>
</tr>
<tr>
<td>Data</td>
<td>8 bit</td>
</tr>
<tr>
<td>Stopbit</td>
<td>1 bit</td>
</tr>
<tr>
<td>Handshake</td>
<td>off</td>
</tr>
<tr>
<td>Parity</td>
<td>none</td>
</tr>
</tbody>
</table>
Perform the following steps:

- Connect the device to a terminal using the serial interface. Alternatively, connect the device to a COM port of your PC using terminal emulation based on VT100 and press any key.
- Alternatively, you set up the serial data connection to the device with the serial interface using the PuTTY program. Press the <Enter> key.

- Press any key on your terminal keyboard a number of times until the login screen indicates the CLI mode.
- Enter the user name.
  - The default user name is **admin**.
- Press the <Enter> key.
- Enter the password.
  - The default password is **private**.
- Press the <Enter> key.

**Note:** This device is a security-relevant product. Change the password during the first startup procedure.
1.2Command Line Interface

In the Command Line Interface, the commands are grouped in the related modes, according to the type of the command. Every command mode supports specific Hirschmann software commands.

The commands available to you as a user depend on your privilege level (administrator, operator, guest, auditor). They also depend on the mode in which you are currently working. When you switch to a specific mode, the commands of the mode are available to you.

The User Exec mode commands are an exception. The Command Line Interface also enables you to execute these commands in the Privileged Exec mode.
The Command Line Interface supports, depending on the user level, the following modes:

- **User Exec mode**
  When you log in with the Command Line Interface, you enter the User Exec mode. The User Exec mode contains a limited range of commands.
  Command prompt: (EAGLE) >

- **Privileged Exec mode**
  To access the entire range of commands, you enter the Privileged Exec mode. If you log in as a privileged user, then you are able to enter the Privileged Exec mode. In the Privileged Exec mode, you are able to execute the User Exec mode commands, too.
  Command prompt: (EAGLE) #

- **VLAN mode**
  The VLAN mode contains VLAN-related commands.
  Command prompt: (EAGLE) (VLAN) #

- **Service Shell**
  The Service Shell is for service purposes only.
  Command prompt: /mnt/fastpath #

- **Global Config mode**
  The Global Config mode lets you perform modifications to the current configuration. This mode groups general setup commands.
  Command prompt: (EAGLE) (config) #

- **Interface Range mode**
  The commands in the Interface Range mode affect a specific port, a selected group of multiple ports or all port of the device. The commands modify a value or switch a function on/off on one or more specific ports.
User interfaces
1.2 Command Line Interface

- All physical ports in the device
  Command prompt: `(EAGLE) (interface all)`
  Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
  
  `{EAGLE} (config)#interface all
  {EAGLE} (Interface) all`

- A single port on one interface
  Command prompt: `(EAGLE) (interface <slot/port>)`
  Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
  
  `{EAGLE} (config)#interface 2/1
  {EAGLE} (interface 2/1)`

- A range of ports on one interface
  Command prompt: `(EAGLE) (interface <interface range>)`
  Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
  
  `{EAGLE} (config)#interface 1/2-1/4
  {EAGLE} (Interface) 1/2-1/4`

- A list of single ports
  Command prompt: `(EAGLE) (interface <interface list>)`
  Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
  
  `{EAGLE} (config)#interface 1/2,1/4,1/5
  {EAGLE} (Interface) 1/2,1/4,1/5`

- A list of port ranges and single ports
  Command prompt: `(EAGLE) (interface <complex range>)`
  Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
  
  `{EAGLE} (config)#interface 1/2-1/4,1/6-1/9
  {EAGLE} (Interface) 1/2-1/4,1/6-1/9`

The following table displays the command modes, the command prompts (input request characters) visible in the corresponding mode, and the option with which you quit this mode.

<table>
<thead>
<tr>
<th>Command mode</th>
<th>Access method</th>
<th>Quit or start next mode</th>
</tr>
</thead>
</table>
| User Exec mode        | First access level. Perform basic tasks and list system information.         | To quit you enter `logout`:
                        |                                                                              | (EAGLE) >logout
                        |                                                                              | Are you sure (Y/N)? y                                         |
| Privileged Exec mode  | From the User Exec mode, you enter the command `enable`:
                        |                                                                              | To quit the Privileged Exec mode and return to the User Exec mode, you enter
                        | (EAGLE) >enable                                                             | exit:
                        | (EAGLE) #                                                                   | (EAGLE) #exit
                        |                                                                              | (EAGLE) >
### Command Modes

**Table 2: Command modes**

<table>
<thead>
<tr>
<th>Command mode</th>
<th>Access method</th>
<th>Quit or start next mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VLAN mode</strong></td>
<td>From the Privileged Exec mode, you enter the command <code>vlan database</code></td>
<td>To end the VLAN mode and return to the Privileged Exec mode, you enter <code>exit</code> or press Ctrl Z.</td>
</tr>
<tr>
<td></td>
<td>(EAGLE) <code>#vlan database</code></td>
<td>(EAGLE) <code>(Vlan)#exit</code></td>
</tr>
<tr>
<td></td>
<td>(EAGLE) <code>#</code></td>
<td>(EAGLE) <code>#</code></td>
</tr>
<tr>
<td><strong>Global Config mode</strong></td>
<td>From the Privileged Exec mode, you enter the command <code>configure</code></td>
<td>To quit the Global Config mode and return to the Privileged Exec mode, you enter <code>exit</code></td>
</tr>
<tr>
<td></td>
<td>(EAGLE) <code>#configure</code></td>
<td>(EAGLE) <code>#exit</code></td>
</tr>
<tr>
<td></td>
<td>(EAGLE) <code>#</code></td>
<td>(EAGLE) <code>#</code></td>
</tr>
<tr>
<td></td>
<td>From the User Exec mode, you enter the command <code>enable</code>, and then in Privileged Exec mode, enter the command <code>configure</code></td>
<td>To then quit the Privileged Exec mode and return to the User Exec mode, you enter <code>exit</code> again:</td>
</tr>
<tr>
<td></td>
<td>(EAGLE) <code>&gt;enable</code></td>
<td>(EAGLE) <code>#exit</code></td>
</tr>
<tr>
<td></td>
<td>(EAGLE) <code>#configure</code></td>
<td>(EAGLE) <code>#</code></td>
</tr>
<tr>
<td></td>
<td>(EAGLE) <code>(config)#</code></td>
<td>(EAGLE) <code>#</code></td>
</tr>
<tr>
<td><strong>Interface Range mode</strong></td>
<td>From the Global Config mode you enter the command `interface {all</td>
<td>&lt;slot/port&gt;</td>
</tr>
<tr>
<td></td>
<td>(EAGLE) <code>(config)</code>&lt;interface &lt;slot/port&gt;`</td>
<td>(EAGLE) <code>#exit</code></td>
</tr>
<tr>
<td></td>
<td>(EAGLE) <code>(interface slot/port)#</code></td>
<td>(EAGLE) <code>#</code></td>
</tr>
</tbody>
</table>

When you enter a question mark (?) after the prompt, the Command Line Interface displays a list of the available commands and a short description of the commands.

```plaintext
{EAGLE}> 
cli              Set the CLI preferences.
enable           Turn on privileged commands.
help             Display help for various special keys.
history          Show a list of previously run commands.
logout           Exit this session.
ping             Send ICMP echo packets to a specified IP address.
show             Display device options and settings.
{EAGLE}> 
```

**Figure 7: Commands in the User Exec mode**
1.2.5 Executing the commands

Syntax analysis

When you log in with the Command Line Interface, you enter the User Exec mode. The Command Line Interface displays the prompt `(EAGLE)>` on the screen.

When you enter a command and press the <Enter> key, the Command Line Interface starts the syntax analysis. The Command Line Interface searches the command tree for the desired command.

When the command is outside the Command Line Interface command range, a message informs you of the detected error.

Example:

You want to execute the `show system info` command, but enter `info` without `f` and press the <Enter> key.

The Command Line Interface then displays a message:

```
(EAGLE)>show system info
Error: Invalid command 'info'
```

Command tree

The commands in the Command Line Interface are organized in a tree structure. The commands, and where applicable the related parameters, branch down until the command is completely defined and therefore executable. The Command Line Interface checks the input. When you entered the command and the parameters correctly and completely, you execute the command with the <Enter> key.

After you entered the command and the required parameters, the other parameters entered are treated as optional parameters. When one of the parameters is unknown, the Command Line Interface displays a syntax message.

The command tree branches for the required parameters until the required parameters have reached the last branch in the structure.

With optional parameters, the command tree branches until the required parameters and the optional parameters have reached the last branch in the structure.

1.2.6 Structure of a command

This section describes the syntax, conventions and terminology, and uses examples to represent them.
Format of commands

Most of the commands include parameters.

When the command parameter is missing, the Command Line Interface informs you about the detection of an incorrect command syntax.

This manual displays the commands and parameters in the Courier font.

Parameters

The sequence of the parameters is relevant for the correct syntax of a command.

Parameters are required values, optional values, selections, or a combination of these things. The representation indicates the type of the parameter.

Table 3: Parameter and command syntax

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;command&gt;</code></td>
<td>Commands in pointed brackets (&lt;&gt; ) are obligatory.</td>
</tr>
<tr>
<td><code>[command]</code></td>
<td>Commands in square brackets ([ ]) are optional.</td>
</tr>
<tr>
<td><code>&lt;parameter&gt;</code></td>
<td>Parameters in pointed brackets (&lt;&gt; ) are obligatory.</td>
</tr>
<tr>
<td><code>[parameter]</code></td>
<td>Parameters in square brackets ([ ]) are optional.</td>
</tr>
<tr>
<td>...</td>
<td>An ellipsis (3 points in sequence without spaces) after an element indicates that you can repeat the element.</td>
</tr>
<tr>
<td>`[Choice1</td>
<td>Choice2]`</td>
</tr>
<tr>
<td><code>{list}</code></td>
<td>Curved brackets ({ }) indicate that a parameter is to be selected from a list of options.</td>
</tr>
<tr>
<td>`[Choice1</td>
<td>Choice2]`</td>
</tr>
<tr>
<td>`[param1 {Choice1</td>
<td>Choice2}]`</td>
</tr>
<tr>
<td><code>&lt;a.b.c.d&gt;</code></td>
<td>Small letters are wild cards. You enter parameters with the notation a.b.c.d with decimal points (for example IP addresses)</td>
</tr>
<tr>
<td><code>&lt;cr&gt;</code></td>
<td>You press the &lt;Enter&gt; key to create a line break (carriage return).</td>
</tr>
</tbody>
</table>
Network addresses

Network addresses are a requirement for establishing a data connection to a remote workstation, a server, or another network. You distinguish between IP addresses and MAC addresses.

The IP address is an address allocated by the network administrator. The IP address is unique in one network area.

The MAC addresses are assigned by the hardware manufacturer. MAC addresses are unique worldwide.

The following table displays the representation and the range of the address types:

### Table 5: Format and range of network addresses

<table>
<thead>
<tr>
<th>Address Type</th>
<th>Format</th>
<th>Range</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>nnn.nnn.nnn.nnn</td>
<td>nnn: 0 to 255 (decimal)</td>
<td>192.168.11.10</td>
</tr>
<tr>
<td>MAC Address</td>
<td>mm:mm:mm:mm:mm:mm</td>
<td>mm: 00 to ff (hexadecimal number pairs)</td>
<td>A7:C9:89:DD:A9:B3</td>
</tr>
</tbody>
</table>

Strings

A string is indicated by quotation marks. For example, "System name with space character". Space characters are not valid user-defined strings. You enter a space character in a parameter between quotation marks.

Example:

```
*(EAGLE)#cli prompt Device name
Error: Invalid command 'name'
```
1.2.7 Examples of commands

**Example 1: clear arp-table-switch**

Command for clearing the ARP table of the management agent (cache).

`clear arp-table-switch` is the command name. The command is executable without any other parameters by pressing the <Enter> key.

**Example 2: radius server timeout**

Command to configure the RADIUS server timeout value.

```
(radius) (config)#radius server timeout
<1..30>       Timeout in seconds (default: 5).
```

`radius server timeout` is the command name.

The parameter is required. The value range is `1..30`.

**Example 3: radius server auth modify <1..8>**

Command to set the parameters for RADIUS authentication server 1.

```
(radius) (config)#radius server auth modify 1
[name]                RADIUS authentication server name.
[port]                RADIUS authentication server port.
                     (default: 1812).
[msgauth]             Enable or disable the message authenticator attribute for this server.
[primary]             Configure the primary RADIUS server.
[status]              Enable or disable a RADIUS authentication server entry.
[secret]              Configure the shared secret for the RADIUS authentication server.
[encrypted]           Configure the encrypted shared secret.
<cr>                 Press Enter to execute the command.
```

`radius server auth modify` is the command name.

The parameter `<1..8>` (RADIUS server index) is required. The value range is `1..8` (integer).

The parameters `[name],[port],[msgauth],[primary],[status],[secret]` and `[encrypted]` are optional.
1.2.8 Input prompt

Command mode

With the input prompt, the Command Line Interface displays which of the three modes you are in:

- **User Exec mode**
  - `(EAGLE) >`
- **Privileged Exec mode**
  - `(EAGLE) #`
- **Global Config mode**
  - `(EAGLE) (config)#`
- **VLAN Database mode**
  - `(EAGLE) (Vlan)#`
- **Interface Range mode**
  - `(EAGLE) ((Interface)all)#`
  - `(EAGLE) ((Interface)2/1)#`
  - `(EAGLE) ((Interface)1/2-1/4)#`
  - `(EAGLE) ((Interface)2/1-1/2,1/4-1/6)#`

Asterisk, pound sign and exclamation point

- **Asterisk** *
  - An asterisk * in the first or second position of the input prompt displays you that the settings in the volatile memory and the settings in the non-volatile memory are different. In your configuration, the device has detected modifications which have not been saved.
    - `*(EAGLE)>`
- **Pound sign** #
  - A pound sign # at the beginning of the input prompt displays you that the boot parameters and the parameters during the boot phase are different.
    - `#(EAGLE)>`
- **Exclamation point** !
  - An exclamation point ! at the beginning of the input prompt displays: the password for the user or admin user account corresponds with the default setting.
    - `!(EAGLE)>`

Wildcards

The device lets you change the command line prompt.

The Command Line Interface supports the following wildcards:

<table>
<thead>
<tr>
<th>Wildcard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%d</td>
<td>System date</td>
</tr>
<tr>
<td>%t</td>
<td>System time</td>
</tr>
</tbody>
</table>
1.2 Command Line Interface

% (EAGLE) > enable

% (EAGLE) # cli prompt %i

% (EAGLE) # cli prompt (EAGLE) %d

% (EAGLE) # cli prompt (EAGLE) %d %t

% (EAGLE) # cli prompt %m

% (EAGLE) # cli prompt %m

1.2.9 Key combinations

The following key combinations make it easier for you to work with the Command Line Interface:

<table>
<thead>
<tr>
<th>Key combination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;CTRL&gt; + &lt;H&gt;, &lt;Backspace&gt;</td>
<td>Delete previous character</td>
</tr>
<tr>
<td>&lt;CTRL&gt; + &lt;A&gt;</td>
<td>Go to beginning of line</td>
</tr>
<tr>
<td>&lt;CTRL&gt; + &lt;E&gt;</td>
<td>Go to end of line</td>
</tr>
<tr>
<td>&lt;CTRL&gt; + &lt;F&gt;</td>
<td>Go forward one character</td>
</tr>
<tr>
<td>&lt;CTRL&gt; + &lt;B&gt;</td>
<td>Go backward one character</td>
</tr>
<tr>
<td>&lt;CTRL&gt; + &lt;D&gt;</td>
<td>Delete current character</td>
</tr>
<tr>
<td>&lt;CTRL&gt; + &lt;U&gt;, &lt;X&gt;</td>
<td>Delete to beginning of line</td>
</tr>
<tr>
<td>&lt;CTRL&gt; + &lt;K&gt;</td>
<td>Delete to end of line</td>
</tr>
<tr>
<td>&lt;CTRL&gt; + &lt;W&gt;</td>
<td>Delete previous word</td>
</tr>
<tr>
<td>&lt;CTRL&gt; + &lt;P&gt;</td>
<td>Go to previous line in history buffer</td>
</tr>
<tr>
<td>&lt;CTRL&gt; + &lt;R&gt;</td>
<td>Rewrite or paste the line</td>
</tr>
<tr>
<td>&lt;CTRL&gt; + &lt;N&gt;</td>
<td>Go to next line in history buffer</td>
</tr>
<tr>
<td>&lt;CTRL&gt; + &lt;Z&gt;</td>
<td>Return to root command prompt</td>
</tr>
<tr>
<td>&lt;CTRL&gt; + &lt;G&gt;</td>
<td>Aborts running tcpdump session</td>
</tr>
<tr>
<td>&lt;Tab&gt;, &lt;SPACE&gt;</td>
<td>Command line completion</td>
</tr>
<tr>
<td>Exit</td>
<td>Go to next lower command prompt</td>
</tr>
<tr>
<td>&lt;?&gt;</td>
<td>List choices</td>
</tr>
</tbody>
</table>
The Help command displays the possible key combinations in Command Line Interface on the screen:

```
(EAGLE) #help

HELP:
Special keys:

Ctrl-H, BkSp delete previous character
Ctrl-A .... go to beginning of line
Ctrl-E .... go to end of line
Ctrl-F .... go forward one character
Ctrl-B .... go backward one character
Ctrl-D .... delete current character
Ctrl-U, X .. delete to beginning of line
Ctrl-K .... delete to end of line
Ctrl-W .... delete previous word
Ctrl-P .... go to previous line in history buffer
Ctrl-R .... rewrites or pastes the line
Ctrl-N .... go to next line in history buffer
Ctrl-Z .... return to root command prompt
Ctrl-G .... aborts running tcpdump session
Tab, <SPACE> command-line completion
Exit .... go to next lower command prompt
? .... list choices
```

Figure 8: Listing the key combinations with the Help command
User interfaces
1.2 Command Line Interface

1.2.10 Data entry elements

Command completion

To simplify typing commands, the Command Line Interface lets you use command completion (Tab Completion). Thus you are able to abbreviate key words.

- Type in the beginning of a keyword. When the characters entered identify a keyword, the Command Line Interface completes the keyword after you press the tab key or the space key. When there is more than one option for completion, enter the letter or the letters necessary for uniquely identifying the keyword. Press the tab key or the space key again. After that, the system completes the command or parameter.
- When you make a non-unique entry and press <Tab> or <Space> twice, the Command Line Interface provides you with a list of options.
- On a non-unique entry and pressing <Tab> or <Space>, the Command Line Interface completes the command up to the end of the uniqueness. When several commands exist and you press <Tab> or <Space> again, the Command Line Interface provides you with a list of options.

Example:

(EAGLE) (Config)#lo
(EAGLE) (Config)#log
logging logout

When you enter lo and <Tab> or <Space>, the Command Line Interface completes the command up to the end of the uniqueness to log.
When you press <Tab> or <Space> again, the Command Line Interface provides you with a list of options (logging logout).

Possible commands/parameters

You can obtain a list of the commands or the possible parameters by entering help or ?, for example by entering (EAGLE) >show ?

When you enter the command displayed, you get a list of the parameters available for the command show.

When you enter the command without space character in front of the question mark, the device displays the help text for the command itself:

!*#(EAGLE) (Config)#show?

    show             Display device options and settings.
1.2.11 Use cases

Saving the Configuration

To help ensure that your password settings and your other configuration changes are kept after the device is reset or after an interruption of the voltage supply, you save the configuration. To do this, perform the following steps:
- Enter `enable` to switch to the Privileged Exec mode.
- Enter the following command:
  ```
  save [profile]
  ```
- Execute the command by pressing the <Enter> key.

Syntax of the “radius server auth add” command

Use this command to add a RADIUS authentication server.

- Mode: Global Config mode
- Privilege Level: Administrator
- Format: `radius server auth add <1..8> ip <a.b.c.d> [name <string>] [port <1..65535>]`
  - `[name]`: RADIUS authentication server name.
  - `[port]`: RADIUS authentication server port (default value: 1813).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
<th>Possible values</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1..8&gt;</code></td>
<td>RADIUS server index.</td>
<td>1..8</td>
</tr>
<tr>
<td><code>&lt;a.b.c.d&gt;</code></td>
<td>RADIUS accounting server IP address.</td>
<td>IP address</td>
</tr>
<tr>
<td><code>&lt;string&gt;</code></td>
<td>Enter a user-defined text, max. 32 characters.</td>
<td></td>
</tr>
<tr>
<td><code>&lt;1..65535&gt;</code></td>
<td>Enter port number between 1 and 65535.</td>
<td>1..65535</td>
</tr>
</tbody>
</table>

Mode and Privilege Level:
- The prerequisite for executing the command: You are in the Global Config mode. See “Mode-based command hierarchy” on page 21.
- The prerequisite for executing the command: You have the Administrator access role.

Syntax of commands and parameters: See “Structure of a command” on page 25.

Examples for executable commands:
- `radius server auth add 1 ip 192.168.30.40`
- `radius server auth add 2 ip 192.168.40.50 name radiusserver2`
- `radius server auth add 3 ip 192.168.50.60 port 1813`
- `radius server auth add 4 ip 192.168.60.70 name radiusserver4 port 1814`
**Service Shell**

The Service Shell is for service purposes only.

The Service Shell lets users have access to internal functions of the device. When you need assistance with your device, the service personnel use the Service Shell to monitor internal conditions for example, the switch or CPU registers.

Do not execute internal functions without service technician instructions. Executing internal functions such as deleting the content of the non-volatile memory (NVM) possibly leads to inoperability of your device.

**Start the Service Shell**

The prerequisite is that you are in User Exec mode: (EAGLE) >

Perform the following steps:

- Enter `enable` and press the <Enter> key.
  - To reduce the effort when typing:
    - Enter `e` and press the <Tab> key.

- Enter `serviceshell start` and press the <Enter> key.
  - To reduce the effort when typing:
    - Enter `ser` and press the <Tab> key.
    - Enter `s` and press the <Tab> key.

```
!EAGLE >enable
!*EAGLE #serviceshell start
WARNING! The service shell offers advanced diagnostics and functions.
Proceed only when instructed by a service technician.

You can return to the previous mode using the 'exit' command.

BusyBox v1.31.0 (2019-09-05 12:17:22 UTC) built-in shell (ash)
Enter 'help' for a list of built-in commands.

!/mnt/fastpath #
```

**Working with the Service Shell**

When the Service Shell is active, the timeout of the Command Line Interface is inactive. To help prevent configuration inconsistencies, end the Service Shell before any other user starts transferring a new configuration to the device.
Display the Service Shell commands

The prerequisite is that you already started the Service Shell.

Perform the following steps:
- Enter `help` and press the <Enter> key.

```
/mnt/fastpath # help
Built-in commands:
------------------
  . : [ ]( alias bg break cd chdir command continue echo eval exec
  exit export false fg getopts hash help history jobs kill let
  local pwd read readonly return set shift source test times trap
  true type ulimit umask unalias unset wait
/mnt/fastpath #
```

End the Service Shell

Perform the following steps:
- Enter `exit` and press the <Enter> key.

Deactivate the Service Shell permanently in the device

When you deactivate the Service Shell, you are still able to configure the device. However, you limit the service personnel's possibilities to perform system diagnostics. The service technician will no longer be able to access internal functions of your device.

The deactivation is irreversible. The Service Shell remains permanently deactivated. In order to reactivate the Service Shell, the device requires disassembly by the manufacturer.

The prerequisites are:
- The Service Shell is not started.
- You are in User Exec mode: (EAGLE) >

Perform the following steps:
- Enter `enable` and press the <Enter> key.
  To reduce the effort when typing:
  - Enter `e` and press the <Tab> key.
- Enter `servicesshell deactivate` and press the <Enter> key.
  To reduce the effort when typing:
1.2 Command Line Interface

- Enter `ser` and press the <Tab> key.
- Enter `dea` and press the <Tab> key.

☐ **This step is irreversible!**

Press the <Y> key.

---

`!EAGLE >enable`

`!*EAGLE #serviceshell deactivate`

Notice: If you continue, then the Service Shell is permanently deactivated.

This step is irreversible!

For details, refer to the Configuration Manual.

Are you sure (Y/N) ?
1.3 System monitor

The System Monitor lets you set basic operating parameters before starting the operating system.

1.3.1 Functional scope

In the System Monitor, you carry out the following tasks, for example:
- Managing the operating system and verifying the software image
- Updating the operating system
- Starting the operating system
- Deleting configuration profiles, resetting the device to the factory defaults
- Checking boot code information

1.3.2 Starting the System Monitor

Prerequisite:
- Terminal cable for connecting the device to your PC (available as an optional accessory).
- PC with VT100 terminal emulation (such as the PuTTY program) or serial terminal
Perform the following steps:

- Use the terminal cable to connect the serial interface of the device with the COM port of the PC.
- Start the VT100 terminal emulation on the PC.
- Specify the following transmission parameters:

<table>
<thead>
<tr>
<th>VT 100 terminal settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>115200 bit/s</td>
</tr>
<tr>
<td>Data</td>
<td>8 bit</td>
</tr>
<tr>
<td>Stopbit</td>
<td>1 bit</td>
</tr>
<tr>
<td>Handshake</td>
<td>off</td>
</tr>
<tr>
<td>Parity</td>
<td>none</td>
</tr>
</tbody>
</table>

- Set up a connection to the device.
- Turn on the device. When the device is already on, reboot it.
  - The screen displays the following message after rebooting:
    - Press <1> to enter System Monitor 1.
    - Press the <1> key within 3 seconds.
  - The device starts the System Monitor. The screen displays the following view:

```
System Monitor 1
(Selected OS: ...,v-4.0 (2019-02-05 19:17))

1  Manage operating system
2  Update operating system
3  Start selected operating system
4  Manage configurations
5  Show boot code information
q  End (reset and reboot)
```

```
sysMon1>
```

*Figure 9: System Monitor 1 screen display*

- Select a menu item by entering the number.
- To leave a submenu and return to the main menu of System Monitor 1, press the <ESC> key.
2 Specifying the IP parameters

When you install the device for the first time, enter the IP parameters.

The device provides the following options for entering the IP parameters during the first installation:

- **Entry using the Command Line Interface.**
  When you preconfigure your device outside its operating environment, or restore the network access (“In-Band”) to the device, choose this “Out-of-Band” method.

- **Entry using the HiDiscovery protocol.**
  When you have a previously installed network device or you have another Ethernet connection between your PC and the device, you choose this “In-Band” method.

- **Configuration using the external memory.**
  When you are replacing a device with a device of the same type and have already saved the configuration in the external memory, you choose this method.

- **Configuration using the Graphical User Interface.**
  When the device already has an IP address and is reachable using the network, the Graphical User Interface provides you with another option for configuring the IP parameters.

2.1 IP parameter basics

2.1.1 IPv4

**IP address**

The IP addresses consist of 4 bytes. Write these 4 bytes in decimal notation, separated by a decimal point.

RFC 1340 written in 1992, defines 5 IP Address classes.

<table>
<thead>
<tr>
<th>Class</th>
<th>Network address</th>
<th>Host address</th>
<th>Address range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1 Byte</td>
<td>3 Bytes</td>
<td>0.0.0.0 to 127.255.255.255</td>
</tr>
<tr>
<td>B</td>
<td>2 Bytes</td>
<td>2 Bytes</td>
<td>128.0.0.0 to 191.255.255.255</td>
</tr>
<tr>
<td>C</td>
<td>3 Bytes</td>
<td>1 Byte</td>
<td>192.0.0.0 to 223.255.255.255</td>
</tr>
<tr>
<td>D</td>
<td></td>
<td></td>
<td>224.0.0.0 to 239.255.255.255</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td></td>
<td>240.0.0.0 to 255.255.255.255</td>
</tr>
</tbody>
</table>

The first byte of an IP address is the network address. The worldwide leading regulatory board for assigning network addresses is the IANA (“Internet Assigned Numbers Authority”). When you require an IP address block, contact your Internet Service Provider (ISP). Your ISP contacts their local higher-level organization to reserve an IP address block:

- APNIC (Asia Pacific Network Information Center)
  Asia/Pacific Region
- ARIN (American Registry for Internet Numbers)
  Americas and Sub-Sahara Africa
LACNIC (Regional Latin-American and Caribbean IP Address Registry)
Latin America and some Caribbean Islands
RIPE NCC (Réseaux IP Européens)
Europe and Surrounding Regions

When the first bit of an IP address is a zero, it belong to class A for example, the first octet is less than 128.

When the first bit of an IP address is a one and the second bit is a zero, it belongs to class B for example, the first octet is between 128 and 191.

When the first 2 bits of an IP address are a one, it belongs to class C for example, the first octet is higher than 191.

Assigning the host address (host ID) is the responsibility of the network operator. The network operator alone is responsible for the uniqueness of the assigned IP addresses.

**Netmask**

Routers and Gateways subdivide large networks into subnetworks. The netmask assigns the IP addresses of the individual devices to a particular subnetwork.

You perform subnetwork division using the netmask in much the same way as the division of the network addresses (net id) into classes A to C.

Set the bits of the host address (host id) that represent the mask to one. Set the remaining host address bits to zero (see the following examples).

Example of a subnet mask:

Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000

Subnetwork mask bits Class B
Example of applying the subnet mask to IP addresses for subnetwork assignment:

Decimal notation
129.218.65.17

Binary notation
10000001.11011010.01000001.00010001

Example of how the netmask is used

In a large network it is possible that Gateways and routers separate the management agent from its network management station. How does addressing work in such a case?

The network management station “Romeo” wants to send data to the management agent “Juliet”. Romeo knows Juliet's IP address and also knows that the router “Lorenzo” knows the way to Juliet.

Romeo therefore puts his message in an envelope and writes Juliet's IP address as the destination address; for the source address he writes his own IP address on the envelope.

Romeo then places this envelope in a second one with Lorenzo's MAC address as the destination and his own MAC address as the source. This process is comparable to going from Layer 3 to Layer 2 of the ISO/OSI base reference model.

Finally, Romeo puts the entire data packet into the mailbox which is comparable to going from Layer 2 to Layer 1, that means to sending the data packet over the Ethernet.
Lorenzo receives the letter, removes the outer envelope and recognizes from the inner envelope that the letter is meant for Juliet. He places the inner envelope in a new outer envelope and searches his address list (the ARP table) for Juliet’s MAC address; he writes her MAC address on the outer envelope as the destination address and his own MAC address as the source address. He then places the entire data packet in the mail box.

Juliet receives the letter and removes the outer envelope. She finds the inner envelope with Romeo’s IP address. Opening the inner envelope and reading its contents corresponds to transferring the message to the higher protocol layers of the ISO/OSI layer model.

Juliet would now like to send a reply to Romeo. She places her reply in an envelope with Romeo’s IP address as destination and her own IP address as source. But where is she to send the answer? For she did not receive Romeo’s MAC address. It was lost, because Lorenzo replaced the outer envelope.

In the MIB, Juliet finds Lorenzo listed under the variable hmNetGatewayIPAddr as a means of communicating with Romeo. She therefore puts the envelope with the IP addresses in a further envelope with Lorenzo’s MAC destination address.

The letter now travels back to Romeo via Lorenzo, the same way the first letter traveled from Romeo to Juliet.

**Classless Inter-Domain Routing**

Class C with a maximum of 254 addresses was too small, and class B with a maximum of 65534 addresses was too large for most users. Resulting in an ineffective usage of the available class B addresses.

Class D contains reserved Multicast addresses. Class E is for experimental purposes. A non-participating Gateway ignores experimental datagrams with these destination addresses.

Since 1993, RFC 1519 has been using Classless Inter-Domain Routing (CIDR) to provide a solution. CIDR overcomes these class boundaries and supports classless address ranges.

With CIDR, you enter the number of bits that designate the IP address range. You represent the IP address range in binary form and count the mask bits that designate the netmask. The mask bits equal the number of bits used for the subnet in a given IP address range.

Example:

<table>
<thead>
<tr>
<th>IP address, decimal</th>
<th>Network mask, decimal</th>
<th>IP address, binary</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.112.1</td>
<td>255.255.255.128</td>
<td>\textcolor{red}{11000000<del>10101000</del>01110000~00000001}</td>
</tr>
<tr>
<td>192.168.112.127</td>
<td></td>
<td>\textcolor{red}{11000000<del>10101000</del>01110000~01111111}</td>
</tr>
</tbody>
</table>

CIDR notation: 192.168.112.0/25

The term “supernetting” refers to combing a number of class C address ranges. Supernetting enables you to subdivide class B address ranges to a fine degree.
2.2 Specifying the IP parameters using the Command Line Interface

2.2.1 IPv4

There are the following methods you enter the IP parameters:
- HiDiscovery protocol
- External memory
- Command Line Interface using the serial connection

The device lets you specify the IP parameters using the HiDiscovery protocol or using the Command Line Interface over the serial interface.

Perform the following steps:

1. Set up a connection to the device.
2. The start screen appears.

Note: If a terminal or PC with terminal emulation is unavailable in the vicinity of the installation location, you can configure the device at your own workstation, then take it to its final installation location.
Specifying the IP parameters
2.2 Specifying the IP parameters using the Command Line Interface

- Enter the IP parameters.
  - Local IP address
    - In the default setting, the local IP address is 0.0.0.0.
  - Netmask
    - When you divided your network into subnetworks, and these are identified with a netmask, enter the netmask here. In the default setting, the local netmask is 0.0.0.0.
  - IP address of the Gateway.
    - This entry is only required, in cases where the device and the network management station are located in different subnetworks (see on page 41 “Example of how the netmask is used”). Specify the IP address of the Gateway between the subnetwork with the device and the path to the network management station. In the default setting, the IP address is 0.0.0.0.

- Save the configuration specified using `copy config running-config nvm`.

```plaintext
enable
network parms 10.0.1.23 255.255.255.0

copy config running-config nvm
```

Change to the Privileged EXEC mode.
Assign the device the IP address 10.0.1.23 and the netmask 255.255.255.0. You have the option of also assigning a Gateway address.
Save the current settings in the non-volatile memory (nvm) in the “selected” configuration profile.

After entering the IP parameters, you easily configure the device using the Graphical User Interface.
2.3 Specifying the IP parameters using HiDiscovery

The HiDiscovery protocol enables you to assign IP parameters to the device using the Ethernet.

You easily configure other parameters using the Graphical User Interface.

Install the HiDiscovery software on your PC. The software is on the product DVD supplied with the device.

Perform the following steps:
- To install it, you start the installation program on the DVD.
- Start the HiDiscovery program.

When HiDiscovery is started, HiDiscovery automatically searches the network for those devices which support the HiDiscovery protocol.

HiDiscovery uses the first network interface found for the PC. When your computer has several network cards, you can select the one you desire in the HiDiscovery toolbar.

HiDiscovery displays a line for every device that responds to a HiDiscovery protocol inquiry.

HiDiscovery enables you to identify the devices displayed.
- Select a device line.
- To set the LEDs to flashing for the selected device, click the Signal button on the tool bar. To stop the flashing, click the Signal button again.
- By double-clicking a line, you open a window in which you specify the device name and the IP parameter.
**Note:** Disable the HiDiscovery function in the device, after you have assigned the IP parameters to the device.

**Note:** Save the settings so that you will still have the entries after a restart.
2.4 Specifying the IP parameters using the Graphical User Interface

2.4.1 IPv4

Perform the following steps:

- Open the **Basic Settings > Network > Global** dialog.
  
  In this dialog you specify the VLAN in which the device management can be accessed and configure the HiDiscovery access.

- In the **VLAN ID** column you specify the VLAN in which the device management can be accessed over the network.
  
  Note here that you can only access the device management using ports that are members of the relevant VLAN.
  
  The **MAC address** field displays the MAC address of the device with which you access the device over the network.

- In the **HiDiscovery protocol v1/v2** frame you specify the settings for accessing the device using the HiDiscovery software.
  
  The HiDiscovery protocol lets you 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 HiDiscovery software.

- Open the **Basic Settings > Network > IPv4** dialog.
  
  In this dialog you specify the source from which the device gets its IP parameters after starting.

- In the **Management interface** frame you first specify where the device gets its IP parameters from:
  
    - In the **Local** mode, the device uses the network parameters from the internal device memory.

  **Note:** When you change the allocation mode of the IP address, the device activates the new mode immediately after you click the ✔️ button.

- If required, you enter the IP address, the netmask and the Gateway in the **IP parameter** frame.

- Save the changes temporarily. To do this, click the ✔️ button.
Specifying the IP parameters

2.4 Specifying the IP parameters using the Graphical User Interface
3 Access to the device

3.1 Access roles

The device functions available to you as a user depend on your access role. When you are logged in with a specific access role, the functions of the access role are available to you.

The commands available to you as a user, also depend on the Command Line Interface mode in which you are currently working. See “Mode-based command hierarchy” on page 21.

The device offers the following access roles:

![Diagram of access roles]

Table 9: Access roles and scope of user authorizations

<table>
<thead>
<tr>
<th>Access role</th>
<th>User authorizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Users logged in with the access role User are authorized to monitor the device.</td>
</tr>
<tr>
<td>Auditor</td>
<td>Users logged in with the access role Auditor are authorized to monitor the device and to save the log file in the Diagnostics &gt; Report &gt; Audit Trail dialog.</td>
</tr>
<tr>
<td>Operator</td>
<td>Users logged in with the access role Operator are authorized to monitor the device and to change the settings – with the exception of security settings for device access.</td>
</tr>
<tr>
<td>Administrator</td>
<td>Users logged in with the access role Administrator are authorized to monitor the device and to change the settings.</td>
</tr>
<tr>
<td>Unauthorized</td>
<td>Unauthorized users are blocked, and the device rejects the user login. Assign this value to temporarily lock the user account. If a detected error occurs during an access role change, then the device assigns this access role to the user account.</td>
</tr>
</tbody>
</table>
3.2 First login (Password change)

To help prevent undesired access to the device, it is imperative that you change the default password during initial setup.

Perform the following steps:
- Open the Graphical User Interface, the HiView application, or the Command Line Interface the first time you log in.
- Log in with the default password.
- Type in your new password.
  - To help increase security, choose a password that contains at least 8 characters which includes upper-case characters, lower-case characters, numerical digits, and special characters.
- When you log in with the Command Line Interface, the device prompts you to confirm your new password.
- Log in again with your new password.

Note: If you lost your password, then use the System Monitor to reset the password.

For further information see hirschmann-support.belden.com.
3.3 Authentication lists

When a user accesses the device using a specific connection, the device verifies the login credentials of the user in an authentication list which contains the policies that the device applies for authentication.

The prerequisite for a user's access to the device management is that at least one policy is assigned to the authentication list of the application through which access is performed.

3.3.1 Applications

The device provides an application for each type of connection through which someone accesses the device:

- Access to the Command Line Interface using a serial connection: Console(V.24)
- Access to the Command Line Interface using SSH: SSH
- Access to the Graphical User Interface: WebInterface

3.3.2 Policies

When a user logs in with valid login data, the device lets the user have access to its device management. The device authenticates the users using the following policies:

- User management of the device
- LDAP
- RADIUS

The device gives you the option of a fall-back solution. For this, you specify more than one policy in the authentication list. When authentication is unsuccessful using the current policy, the device applies the next specified policy.

3.3.3 Managing authentication lists

You manage the authentication lists in the Graphical User Interface or in the Command Line Interface. To do this, perform the following steps:

1. Open the Device Security > Authentication List dialog.
   The dialog displays the authentication lists that are set up.
2. Deactivate the authentication list for those applications by means of which no access to the device is performed.
3. In the Active column of the desired authentication list, unmark the checkbox.
4. Save the changes temporarily. To do this, click the button.
Access to the device
3.3 Authentication lists

3.3.4 Adjust the settings

Example: Set up a separate authentication list for the application WebInterface which is by default included in the authentication list defaultLoginAuthList.

The device forwards authentication requests to a RADIUS server in the network. As a fall-back solution, the device authenticates users using the local user management. To do this, perform the following steps:

- Create an authentication list loginGUI.
  - Open the Device Security > Authentication List dialog.
  - Click the button.
  - The dialog displays the Create window.
  - Enter a meaningful name in the Name field. In this example, enter the name loginGUI.
  - Click the Ok button.
  - The device adds a new table entry.

- Change to the Privileged EXEC mode.
  - Change to the Configuration mode.
  - Creates the authentication list loginGUI.

- Select the policies for the authentication list loginGUI.
  - In the Policy 1 column, select the value radius.
  - In the Policy 2 column, select the value local.
  - In the Policy 3 to Policy 5 columns, select the value reject to help prevent further fall-back.
  - In the Active column, mark the checkbox.
  - Save the changes temporarily. To do this, click the button.

- Assign an application to the authentication list loginGUI.
  - In the Device Security > Authentication List dialog, highlight the authentication list loginGUI.
  - Click the button and then the Allocate applications item.
  - The dialog displays the Allocate applications window.
  - In the left column, highlight the application WebInterface.
☐ Click the button.
The right column now displays the application WebInterface.

☐ Click the Ok button.
The dialog displays the updated settings:
- The Dedicated applications column of authentication list loginGUI displays the application WebInterface.
- The Dedicated applications column of authentication list defaultLoginAuthList does not display the application WebInterface anymore.

☐ Save the changes temporarily. To do this, click the button.

```
show applists
applists set-authlist WebInterface loginGUI
```
3.4 User management

When a user logs in with valid login data, the device lets the user have access to its device management. The device authenticates the users either using the local user management or with a RADIUS server in the network. To get the device to use the user management, assign the local policy to an authentication list, see the Device Security > Authentication List dialog.

In the local user management, you manage the user accounts. One user account is usually allocated to each user.

3.4.1 Access roles

The device lets you use a role-based authorization model to specifically control the access to the device management. Users to whom a specific authorization profile is allocated are allowed to use commands and functions from the same authorization profile or a lower one.

The device uses the authorization profiles on every application with which the device management can be accessed.
Every user account is linked to an access role that regulates the access to the individual functions of the device. Depending on the planned activity for the respective user, you assign a pre-defined access role to the user. The device differentiates between the following access roles.

Table 10: Access roles for user accounts

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Authorized for the following activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>The user is authorized to monitor and administer the device.</td>
<td>All activities with read/write access, including the following activities reserved for an administrator:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Add, modify or delete user accounts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Activate, deactivate or unlock user accounts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Change every password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configure password management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set or change system time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Load files to the device, for example device configurations, certificates or software images</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reset settings and security-related settings to the state on delivery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configure RADIUS server and authentication lists</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Apply scripts using the Command Line Interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enable/disable CLI logging and SNMP logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>External memory activation and deactivation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System monitor activation and deactivation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enable/disable the services for the access to the device management (for example SNMP).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configure access restrictions to the Graphical User Interface or the Command Line Interface based on the IP addresses</td>
</tr>
<tr>
<td>Operator</td>
<td>The user is authorized to monitor and configure the device - with the exception of security-related settings.</td>
<td>All activities with read/write access, with the exception of the above-named activities, which are reserved for an administrator:</td>
</tr>
<tr>
<td>Auditor</td>
<td>The user is authorized to monitor the device and to save the log file in the Diagnostics &gt; Report &gt; Audit Trail dialog.</td>
<td>Monitoring activities with read access.</td>
</tr>
<tr>
<td>Guest</td>
<td>The user is authorized to monitor the device - with the exception of security-related settings.</td>
<td>Monitoring activities with read access.</td>
</tr>
<tr>
<td>Unauthorized</td>
<td>No access to the device possible.</td>
<td>No activities allowed.</td>
</tr>
<tr>
<td></td>
<td>As an administrator you assign this access role to temporarily lock a user account.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If an administrator assigns a different access role to the user account and an error occurs, then the device assigns this access role to the user account.</td>
<td></td>
</tr>
</tbody>
</table>
### 3.4.2 Managing user accounts

You manage the user accounts in the Graphical User Interface or in the Command Line Interface. To do this, perform the following steps:

- Open the *Device Security > User Management* dialog. The dialog displays the user accounts that are set up.
- `show users` Displays the user accounts that are set up.

### 3.4.3 Default setting

In the state on delivery, the user accounts *admin* and *user* are set up in the device.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>User name</em></td>
<td>admin user</td>
</tr>
<tr>
<td><em>Password</em></td>
<td>private public</td>
</tr>
<tr>
<td><em>Role</em></td>
<td>administrator guest</td>
</tr>
<tr>
<td><em>User locked</em></td>
<td>unmarked unmarked</td>
</tr>
<tr>
<td><em>Policy check</em></td>
<td>unmarked unmarked</td>
</tr>
<tr>
<td><em>SNMP auth type</em></td>
<td>hmacmd5 hmacmd5</td>
</tr>
<tr>
<td><em>SNMP encryption type</em></td>
<td>des des</td>
</tr>
</tbody>
</table>

Change the password for the *admin* user account before making the device available in the network.

### 3.4.4 Changing default passwords

To help prevent undesired access, change the password of the default user accounts. To do this, perform the following steps:

- Change the passwords for the *admin* and *user* user accounts.

- Open the *Device Security > User Management* dialog. The dialog displays the user accounts that are set up.
- To obtain a higher level of complexity for the password, mark the checkbox in the *Policy check* column.
  Before saving it, the device checks the password according to the policy specified in the *Password policy* frame.
### 3.4.5 Setting up a new user account

Allocate a separate user account to each user that accesses the device management. In this way you can specifically control the authorizations for the access.

In the following example, we will set up the user account for a USER user with the role operator. Users with the operator role are authorized to monitor and configure the device - with the exception of security-related settings. To do this, perform the following steps:

- Open the Device Security > User Management dialog.
- Click the **Create** button. The dialog displays the **Create** window.
- Enter the name in the **User name** field. In this example, we give the user account the name **USER**.
- Click the **Ok** button.
- To obtain a higher level of complexity for the password, mark the checkbox in the **Policy check** column. Before saving it, the device checks the password according to the policy specified in the **Password policy** frame.

```
Note: The password check can lead to a message in the Security status frame in the Basic Settings > System dialog. You specify the settings that cause this message in the Basic Settings > System dialog.

- Click the row of the relevant user account in the Password field. Enter a password of at least 6 characters.
  - Up to 64 alphanumeric characters are allowed.
  - The device differentiates between upper and lower case.
  - The minimum length of the password is specified in the Configuration frame. The device constantly checks the minimum length of the password.

- Save the changes temporarily. To do this, click the **check** button.
```

```
**Note:** When you display the security status, the password check can lead to a message (show security-status all). You specify the settings that cause this message with the command security-status monitor pwd-policy-inactive. Users password-policy-check <user>

**Note:** When you display the security status, the password check can lead to a message (show security-status all). You specify the settings that cause this message with the command security-status monitor pwd-policy-inactive.

users password-policy-check <user>

enable

configure

users password-policy-check <user>

enable

- Change to the Privileged EXEC mode.
- Change to the Configuration mode.
- Activates the checking of the password for the <user> user account based on the specified policy.
  - In this way, you obtain a higher level of complexity for the password.

**Note:** When you display the security status, the password check can lead to a message (show security-status all). You specify the settings that cause this message with the command security-status monitor pwd-policy-inactive.

users password <user> SECRET

save

- Specifies the password SECRET for the <user> user account. Enter at least 6 characters.
- Save the settings in the non-volatile memory (nvram) in the “selected” configuration profile.
```
3.4 User management

3.4.6 Deactivating the user account

After a user account is deactivated, the device denies the related user access to the device management. In contrast to completely deleting it, deactivating a user account lets you keep the settings and reuse them in the future. To do this, perform the following steps:

- To keep the user account settings and reuse them in the future, you temporarily deactivate the user account.

- Open the Device Security > User Management dialog. The dialog displays the user accounts that are set up.
- In the row for the relevant user account, unmark the checkbox in the Active column.
- Save the changes temporarily. To do this, click the check button.

Note: When you are setting up a new user account in the Command Line Interface, remember to allocate the password.

enable
configure
users add USER
users password-policy-check USER
enable
users password USER SECRET
users access-role USER operator
users enable USER
show users
save

Change to the Privileged EXEC mode.

Change to the Configuration mode.

Creates the USER user account.

Activates the checking of the password for the USER user account based on the specified policy. In this way, you obtain a higher level of complexity for the password.

Specifies the password SECRET for the user account USER. Enter at least 6 characters.

Assign the user role operator to the user account USER.

Activates the user account USER.

Displays the user accounts that are set up.

Save the settings in the non-volatile memory (nvm) in the "selected" configuration profile.
To permanently deactivate the user account settings, you delete the user account.

To highlight the row for the relevant user account:

- Enter `users disable <user>` to disable the user account.
- Enter `show users` to display the user accounts that are set up.
- Enter `save` to save the settings in the non-volatile memory (nvm) in the “selected” configuration profile.

**3.4.7 Adjusting policies for passwords**

The device lets you check if the passwords for the user accounts adhere to the specified policy. When the passwords adhere to the policy, you obtain a higher level of complexity for the passwords.

The user management of the device lets you activate or deactivate the check separately in each user account. When you mark the checkbox and the new password fulfills the requirements of the policy, the device accepts the password change.
In the default settings, practical values for the policy are set up in the device. You have the option of adjusting the policy to meet your requirements. To do this, perform the following steps:

☐ Adjust the policy for passwords to meet your requirements.

☐ Open the **Device Security > User Management** dialog.

In the **Configuration** frame you specify the number user login attempts before the device locks out the user. You also specify the minimum number of characters that defines a password.

**Note:** The device lets only users with the **administrator** authorization remove the lock.

The number of login attempts as well as the possible lockout of the user apply only when accessing the device management through:

- the Graphical User Interface
- the SSH protocol

**Note:** When accessing the device management using the Command Line Interface through the serial connection, the number of login attempts is unlimited.

☐ Specify the values to meet your requirements.

  ▶ In the **Login attempts** field you specify the number of times that a user attempts to log in. The field lets you define this value in the range **0..5**. In the above example, the value 0 deactivates the function.

  ▶ The **Min. password length** field lets you enter values in the range **1..64**.

The dialog displays the policy set up in the **Password policy** frame.

☐ Adjust the values to meet your requirements.

  ▶ Values in the range **1** through **16** are allowed. The value 0 deactivates the relevant policy.

To apply the entries specified in the **Configuration** and **Password policy** frames, mark the checkbox in the **Policy check** column for a particular user.

☐ Save the changes temporarily. To do this, click the **✓** button.

```
enable
configure
passwords min-length 6
passwords min-lowercase-chars 1
passwords min-numeric-chars 1
passwords min-special-chars 1
passwords min-uppercase-chars 1
show passwords
save
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Specifies the policy for the minimum length of the password.
Specifies the policy for the minimum number of lower-case letters in the password.
Specifies the policy for the minimum number of digits in the password.
Specifies the policy for the minimum number of special characters in the password.
Specifies the policy for the minimum number of upper-case letters in the password.
Displays the policies that are set up.
Save the settings in the non-volatile memory (**nvm**) in the “selected” configuration profile.
3.5 LDAP

Server administrators manage Active Directories which contain user login credentials for applications used in the office environment. The Active Directory is hierarchical in nature, containing user names, passwords, and the authorized read/write permission levels for each user.

This device uses the Lightweight Directory Access Protocol (LDAP) to retrieve user login information and permission levels from a Active Directory. This provides a “single sign on” for network devices. Retrieving the login credentials from an Active Directory lets the user log in with the same login credentials used in the office environment.

An LDAP session starts with the device contacting the Directory System Agent (DSA) to search the Active Directory of an LDAP server. If the server finds multiple entries in the Active Directory for a user, then the server sends the higher permission level found. The DSA listens for information requests and sends responses on TCP port 389 for LDAP, or on TCP port 636 for LDAP over SSL (LDAPS). Clients and servers encode LDAPS requests and responses using the Basic Encoding Rules (BER). The device opens a new connection for every request and closes the connection after receiving a response from the server.

The device lets you upload a CA certificate to validate the server for Secure Socket Level (SSL) and Transport Layer Security (TLS) sessions. Whereby, the certificate is optional for TLS sessions.

The device is able to cache login credentials for up to 1024 users in memory. If the active directory servers are unreachable, then the users are still able to log in using their office login credentials.

3.5.1 Coordination with the server administrator

Configuring the LDAP function requires that the network administrator request the following information from the server administrator:
- The server name or IP address
- The location of the Active Directory on the server
- The type of connection used
- The TCP listening port
- When required, the location of the CA certificate
- The name of the attribute containing the user login name
- The names of the attribute containing the user permission levels

The server administrator can assign permission levels individually using an attribute such as description, or to a group using thememberOf attribute. In the Device Security > LDAP > Role Mapping dialog you specify which attributes receive the various permission levels.

You also have the option to retrieve the name of the attributes containing the user login name and permission levels using a LDAP browser such as JXplorer or Softerra.
### 3.5.2 **Example configuration**

The device is able to establish an encrypted link to a local server using only the server name or to a server on a different network using an IP address. The server administrator uses attributes to identify login credentials of a user and assign individual and group permission levels.

Using information received from the server administrator, specify which attributes in the Active Directory contain the user login credentials and permission level. The device then compares the user login credentials with the permission levels specified in the device and lets the user log in at the assigned permission level.

![Figure 15: LDAP Example Configuration](image)

For this example, the server administrator sent the following information:

<table>
<thead>
<tr>
<th>Information</th>
<th>Primary Server</th>
<th>Backup Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>The server name or IP address</td>
<td>local.server</td>
<td>10.16.1.2</td>
</tr>
<tr>
<td>The location of the Active Directory on the server</td>
<td>Country/City/User</td>
<td>Country/Company/User</td>
</tr>
<tr>
<td>The type of connection used</td>
<td>TLS (with certificate)</td>
<td>SSL</td>
</tr>
<tr>
<td>The server administrator sent the CA certificate in an email.</td>
<td>CA certificate for primary server saved locally</td>
<td>CA certificate for backup server saved locally</td>
</tr>
<tr>
<td>The TCP listening port</td>
<td>389 (tls)</td>
<td>636 (ssl)</td>
</tr>
<tr>
<td>Name of the attribute containing the user name</td>
<td>userPrincipalName</td>
<td>userPrincipalName</td>
</tr>
<tr>
<td>The names of the attribute containing the user permission levels</td>
<td>OPERATOR</td>
<td>OPERATOR</td>
</tr>
<tr>
<td></td>
<td>ADMINISTRATOR</td>
<td>ADMINISTRATOR</td>
</tr>
</tbody>
</table>

Perform the following steps:

- Open the **Device Security > Authentication List** dialog.
- To configure the device to retrieve the user login credentials, during login using the Graphical User Interface, from the Active Directory first, specify for the `defaultLoginAuthList` list the value `ldap` in the `Policy 1` column.
- Open the **Device Security > LDAP > Configuration** dialog.
- The device lets you specify the length of time that it saves the user login credentials in the cache. To cache user login credentials for a day, in the `Configuration` frame, `Client cache timeout [min]` field, enter the value `1440`.
- The `Bind user` entry is optional. When specified, users enter only their user name to log in. The service user can be anyone with login credentials listed in the Active Directory under the attribute specified in the `User name attribute` column. In the `Bind user` column, enter the user name and the domain.
The **Base DN** is a combination of the domain component (dc) and the organizational unit (ou). The **Base DN** lets the device locate a server in a domain (dc) and find the Active Directory (ou). Specify the location of the Active Directory. In the **Base DN** column, specify the value `ou=Users,ou=City,ou=Country,dc=server,dc=local`.

In the **User name attribute** column, enter the value `userPrincipalName` to specify the attribute under which the server administrator lists the users.

The device uses a CA certificate to verify the server.

- When the certificate is located on your PC or on a network drive, drag and drop the certificate in the **Certificate** area. Alternatively click in the area to select the certificate.
- To transfer the CA certificate onto the device, click the **Start** button.
- To add a table entry, click the **Add** button.
- To specify a description, enter the value **Primary AD Server** in the **Description** column.
- To specify the server name and domain of the primary server, in the **Address** column, enter the value `local.server`.
- The primary server uses the TCP port 389 for communication which is the **Destination TCP port** default value.
- The primary server uses TLS for encrypting communication and a CA certificate for server validation. In the **Connection security** column, specify the value `startTLS`.
- To activate the entry, mark the checkbox in the **Active** column.
- Using the information received from the server administrator for the Backup server, add, configure and activate another row.

Open the **Device Security > LDAP > Role Mapping** dialog.

- To add a table entry, click the **Add** button.

When a user logs in, with LDAP configured and enabled, the device searches the Active Directory for the login credentials of the user. If the device finds the user name and the password is correct, then the device searches for the value specified in the **Type** column. If the device finds the attribute and the text in the **Parameter** column matches the text in the Active Directory, then the device lets the user log in with the assigned permission level. When the value `attribute` is specified in the **Type** column, specify the value in the **Parameter** column in the following form: `attributeName=attributeValue`.

- In the **Role** column, enter the value **operator** to specify the user role.
- To activate the entry, mark the checkbox in the **Active** column.

Click the **Create** button.

The dialog displays the **Create** window.

Enter the values received from the server administrator for the **administrator** role.

To activate the entry, mark the checkbox in the **Active** column.

Open the **Device Security > LDAP > Configuration** dialog.

To enable the function, select the **On** radio button in the **Operation** frame.

The following table describes how to configure the **LDAP** function in the device using the Command Line Interface. The table displays the commands for **Index 1**. To configure **Index 2**, use the same commands and substitute the appropriate information.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Change to the Privileged EXEC mode.</td>
</tr>
<tr>
<td><code>configure</code></td>
<td>Change to the Configuration mode.</td>
</tr>
<tr>
<td><code>ldap cache-timeout 1440</code></td>
<td>Specify the device to flush the non-volatile memory after a day.</td>
</tr>
</tbody>
</table>
Access to the device
3.5 LDAP

```plaintext
ldap client server add 1 local.server port 389
ldap client server modify 1 security startTLS
ldap client server modify 1 description Primary_AD_Server
ldap basedn ou=Users,ou=City,ou=Country,dc=server, dc=local
ldap search-attr userPrincipalName

ldap bind-user user@company.com
ldap bind-passwd Ur-123456
ldap client server enable 1

ldap mapping add 1 access-role operator mapping-type attribute mapping-parameter OPERATOR
ldap mapping enable 1

ldap operation
```

Add a connection to the remote authentication client server with the host name `local.server` and the UDP port **389**.

Specify the type of security used for the connection.

Specify the configuration name of the entry.

Specify the Base Domain Name used to find the Active Directory on the server.

Specify the attribute to search for in the Active Directory which contains the login credential of the users.

Specify the name and domain of the service user.

Specify the password of the service user.

Enable the remote authentication client server connection.

Add a remote authentication role mapping entry for the **Operator** role. Map the **operator** role to the attribute containing the word **OPERATOR**.

Enable the remote authentication role mapping entry.

Enable the remote authentication function.
3.6 **SNMP access**

The SNMP protocol lets you work with a network management system to monitor the device over the network and change its settings.

### 3.6.1 SNMPv1/v2 access

Using SNMPv1 or SNMPv2 the network management system and the device communicate unencrypted. Every SNMP packet contains the community name in plain text and the IP address of the sender.

The community names **public** for read accesses and **private** for write accesses are preset in the device. If SNMPv1/v2 is enabled, then the device lets anyone who knows the community name have access to the device.

Make undesired access to the device more difficult. To do this, perform the following steps:

- Change the default community names in the device.
- Treat the community names with discretion. Anyone who knows the community name for write access, has the ability to change the settings of the device.
- Specify a different community name for read/write access than for read access.
- Use SNMPv1 or SNMPv2 only in environments protected from eavesdropping. The protocols do not use encryption.
- We recommend using SNMPv3 and disabling the access using SNMPv1 and SNMPv2 in the device.

### 3.6.2 SNMPv3 access

Using SNMPv3 the network management system and the device communicate encrypted. The network management system authenticates itself with the device using the login credentials of a user. The prerequisite for the SNMPv3 access is that in the network management system uses the same settings that are defined in the device.

The device lets you specify the **SNMP auth type** and **SNMP encryption type** parameters individually in each user account.

When you set up a new user account in the device, the parameters are preset so that the network management system Industrial HiVision reaches the device immediately.

The user accounts set up in the device use the same passwords in the Graphical User Interface, in the Command Line Interface, and for SNMPv3.

To adapt the SNMPv3 parameters of the user account settings to the settings in your network management system, perform the following steps:

- Open the *Device Security > User Management* dialog.

  The dialog displays the user accounts that are set up.
Access to the device
3.6 SNMP access

- Click the row of the relevant user account in the *SNMP auth type* field. Select the desired setting.
- Click the row of the relevant user account in the *SNMP encryption type* field. Select the desired setting.
- Save the changes temporarily. To do this, click the  button.

```bash
enable
configure
users snmpv3 authentication <user> md5 | sha1
users snmpv3 encryption <user> des | aescfb128 | none
show users
save
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Assigning the HMAC-MD5 or HMAC-SHA protocol for authentication requests to the user account `<user>`.
Assigns the DES or AES-128 algorithm to the user account `<user>`.
With this algorithm, the device encrypts authentication requests. The value `none` removes the encryption.
Display the user accounts that have been configured.
Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile.
4 VPN – Virtual Private Network

A virtual private network (VPN) refers to the part of a public network that someone uses for their private purposes.

The special feature of a VPN, as the name “private” suggests, is that the VPN tunnels the private data through a public network. Different measures help protect the data of the virtual private network from spying, data falsification and other attacks from external subscribers.

In the industrial environment, for example, a VPN serves to connect 2 plant sections with each other using the public Internet.

4.1 IPsec – Internet Protocol Security

IPsec is a protocol suite that authenticates and encrypts data packets sent over public networks.

Data transmission in a VPN involves:

- **Integrity protection**
  Integrity protection helps verify that the data transmitted is genuine, for example, that the data source is a trustworthy sender (is authentic) and that the recipient receives the data in its true form.

- **Encryption**
  Encryption helps protect the data prohibiting unauthorized persons from viewing the data. Encryption procedures code the data being transmitted using a code (key) that is only available to the authorized communication subscribers.

- **Traffic flow confidentiality**
  The traffic flow confidentiality helps protect the identification of the recipient and sender of the data packet from unauthorized person. IPsec performs this in the tunnel mode by encrypting the complete IP packet.

Figure 16: VPN for connecting 2 plant sections
The 2 endpoints negotiation which security parameters to use on the VPN connection. IPsec provides 2 modes for the negotiations

- **Transport mode**
  
  In the transport mode, the 2 endpoints authenticate themselves to each other, then they set up the parameters required for signatures and encryption. As the communication is taking place between the 2 specific endpoints, the recipient and sender addresses remain visible.

- **Tunnel mode**
  
  In the tunnel mode, the 2 Routers/Gateways authenticate themselves to each other, then they set up the parameters required for signatures and encryption. With the 2 Routers/Gateways specific, the VPN connection has 2 addressable endpoints. But the communication takes place between the subscribers of the network connected to the Routers/Gateways. This enables the transmission of encryption communication data, including the recipient and sender addresses. The endpoints of the VPN connection use the addresses of the Routers/Gateways to send data.
  
  The device also lets you use the tunnel mode for the VPN connection between an endpoint and a Router/Gateway. Thus, the address data within the network connected to the Router/Gateway remains hidden.
4.2 IKE – Internet Key Exchange

IPsec uses the IKE protocol (Internet Key Exchange) for authentication, for exchanging keys and for agreeing on further parameters for the security arrangement of a VPN connection.

4.2.1 Authentication

Use authentication as part of the security arrangement. During authentication, the connection peers display each other their ID cards, so to speak.

This ID card consists of the following:
- a pre-shared key, which is a character string previously exchanged using a different communication channel.
- a digital certificate, which was issued by a certification authority (CA).
  Certificates based on the X.509 standard contain the following:
  - information about the certification authority
  - validity period of the certificate
  - information about the permitted usage
  - the designated name (X.500 DN), which is the identity of the person that the certification authority assigned the certificate too
  - the public key belonging to this identity
  - the digital signature for verifying the connection between this identity and its related public key

Larger companies and authorities usually have their own certification authority.
A commonly used file extension for a certificate based on the PKCS#12 standard is `.p12`.
You can also find the information contained in a PKCS#12 file separately in individual files with the file extension `.pem`.

4.2.2 Encryption

To help protect the data, IKE uses various cryptographic algorithms for data encryption. The endpoints of the VPN connection require the key to code and decode the data.

The following list contains the initial steps in setting up the IKE security arrangement between the VPN connection endpoints:
- the endpoints agree on a cryptographic algorithm which subsequently uses the key for coding and decoding the IKE protocol messages
- the endpoints specify the time periods during which the key exchange takes place
- the endpoints identify the devices on which the coding and decoding takes place. The administrator specifies the endpoints beforehand in the settings of each endpoint.

After the endpoints complete the steps listed above, the devices agree on the key to code and decode the data.
4.2.3 Creating a certificate using OpenSSL

Using OpenSSL lets you create and sign a server certificate to use for VPN authentication.

Prerequisite: On a Windows system, you need a text editor that correctly handles Unix line breaks, for example the Notepad++ application.

Create a certificate. To do this, perform the following steps:

- Download OpenSSL from https://www.openssl.org and install the application.
- Specify the install directory c:\openssl and accept the other installation defaults.
- Start the Command Prompt program on your computer.
- To create the appropriate directories and files, enter the following commands in the Command Prompt window:
  
  C:\Users\username> cd \ 
  C:\> cd openssl 
  C:\openssl> md certs 
  C:\openssl> cd certs 
  C:\openssl\certs> md nameCA 
  C:\openssl\certs> md nameCA\newcerts 
  C:\openssl\certs> notepad++ nameCA\index.txt 
- Save the index.txt file and exit the Notepad++ program.
- In the Command Prompt window, create a file named serial.txt, with the following command:
  
  C:\openssl\certs> notepad++ nameCA\serial.txt 
- Open the serial.txt file using the Notepad++ program.
- In the Notepad++ window, enter the value 01 on the first line.
- Save the serial.txt file and exit the Notepad++ program.
- To set the path to the OpenSSL application, enter the following command in the Command Prompt window:
  
  C:\> set path=c:\openssl\bin;%path%
- To set the path to the OpenSSL configuration file, enter the following command in the Command Prompt window:
  
  C:\openssl\certs> set OPENSSL_CONF=c:\openssl\bin\openssl.cfg
- Using a text editor, edit the configuration file openssl.cfg located in the c:\openssl\bin directory. The countryName and stateOrProvinceName values are optional. Therefore change the value match to optional. Save the settings. The resulting configuration is as follows:

```
# For the CA policy
[policy_match]
countryName = optional
stateOrProvinceName = optional
organizationName = match
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
```
- To create an RSA certificate named ca.key, enter the following commands in the Command Prompt window:
  
  C:\openssl\certs> openssl genrsa -out ca.key 1024

The window displays the following text during certificate generation:

```
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.................................................++++++
...........................................................++++++
e is 65537 (0x10001)
```
The OpenSSL application also lets you generate other certificate types. To display the various certificate types, open the openssl.exe application located in the c:\OpenSSL\bin directory, and enter the ? character in the Command Prompt window.

To create and sign a Certificate Signing Request (CSR), enter the following commands in the Command Prompt window:

```
C:\OpenSSL\certs> openssl req -new -x509 -days 365 -key ca.key -out nameCA/cacert.pem
```

When requested, enter the appropriate distinguished name (DN) information for the CA certificate. When you press the <Enter> key, you can leave the optional fields blank.

For example, enter the following values:

<table>
<thead>
<tr>
<th>Country Name:</th>
<th>de</th>
</tr>
</thead>
<tbody>
<tr>
<td>State or Province Name:</td>
<td>BW</td>
</tr>
<tr>
<td>Locality Name:</td>
<td>Neckartenzlingen</td>
</tr>
<tr>
<td>Organization Name:</td>
<td>Hirschmann Automation and Control</td>
</tr>
<tr>
<td>Org. Unit Name:</td>
<td>INET</td>
</tr>
<tr>
<td>Common Name:</td>
<td>EAGLE-FD122E</td>
</tr>
</tbody>
</table>
4.3 Application examples

The following examples describe the special features occurring in frequently used applications.

4.3.1 Connecting 2 subnetworks

In a large company network, a transfer network connects the subnetworks to each other. A VPN connects 2 of these subnetworks for example, the production control and the production hall. To hide the internal IP addresses, configure the VPN to function in the tunnel mode.

The following information about the VPN is available:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Router 1</th>
<th>Router 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of internal port</td>
<td>10.0.1.201</td>
<td>10.0.3.201</td>
</tr>
<tr>
<td>IP address of external port</td>
<td>10.0.2.1</td>
<td>10.0.2.2</td>
</tr>
<tr>
<td>Pre-shared key</td>
<td>123456abcdef</td>
<td>123456abcdef</td>
</tr>
<tr>
<td>Start IKE mode as</td>
<td>Initiator</td>
<td>Responder</td>
</tr>
<tr>
<td>IP parameters of the connecting networks</td>
<td>10.0.1.0/24</td>
<td>10.0.3.0/24</td>
</tr>
</tbody>
</table>

Prerequisite for further configuration:
- Both device 1 and 2 are in the router mode.
- Specify the IP parameters on the router interfaces.
- The devices in the 10.0.1.0/24 subnet have the IP address of the internal interface on Router 1, as their Gateway.

![Figure 17: Connecting 2 subnetworks using a transfer network](image)
Perform the following steps:

☐ Create a VPN connection.

☐ Open the **Virtual Private Network > Connections** dialog.

☐ Click the **Create** button.

The **Create or select entry** table displays the VPN connections already available in the device.

☐ In the **VPN index** field, enter an available index number.

☐ In the **VPN description** column, specify a connection name for example, **Production Control – Production Hall 1**.

☐ Click the **Next** button.

☐ Specify the authentication parameters.

The device uses the values specified in the **Authentication** dialog to validate its identity. In this example, the device authenticates itself using a pre-shared key.

☐ Select in the **Authentication type** frame, **Authentication type** field the value **Pre-shared key (PSK)**.

☐ In the **Pre-shared key (PSK)** frame, specify the following settings:

  ▶ The value 123456abcdef in the **Pre-shared key** column
  ▶ The value 123456abcdef in the **Confirm** column

The default setting of the **Change** checkbox lets you enter and confirm the pre-shared key for new VPN connections. For existing VPN connections the **Pre-shared key** and the **Confirm** fields are inactive. To activate the fields, mark the checkbox in the **Change** column.

☐ Click the **Next** button.

☐ Specify the Endpoint and Traffic Selector parameters.

The device uses the values specified in the **Endpoint and traffic selectors** dialog to identify the data source and destination. The table displays the type of data to send through the VPN tunnel.

☐ In the **Endpoints** frame, specify the following settings:

  ▶ The value 10.0.2.1 in the **Local endpoint** column
  ▶ The value 10.0.2.2 in the **Remote endpoint** column

In the current example, the external ports of the 2 device are the endpoints for of the VPN connection.

☐ To identify data that the device sends through the VPN tunnel, click the **Add traffic selector** button in the **Add traffic selector** frame.
In the **Add traffic selector** dialog, specify the following settings:

- The value **1** in the **Traffic selector index** column
  The device enters the index number, but also lets you change it.
- The value **Any Traffic** in the **Traffic selector description** column
- The value **10.0.1.0/24** in the **Source address (CIDR)** column
- The value in the **Source restrictions** column is optional.
  The default setting is **any/any**. The device sends only the type of data specified through the VPN tunnel.
- The value **10.0.3.0/24** in the **Destination address (CIDR)** column
- The value in the **Destination restrictions** column is optional.
  The default setting is **any/any**. The device excepts only the specified type of data from the VPN tunnel.

- Click the **Ok** button.
- Click the **Next** button.
☐ Enter the IKE key exchange IPSec parameters.

The device uses the values specified in the Advanced configuration dialog. In this example the device is the initiator and selects the protocol automatically.

☐ In the General frame, Margin time [s] field, the default setting is 540 s. This is equal to 9 minutes.

☐ In the IKE/Key-exchange frame, specify the following settings:
  ▶ The value auto in the Version column
    With this, the device selects the protocol version automatically, depending on the VPN remote terminal.
  ▶ The value initiator in the Startup column
    The device initiates the VPN connection to the remote terminal.
  ▶ The value email in the IKE local identifier type column
  ▶ For example, the value user1@company.com in the IKE local ID column
  ▶ The value email in the Remote identifier type column
  ▶ For example, the value user2@company.com in the Remote ID column
  ▶ The value main in the IKE exchange mode column
  ▶ The value modp1024 in the IKE key agreement column
  ▶ The value hmacsha1 in the IKE integrity (MAC) column
  ▶ The value aes128 in the IKE encryption column
  ▶ The value 120 in the DPD timeout [s] column
    If the device does not receive a sign of life from the remote terminal within 120 seconds, then it terminates the VPN connection.
  ▶ The value 28800 in the IKE lifetime [s] column
    After the lifetime elapses, the 2 participating devices agree on new keys for the IKE security arrangement (IKE SA). The lifetime provides a periodic key change for the IKE SA.

☐ In the IPSec/Data-exchange frame, specify the following settings:
  ▶ The value modp1024 in the IPsec key agreement column
  ▶ The value hmacsha1 in the IPsec integrity (MAC) column
  ▶ The value aes128 in the IPsec encryption column
  ▶ The value 3600 in the IPsec lifetime [s] column

☐ To apply the changes, click the Finish button.

☐ Activate the connection.

☐ To activate the connection, mark the checkbox in the VPN active column.

☐ Save the settings.

☐ Save the changes temporarily. To do this, click the button.

☐ Make exactly the same settings on both devices.
  On the second device, replace the IP address and specify the value responder in the Startup column.
Managing configuration profiles

If you change the settings of the device during operation, then the device stores the changes in its memory (RAM). After a reboot the settings are lost.

In order to keep the changes after a reboot, the device lets you save the settings in a configuration profile in the non-volatile memory (NVM). In order to make it possible to quickly switch to other settings, the non-volatile memory offers storage space for multiple configuration profiles.

If an external memory is connected, then the device automatically saves a copy of the configuration profile in the external memory (ENVM). You can disable this function.

Detecting changed settings

The device stores changes made to settings during operation in its volatile memory (RAM). The configuration profile in the non-volatile memory (NVM) remains unchanged until you save the changed settings explicitly. Until then, the configuration profiles in memory and non-volatile memory are different. The device helps you recognize changed settings.

Volatile memory (RAM) and non-volatile memory (NVM)

You can recognize when the configuration profile in the volatile memory (RAM) is different from the "selected" configuration profile in the non-volatile memory (NVM). To do this, perform the following steps:

- Check the status bar at the top of the menu:
  - When a blinking icon is visible, the configuration profiles differ.
  - When no icon is visible, the configuration profiles match.
- Or:
  - Open the Basic Settings > Load/Save dialog.
  - Check the status of the checkbox in the Information frame:
    - When the checkbox is unmarked, the configuration profiles differ.
    - When the checkbox is marked, the configuration profiles match.
5.1.2 **External memory (ACA) and non-volatile memory (NVM)**

You can also recognize when the copy in the external memory (ACA) is different from the configuration profile in the non-volatile memory (NVM). To do this, perform the following steps:

- Open the **Basic Settings > Load/Save** dialog.
- Check the status of the checkbox in the **Information** frame:
  - When the checkbox is unmarked, the configuration profiles differ.
  - When the checkbox is marked, the configuration profiles match.

```
show config status
Configuration Storage sync State
--------------------------------
... 
NV to ACA................................. out of sync
... 
```
5.2 Saving the settings

5.2.1 Saving the configuration profile in the device

If you change the settings of the device during operation, then the device stores the changes in its memory (RAM). In order to keep the changes after a reboot, save the configuration profile in the non-volatile memory (NVM).

Saving a configuration profile

The device stores the settings in the "selected" configuration profile in the non-volatile memory (NVM).

Perform the following steps:

- Open the Basic Settings > Load/Save dialog.
- Verify that the required configuration profile is "Selected".
  You can recognize the "selected" configuration profile because the checkbox in the Selected column is marked.
- Click the enable button.

show config profiles nvm

Displays the configuration profiles contained in the non-volatile memory (nvm).

enable

Change to the Privileged EXEC mode.

save

Save the settings in the non-volatile memory (nvm) in the “selected” configuration profile.

Copying settings to a configuration profile

The device lets you store the settings saved in the memory (RAM) in a configuration profile other than the "selected" configuration profile. In this way you create a new configuration profile in the non-volatile memory (NVM) or overwrite an existing one.

Perform the following steps:

- Open the Basic Settings > Load/Save dialog.
- Click the button and then the Save As.. item.
  The dialog displays the Save As.. window.
- In the Name field, change the name of the configuration profile. If you keep the proposed name, the device will overwrite an existing configuration profile of the same name.
- Click the Ok button.

The new configuration profile is designated as “Selected”.
Managing configuration profiles
5.2 Saving the settings

Selecting a configuration profile

When the non-volatile memory (NVM) contains multiple configuration profiles, you have the option
to select any configuration profile there. The device stores the settings in the “selected”
configuration profile. Upon reboot, the device loads the settings of the “selected” configuration
profile into the memory (RAM).

Perform the following steps:

- Open the Basic Settings > Load/Save dialog.
  The table displays the configuration profiles present in the device. You can recognize the
  “selected” configuration profile because the checkbox in the Selected column is marked.
- In the table select the entry of the required configuration profile stored in the non-volatile
  memory (NVM).
- Click the button and then the Select item.
  In the Selected column, the checkbox of the configuration profile is now marked.

- Change to the Privileged EXEC mode.
- Displays the configuration profiles contained in the non-volatile memory (nvm).
- Show the current settings in the configuration profile named <string> in the non-volatile memory
  (nvm). If present, the device overwrites a configuration profile of the same name. The new
  configuration profile is designated as “Selected”.

- Change to the Configuration mode.
- Identifier of the configuration profile.
- Take note of the adjacent name of the configuration profile.
- Save the settings in the non-volatile memory (nvm)
in the “selected” configuration profile.

show config profiles nvm
enable
copy config running-config nvm profile <string>

Configure
- show config profiles nvm
- configure
- config profile select nvm 1
- save
5.2.2 **Saving the configuration profile in the external memory**

When an external memory is connected and you save a configuration profile, the device automatically saves a copy in the *Selected external memory*. In the default setting, the function is enabled. You can disable this function.

Perform the following steps:

- Open the *Basic Settings > External Memory* dialog.
- Mark the checkbox in the *Backup config when saving* column in order to enable the device to automatically save a copy in the external memory during the saving process.
- To deactivate the function, unmark the checkbox in the *Backup config when saving* column.
- Save the changes temporarily. To do this, click the *button.

---

**enable**  
**configure**  
**config envm config-save usb**  
**save**  

**Change to the Privileged EXEC mode.**  
**Change to the Configuration mode.**  
**Enable the function.**  
When you save a configuration profile, the device saves a copy in the external memory.  
**usb** = External USB memory  
**Save the settings in the non-volatile memory (nvm)** in the “selected” configuration profile.

---

5.2.3 **Exporting a configuration profile**

The device lets you save a configuration profile to a server as an XML file. If you use the Graphical User Interface, then you have the option to save the XML file directly to your PC.

**Prerequisites:**
- To save the file on a server, you need a configured server on the network.
- To save the file to an SCP or SFTP server, you also need the user name and password for accessing this server.

Perform the following steps:

- Open the *Basic Settings > Load/Save* dialog.
- In the table select the entry of the required configuration profile.

Export the configuration profile to your PC. To do this, perform the following steps:

- Click the link in the *Profile name* column.
- Select the storage location and specify the file name.
- Click the *Ok* button.

The configuration profile is now saved as an XML file in the specified location.
Export the configuration profile to a remote server. To do this, perform the following steps:

- Click the button and then the item. The dialog displays the window.
- In the field, specify the file URL on the remote server:
- Click the button.

The configuration profile is now saved as an XML file in the specified location.

```
show config profiles nvm

enable

copy config nvm remote sftp://<user_name>:<password>@<IP_address>/<path>/<file_name>
```

- Displays the configuration profiles contained in the non-volatile memory (nvm).
- Change to the Privileged EXEC mode.
- Save the selected configuration profile in the non-volatile memory (nvm) on a SFTP server.
### 5.3 Loading settings

If you save multiple configuration profiles in the memory, then you have the option to load a different configuration profile.

#### 5.3.1 Activating a configuration profile

The non-volatile memory of the device can contain multiple configuration profiles. If you activate a configuration profile stored in the non-volatile memory (`NVM`), then you immediately change the settings in the device. The device does not require a reboot.

Perform the following steps:

- Open the Basic Settings > Load/Save dialog.
- In the table select the entry of the required configuration profile.
- Click the button and then the Activate item.

The device copies the settings to the memory (`RAM`) and disconnects from the Graphical User Interface. The device immediately uses the settings of the configuration profile.

- Reload the Graphical User Interface.
- Log in again.

In the **Selected** column, the checkbox of the configuration profile that was activated before is marked.

```
show config profiles nvm
```

Displays the configuration profiles contained in the non-volatile memory (`nvm`).

```
enable
```

Change to the Privileged EXEC mode.

```
copy config nvm profile config3 running-config
```

Activate the settings of the configuration profile `config3` in the non-volatile memory (`nvm`). The device copies the settings into the volatile memory and disconnects the connection to the Command Line Interface. The device immediately uses the settings of the configuration profile `config3`.

#### 5.3.2 Loading the configuration profile from the external memory

If an external memory is connected, then the device loads a configuration profile from the external memory upon restart automatically. The device lets you save these settings in a configuration profile in non-volatile memory.

When the external memory contains the configuration profile of an identical device, you have the possibility to transfer the settings from one device to another.
Perform the following steps:

- Verify that the device loads a configuration profile from the external memory upon restart. In the default setting, the function is enabled. If the function is disabled, enable it again as follows:
  - Open the **Basic Settings > External Memory** dialog.
  - In the **Config priority** column, select the value **first**.
  - Save the changes temporarily. To do this, click the **✓** button.

  ```enable
  configure
  config envm load-priority usb first
  ```

- Using the Command Line Interface, the device lets you copy the settings from the external memory directly into the non-volatile memory (**NVM**).

  ```show config envm settings
  Type Status Auto Update Save Config Config Load Prio
  ------ ----------- -------------- ----------- ----------------
  usb ok [x] [x] first
  ```

  ```save
  ```

  Save the settings in a configuration profile in the non-volatile memory (**NVM**) of the device.

  ```show config profiles nvm
  show config profiles nvm
  ```

- Using the Command Line Interface, the device lets you copy the settings from the external memory directly into the non-volatile memory (**NVM**).

  ```enable
  copy config envm profile config3 nvm
  ```

  Copy the configuration profile **config3** from the external memory (**envm**) to the non-volatile memory (**nvm**).

**5.3.3 Importing a configuration profile**

The device lets you import from a server a configuration profile saved as an XML file. If you use the Graphical User Interface, then you can import the XML file directly from your PC.

Prerequisites:
- To save the file on a server, you need a configured server on the network.
- To save the file to an SCP or SFTP server, you also need the user name and password for accessing this server.
Perform the following steps:

- Open the Basic Settings > Load/Save dialog.
- Click the button and then the Import... item. The dialog displays the Import... window.
- In the Select source drop-down list, select the location from where the device imports the configuration profile.
  - PC/URL
    The device imports the configuration profile from the local PC or from a remote server.
  - External memory
    The device imports the configuration profile from the external memory.

Import the configuration profile from the local PC or from a remote server. To do this, perform the following steps:

- Import the configuration profile:
  - When the file is located on your PC or on a network drive, drag and drop the file in the area. Alternatively click in the area to select the file. You also have the option of transferring the file from your PC to the device through SFTP or SCP:
    - On your PC, open an SFTP or SCP client, for example WinSCP.
    - Use the SFTP or SCP client to open a connection to the device.
    - Transfer the file to the directory /nv/cfg in the device.
  - In the Destination frame, specify where the device saves the imported configuration profile:
    - In the Profile name field, specify the name under which the device saves the configuration profile.
    - In the Storage type field, specify the storage location for the configuration profile.
  - Click the Ok button.
    The device copies the configuration profile into the specified memory.

If you specified the value ram in the Destination frame, then the device disconnects the Graphical User Interface and uses the settings immediately.

Import the configuration profile from the external memory. To do this, perform the following steps:

- In the Import profile from external memory frame, Profile name drop-down list, select the name of the configuration profile to be imported. The prerequisite is that the external memory contains an exported configuration profile.
- In the Destination frame, specify where the device saves the imported configuration profile:
  - In the Profile name field, specify the name under which the device saves the configuration profile.
- Click the Ok button.
  The device copies the configuration profile into the non-volatile memory (NVM) of the device.

If you specified the value ram in the Destination frame, then the device disconnects the Graphical User Interface and uses the settings immediately.
Enable

`copy config remote sftp://<user name>:<password>@<IP_address>:/<path>/<file_name> running-config`

Change to the Privileged EXEC mode.

Import and activate the settings of a configuration profile saved on a SFTP server. The device copies the settings into the volatile memory and disconnects the connection to the Command Line Interface. The device immediately uses the settings of the imported configuration profile.
5.4 Reset the device to the factory defaults

If you reset the settings in the device to the delivery state, then the device deletes the configuration profiles in the volatile memory and in the non-volatile memory.

If an external memory is connected, then the device also deletes the configuration profiles saved in the external memory.

The device then reboots and loads the factory settings.

5.4.1 Using the Graphical User Interface or Command Line Interface

Perform the following steps:

- Open the Basic Settings > Load/Save dialog.
- Click the button, then Back to factory....
  The dialog displays a message.
- Click the Ok button.
  The device deletes the configuration profiles in the memory (RAM) and in the non-volatile memory (NVM).

If an external memory is connected, then the device also deletes the configuration profiles saved in the external memory.

After a brief period, the device restarts and loads the delivery settings.

```plaintext
enable
clear factory
```

Change to the Privileged EXEC mode.

Deletes the configuration profiles from the non-volatile memory and from the external memory. If an external memory is connected, then the device also deletes the configuration profiles saved in the external memory. After a brief period, the device restarts and loads the delivery settings.

5.4.2 Using the System Monitor

Prerequisite:
- Your PC is connected with the serial connection of the device using a terminal cable.

Perform the following steps:
- Restart the device.
- To change to the System Monitor, press the <1> key within 3 seconds when prompted during reboot.
  The device loads the System Monitor.
- To change from the main menu to the Manage configurations menu, press the <4> key.
- To execute the Clear configs and boot params command, press the <1> key.
To load the factory settings, press the <Enter> key. The device deletes the configuration profiles in the memory (RAM) and in the non-volatile memory (NVM). If an external memory is connected, then the device also deletes the configuration profiles saved in the external memory.

To change to the main menu, press the <q> key.
To reboot the device with factory settings, press the <q> key.
6 Loading software updates

Hirschmann is continually working on improving and developing their software. Check regularly if there is an updated version of the software that provides you with additional benefits. You find information and software downloads on the Hirschmann product pages on the Internet at www.hirschmann.com.

The device gives you the following options for updating the device software:

- Software update from the PC
- Software update from a server
- Software update from the external memory
- Loading a previous software version

Note: The device settings are kept after updating the device software.

You see the version of the installed device software in the login dialog of the Graphical User Interface.

To display the version of the installed software when you are already logged in, perform the following steps:

- Open the Basic Settings > Software dialog.
  The Running version field displays the version number and creation date of the device software that the device loaded during the last restart and is currently running.

- Change to the Privileged EXEC mode.
  show system info

  Displays the system information such as the version number and creation date of the device software that the device loaded during the last restart and is currently running.

6.1 Software update from the PC

The prerequisite is that the image file of the device software is saved on a data carrier which is accessible from your PC.

Perform the following steps:

- Navigate to the folder where the image file of the device software is saved.
- Open the Basic Settings > Software dialog.
- Drag and drop the image file in the area. Alternatively click in the area to select the file.
- To start the update procedure, click the Start button.
  As soon as the update procedure is completed successfully, the device displays an information that the software is successfully updated.
  Upon restart, the device loads the installed device software.
You also have the option of transferring the file from your PC to the device through SFTP or SCP. To do this, perform the following steps:

- On your PC, open an SFTP or SCP client, for example WinSCP.
- Use the SFTP or SCP client to open a connection to the device.
- Transfer the file to the directory `/upload/firmware` in the device.

When the file transfer is complete, the device starts updating the device software. When the update was successful, the device creates an `ok` file in the directory `/upload/firmware` and deletes the image file.

The device loads the device software during the next restart.
6.2 Software update from a server

To update the software using SFTP or SCP you need a server on which the image file of the device software is saved.

Perform the following steps:

- Open the Basic Settings > Software dialog.
- To start the update procedure, click the Start button. The device copies the currently running device software into the backup memory. As soon as the update procedure is completed successfully, the device displays an information that the software is successfully updated. Upon restart, the device loads the installed device software.
6.3 Software update from the external memory

6.3.1 Manually—initiated by the administrator

The device lets you update the device software with a few mouse clicks. The prerequisite is that the image file of the device software is located in the external memory.

Perform the following steps:

- Open the Basic Settings > Software dialog.
- In the table mark the row which displays the name of the desired image file in the external memory.
- Right-click to display the context menu.
- To start the update procedure, click in the context menu the Update item.

The device copies the currently running device software into the backup memory. As soon as the update procedure is completed successfully, the device displays an information that the software is successfully updated. Upon restart, the device loads the installed device software.

6.3.2 Automatically—initiated by the device

When the following files are located in the external memory during a restart, the device updates the device software automatically:
- the image file of the device software
- a text file startup.txt with the content autoUpdate=<Image_file_name>.bin

The prerequisite is that in the Basic Settings > External Memory dialog, you mark the checkbox in the Software auto update column. This is the default setting in the device.

Perform the following steps:

- Copy the image file of the new device software into the main directory of the external memory. Use only an image file suitable for the device.
- Create a text file startup.txt in the main directory of the external memory.
- Open the startup.txt file in the text editor and add the following line:
  autoUpdate=<Image_file_name>.bin
- Install the external memory in the device.
- Restart the device.

During the booting process, the device checks automatically the following criteria:
- Is an external memory connected?
- Is a startup.txt file in the main directory of the external memory?
- Does the image file exist which is specified in the startup.txt file?
- Is the software version of the image file more recent than the software currently running in the device?

When the criteria are fulfilled, the device starts the update procedure. The device copies the currently running device software into the backup memory. As soon as the update procedure is completed successfully, the device reboots automatically and loads the new software version.

Check the result of the update procedure. The log file in the Diagnostics > Report > System Log dialog contains one of the following messages:
- S.watson.AUTOMATIC_SNUPDATE_SUCCESS
  Software update completed successfully
- S_watson_AUTOMATIC_SWUPDATE_ABORTED
  Software update aborted
- S_watson_AUTOMATIC_SWUPDATE_ABORTED_WRONG_FILE
  Software update aborted due to wrong image file
- S_watson_AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE
  Software update aborted because the device did not save the image file.
6.4 Loading a previous software version

The device lets you replace the device software with a previous version. The basic settings in the device are kept after replacing the device software.

Note: Only the settings for functions which are available in the newer device software version are lost.
7 Configuring the ports

The following port configuration functions are available.
- Enabling/disabling the port
- Selecting the operating mode
- Hardware LAN bypass

7.1 Enabling/disabling the port

In the default setting, every port is enabled. For a higher level of access security, disable unconnected ports. To do this, perform the following steps:

- Open the Basic Settings > Port dialog, Configuration tab.
- To enable a port, mark the checkbox in the Port on column.
- To disable a port, unmark the checkbox in the Port on column.
- Save the changes temporarily. To do this, click the button.

```
enable
configure
interface 1/1
no shutdown
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Change to the interface configuration mode of interface 1/1.
Enable the interface.
7.2 Selecting the operating mode

In the default setting, the ports are set to *Automatic configuration* operating mode.

**Note:** The active automatic configuration has priority over the manual configuration.

Perform the following steps:

- Open the *Basic Settings > Port* dialog, *Configuration* tab.
- If the device connected to this port requires a fixed setting, then perform the following steps:
  - Deactivate the function. Unmark the checkbox in the *Automatic configuration* column.
  - In the *Manual configuration* column, enter the desired operating mode (transmission rate, duplex mode).
- Save the changes temporarily. To do this, click the ✅ button.

```bash
enable
configure
interface 1/1
no auto-negotiate
speed 100 full
```

- Change to the Privileged EXEC mode.
- Change to the Configuration mode.
- Change to the interface configuration mode of interface 1/1.
- Disable the automatic configuration mode.
- Port speed 100 MBit/s, full duplex
7.3 Hardware LAN bypass

The hardware LAN bypass function is used to maintain the data communication in case of a detected failure. The hardware LAN bypass function forwards the data packets between port 1/1 and port 1/2.

The device enables the hardware LAN bypass function on the following events:
- When the device powers down or when it detects a power failure or hardware defect.
- Upon user request during operation.

When the hardware LAN bypass function is enabled, the device disconnects port 1/1 and port 1/2. The ports connect physically to each other.

Figure 18: States of the hardware LAN bypass

The hardware LAN bypass function can be in one of the following modes:
- System-off bypass
- Run-time bypass

7.3.1 System-off bypass

When the device powers down, the device enables the System-off bypass mode automatically. The device continuously forwards the data packets between port 1/1 and port 1/2.

To help prevent a data stream between the connected networks, you manually disconnect the cable from the device.

7.3.2 Run-time bypass

The Run-time bypass mode is disabled by default.

During operation, you can intentionally enable the Run-time bypass mode. The device continuously forwards the data packets between port 1/1 and port 1/2 with the following limitations:
- The LEDs of port 1/1 and port 1/2 extinguish.
- The ports 1/1 and 1/2 are physically disabled. In the Basic Settings > Port dialog, Configuration tab, the checkbox for these ports in the State column is unmarked.
- The functions that the device uses to control the data stream from and to port 1/1 and port 1/2 are disabled.
### Enable the Run-time bypass mode

You enable the *Run-time bypass* mode using the Command Line Interface.

The prerequisite is that you access the device management using port 1/3 or a serial connection. Otherwise, the device management becomes unreachable when the *Run-time bypass* mode is enabled.

Perform the following steps:

1. `enable`                      Change to the Privileged EXEC mode.
2. `configure`                   Change to the Configuration mode.
3. `hardware by-pass enable`     Enable the *Run-time bypass* mode.
4. `show hardware by-pass`       Display the status of the *Run-time bypass* mode.

Run-time hardware Lan By-Pass Information
-------------------------------------------
Operation State.............................enabled
save

Save the settings in the non-volatile memory (NVM) in the Selected configuration profile.

### Disable the Run-time bypass mode

You disable the *Run-time bypass* mode using the Command Line Interface.

Perform the following steps:

1. `enable`                      Change to the Privileged EXEC mode.
2. `configure`                   Change to the Configuration mode.
3. `hardware by-pass disable`    Disable the *Run-time bypass* mode.
4. `show hardware by-pass`       Display the status of the *Run-time bypass* mode.

Run-time hardware Lan By-Pass Information
-------------------------------------------
Operation State.............................disabled
save

Save the settings in the non-volatile memory (NVM) in the Selected configuration profile.
8 Assistance in the protection from unauthorized access

The device offers functions that help you protect the device against unauthorized access.

After you set up the device, carry out the following steps in order to reduce possible unauthorized access to the device.

- Changing the SNMPv1/v2 community
- Disabling SNMPv1/v2
- Disabling HTTP
- Using your own HTTPS certificate
- Using your own SSH key
- Disabling HiDiscovery
- Enable IP access restriction
- Adjusting the session timeouts

8.1 Changing the SNMPv1/v2 community

SNMPv1/v2 works unencrypted. Every SNMP packet contains the IP address of the sender and the plaintext community name with which the sender accesses the device. If SNMPv1/v2 is enabled, then the device lets anyone who knows the community name access the device.

The community names public for read accesses and private for write accesses are preset. If you are using SNMPv1 or SNMPv2, then change the default community name. Treat the community names with discretion. To do this, perform the following steps:

1. Open the Device Security > Management Access > SNMPv1/v2 Community dialog. The dialog displays the communities that are set up.
2. For the Write community, specify in the Name column the community name.
   - Up to 32 alphanumeric characters are allowed.
   - The device differentiates between upper and lower case.
   - Specify a different community name than for read access.
3. Save the changes temporarily. To do this, click the button.

```
enable
configure
snmp community rw <community name>
show snmp community
save
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Specify the community for read/write access.
Display the communities that have been configured.
Save the settings in the non-volatile memory (nvm) in the "selected" configuration profile.
8.2 Disabling SNMPv1/v2

If you need SNMPv1 or SNMPv2, then use these protocols only in environments protected from eavesdropping. SNMPv1 and SNMPv2 do not use encryption. The SNMP packets contain the community in clear text. We recommend using SNMPv3 in the device and disabling the access using SNMPv1 and SNMPv2. To do this, perform the following steps:

2. To deactivate the SNMPv1 protocol, you unmark the SNMPv1 checkbox.
3. To deactivate the SNMPv2 protocol, you unmark the SNMPv2 checkbox.
4. Save the changes temporarily. To do this, click the button.

```
enable
configure
no snmp access version v1
no snmp access version v2
show snmp access
save
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Deactivate the SNMPv1 protocol.
Deactivate the SNMPv2 protocol.
Display the SNMP server settings.
Save the settings in the non-volatile memory (nvm) in the “selected” configuration profile.
8.3 Disabling HTTP

The web server provides the Graphical User Interface with the protocol HTTP or HTTPS. HTTPS connections are encrypted, while HTTP connections are unencrypted.

The HTTP protocol is enabled by default. If you disable HTTP, then no unencrypted access to the Graphical User Interface is possible. To do this, perform the following steps:

2. To disable the HTTP protocol, select the Off radio button in the Operation frame.
3. Save the changes temporarily. To do this, click the ✓ button.

If the HTTP protocol is disabled, then you can reach the Graphical User Interface of the device only by HTTPS. In the address bar of the web browser, enter the string https:// before the IP address of the device.

If the HTTPS protocol is disabled and you also disable HTTP, then the Graphical User Interface is unaccessible. To work with the Graphical User Interface, enable the HTTPS server using the Command Line Interface. To do this, perform the following steps:

1. enable
2. configure
3. no http server

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Disable the HTTP protocol.

1. enable
2. configure
3. https server

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Enable the HTTPS protocol.
8.4 Disabling the HiDiscovery access

HiDiscovery lets you assign IP parameters to the device over the network during commissioning. HiDiscovery communicates in the device management VLAN without encryption and authentication.

After the device is commissioned, we recommend to set HiDiscovery to read-only or to disable HiDiscovery access completely. To do this, perform the following steps:

- Open the Basic Settings > Network dialog.
- To take away write permission from the HiDiscovery software, in the HiDiscovery protocol v1/v2 frame, specify the value readOnly in the Access field.
- To disable HiDiscovery access completely, select the Off radio button in the HiDiscovery protocol v1/v2 frame.
- Save the changes temporarily. To do this, click the button.

```
enable
network hidiscovery mode read-only
no network hidiscovery operation
```

Change to the Privileged EXEC mode.
Disable write permission of the HiDiscovery software.
Disable HiDiscovery access.
8.5 Activating the IP access restriction

In the default setting, you access the device management from any IP address and with the supported protocols.

The IP access restriction lets you restrict access to the device management to selected IP address ranges and selected IP-based protocols.

Example:

The device is to be accessible only from the company network using the Graphical User Interface. The administrator has additional remote access using SSH. The company network has the address range 192.168.1.0/24 and remote access from a mobile network with the IP address range 109.237.176.0/24. The SSH application program knows the fingerprint of the RSA key.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Company network</th>
<th>Mobile phone network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network address</td>
<td>192.168.1.0/24</td>
<td>109.237.176.0/24</td>
</tr>
<tr>
<td>Netmask</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>Desired protocols</td>
<td>https, snmp</td>
<td>ssh</td>
</tr>
</tbody>
</table>

Perform the following steps:

- Open the Device Security > Management Access > IP Access Restriction dialog.
- Unmark the checkbox in the Active column for the entry. This entry lets users have access to the device from any IP address and the supported protocols.
- Address range of the company network:
  - To add a table entry, click the button.
  - Specify the address range of the company network in the IP address range column: 192.168.1.0/24
  - For the address range of the corporate network, deactivate the undesired protocols. The HTTPS, SNMP, and Active checkboxes remain marked.
- Address range of the mobile phone network:
  - To add a table entry, click the button.
  - Specify the address range of the mobile network in the IP address range column: 109.237.176.0/24
  - For the address range of the mobile network, deactivate the undesired protocols. The SSH and Active checkboxes remain marked.
- Before you enable the function, verify that at least one active entry in the table lets you have access. Otherwise, if you change the settings, then the connection to the device terminates. Access to the device management is only possible using the Command Line Interface through the serial interface of the device.
- To enable IP access restriction, select the On radio button in the Operation frame.
- Save the changes temporarily. To do this, click the button.
8.5 Activating the IP access restriction

- **enable**
- **show network management access global**
- **show network management access rules**
- **no network management access operation**
- **network management access add 2**
- **network management access modify 2 ip 192.168.1.0**
- **network management access modify 2 mask 24**
- **network management access modify 2 ssh disable**
- **network management access add 3**
- **network management access modify 3 ip 109.237.176.0**
- **network management access modify 3 mask 24**
- **network management access modify 3 snmp disable**
- **no network management access status 1**
- **network management access status 2**
- **network management access status 3**
- **show network management access rules**
- **network management access operation**

Change to the Privileged EXEC mode.
Displays if IP access restriction is enabled or disabled.
Display the entries that have been configured.
Disable the IP access restriction.
Create the entry for the address range of the company network.
Number of the next available index in this example: 2.
Specify the IP address of the company network.
Specify the netmask of the company network.
Deactivate SSH for the address range of the company network.
Repeat the operation for every unwanted protocol.
Create an entry for the address range of the mobile phone network.
Number of the next available index in this example: 3.
Specify the IP address of the mobile phone network.
Specify the netmask of the mobile phone network.
Deactivate SNMP for the address range of the mobile phone network.
Repeat the operation for every unwanted protocol.
Deactivate the default entry.
This entry lets users have access to the device from any IP address and the supported protocols.
Activate an entry for the address range of the company network.
Activate an entry for the address range of the mobile phone network.
Display the entries that have been configured.
Enable the IP access restriction.
8.6 Adjusting the session timeouts

The device lets you automatically terminate the session upon inactivity of the logged-on user. The session timeout is the period of inactivity after the last user action.

You can specify a session timeout for the following applications:
- Command Line Interface sessions using an SSH connection
- Command Line Interface sessions using a serial connection
- Graphical User Interface

**Timeout for Command Line Interface sessions using a SSH connection**

Perform the following steps:

- Open the Device Security > Management Access > Server dialog, SSH tab.
- Specify the timeout period in minutes in the Configuration frame, Session timeout [min] field.
- Save the changes temporarily. To do this, click the button.

```
enable
configure
ssh timeout <0..160>
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Specify the timeout period in minutes for Command Line Interface sessions using an SSH connection.

**Timeout for Command Line Interface sessions using a serial connection**

Perform the following steps:

- Open the Device Security > Management Access > CLI dialog, Global tab.
- Specify the timeout period in minutes in the Configuration frame, Serial interface timeout [min] field.
- Save the changes temporarily. To do this, click the button.

```
enable
cli serial-timeout <0..160>
```

Change to the Privileged EXEC mode.
Specify the timeout period in minutes for Command Line Interface sessions using a serial connection.
Session timeout for the Graphical User Interface

Perform the following steps:

- Open the Device Security > Management Access > Web dialog.
- Specify the timeout period in minutes in the Configuration frame, Web interface session timeout [min] field.
- Save the changes temporarily. To do this, click the button.

Change to the Privileged EXEC mode.

Specify the timeout period in minutes for Graphical User Interface sessions.
9 Controlling the data traffic

The device checks the data packets to be forwarded in accordance with defined rules. Data packets to which the rules apply are either forwarded by the device or blocked. If data packets do not correspond to any of the rules, then the device blocks the packets.

Routing ports to which no rules are assigned allow packets to pass. As soon as a rule is assigned, the assigned rules are processed first. After that, the specified standard action of the device takes effect.

The device provides the following functions for controlling the data stream:
- Checking the contents and states of data packets (packet filter)
- Service request control (Denial of Service, DoS)

The device observes and monitors the data stream. The device takes the results of the observation and the monitoring and combines them with the rules for the network security to create what is known as a status table. Based on this status table, the device decides whether to accept, drop or reject data.

The device processes data packets in the following sequence:

![Processing sequence of the data packets in the device](image)

**Note:** The device uses hardware to filter the data stream through the packet filters. This causes the device to process the data stream at a slow rate. For this reason, when you expect high volumes, use ACLs. To track the “connection state”, use packet filters.
9.1 Packet Filter – Routed Firewall Mode

9.1.1 Description

The Routed Firewall Mode (Layer 3) packet filter contains rules which the device applies successively to the data stream on its routing ports. The filtering naturally includes checking and evaluation of the data stream. The device contains a stateful firewall. A stateful firewall tracks the state of the connections transversing it.

The firewall filters both the contents and the status of the conveyed data packets. For each type, you have different criteria that you compile into individual rules as required.

In case of filtering for the content of a packet, the device checks the following criteria:
- IP header (source address, target address, protocol)
- TCP/UDP header (source port, target port)

You can configure the corresponding values in the table of the Network Security > Packet Filter > Routed Firewall Mode > Rule dialog.

When filtering according to the status of a packet, the firewall checks the criteria, which you can optionally configure in the Network Security > Packet Filter > Routed Firewall Mode > Rule dialog, Parameters field.

When you create a rule in this dialog, the value in the Parameters column is none initially. This default value causes filtering according to the status or the Ethernet header of a packet.

In order to activate optional, status or content filter criteria, you can enter different parameters, which each have the form key=value. Which keys are valid depends in part on the protocol of the rule. The keys mac=<$value> and state=<$value> apply everywhere and are independent of the protocol. The keys type=<$value> and code=<$value> are permitted only for the ICMP protocol; the key flags=<$value> is only permitted for the TCP protocol.

In the table below, you will find several examples for entries in the Parameters column and their effect on filtering. You have the option to enter several keys separated by commas. You can also enter several values separated by dashes. In addition, you can also enter different keys with several values in each case.

Table 13: Possible entries in the Parameters column

<table>
<thead>
<tr>
<th>Entry</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac=de:ad:de:ad:be:ef</td>
<td>This rule only applies to packets with the source MAC address de:ad:be:ef.</td>
</tr>
<tr>
<td>state=new</td>
<td>This rule only applies to packets coming from a new connection.</td>
</tr>
<tr>
<td>state=est</td>
<td>This rule only applies to packets coming from a connection that already exists.</td>
</tr>
<tr>
<td>state=new</td>
<td>est</td>
</tr>
<tr>
<td>type=5</td>
<td>This rule only applies to packets with ICMP type 5.</td>
</tr>
<tr>
<td>flags=syn</td>
<td>This rule only applies to packets for which the SYN flag is set.</td>
</tr>
<tr>
<td>state=new</td>
<td>rel,flags=rst</td>
</tr>
</tbody>
</table>

You find more information on valid entries in the Parameters column in the "Graphical User Interface" reference manual.
Since the device enables simultaneous filtering according to content and status of data packets, you can compile any combinations of both types of filtering into individual rules. The device lets you create up to 2048 individual rules.

Upon receipt of a data packet to be routed, the device generally applies the packet filer rules to the data packet. The device executes one rule after the other, until the data packet reaches the first rule that applies to it. The rules that follow are ignored.

To remove a rule, highlight the affected table entry and click the button.

When none of the rules you configured applies to a data packet or you have not configured individual rules, the Routed Firewall Mode packet filter applies a standard rule. Three possible standard rules are available here:

Table 14: Handling filtered data packets

<table>
<thead>
<tr>
<th>Rule</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept</td>
<td>The device forwards the data packet in accordance with the address information.</td>
</tr>
<tr>
<td>drop</td>
<td>The device deletes the data packet without informing the sender.</td>
</tr>
<tr>
<td>reject</td>
<td>The device deletes the data packet and informs the sender.</td>
</tr>
</tbody>
</table>

Note: In the default setting, the device applies the accept action. You can change this setting in the Network Security > Packet Filter > Routed Firewall Mode > Global dialog, Default policy field.

The Routed Firewall Mode packet filter follows a two-stage concept to activate newly created or modified rules. If you click the button, then the rules listed in the table are initially saved without activation taking place.

To transfer the rules and apply them to the device, in the Network Security > Packet Filter > Routed Firewall Mode > Global dialog, click the button and then the Commit changes item.

When you have configured and activated the status-dependent filter criteria, you can have the corresponding effects displayed in the status table. You can find this table with the name “Firewall state (connection tracking) table” on the bottom of the Diagnostics > System > System Information dialog. Based on the entries listed there, you can check which connections are currently established. Verify that the data packets permitted by you actually pass through the firewall, for example.

Note: To delete the information from the firewall state table, click in the Basic Settings > Restart dialog the Clear firewall table button.

9.1.2 Application example

The figure displays a typical application case:

A production controller wants to request data from a production robot.

The production robot is located in a production cell which a firewall keeps separate from the company network. The firewall is to help prevent data stream between the production cell and the rest of the company network. Only the data stream between the robot and the production controller’s PC is allowed to flow freely.
The following is known:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Robot</th>
<th>Firewall</th>
<th>PC</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address interface 1/1</td>
<td>10.0.1.201</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP address interface 1/4</td>
<td></td>
<td>10.0.2.1</td>
<td></td>
</tr>
<tr>
<td>IP address 10.0.1.5</td>
<td>10.0.1.5</td>
<td>10.0.2.17</td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td>10.0.1.201</td>
<td>10.0.2.1</td>
<td></td>
</tr>
</tbody>
</table>

Prerequisite for further configuration:

- The firewall is in Router mode.
- The IP parameters of the firewall router interface are configured.
- The devices in the internal network have the IP address of port 1 of the firewall as their Gateway.
- The Gateway and the IP address of the PC and the robot are configured.

![Figure 20: Application example for Packet Filter](image)

Create a rule for incoming IP packets. To do this, perform the following steps:

- Open the *Network Security > Packet Filter > Routed Firewall Mode > Rule* dialog.
  
  By default, no interface is assigned an explicit rule. In the *Default policy* field, the value `accept` is specified. Consequently, the data stream passes through the device without restriction. Creating a rule and assigning it to the relevant interface changes this condition.

- Create a new rule.

  Specify the following settings for the rule:

  - The value `10.0.2.17` or `10.0.2.17/32` in the *Source address* column
  - The value `any` in the *Source port* column
  - The value `10.0.1.5` or `10.0.1.5/32` in the *Destination address* column
  - The value `any` in the *Destination port* column
  - The value `any` in the *Protocol* column
  - The value `accept` in the *Action* column

  The device lets you limit the rule to IP packets that fulfill certain ICMP criteria. Additionally, specify the following settings for the rule:

  - The value `icmp` in the *Protocol* column
  - The value `type=3,code=1` in the *Parameters* column

  The values behind `type` and `code` are 1- to 3-digit decimal values. For the possible values, see the "Graphical User Interface" reference manual. Entering an ICMP code is optional.

- To activate the rule, mark the checkbox in the *Active* column.

- Save the changes temporarily. To do this, click the ✅ button.
Controlling the data traffic

9.1 Packet Filter – Routed Firewall Mode

Create rules for sending IP packets. To do this, perform the following steps:

- Open the **Network Security > Packet Filter > Routed Firewall Mode > Rule** dialog.
- Create a new rule **drop everything** that drops every IP packet. Specify the following settings for the rule:
  - The value **drop everything** in the **Description** column
  - The value **any** in the **Source address** column
  - The value **any** in the **Source port** column
  - The value **any** in the **Destination address** column
  - The value **any** in the **Destination port** column
  - The value **any** in the **Protocol** column
  - The value **drop** in the **Action** column
  - Unmarking the checkbox in the **Log** column
- Save the changes temporarily. To do this, click the **button.
- Open the **Network Security > Packet Filter > Routed Firewall Mode > Assignment** dialog.
- To assign the rule to an interface, click the **button and then the **Assign** item.
- In the **Interface** field, specify the value **1/4**.
- In the **Direction** field, specify the value **ingress** to activate this rule for the incoming data stream.
- In the **Rule index** column, specify the index number of the rule.
- Save the changes temporarily. To do this, click the **button.

- Open the **Network Security > Packet Filter > Routed Firewall Mode > Rule** dialog.
- Create a new rule **filter data** that explicitly allows to send selected IP packets. Specify the following settings for the rule:
  - The value **filter data** in the **Description** column
  - The value **10.0.1.5/32** in the **Source address** column
  - The value **any** in the **Source port** column
  - The value **10.0.2.17/32** in the **Destination address** column
  - The value **any** in the **Destination port** column
  - The value **any** in the **Protocol** column
  - The value **accept** in the **Action** column
- Save the changes temporarily. To do this, click the **button.
- Open the **Network Security > Packet Filter > Routed Firewall Mode > Assignment** dialog.
- To assign the rule to an interface, click the **button and then the **Assign** item.
- In the **Interface** field, specify the interface to which you want the rule assigned.
- In the **Direction** field, specify the value **egress** to activate this rule for the outbound data stream.
- In the **Rule index** column, specify the index number of the **filter data** rule.
- Repeat these steps to allocate the rule **drop everything** to the interface.
- Specify the priority of the rules in the **Priority** column:
  - The value **1** for the **filter data** rule
  - The value **2** for the **drop everything** rule
- To activate the rules, mark the checkbox in the **Active** column.
- Save the changes temporarily. To do this, click the **button.
- Open the **Network Security > Packet Filter > Routed Firewall Mode > Global** dialog.
- To apply the rules to the data stream, click the **button and then the **Commit changes** item.
9.2 Packet Filter – Transparent Firewall Mode

9.2.1 Description

The Transparent Firewall Mode (Layer 2) packet filter contains rules which the device applies successively to the data stream on its non-routing ports or VLAN interfaces. The Transparent Firewall Mode packet filter evaluates every data packet that passes through the firewall regardless of the connection status (Stateless Packet Inspection). The device filters the undesired data packets selectively while the connection is unknown.

The rules contain specific match criteria and actions. The device lets you specify the following criteria in the rules to filter the data packets:

- Ethernet header
  - Source MAC address
  - Destination MAC address
  - Ethertype
- IP header
  - Source IP address
  - Destination IP address
  - Protocol
- TCP/UDP header
  - Source port
  - Destination port

The available actions are as follows:

- accept
- drop

If a data packet matches the criteria of one or more rules, then the device applies the action specified in the first applicable rule to the data stream. The device ignores the rules that follow the first applicable rule.

If no rule matches, then the device applies the default rule. In the default setting, the default rule has the value accept. As a result, the device accepts the received data packets. The device lets you change the default rule in the Network Security > Packet Filter > Transparent Firewall Mode > Global dialog, Default policy field.

You create, modify or delete rules and specify the filtering criteria in Network Security > Packet Filter > Transparent Firewall Mode > Rule dialog. The device lets you create up to 999 individual rules. You can assign a single rule to any number of ports or VLANs.

The Transparent Firewall Mode packet filter follows a two-stage concept to activate newly created or modified rules. If you click the button, then the rules listed in the table are saved temporarily. To apply the rules to the data stream, in the Network Security > Packet Filter > Transparent Firewall Mode > Global dialog, click the button and then the Commit item.

The prerequisite to accept IP data packets is that the device accepts ARP data packets. In the default setting, the device accepts ARP data packets.
9.2.2 Application examples

The below examples describe how to set up the rules for the Transparent Firewall Mode packet filter:

- In the example 1, the network administrator wants to set up the rule based on the IP address of the devices.
- In the example 2, the network administrator wants to set up the rule based on the MAC address of the devices.

Example 1

In this example, the network administrator wants to accept the data packets from computers B and C to computer A based on the IP address of the devices. The firewall keeps computer A separate from the company network. The firewall helps prevent access between computer A and the rest of the company network. The firewall only permits access from computers B and C to computer A.

Prerequisites:

- Firewall is in Bridge mode
- In the Default policy field, the value drop is specified.

Perform the following steps:
- Create an IP rule for end device B.

  - Open the Network Security > Packet Filter > Transparent Firewall Mode > Rule dialog.
  - Click the + button. The device creates a new rule.
  - Specify the following settings for the rule:
    - Description column = accept ipv4 dev b to dev a
    - Ethertype column = ipv4
    - Source IP address column = 10.0.1.11
    - Destination IP address column = 10.0.1.158
  - Activate the rule. To do this, mark the checkbox in the Active column.
  - Save the changes temporarily. To do this, click the button.
  - Open the Network Security > Packet Filter > Transparent Firewall Mode > Assignment dialog.
Create an IP rule for end device C.

- Click the button.
- The dialog displays the Create window.
- In the Port/VLAN drop-down list, select the port 1/1.
- In the Direction drop-down list, select the value ingress to activate the rule for incoming data packets.
- In the Index drop-down list, select the value accept ipv4 dev b to dev a: 1.
- Click the Ok button.
- Apply the rule to the data stream. To do this, click the button and then the Commit item.

Change to the Privileged EXEC mode.

Change to the Configuration mode.

Create a Transparent Firewall Mode packet filter rule.

- packet-filter l2 rule add 1
  - action accept
  - src-ip 10.0.1.11
  - dest-ip 10.0.1.158
  - ethertype ipv4
  - description accept ipv4 dev b to dev a
- packet-filter l2 rule enable 1
- packet-filter l2 if add port 1 ingress 1

Open the Network Security > Packet Filter > Transparent Firewall Mode > Rule dialog.

- Click the button.
- The device creates a new rule.
- Specify the following settings for the rule:
  - Description column = accept ipv4 dev c to dev a
  - Ethertype column = ipv4
  - Source IP address column = 10.0.1.13
  - Destination IP address column = 10.0.1.158
- Activate the rule. To do this, mark the checkbox in the Active column.
- Save the changes temporarily. To do this, click the button.
- Open the Network Security > Packet Filter > Transparent Firewall Mode > Assignment dialog.
9.2 Packet Filter – Transparent Firewall Mode

- Click the button.
  The dialog displays the Create window.
- In the Port/VLAN drop-down list, select the port 1/2.
- In the Direction drop-down list, select the value ingress to activate the rule for incoming data packets.
- In the Index drop-down list, select the value accept ipv4 dev c to dev a: 2.
- Click the Ok button.
- Apply the rule to the data stream. To do this, click the button and then the Commit item.

enable
configure

```bash
packet-filter l2 rule add 2 action accept src-ip 10.0.1.13 dest-ip 10.0.1.158 ethertype ipv4 description accept ipv4 dev c to dev a
```

Create a Transparent Firewall Mode packet filter rule.
- `packet-filter l2 rule add 2 action accept src-ip 10.0.1.13 dest-ip 10.0.1.158 ethertype ipv4 description accept ipv4 dev c to dev a` Add a Transparent Firewall Mode packet filter rule with index = 2.
  - action accept
  - src-ip 10.0.1.13
  - dest-ip 10.0.1.158
  - ethertype ipv4
  - description accept ipv4 dev c to dev a
  Specify the user-specific name accept ipv4 dev c to dev a.

```bash
packet-filter l2 rule enable 2
```

Activate the Transparent Firewall Mode packet filter rule 2.

```bash
packet-filter l2 if add port 2 ingress 2 1
```

Apply the Transparent Firewall Mode packet filter rule 2 on port 1/2.
- `packet-filter l2 if add port 2 ingress` Add a Transparent Firewall Mode packet filter rule for port 1/2.
  - ingress
  - `2`
  Apply the Transparent Firewall Mode packet filter rule to the data packets received.
  - `2`
  Select the Transparent Firewall Mode packet filter rule 2.
  - `1`
  Priority = 1
Example 2

In this example, the network administrator wants to accept the data packets from computers B and C to computer A based on the MAC address of the devices. The firewall keeps computer A separate from the company network. The firewall helps prevent access between computer A and the rest of the company network. The firewall only permits access from computers B and C to computer A. The computers B and C are part of VLAN 10.

![Diagram](image)

**Figure 22: Application example for packet filter based on MAC addresses**

Prerequisites:
- Firewall is in Bridge mode
- In the *Default policy* field, the value *drop* is specified.

Perform the following steps:
- Create a MAC rule for end device B.

- Open the *Network Security > Packet Filter > Transparent Firewall Mode > Rule* dialog.
- Click the button.
  
  The device creates a new rule.
- Specify the following settings for the rule:
  - *Description* column = *accept mac dev b to dev a*
  - *Ethertype* column = vlan8021q
  - *VLAN ID* column = 10

  The prerequisite to change the value in the *VLAN ID* column is:
  - In the *Ethertype* column, the value *vlan8021q* is specified.
  - or
  - In the *Ethertype* column, the value *custom* is specified and in the *Ethertype custom value* column, a valid value is specified.
- Activate the rule. To do this, mark the checkbox in the *Active* column.
- Save the changes temporarily. To do this, click the button.
Open the Network Security > Packet Filter > Transparent Firewall Mode > Assignment dialog.

Click the button.
The dialog displays the Create window.

- In the Port/VLAN drop-down list, select the port 1/1.
- In the Direction drop-down list, select the value ingress to activate the rule for incoming data packets.
- In the Index drop-down list, select the value accept mac dev b to dev a: 1.

Apply this rule to the data stream. To do this, click the button and then the Commit item.
Controlling the data traffic

9.2 Packet Filter – Transparent Firewall Mode

Create a MAC rule for end device C.

- Enable
- Configure

```
```

- Change to the Privileged EXEC mode.
- Change to the Configuration mode.

Create a **Transparent Firewall Mode** packet filter rule.

- Add a **Transparent Firewall Mode** packet filter rule with index = 1.

```
packet-filter 12 rule add 1

Action = accept
ethertype vlan8021q
vlan 10
description accept mac dev b to dev a
```

Specify the user-specific name accept mac dev b to dev a.

- Activate the **Transparent Firewall Mode** packet filter rule 1.
- Apply the **Transparent Firewall Mode** packet filter rule 1 on port 1/1.

```
packet-filter 12 if add port 1 ingress 1
```

- Select the **Transparent Firewall Mode** packet filter rule 1.
- Priority = 1

Open the **Network Security > Packet Filter > Transparent Firewall Mode > Rule** dialog.

- Click the ![New Rule](button.png) button.
  The device creates a new rule.

Specify the following settings for the rule:

- **Description** column = accept mac dev c to dev a
- **Source MAC address** column = 10:22:33:44:55:77
- **Ethertype** column = vlan8021q
- **VLAN ID** column = 10

The prerequisite to change the value in the **VLAN ID** column is:

- In the **Ethertype** column, the value vlan8021q is specified.
  or
- In the **Ethertype** column, the value custom is specified and in the **Ethertype custom value** column, a valid value is specified.

- Activate the rule. To do this, mark the checkbox in the **Active** column.
- Save the changes temporarily. To do this, click the ![Save Changes](button.png) button.
- Open the **Network Security > Packet Filter > Transparent Firewall Mode > Assignment** dialog.
Controlling the data traffic

9.2 Packet Filter – Transparent Firewall Mode

- Click the button. The dialog displays the Create window.
- In the Port/VLAN drop-down list, select the port 1/2.
- In the Direction drop-down list, select the value ingress to activate the rule for incoming data packets.
- In the Index drop-down list, select the value accept mac dev c to dev a: 2.
- Click the Ok button.
- Apply the rule to the data stream. To do this, click the button and then the Commit item.

Enable

Configure


Packet filter 12 rule enable 2

Packet filter 12 if add port 2 ingress 2 1

Change to the Privileged EXEC mode.

Change to the Configuration mode.

Create a Transparent Firewall Mode packet filter rule.
- Packet filter 12 rule add 2
  Add a Transparent Firewall Mode packet filter rule with index = 2.
  - Action accept
  - ethertype vlan8021q
  - vlan 10
  - description accept mac dev c to dev a
    Specify the user-specific name accept mac dev c to dev a.

Activate the Transparent Firewall Mode packet filter rule 2.

Apply the Transparent Firewall Mode packet filter rule 2 on port 1/2.
- Packet filter 12 if add port 2
  Add a Transparent Firewall Mode packet filter rule for port 1/2.
  - Ingress
    Apply the Transparent Firewall Mode packet filter rule to the data packets received.
  - 2
    Select the Transparent Firewall Mode packet filter rule 2.
  - 1
    Priority = 1
9.3 Helping protect against unauthorized access

With this function, the device supports you in helping protect against invalid or falsified data packets targeted at causing the failure of certain services or devices. You have the option of specifying filters in order to restrict data stream for protection against denial-of-service attacks. The activated filters check incoming data packets and discard them as soon as a match with the filter criteria is found.

The Network Security > DoS > Global dialog contains 2 frames in which you activate different filters. To activate them, mark the corresponding checkboxes.

In the TCP/UDP frame, you activate up to 4 filters that only influence TCP and UDP packets. Using this filter, you deactivate port scans, which attackers use to try to recognize devices and services offered. The filters operate as follows:

Table 15: DoS filters for TCP packets

<table>
<thead>
<tr>
<th>Filter</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate Null Scan Filter</td>
<td>The device detects and discards TCP packets for which no TCP flags are set.</td>
</tr>
<tr>
<td>Activate Xmas Filter</td>
<td>The device detects and discards TCP packets for which the TCP flags FIN, URG and PUSH are simultaneously set.</td>
</tr>
<tr>
<td>Activate SYN/FIN Filter</td>
<td>The device detects and discards TCP packets for which the TCP flags SYN and FIN are simultaneously set.</td>
</tr>
<tr>
<td>Activate Minimal Header Filter</td>
<td>The device detects and discards TCP packets for which the TCP header is too short.</td>
</tr>
</tbody>
</table>

The ICMP frame offers you 2 filter options for ICMP packets. Fragmentation of incoming ICMP packets is a sign of an attack. If you activate this filter, the device detects fragmented ICMP packets and discards them. Using the Allowed payload size [byte] parameter, you can also specify the maximum permissible size of the payload of the ICMP packets. The device discards data packets that exceed this byte specification.

Note: You can combine the filters in any way in the Network Security > DoS > Global dialog. When several filters are selected, a logical Or applies: If the first or second (or the third, etc.) filter applies to a data packet, then the device discards it.
9.4 Deep Packet Inspection

The Deep Packet Inspection function (DPI) lets you monitor and filter data packets. The function supports you in protecting your network from undesirable content, such as spam or viruses.

The Deep Packet Inspection function inspects data packets for undesirable characteristics and protocol violations. The protocol inspects the header and the payload of the data packets.

9.4.1 Deep Packet Inspection - Modbus Enforcer function

The Modbus protocol is widely used in the Automation sector.
- The protocol is based on Function code, the commands.
- Some of the Function code let you specify register or coil address ranges.

The device uses the Deep Packet Inspection function to block data packets that violate the specified rules. On request, the device terminates the Modbus or TCP connection if it detects any of the following events:
- Violation of the Modbus standard as specified in the Sanity check column.
- Violation of the possible function codes as specified in the Function code column.

9.4.2 Application example for Modbus Enforcer

The device uses the Deep Packet Inspection function to monitor the data stream between the Modbus master and Modbus client (outstation). The Deep Packet Inspection function inspects the data packets for the specified characteristics.

Example: The network administrator wants the device to forward data packets from the Modbus master to Modbus client (outstation).

The data packets contain the following function codes and unit identifiers:
- **Function code** = 1 (Read Coils)
- **Function code** = 2 (Read Discrete Inputs)
- **Function code** = 3 (Read Holding Registers)
- **Function code** = 23|128-255|512-1023 (Read/Write Multiple Registers), read address range 128..255, write address range 512..1023.
- **Unit identifier** = 254,255

For this purpose, create the Modbus Enforcer rule with the above values.

![Figure 23: Inspection of data packets](image)
9.4.3 Create and edit Modbus Enforcer rules

Create a rule with the name *my-modbus* according to the example above.

**Create a Modbus Enforcer rule**

Perform the following steps:

- Open the *Network Security > DPI > Modbus Enforcer* dialog.
- Click the **button. The dialog displays the *Create* window.
- In the **Index** field, specify the value **1**.
- Click the **Ok** button. The device creates a new rule with the following settings:
  - **Index column** = **1**
  - **Description column** = **modbus**
  - **Function type column** = **readonly**
  - **Function code column** = **1,2,3,4,7,11,12,17,20,24**
  - **Unit identifier column** = **none**
  - Checkbox in the **Sanity check column** = **marked**
  - Checkbox in the **Exception column** = **unmarked**
  - Checkbox in the **Reset column** = **marked**
  - Checkbox in the **Profile active column** = **unmarked**
- Modify the description to **my-modbus**. To do this, double-click the corresponding field in the **Description** column and edit the string.
- In the **Function type column**, specify the value **advanced**.
- Save the changes temporarily. To do this, click the **button.
- Edit the **function codes**. To do this, double-click the corresponding field in the **Function code** column and enter the values **1,2,3,23**.
  As an alternative, you can use the **Edit** dialog. To do this, click the **button and then the **Edit** item.
  - In the right column, highlight the values **4,7,11,12,17,20,24**.
  - Move the highlighted values to the left column by clicking the **<** button.
  - In the left column, highlight the value **23**.
  - Move the highlighted value to the right column by clicking the **>** button.
  - Click the **Ok** button. The **Function code** column displays the value **1,2,3,23**.
- For **Function code = 23**, add the address ranges **128–255|512–1023**. Separate the address ranges with a vertical bar (pipe).
  The **Function code** column displays the value **1,2,3,23|128–255|512–1023**.
- Only allow data packets with **unit identifier** = **254,255**. To do this, enter the value **254,255** in the **Unit identifier** column.
- Save the changes temporarily. To do this, click the **button.
Aktivieren des Modbus Enforcer-Regels

* Markieren Sie das Kontrollkästchen im Profil aktiv-Spalte.
* Speichern Sie die Änderungen temporär. Um dies zu tun, klicken Sie auf den Schaltfläche.

DPI Modbus EnableProfile 1

Aktivieren Sie die Modbus Enforcer-Regel 1. Nach Aktivierung der Regel hilft das Gerät, die Regeländerungen zu verhindern.

Klicken Sie auf den Schaltfläche und dann auf das Item Änderungen speichern.

DPI Modbus Commit

Anwenden der Modbus Enforcer-Regeln.

**Aktivieren des Modbus Enforcer-Regels**

Ausführen der folgenden Schritte:

- Markieren Sie das Kontrollkästchen in der Spalte Profil aktiv.
- Speichern Sie die Änderungen vorübergehend. Um dies zu tun, klicken Sie auf den Schaltfläche.

DPI Modbus EnableProfile 1

Aktivieren Sie die Modbus Enforcer-Regel 1. Nach Aktivierung der Regel hilft das Gerät, die Regeländerungen zu verhindern.

Klicken Sie auf den Schaltfläche und dann auf das Item Änderungen speichern.

DPI Modbus Commit

Anwenden der Modbus Enforcer-Regeln.

**9.4.4 Tiefenpaketeinspektion - DNP3-Enforcerfunktion**


- Zum Steuern, wie das Gerät die Datenpakete während der Einspeisung verarbeitet, geben Sie den Wert jedes Objekts in den folgenden Feldern im Benutzeroberfläche an:
  - Objekttyp
  - Gruppe
  - Variation
The device uses the Deep Packet Inspection function to block data packets that violate the specified rules. On request, the device terminates the TCP connection if it detects any of the following events:

- Violation of the DNP3 standard as specified in the Sanity check and CRC check columns.
- Violation of the allowed function codes as specified in the Function code list column.
- Violation of the allowed objects as specified in the following fields in the Graphical User Interface:
  - Object type
  - Group no.
  - Variation no.
  - Function code
  - Function name
  - Length
  - Qualifier code
  - Index

9.4.5 Application example for DNP3 Enforcer

The device uses the Deep Packet Inspection function to monitor the data stream between the DNP3 master and DNP3 client (outstation). The Deep Packet Inspection function inspects the data packets for the specified characteristics.

Example: The network administrator wants the device to forward data packets from the DNP3 master to DNP3 client (outstation).

The data packets contain the following function code list and objects:

**Function codes:**
- 1 (Read)
- 2 (Write)
- 3 (Select)
- 23 (Delay Measurement)

**Objects:**
- Object type = 1 - Request
- Group no. = 5
- Variation no. = 1
- Function code = 2
- Function name = WRITE
- Length = 1
- Qualifier code = 0x17, 0x28
- Index of Default Object List = 6

For this purpose, create the DNP3 Enforcer rule with the above values.

Figure 24: Inspection of data packets
9.4.6 Create and edit a DNP3 Enforcer rule

Create a rule with the name my-dnp3 according to the example above.

Create a DNP3 Enforcer rule

Perform the following steps:

- Open the Network Security > DPI > DNP3 Enforcer dialog.
- Click the button. The dialog displays the Create window.
- In the Index field, specify the value 1.
- Click the Ok button. The device creates a new rule with the following settings:
  - Index column = 1
  - Description column = dnp3
  - Function code list column = 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,129,130,131
  - Checkbox in the CRC check column = marked
  - Checkbox in the Sanity check column = marked
  - Checkbox in the Check outstation traffic column = unmarked
  - Checkbox in the TCP reset column = marked
  - Checkbox in the Profile active column = unmarked
  - Index field = all
- Change the name of the DNP3 Enforcer entry to my-dnp3. To do this, double-click the corresponding field in the Description column and enter the string.
- Edit the function codes of the DNP3 Enforcer entry. To do this, double-click the corresponding field in the Function code list column and enter the value 1,2,3,23. As an alternative, you can use the Edit dialog. To do this, click the button and then the Edit item. In the Selected function codes column, highlight every value except 1, 2, 3 and 23. Move the highlighted values to the Available function codes column. To do this, click the button. Click the Ok button. The Function code column displays the value 1,2,3,23.

The Edit dialog lets you specify only the following function codes: 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,129,130,131. To specify other function codes within the range of 0..255, double-click the corresponding field in the Function code list column and enter the desired values. You separate multiple function codes with a comma.
Controlling the data traffic

9.4 Deep Packet Inspection

- Save the changes temporarily. To do this, click the ✅ button.
- Edit the default object list. To do this, proceed as follows:
  - Open the Wizard dialog. To do this, click the 📝 button.
  - The dialog displays the DNP3 Enforcer - Object wizard window.
  - In the table, highlight the row with Index = 1.
  - Click the Next button.
  - In the Index of Default Object List field, specify the value 6.
- Create and apply the objects to the DNP3 Enforcer rule. To do this, enter the respective values in the following fields:
  - Index field = 1
  - Object type field = 1 - Request
  - Group no. field = 5
  - Variation no. field = 1
  - Function code field = 2
  - Function name field = WRITE
  - Length field = 1
  - Qualifier code field = 0x17,0x28
  - Click the Add button.
  - The table above displays a row with the values you specified.
  - Apply the changes. To do this, click the Finish button.
  - Save the changes temporarily. To do this, click the ✅ button.

enable
configure
dpi dnp3 profile add 1 description my-dnp3 function-code-list 1,2,3,23 default-object-list 6

dpi dnp3 object 1 add 1 object-type request group-number 5 variation-number 1 function-code 2 function-name write function-length 1 qualifier-code-list 0x17,0x28

Create a DNP3 Enforcer rule.
- dpi dnp3 profile add 1
  - description my-dnp3
  - function-code-list 1,2,3,23
  - default-object-list 6

Add the user-specific objects to the DNP3 Enforcer rule 1.
- dpi dnp3 object 1
  - add 1
    - object-type request
    - group-number 5
    - variation-number 1
    - function-code 2
    - function-name write
    - function-length 1
    - qualifier-code-list 0x17,0x28

Activate the DNP3 Enforcer rule

Perform the following steps:

- Mark the checkbox in the Profile active column.
- Save the changes temporarily. To do this, click the ✅ button.
Apply the DNP3 Enforcer rule to the data stream

Perform the following steps:

- Click the button and then the Edit item.
  - In the Selected function codes column, highlight every value except 1, 2, 3 and 23.
  - Move the highlighted values to the Available function codes column. To do this, click the < button.
  - Click the Ok button.
  
  The Function code column displays the value 1, 2, 3, 23.

The Edit dialog lets you specify only the following function codes:
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27
28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131. To specify other function codes within the range of 0..255, double-click the corresponding field in the Function code list column and enter the desired values. You separate multiple function codes with a comma.

- Save the changes temporarily. To do this, click the button.

- Edit the default object list. To do this, perform the following steps:
  - Open the Wizard dialog. To do this, click the button.
  
  The dialog displays the DNP3 Enforcer - Object wizard window.
  - In the table, highlight the row with Index = 1.
  - Click the Next button.
  - In the Index of Default Object List field, specify the value 6.

- Create and apply the objects to the DNP3 Enforcer rule. To do this, enter the respective values in the following fields:
  - Index field = 1
  - Object type field = 1 - Request
  - Group no. field = 5
  - Variation no. field = 1
  - Function code field = 2
  - Function name field = WRITE
  - Length field = 1
  - Qualifier code field = 0x17, 0x28

  - Click the Add button.
  
  The table above displays a row with the values you specified.

- Apply the changes. To do this, click the Finish button.

- Save the changes temporarily. To do this, click the button.
Create a **DNP3 Enforcer** rule.

- **dpi dnp3 profile add 1**
  - Add a **DNP3 Enforcer** rule with index = 1.
  - description **my-dnp3**
  - Specify the user-specific name **my-dnp3**.
  - function-code-list 1,2,3,23
  - default-object-list 6

Add the user-specific **objects** to the **DNP3 Enforcer** rule 1.

```plaintext
dpi dnp3 object 1 add 1 object-type
request group-number 5 variation-number
1 function-code 2 function-name write
function-length 1 qualifier-code-list
D0x7,0x28
```

<table>
<thead>
<tr>
<th>Index</th>
<th>Object Type</th>
<th>Group Number</th>
<th>Variation</th>
<th>Function Code</th>
<th>Function Name</th>
<th>Function Length</th>
<th>Qualifier List</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>request</td>
<td>5</td>
<td>1</td>
<td>2</td>
<td>write</td>
<td>1</td>
<td>D0x7,0x28</td>
</tr>
</tbody>
</table>
10  Synchronizing the system time in the network

Many applications rely on a time that is as correct as possible. The necessary accuracy, and thus the allowable deviation from the actual time, depends on the application area.

Examples of application areas include:
- Log entries
- Time stamping of production data
- Process control

The device lets you synchronize the time on the network using the following options:
- The Network Time Protocol (NTP) is accurate to the order of sub-milliseconds.

10.1  Basic settings

In the Time > Basic Settings dialog, you specify general settings for the time.

10.1.1  Setting the time

When no reference time source is available to you, you have the option to set the time in the device.

After a cold start or reboot, if no real-time clock is available or the real-time clock contains an invalid time, then the device initializes its clock with January 1, 00:00h. After the power supply is switched off, the device buffers the settings of the real-time clock up to 24 hours.

Alternatively, you configure the settings in the device so that it automatically obtains the current time from an NTP server.

Perform the following steps:

- Open the Time > Basic Settings dialog.

  - The System time (UTC) field displays the current UTC (Universal Time Coordinated) of the device. UTC is the time relating to the coordinated world time measurement. UTC is the same worldwide and does not take local time shifts into account.

  - The time in the System time field comes from the System time (UTC) plus the Local offset [min] value and a possible shift due to daylight saving time.

- In order to cause the device to apply the time of your PC to the System time field, click the Set time from PC button. Based on the value in the Local offset [min] field, the device calculates the time in the System time (UTC) field: The System time (UTC) comes from the System time minus the Local offset [min] value and a possible shift due to daylight saving time.

  - The Time source field displays the origin of the time data. The device automatically selects the source with the greatest accuracy.

  - The source is initially local.

  - When NTP is active and the device receives a valid NTP packet, the device sets its time source to ntp.
Synchronizing the system time in the network

10.1 Basic settings

10.1.2 Automatic daylight saving time changeover

When you operate the device in a time zone in which there is a summer time change, you set up the automatic daylight saving time changeover on the Daylight saving time tab.

When daylight saving time is enabled, the device sets the local system time forward by 1 hour at the beginning of daylight saving time. At the end of daylight saving time, the device sets the local system time back again by 1 hour. To do this, perform the following steps:

- Open the Time > Basic Settings dialog, Daylight saving time tab.
- To select a preset profile for the start and end of daylight saving time, click the Profile... button in the Operation frame.
- When no matching daylight saving time profile is available, you specify the changeover times in the Summertime begin and Summertime end fields. For both time points, you specify the month, the week within this month, the weekday, and the time of day.
- To enable the function, select the On radio button in the Operation frame.
- Save the changes temporarily. To do this, click the button.

**Enable**

```
enable
```

Change to the Privileged EXEC mode.

**Configure**

```
configure
```

Change to the Configuration mode.

**Clock set**

```
clock set <YYYY-MM-DD> <HH:MM:SS>
```

Set the system time of the device.

**Clock timezone offset**

```
clock timezone offset <-780..840>
```

Enter the time difference between the local time and the received UTC time in minutes.

**Save**

```
save
```

Save the settings in the non-volatile memory (nvm) in the “selected” configuration profile.
10.2 NTP

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.

NTP uses levels, or hierarchies, of clock sources called stratum layers. Stratum layers define the distance from the reference clock. The layers start with zero as the top layer. The stratum zero layer consists of clock devices such as radio clocks, atomic clocks, or GPS clocks. The device operates at stratum layers 1 through 16.

Furthermore, an NTP device operates as a primary server, secondary server, or client. Synchronize the primary NTP-Server directly to the stratum zero layer.

A secondary NTP-Server synchronizes to one or more servers and provides a synchronization signal for one or more servers or clients. When you use the device in client mode, the device sends requests to the active NTP-Servers listed in the Time > NTP > Server dialog. In the client-server mode, the device also answers requests sent from dependent servers and clients.

An NTP-Client synchronizes to one or more upstream NTP-Servers. In order to synchronize to the NTP-Server, configure the client devices to send Unicast requests or listen for Broadcasts.

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

10.2.1 Preparing the NTP configuration

Perform the following steps:
- To get an overview of how the time is passed on, draw a network plan with the devices participating in NTP. When planning, bear in mind that the accuracy of the time depends on the signal runtime.

![NTP cascading diagram](image)

*Figure 25: NTP cascading*
Synchronizing the system time in the network

10.2 NTP

Enable the NTP function in the devices whose time you want to set using NTP. The NTP server of the device responds to received Unicast requests and sends Broadcast requests as soon as it is configured and enabled.

If no reference clock is available, then specify a device as the reference clock and set its system time as accurately as possible.

10.2.2 NTP configuration

In the Client only frame:
- **Client** – Enable/disable the function
- **Mode** – In the unicast mode the device sends a request to a designated Unicast server and expects a reply from that server. In the broadcast mode, the device sends no request and waits for a Broadcast from one or more Broadcast servers.

In the Client and server frame:
- **Server** – Enable/disable the function
- **Mode** – Set the connection parameters
- **Stratum** – This setting helps prevent other clients from using the device as a reference time source (default setting: 12).

Configure an NTP client, using the example for switch 2. To do this, perform the following steps:

- Open the Time > NTP > Global dialog.
- Before you enable the Client function, disable the Server function. Select the Off radio button in the Client and server frame.
  - To enable the function, select the On radio button in the Client only frame.
- In the Mode field, specify the value unicast.
- Save the changes temporarily. To do this, click the button.
- Open the Time > NTP > Server dialog.
- To create an entry, click the button.
- For switch 2:
  - In the Address column, specify the value 192.168.1.2.
  - To activate the entry, mark the checkbox in the Active column.
- Save the changes temporarily. To do this, click the button.

<table>
<thead>
<tr>
<th>Device</th>
<th>192.168.1.2</th>
<th>192.168.1.3</th>
<th>192.168.1.4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client only frame</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Mode</td>
<td>unicast</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Client and server frame</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>On</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>Mode</td>
<td>client-server</td>
<td>client-server</td>
<td></td>
</tr>
<tr>
<td>ServerAddress</td>
<td>192.168.43.17</td>
<td>192.168.1.2</td>
<td>192.168.43.17</td>
</tr>
</tbody>
</table>
Synchronizing the system time in the network

10.2 NTP

Configure an NTP client server, using the example for switch 1 and 3. To do this, perform the following steps:

- Open the `Time > NTP > Global` dialog.
- Before you enable the `Server` function, disable the `Client` function. Select the `Off` radio button in the `Client only` frame. To enable the function, select the `On` radio button in the `Client and server` frame.
- In the `Mode` field, specify the value `client-server`.
- Save the changes temporarily. To do this, click the button.
- Open the `Time > NTP > Server` dialog.
- To create an entry, click the button.
- For switch 1 and switch 3:
  - In the `Address` column, specify the value `192.168.43.17`.
  - To activate the entry, mark the checkbox in the `Active` column.
- Save the changes temporarily. To do this, click the button.

Configure both switch 1 and 3 with the following commands:

```
enable
configure
ntp client operation enable
ntp server operation enable
ntp server operating-mode client-server
ntp peers add 1 ip 192.168.43.17
```
Synchronizing the system time in the network
10.2 NTP
11 Network load control

The device features a number of functions that can help you reduce the network load:

- Direct packet distribution
- Rate limiter
- Prioritization - QoS
- Flow control

11.1 Direct packet distribution

The device reduces the network load with direct packet distribution.

On each of its ports, the device learns the sender MAC address of received data packets. The device stores the combination “port and MAC address” in its MAC address table (FDB).

By applying the “Store and Forward” method, the device buffers data received and checks it for validity before forwarding it. The device rejects invalid and defective data packets.

11.1.1 Learning MAC addresses

When the device receives a data packet, it checks if the MAC address of the sender is already stored in the MAC address table (FDB). When the MAC address of the sender is unknown, the device generates a new entry. The device then compares the destination MAC address of the data packet with the entries stored in the MAC address table (FDB):

- The device forwards packets with a known destination MAC address directly to ports that have already received data packets from this MAC address.
- The device floods data packets with unknown destination addresses, that is, the device forwards these data packets to every port.

11.1.2 Aging of learned MAC addresses

Addresses that have not been detected by the device for an adjustable period of time (aging time) are deleted from the MAC address table (FDB) by the device. A reboot or resetting of the MAC address table deletes the entries in the MAC address table (FDB).

11.1.3 Static address entries

In addition to learning the sender MAC address, the device also provides the option to set MAC addresses manually. These MAC addresses remain configured and survive resetting of the MAC address table (FDB) as well as rebooting of the device.

Static address entries allow the device to forward data packets directly to selected ports. If you do not specify a destination port, then the device discards the corresponding data packets.
You manage the static address entries in the Graphical User Interface or in the Command Line Interface.

Perform the following steps:

1. Create a static address entry.

- Open the **Switching > Filter for MAC Addresses** dialog.
- Add a user-configurable MAC address:
  - Click the **button**.
  - The dialog displays the **Create** window.
  - In the **Address** field, specify the destination MAC address.
  - In the **VLAN ID** field, specify the ID of the VLAN.
  - In the **Port** list, select the ports to which the device forwards data packets with the specified destination MAC address in the specified VLAN.
  - When you have defined a Unicast MAC address in the **Address** field, select only one port.
  - When you have defined a Multicast MAC address in the **Address** field, select one or more ports.
  - If you want the device to discard data packets with the destination MAC address, then do not select any port.
  - Click the **Ok** button.
- Save the changes temporarily. To do this, click the **button**.

```plaintext
enable
configure
mac-filter <MAC address> <VLAN ID>
interface 1/1
mac-filter <MAC address> <VLAN ID>
save
```

- Convert a learned MAC address into a static address entry.

- Open the **Switching > Filter for MAC Addresses** dialog.
- To convert a learned MAC address into a static address entry, select the value **permanent** in the **Status** column.
- Save the changes temporarily. To do this, click the **button**.

- Disable a static address entry.

- Open the **Switching > Filter for MAC Addresses** dialog.
- To disable a static address entry, select the value **invalid** in the **Status** column.
- Save the changes temporarily. To do this, click the **button**.
enable
configure
interface 1/1
no mac-filter <MAC address> <VLAN ID>
exit
no mac-filter <MAC address> <VLAN ID>
exit
save

☐ Delete learned MAC addresses.

☐ To delete the learned addresses from the MAC address table (FDB), open the Basic Settings > Restart dialog and click the Reset MAC address table button.

clear mac-addr-table

Delete the learned MAC addresses from the MAC address table (FDB).
The rate limiter function helps ensure stable operation even with high traffic volumes by limiting traffic on the ports. The rate limitation is performed individually for each port, as well as separately for inbound and outbound traffic.

If the data rate on a port exceeds the defined limit, then the device discards the overload on this port.

Rate limitation occurs entirely on Layer 2. In the process, the rate limiter function ignores protocol information on higher levels such as IP or TCP. This can affect the TCP traffic.

To minimize these effects, use the following options:
- Limit the rate limitation to certain packet types, for example, Broadcasts, Multicasts, and Unicasts with an unknown destination address.
- Limit the outbound data traffic instead of the inbound traffic. The outbound rate limitation works better with TCP flow control due to device-internal buffering of the data packets.
- Increase the aging time for learned Unicast addresses.

Perform the following steps:

1. Open the **Switching > Rate Limiter** dialog.
2. Activate the rate limiter and set limits for the data rate. The settings apply on a per port basis and are broken down by type of traffic:
   - Received Broadcast data packets
   - Received Multicast data packets
   - Received Unicast data packets with an unknown destination address
   To activate the rate limiter on a port, mark the checkbox for at least one category. In the **Threshold unit** column, you specify if the device interprets the threshold values as percent of the port bandwidth or as packets per second. The threshold value 0 deactivates the rate limiter.
3. Save the changes temporarily. To do this, click the **✓** button.
11.3  QoS/Priority

QoS (Quality of Service) is a procedure defined in IEEE 802.1D which is used to distribute resources in the network. QoS lets you prioritize the data of necessary applications.

When there is a heavy network load, prioritizing helps prevent data traffic with lower priority from interfering with delay-sensitive data traffic. Delay-sensitive data traffic includes, for example, voice, video, and real-time data.

11.3.1  Handling of received priority information

Applications label data packets with the following prioritization information:

- VLAN priority based on IEEE 802.1Q/802.1D (Layer 2)

11.3.2  VLAN tagging

For the VLAN and prioritizing functions, the IEEE 802.1Q standard provides for integrating a MAC frame in the VLAN tag. The VLAN tag consists of 4 bytes and is between the source address field ("Source Address Field") and type field ("Length / Type Field").

Figure 26: Ethernet data packet with tag
For data packets with VLAN tags, the device evaluates the following information:

- Priority information
- When VLANs are configured, VLAN tagging

Data packets with VLAN tags containing priority information but no VLAN information (VLAN ID = 0), are known as Priority Tagged Frames.

**Note:** Network protocols and redundancy mechanisms use the highest traffic class 7. Therefore, select other traffic classes for application data.

When using VLAN prioritizing, consider the following special features:

- End-to-end prioritizing requires the VLAN tags to be transmitted to the entire network. The prerequisite is that every network component is VLAN-capable.
- Routers are not able to send and receive packets with VLAN tags through port-based router interfaces.

### 11.3.3 Setting prioritization

#### Assigning the port priority

Perform the following steps:

1. Open the **Switching > QoS/Priority > Port Configuration** dialog.
2. In the **Port priority** column, you specify the priority with which the device forwards the data packets received on this port without a VLAN tag.
3. Save the changes temporarily. To do this, click the **✓** button.

```shell
enable
configure
interface 1/1
vlan priority 3
exit
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Change to the interface configuration mode of interface 1/1.
Assign interface 1/1 the port priority 3.
Change to the Configuration mode.
Assigning VLAN priority to a traffic class

Perform the following steps:

- Open the Switching > QoS/Priority > 802.1D/p Mapping dialog.
- To assign a traffic class to a VLAN priority, insert the associated value in the Traffic class column.
- Save the changes temporarily. To do this, click the ✓ button.

```
enable
configure
classofservice dot1p-mapping 0 2
classofservice dot1p-mapping 1 2
exit
show classofservice dot1p-mapping
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Assigning a VLAN priority of 0 to traffic class 2.
Assigning a VLAN priority of 1 to traffic class 2.
Change to the Privileged EXEC mode.
Display the assignment.
11.4 Flow control

If a large number of data packets are received in the priority queue of a port at the same time, then this can cause the port memory to overflow. This happens, for example, when the device receives data on a Gigabit port and forwards it to a port with a lower bandwidth. The device discards surplus data packets.

The flow control mechanism described in standard IEEE 802.3 helps ensure that no data packets are lost due to a port memory overflowing. Shortly before a port memory is completely full, the device signals to the connected devices that it is not accepting any more data packets from them.

- In full-duplex mode, the device sends a pause data packet.
- In half-duplex mode, the device simulates a collision.

The following figure displays how flow control works. Workstations 1, 2, and 3 want to simultaneously transmit a large amount of data to Workstation 4. The combined bandwidth of Workstations 1, 2, and 3 is greater than the bandwidth of Workstation 4. This causes an overflow on the receive queue of port 4. The left funnel symbolizes this status.

When the flow control function on ports 1, 2 and 3 of the device is enabled, the device reacts before the funnel overflows. The funnel on the right illustrates ports 1, 2 and 3 sending a message to the transmitting devices to control the transmission speed. This results in the receiving port no longer being overwhelmed and is able to process the incoming traffic.

11.4.1 Halfduplex or fullduplex link

Flow Control with a half duplex link

In the example, there is a halfduplex link between Workstation 2 and the device.

Before the send queue of port 2 overflows, the device sends data back to Workstation 2. Workstation 2 detects a collision and stops transmitting.
Flow Control with a full duplex link

In the example, there is a fullduplex link between Workstation 2 and the device.

Before the send queue of port 2 overflows, the device sends a request to Workstation 2 to include a small break in the sending transmission.

11.4.2 Setting up the Flow Control

Perform the following steps:

- Open the Switching > Global dialog.
- Mark the Flow control checkbox. With this setting you enable flow control in the device.
- Open the Basic Settings > Port dialog, Configuration tab.
- To enable the Flow Control on a port, mark the checkbox in the Flow control column.
- Save the changes temporarily. To do this, click the button.
Network load control
11.4 Flow control
12 VLANs

In the simplest case, a virtual LAN (VLAN) consists of a group of network participants in one network segment who can communicate with each other as though they belonged to a separate LAN.

More complex VLANs span out over multiple network segments and are also based on logical (instead of only physical) connections between network participants. VLANs are an element of flexible network design. It is easier to reconfiguring logical connections centrally than cable connections.

The device supports independent VLAN learning in accordance with the IEEE 802.1Q standard which defines the VLAN function.

Using VLANs has many benefits. The following list displays the top benefits:

- Network load limiting
  VLANs reduce the network load considerably as the devices transmit Broadcast, Multicast, and Unicast packets with unknown (unlearned) destination addresses only inside the virtual LAN. The rest of the data network forwards traffic as normal.
- Flexibility
  You have the option of forming user groups based on the function of the participants apart from their physical location or medium.
- Clarity
  VLANs give networks a clear structure and make maintenance easier.

12.1 Examples of VLANs

The following practical examples provide a quick introduction to the structure of a VLAN.

Note: When configuring VLANs you use an interface for accessing the device management that will remain unchanged. For this example, you use either interface 1/6 or the serial connection to configure the VLANs.
12.1 Examples of VLANs

12.1.1 Example 1

The example displays a minimal VLAN configuration (port-based VLAN). An administrator has connected multiple end devices to a transmission device and assigned them to 2 VLANs. This effectively prohibits any data transmission between the VLANs, whose members communicate only within their own VLANs.

![Figure 29: Example of a simple port-based VLAN](image)

When setting up the VLANs, you create communication rules for every port, which you enter in ingress (incoming) and egress (outgoing) tables.

The ingress table specifies which VLAN ID a port assigns to the incoming data packets. Hereby, you use the port address of the end device to assign it to a VLAN.

The egress table specifies on which ports the device sends the packets from this VLAN.

- **T** = Tagged (with a tag field, marked)
- **U** = Untagged (without a tag field, unmarked)

For this example, the status of the TAG field of the data packets has no relevance, so you use the setting **U**.

<table>
<thead>
<tr>
<th>Terminal</th>
<th>Port</th>
<th>Port VLAN identifier (PVID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>B</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>D</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Port</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>U</td>
</tr>
<tr>
<td>2</td>
<td>U</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>U</td>
</tr>
<tr>
<td>3</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 17: Ingress table

Table 18: Egress table
Perform the following steps:

☐ Setting up the VLAN

☐ Open the **Switching > VLAN > Configuration** dialog.

☐ Click the **Create** button.
   The dialog displays the **Create** window.

☐ In the **VLAN ID** field, specify the value 2.

☐ Click the **Ok** button.

☐ For the VLAN, specify the name **VLAN2**:
   Double-click in the **Name** column and specify the name.
   For VLAN 1, in the **Name** column, change the value **Default** to **VLAN1**.

☐ Repeat the previous steps to create a VLAN 3 with the name **VLAN3**.

```enable
vlan database
vlan add 2
name 2 VLAN2
vlan add 3
name 3 VLAN3
name 1 VLAN1
exit
show vlan brief
```

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>VLAN Name</th>
<th>VLAN Type</th>
<th>VLAN Creation Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VLAN1</td>
<td>default</td>
<td>0 days, 00:00:05</td>
</tr>
<tr>
<td>2</td>
<td>VLAN2</td>
<td>static</td>
<td>0 days, 02:44:29</td>
</tr>
<tr>
<td>3</td>
<td>VLAN3</td>
<td>static</td>
<td>0 days, 02:52:26</td>
</tr>
</tbody>
</table>

☐ Setting up the ports

☐ Open the **Switching > VLAN > Port** dialog.

☐ To assign the port to a VLAN, specify the desired value in the corresponding column.
   Possible values:
   - **T** = The port is a member of the VLAN. The port transmits tagged data packets.
   - **U** = The port is a member of the VLAN. The port transmits untagged data packets.
   - **F** = The port is not a member of the VLAN.
   - **-** = The port is not a member of this VLAN.
   
   Because end devices usually interpret untagged data packets, you specify the value **U**.

☐ Save the changes temporarily. To do this, click the **Save** button.

☐ Open the **Switching > VLAN > Port** dialog.

☐ In the **Port-VLAN ID** column, specify the VLAN ID of the related VLAN:
   2 or 3
Because end devices usually interpret untagged data packets, in the **Acceptable packet types** column, you specify the value **admitAll** for end device ports.

Save the changes temporarily. To do this, click the **✓** button. The value in the **Ingress filtering** column has no affect on how this example functions.

enable
configure
interface 1/1

**vlan participation include 2**

**vlan pvid 2**
exit
interface 1/2

**vlan participation include 3**

**vlan pvid 3**
exit
interface 1/3

**vlan participation include 3**

**vlan pvid 3**
exit
interface 1/4

**vlan participation include 2**

**vlan pvid 2**
exit
exit

```
show vlan id 3
```

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Name</td>
<td>VLAN3</td>
</tr>
<tr>
<td>VLAN Type</td>
<td>Static</td>
</tr>
<tr>
<td>Interface</td>
<td>Current</td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
</tr>
<tr>
<td>1/1</td>
<td>-</td>
</tr>
<tr>
<td>1/2</td>
<td>Include</td>
</tr>
<tr>
<td>1/3</td>
<td>Include</td>
</tr>
<tr>
<td>1/4</td>
<td>-</td>
</tr>
<tr>
<td>1/5</td>
<td>-</td>
</tr>
</tbody>
</table>
12.1.2 Example 2

The second example displays a more complex configuration with 3 VLANs (1 to 3). Along with the Switch from example 1, you use a 2nd Switch (on the right in the example).

![Figure 30: Example of a more complex VLAN configuration](image)

The terminal devices of the individual VLANs (A to H) are spread over 2 transmission devices (Switches). Such VLANs are therefore known as distributed VLANs. If the VLAN is configured correctly, then an optional network management station is also shown, which enables access to every network component.

**Note:** In this case, VLAN 1 has no significance for the end device communication, but it is required for the administration of the transmission devices via what is known as the Management VLAN.

As in the previous example, uniquely assign the ports with their connected terminal devices to a VLAN. With the direct connection between the 2 transmission devices (uplink), the ports transport packets for both VLANs. To differentiate these uplinks you use “VLAN tagging”, which handles the data packets accordingly. Thus, you maintain the assignment to the respective VLANs.

Perform the following steps:
- Add Uplink Port 5 to the ingress and egress tables from example 1.
- Create new ingress and egress tables for the right switch, as described in the first example.

The egress table specifies on which ports the device sends the packets from this VLAN.
- T = Tagged (with a tag field, marked)
- U = Untagged (without a tag field, unmarked)

In this example, tagged packets are used in the communication between the transmission devices (Uplink), as packets for different VLANs are differentiated at these ports.

<table>
<thead>
<tr>
<th>Terminal</th>
<th>Port</th>
<th>Port VLAN identifier (PVID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>B</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>D</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Uplink</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>
The communication relationships here are as follows: end devices on ports 1 and 4 of the left device and end devices on ports 2 and 4 of the right device are members of VLAN 2 and can thus communicate with each other. The behavior is the same for the end devices on ports 2 and 3 of the left device and the end devices on ports 3 and 5 of the right device. These belong to VLAN 3.

The end devices “see” their respective part of the network. Participants outside this VLAN cannot be reached. The device also sends Broadcast, Multicast, and Unicast packets with unknown (unlearned) destination addresses only inside a VLAN.

Here, the devices use VLAN tagging (IEEE 801.1Q) within the VLAN with the ID 1 (Uplink). The letter T in the egress table of the ports indicates VLAN tagging.

The configuration of the example is the same for the device on the right. Proceed in the same way, using the ingress and egress tables created above to adapt the previously configured left device to the new environment.

Perform the following steps:

- Setting up the VLAN

- Open the **Switching > VLAN > Configuration** dialog.
- Click the **Create** button.
  - The dialog displays the **Create** window.
- In the **VLAN ID** field, specify the VLAN ID, for example **2**.

---

**Table 20: Ingress table for device on right**

<table>
<thead>
<tr>
<th>Terminal</th>
<th>Port</th>
<th>Port VLAN identifier (PVID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uplink</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>E</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>F</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>G</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>H</td>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>

**Table 21: Egress table for device on left**

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Port</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>U</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>U</td>
<td>U</td>
<td></td>
<td></td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>U</td>
<td>U</td>
<td>T</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 22: Egress table for device on right**

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Port</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>U</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>T</td>
<td>U</td>
<td>U</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>T</td>
<td>U</td>
<td></td>
<td>U</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Setting up the ports**

- Click the **Ok** button.
- For the VLAN, specify the name **VLAN2**:
  - Double-click in the **Name** column and specify the name.
  - For VLAN 1, in the **Name** column, change the value **Default** to **VLAN1**.
- Repeat the previous steps to create a VLAN 3 with the name **VLAN3**.

```
enable
vlan database
vlan add 2
  name 2 VLAN2
vlan add 3
  name 3 VLAN3
vlan add 1 VLAN1
exit
show vlan brief
```

---

**Max. VLAN ID**................................... 4042
**Max. supported VLANs**........................... 64
**Number of currently configured VLANs**........... 3
**VLAN unaware mode**.............................. disabled

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>VLAN Name</th>
<th>VLAN Type</th>
<th>VLAN Creation Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VLAN1</td>
<td>default</td>
<td>0 days, 00:00:05</td>
</tr>
<tr>
<td>2</td>
<td>VLAN2</td>
<td>static</td>
<td>0 days, 02:44:29</td>
</tr>
<tr>
<td>3</td>
<td>VLAN3</td>
<td>static</td>
<td>0 days, 02:52:26</td>
</tr>
</tbody>
</table>

- Open the **Switching > VLAN > Port** dialog.
- To assign the port to a VLAN, specify the desired value in the corresponding column. Possible values:
  - T = The port is a member of the VLAN. The port transmits tagged data packets.
  - U = The port is a member of the VLAN. The port transmits untagged data packets.
  - F = The port is not a member of the VLAN.
  - - = The port is not a member of this VLAN.

Because end devices usually interpret untagged data packets, you specify the value **U**.
You specify the **T** setting on the uplink port on which the VLANs communicate with each other.

- Save the changes temporarily. To do this, click the **✓** button.
- Open the **Switching > VLAN > Port** dialog.
- In the **Port-VLAN ID** column, specify the VLAN ID of the related VLAN: 1, 2 or 3
- Because end devices usually interpret untagged data packets, in the **Acceptable packet types** column, you specify the value **admitAll** for end device ports.
- For the uplink port, in the **Acceptable packet types** column, specify the value **admitOnlyVlanTagged**.
- Mark the checkbox in the **Ingress filtering** column for the uplink ports to evaluate VLAN tags on this port.
- Save the changes temporarily. To do this, click the **✓** button.
enable
configure
interface 1/1
  vlan participation include 1
  vlan participation include 2
  vlan tagging 2 enable
  vlan participation include 3
  vlan tagging 3 enable
  vlan pvid 1
  vlan ingressfilter
  vlan acceptframe vlanonly
  exit
interface 1/2
  vlan participation include 2
  vlan pvid 2
  exit
interface 1/3
  vlan participation include 3
  vlan pvid 3
  exit
interface 1/4
  vlan participation include 2
  vlan pvid 2
  exit
interface 1/5
  vlan participation include 3
  vlan pvid 3
  exit

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Change to the interface configuration mode of interface 1/1.
The port 1/1 becomes a member of the VLAN 1 and transmits the data packets without a VLAN tag.
The port 1/1 becomes a member of the VLAN 2 and transmits the data packets without a VLAN tag.
The port 1/1 becomes a member of the VLAN 2 and transmits the data packets with a VLAN tag.
The port 1/1 becomes a member of the VLAN 3 and transmits the data packets without a VLAN tag.
The port 1/1 becomes a member of the VLAN 3 and transmits the data packets with a VLAN tag.
Assigning the Port VLAN ID 1 to port 1/1.
Activating ingress filtering on port 1/1.
Port 1/1 only forwards packets with a VLAN tag.
Change to the Configuration mode.
Change to the interface configuration mode of interface 1/2.
The port 1/2 becomes a member of the VLAN 2 and transmits the data packets without a VLAN tag.
Assigning the Port VLAN ID 2 to port 1/2.
Change to the Configuration mode.
Change to the interface configuration mode of interface 1/3.
The port 1/3 becomes a member of the VLAN 3 and transmits the data packets without a VLAN tag.
Assigning the Port VLAN ID 3 to port 1/3.
Change to the Configuration mode.
Change to the interface configuration mode of interface 1/4.
The port 1/4 becomes a member of the VLAN 2 and transmits the data packets without a VLAN tag.
Assigning the Port VLAN ID 2 to port 1/4.
Change to the Configuration mode.
Change to the interface configuration mode of interface 1/5.
The port 1/5 becomes a member of the VLAN 3 and transmits the data packets without a VLAN tag.
Assigning the Port VLAN ID 3 to port 1/5.
Change to the Configuration mode.
exit
show vlan id 3
VLAN ID......................3
VLAN Name....................VLAN3
VLAN Type....................Static
VLAN Creation Time..........0 days, 00:07:47 (System Uptime)
VLAN Routing...............disabled

<table>
<thead>
<tr>
<th>Interface</th>
<th>Current</th>
<th>Configured</th>
<th>Tagging</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>Include</td>
<td>Include</td>
<td>Tagged</td>
</tr>
<tr>
<td>1/2</td>
<td>-</td>
<td>Autodetect</td>
<td>Untagged</td>
</tr>
<tr>
<td>1/3</td>
<td>Include</td>
<td>Include</td>
<td>Untagged</td>
</tr>
<tr>
<td>1/4</td>
<td>-</td>
<td>Autodetect</td>
<td>Untagged</td>
</tr>
<tr>
<td>1/5</td>
<td>Include</td>
<td>Include</td>
<td>Untagged</td>
</tr>
</tbody>
</table>
13 Routing

13.1 Configuration

Because the configuration of a router is very dependent on the conditions in your network, you are first provided with a general list of the individual configuration steps. To optimally cover the large number of options, this list is followed by examples of networks that usually occur in the industry sector.

The configuration of the Routing function usually contains the following steps:

- **Drawing a network plan**
  Create a picture of your network so that you can clearly see the division into subnetworks and the related distribution of the IP addresses. This step is necessary. Good planning of the subnetworks with the corresponding network masks makes the router configuration much easier.

- **Router basic settings**
  Along with the global switching on of the Routing function, the router basic settings also contain the assignment of IP addresses and network masks to the router interfaces.

**Note:** Adhere to the sequence of the individual configuration steps so that the configuration computer has access to every Layer 3 device throughout the entire configuration phase.

**Note:** When you assign an IP address from the subnetwork of the device management IP address to a router interface, the device deletes the IP address of the device management. You access the device management via the IP address of the router interface.

Activate the routing globally before you assign an IP address from the subnetwork of the device management IP address to a router interface.

**Note:** When you assign the VLAN ID of the device management VLAN to a router interface, the device deactivates the IP address of the device management. You access the device management via the IP address of the router interface. The device management VLAN is the VLAN by means of which you access the device management of every device.

**Note:** Depending on your configuration steps, it can be necessary to change the IP parameters of your configuration computer to enable access to the Layer 3 devices.

- **Selecting a routing procedure**
  On the basis of the network plan and the communication requirements of the connected devices, you select the optimal routing procedure (static routes, OSPF) for your situation. In doing so, consider which routing procedures the routers can use along a route.

- **Configuring a routing procedure**
  Configure the selected routing procedure.
13.2  Routing - Basics

A router is a node for exchanging data on the Layer 3 of the ISO/OSI reference model.

This ISO/OSI reference model had the following goals:

- To define a standard for information exchange between open systems;
- To provide a common basis for developing additional standards for open systems;
- To provide international teams of experts with functional framework as the basis for independent development of every layer of the model;
- To include in the model developing or already existing protocols for communications between heterogeneous systems;
- To leave sufficient room and flexibility for the inclusion of future developments.

The OSI reference model consists of 7 layers, ranging from the application layer to the physical layer.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application Access to communication services from an application program</td>
</tr>
<tr>
<td>6</td>
<td>Presentation Definition of the syntax for data communication</td>
</tr>
<tr>
<td>5</td>
<td>Session Set up and breakdown of connections by synchronization and organization of the dialog</td>
</tr>
<tr>
<td>7</td>
<td>Transport Specification of the terminal connection, with the necessary transport quality</td>
</tr>
<tr>
<td>3</td>
<td>Network Transparent data exchange between two transport entities</td>
</tr>
<tr>
<td>2</td>
<td>Data-Link Access to physical media and detection of transmission errors</td>
</tr>
<tr>
<td>1</td>
<td>Physical Transmission of bit strings via physical media</td>
</tr>
</tbody>
</table>

What does the data exchange on the Layer 3 mean in comparison with the data exchange on the Layer 2?

On the Layer 2, the MAC address signifies the destination of a data packet. The MAC address is an address tied to the hardware of a device. The Layer 2 expects the receiver in the connected network. The data exchange to another network is the task of Layer 3. Layer 2 data traffic is spread over the entire network. Every subscriber filters the data relevant for him from the data stream. Layer 2 devices are capable of steering the data traffic that is intended for a specific MAC address. It thus relieves some of the load on the network. Broadcast and multicast data packets are forwarded by the Layer 2 devices on every port.
IP is a protocol on the Layer 3. IP provides the IP address for addressing data packets. The IP address is assigned by the network administrator. By systematically assigning IP addresses, he can thus structure his network, breaking it down into subnets (see on page 159 “CIDR”). The bigger a network gets, the greater the data volume. Because the available bandwidth has physical limitations, the size of a network is also limited. Dividing large networks into subnets limits the data volume on these subnets. Routers divide the subnets from each other and only transmit the data that is intended for another subnet.

Figure 32: MAC Data Transmission: Unicast Data Packet (left) and Broadcast Data Packet (right)

This illustration clearly shows that broadcast data packets can generate a considerable load on larger networks. You also make your network easier to understand by forming subnets, which you connect with each other using routers and, strange as it sounds, also separate securely from each other.

A switch uses the MAC destination address to transmit, and thus uses Layer 2. A router uses the IP destination address to transmit, and thus uses Layer 3.

The subscribers associate the MAC and IP addresses using the Address Resolution Protocol (ARP).

13.2.1 ARP

The Address Resolution Protocol (ARP) determines the MAC address that belongs to an IP address. What is the benefit of this?

Let’s suppose that you want to configure the device using the Web-based interface. You enter the IP address of the device in the address line of your browser. But which MAC address will your PC now use to display the information in the device in your browser window?

If the IP address of the device is in the same subnetwork as your PC, then your PC sends what is known as an ARP request. This is a MAC broadcast data packet that requests the owner of the IP address to send back his MAC address. The device replies with a unicast data packet containing its MAC address. This unicast data packet is called an ARP reply.

Figure 33: ARP request and reply
When the IP address of the device is in a different subnetwork, the PC asks for the MAC address of the gateway entered in the PC. The gateway/router replies with its MAC address.

Now the PC packs the IP data packet with the IP address of the device, the final destination, into a MAC frame with the MAC destination address of the gateway/router and sends the data.

The router receives the data and releases the IP data packet from the MAC frame, so that it can then forward it in accordance with its transmission rules.

All end devices still working with IPs of the first generation, for example, are not yet familiar with the term 'subnet'. When they are looking for the MAC address for an IP address in a different subnet, they also send an ARP request. They neither have a network mask with which they could recognize that the subnet is a different one, nor do they have a gateway entry. In the example below, the left PC is looking for the MAC address of the right PC, which is in a different subnet. In this example, it would normally not get a reply.

Because the router knows the route to the right PC, the Proxy ARP function replies to this router interface on behalf of the right PC with its own MAC address. Thus the left PC can address its data to the MAC address of the router, which then forwards the data to the right PC.

The Proxy ARP function is available on the router interfaces on which you enable the proxy ARP.

Note: The 1:1 NAT function also lets you integrate the devices into a larger L3 network.
13.2.2 CIDR

The original class allocation of the IP addresses only planned for three address classes to be used by the users.

Since 1992, five classes of IP address have been defined in the RFC 1340.

Table 24: IP address classes

<table>
<thead>
<tr>
<th>Class</th>
<th>Network part</th>
<th>Host part</th>
<th>Address range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1 byte</td>
<td>3 bytes</td>
<td>1.0.0.0 … 126.255.255.255</td>
</tr>
<tr>
<td>B</td>
<td>2 bytes</td>
<td>2 bytes</td>
<td>128.0.0.0 … 191.255.255.255</td>
</tr>
<tr>
<td>C</td>
<td>3 bytes</td>
<td>1 byte</td>
<td>192.0.0.0 … 223.255.255.255</td>
</tr>
<tr>
<td>D</td>
<td></td>
<td></td>
<td>224.0.0.0 … 239.255.255.255</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td></td>
<td>240.0.0.0 … 255.255.255.255</td>
</tr>
</tbody>
</table>

Class C with a maximum of 254 addresses was too small, and class B with a maximum of 65534 addresses was too large for most users, as they would not require so many addresses. This resulted in ineffective usage of the class B addresses available.

Class D contains reserved multicast addresses. Class E is reserved for experimental purposes. A gateway not participating in these experiments ignores datagrams with this destination address.

The Classless Inter-Domain Routing (CIDR) provides a solution to these problems. The CIDR overcomes these class boundaries and supports classless address ranges.

With CIDR, you enter the number of bits that designate the IP address range. You represent the IP address range in binary form and count the mask bits that designate the network mask. The network mask indicates the number of bits that are identical for every IP address, the network part, in a given address range. Example:

<table>
<thead>
<tr>
<th>IP address, decimal</th>
<th>Network mask, decimal</th>
<th>IP address, binary</th>
</tr>
</thead>
<tbody>
<tr>
<td>149.218.112.1</td>
<td>255.255.255.128</td>
<td>10010101 11011010 01110000 00000001</td>
</tr>
<tr>
<td>149.218.112.127</td>
<td></td>
<td>10010101 11011010 01110000 01111111</td>
</tr>
<tr>
<td></td>
<td>Mask bits</td>
<td>25 mask bits</td>
</tr>
</tbody>
</table>

CIDR notation: 149.218.112.0/25

The combination of a number of class C address ranges is known as “supernetting”. This enables you to subdivide class B address ranges to a very fine degree.

Using mask bits simplifies the routing table. The router determines in that direction in which most of the mask bits match (longest prefix match).
13.2.3 Multinetting

Multinetting lets you connect a number of subnets to one router port. When you want to connect existing subnets to a router within a physical medium, multinetting provides a solution. In this case you can use multinetting to assign a number of IP addresses for the different subnets to the routing port to which you are connecting the physical medium.

For a long-term solution, other network design strategies provide more advantages with regard to problem solving and bandwidth management.

Figure 36: Example of multinetting
13.3 Static Routing

Static routes are user-defined routes which the router uses to transmit data from one subnet to another.

You specify to which router (next hop) the local router forwards data for a particular subnet. Static routes are kept in a table which is permanently stored in the router.

Compared to dynamic routing, the advantage of this transparent route selection is offset by the increased workload involved in configuring the static routes. Static routing is therefore suited to very small networks or to selected areas of larger networks. Static routing makes the routes transparent for the administrator and can be easily configured in small networks.

If, for example, a line interruption causes the topology to change, then the dynamic routing can react automatically to this, in contrast to the static routing. When you combine static and dynamic routing, you can configure the static routes in such a way that they have a higher priority than a route selected by a dynamic routing procedure.

The first step in configuring the router is to globally enable the Routing function and configure the router interfaces.

The device lets you define port-based and VLAN-based router interfaces (see figure 37).

Example: Connecting two production cells

![Figure 37: Static routes](image)

13.3.1 Port-based Router Interface

A characteristic of the port-based router interface is that a subnet is connected to a port (see figure 37).

Special features of port-based router interfaces:
- When there is no active connection, the entry is omitted from the routing table, because the router transmits only to those ports for which the data transfer is likely to be successful. The entry in the interface configuration table remains.
- A port-based router interface does not recognize VLANs, which means that the router rejects tagged packets which it receives on a port-based router interface.
- A port-based router interface rejects the non-routable packets.

Below (see figure 38) you will find an example of the simplest case of a routing application with port-based router interfaces.
Configuration of the router interfaces

Perform the following steps:

```
enable
configure
interface 2/1
   ip address primary 10.0.1.1 255.255.255.0
   ip routing
   exit
interface 2/2
   ip address primary 10.0.2.1 255.255.255.0
   ip routing
   exit
show ip interface 2/1
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Change to the interface configuration mode of interface 2/1.
Assign the interface its primary IP parameters.
Activate the **Routing** function on this interface.
Change to the Configuration mode.
Change to the interface configuration mode of interface 2/2.
Assign the interface its IP parameters.
Activate the **Routing** function on this interface.
Enable the **Routing** function globally.
Change to the Privileged EXEC mode.
Check the entries on interface 2/1.

```
Routing Mode............................. enabled
Admin mode............................... manual
IP address............................... 10.0.1.1/255.255.255.0
Secondary IP address(es).............. none
Proxy ARP................................. disabled
MAC Address............................. EC:E5:F6:3E:09
IP MTU.................................. 1500
ICMP Redirect........................... enabled
ICMP Unreachable......................... enabled
Admin State.............................. enabled
Link State............................... up
```

**Verify the routing table:**

```
Network Address    Protocol  Next Hop IP  Next Hop If  Pref  Active
-----------------  ---------  -----------  ------  -----  ----
10.0.1.0/24    Local     10.0.1.1     2/1          0     [x]
10.0.2.0/24    Local     10.0.2.1     2/2          0     [x]
```

**Note:** To be able to see these entries in the routing table, you need an active connection on the interfaces.
13.3.2 VLAN-based Router-Interface

A characteristic of the VLAN-based router interface is that a number of devices in a VLAN are connected to different ports.

Within a VLAN, the switch exchanges data packets on Layer 2.

Terminal devices address data packets with a destination address in another subnet to the router. The device then exchanges the data packets on Layer 3.

Below you will find an example of the simplest case of a routing application with VLAN-based router interfaces. For VLAN 2, the router combines interfaces 3/1 and 3/2 into the VLAN router interface vlan/2. A VLAN router interface remains in the routing table as long as at least one port of the VLAN has a connection.

Figure 39: VLAN-based router interface

Configure a VLAN router interface. To do this, perform the following steps:

☐ Create a VLAN and assign ports to the VLAN.
☐ Create a VLAN-based router interface.
☐ Assign an IP address to the VLAN-based router interface.
☐ Activate routing on the VLAN-based router interface.
☐ Enable the Routing function globally.

```
enable
vlan database
vlan add 2
name 2 VLAN2
routing add 2
exit
show ip interface
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address</th>
<th>IP Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan/2</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

```
configure
interface vlan/2
ip address primary 10.0.2.1 255.255.255.0
ip routing
exit
```

Change to the Privileged EXEC mode.

Change to the VLAN configuration mode.

Create a VLAN by entering the VLAN ID. The VLAN ID range is between 1 to 4094.

Assign the name VLAN2 to the VLAN.

Create a virtual router interface and activate the Routing function on this interface.

Change to the Privileged EXEC mode.

Check the entry for the virtual router interface.

```
configure
interface 3/1
```

Change to the Configuration mode.

Change to the interface configuration mode of interface vlan/2.

Assign the IP parameters to the virtual router interface.

Activate the Routing function on this interface.

Change to the Configuration mode.

Change to the interface configuration mode of interface 3/1.
Remove port 3/1 from VLAN 1. In the default setting, every port is assigned to VLAN 1.

Declare port 3/1 a member of VLAN 2.

Specify port VLAN ID 2. Therefore, the device assigns data packets that the port receives without a VLAN tag to VLAN 2.

Change to the Configuration mode.

Change to the interface configuration mode of interface 3/2.

Remove port 3/2 from VLAN 1. In the default setting, every port is assigned to VLAN 1.

Declare port 3/2 a member of VLAN 1.

Specify port VLAN ID 2. Therefore, the device assigns data packets that the port receives without a VLAN tag to VLAN 2.

Change to the Configuration mode.

Enable the Routing function globally.

Change to the Privileged EXEC mode.

Check your entries in the static VLAN table.

Open the Routing > Interfaces > Configuration dialog.

Click the button.

The dialog displays the Configure VLAN router interface window.

In the VLAN ID field, specify a number in the range between 1 and 4042.

For this example, specify the value 2.

Click the Next button.
In the **Name** field, specify the name of the VLAN. For this example, specify the value **VLAN002**.

In the **Member** column, mark the check box of the ports which will belong to this VLAN. For this example, mark the check box of port 3/1 and port 3/2.

Click the **Next** button.

In the **Primary address** frame, **Address** field, specify the IP address for the router interface. For this example, specify the value **10.0.2.1**.

In the **Primary address** frame, **Netmask** field, specify the corresponding netmask. For this example, specify the value **255.255.255.0**.

To apply the changes, click the **Finish** button.

In the **Routing > Interfaces > Configuration** dialog, the table displays the virtual router interface **vlan/2**.

In the **Switching > VLAN > Configuration** dialog, the table displays the VLAN **VLAN002**.

Save the changes temporarily. To do this, click the **button.

You delete a router interface highlighted in the **Routing > Interfaces > Configuration** dialog by clicking the **button.

- After deleting a VLAN router interface the associated VLAN is maintained. In the **Switching > VLAN > Configuration** dialog, the table still displays the VLAN.
- After deleting a VLAN in the **Switching > VLAN > Configuration** dialog, the device also deletes the associated VLAN router interface.

### 13.3.3 Configuration of a Static Route

In the example below, router A requires the information that it can reach the subnet 10.0.3.0/24 via the router B (next hop). It can obtain this information via a dynamic routing protocol or via a static routing entry. With this information, router A can transmit data from subnet 10.0.1.0/24 via router B into subnet 10.0.3.0/24.

Vice versa to be able to forward data of subnet 10.0.1.0/24 router B also needs an equivalent route.

**Figure 40: Static Routing**

You can enter static routing for port-based and VLAN-based router interfaces.

### Configuration of a simple static route

Enter a static route for router A based on the configuration of the router interface in the previous example (see figure 38). To do this, perform the following steps:

```plaintext
enable
configure
ip route add 10.0.3.0 255.255.255.0 10.0.2.2
```

Change to the Privileged EXEC mode.

Change to the Configuration mode.

Create the static routing entry.
Enter a static route for router A based on the configuration of the router interface in the previous example (see figure 38):

1. Configure router B in the same way.

**Configuration of a redundant static route**

To establish a stable connection between the two routers, you can connect the two routers with two or more links.

![Redundant static route diagram](image)

You have the option of assigning a Preference (distance) to a route. When there are a number of routes to a destination, the router chooses the route with the highest Preference.

Perform the following steps on router A:

```
enable
configure
interface 2/3
ip address primary 10.0.4.1 255.255.255.0
ip routing
exit
ip route add 10.0.3.0 255.255.255.0 10.0.4.2 preference 2
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Select the port at which you want to connect the redundant route.
Assign the IP parameters to the port.
Activate the Routing function on this interface.
Change to the Configuration mode.
Create the static routing entry for the redundant route. The value 2 at the end of the command indicates the Preference value.
When both routes are available, the router uses the route via subnetwork 10.0.2.0/24, because this route has the higher preference (see on page 165 “Configuration of a simple static route”).
You have the option of changing the default value of the Preference. When you do not assign a value for the Preference during the configuration, the router uses the default value.

```
ip route distance
show ip route all
```

Sets the default preference for static routes. (default setting: 1)
Verify the routing table:

<table>
<thead>
<tr>
<th>Network Address</th>
<th>Protocol</th>
<th>Next Hop IP</th>
<th>Next Hop If</th>
<th>Pref</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.1.0</td>
<td>Local</td>
<td>10.0.1.1</td>
<td>2/1</td>
<td>1</td>
<td>[x]</td>
</tr>
<tr>
<td>10.0.2.0</td>
<td>Local</td>
<td>10.0.2.1</td>
<td>2/2</td>
<td>1</td>
<td>[x]</td>
</tr>
<tr>
<td>10.0.3.0</td>
<td>Static</td>
<td>10.0.2.2</td>
<td>2/2</td>
<td>1</td>
<td>[x]</td>
</tr>
<tr>
<td>10.0.3.0</td>
<td>Static</td>
<td>10.0.4.2</td>
<td>-</td>
<td>2</td>
<td>[ ]</td>
</tr>
<tr>
<td>10.0.4.0</td>
<td>Local</td>
<td>10.0.4.1</td>
<td>2/3</td>
<td>1</td>
<td>[x]</td>
</tr>
</tbody>
</table>

Configure router B in the same way.

**Configuration of a redundant static route with load sharing**

When the routes have the same Preference (distance), the router shares the load between the 2 routes (load sharing). To do this, perform the following steps:

```
enable
configure
ip route modify 10.0.3.0 255.255.255.0
10.0.2.2 preference 2
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Assigns a Preference of 2 to the existing static routing entry (see on page 165 “Configuration of a simple static route”).
When both routes are available, the router uses both routes for the data transmission.
Verify the routing table:

<table>
<thead>
<tr>
<th>Network Address</th>
<th>Protocol</th>
<th>Next Hop IP</th>
<th>Next Hop If</th>
<th>Pref</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.1.0</td>
<td>Local</td>
<td>10.0.1.1</td>
<td>2/1</td>
<td>1</td>
<td>[x]</td>
</tr>
<tr>
<td>10.0.2.0</td>
<td>Local</td>
<td>10.0.2.1</td>
<td>2/2</td>
<td>1</td>
<td>[x]</td>
</tr>
<tr>
<td>10.0.3.0</td>
<td>Static</td>
<td>10.0.2.2</td>
<td>2/2</td>
<td>2</td>
<td>[x]</td>
</tr>
<tr>
<td>10.0.3.0</td>
<td>Static</td>
<td>10.0.4.2</td>
<td>2/3</td>
<td>2</td>
<td>[x]</td>
</tr>
<tr>
<td>10.0.4.0</td>
<td>Local</td>
<td>10.0.4.1</td>
<td>2/3</td>
<td>1</td>
<td>[x]</td>
</tr>
</tbody>
</table>
### 13.3.4 Static route tracking

#### Description of the static route tracking function

With static routing, when there are a number of routes to a destination, the router chooses the route with the highest preference. The router detects an existing route by the state of the router interface. While connection L 1 on the router interface can be fine, the connection to remote router B via L 2 can be interrupted. In this case, the router continues transmitting via the interrupted route.

![Figure 42: Example of static route tracking](image)

With the static route tracking function, the router uses a tracking object such as a ping tracking object to detect the connection interruption. The active static route tracking function then deletes the interrupted route from the current routing table. When the tracking object returns to the up state, the router enters the static route in the current routing table again.

#### Application example for the static route tracking function

The figure displays an example of the static route tracking function (see figure 43).

Router A monitors the best route via L 1 with ping tracking. If there is a connection interruption, then router A transmits using the redundant connection L 3.

For the example the following information is known:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Router A</th>
<th>Router B</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address interface (IF) 1/1</td>
<td>10.0.4.1</td>
<td>10.0.4.2</td>
</tr>
<tr>
<td>IP address interface (IF) 1/2</td>
<td>10.0.2.1</td>
<td>10.0.2.53</td>
</tr>
<tr>
<td>IP address interface (IF) 1/4</td>
<td>10.0.1.112</td>
<td>10.0.5.1</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>
Figure 43: Configuring static route tracking

The following list contains prerequisites for further configuration:

- The IP parameters of the router interfaces are configured. (see on page 162 “Configuration of the router interfaces”)
- The Routing function is activated globally and on the router interface.
- Ping tracking on interface 1/2 of router A is configured (see on page 184 “Ping tracking”).

Perform the following steps:

- Create the tracking objects on router A for the routes to the destination network 10.0.5.0/24. The default values, entered in the other cells, remain unchanged for this example.

  - Open the Routing > Tracking > Configuration dialog.
  - Click the button. The dialog displays the Create window.
  - Enter the data for the first tracking rule:
    - Type: ping
    - Track ID: 1
  - Click the Ok button.
  - In the ping-1 row, IP address column, specify the IP address 10.0.2.53.
  - In the ping-1 row, Ping port column, specify the interface 1/2.
  - To activate the row, mark the Active checkbox.
  - Click the button. The dialog displays the Create window.
  - Enter the data for the first static route:
    - Type: ping
    - Track ID: 2
  - Click the Ok button.
  - In the ping-2 row, IP address column, specify the IP address 10.0.4.2.
  - In the ping-2 row, Ping port column, specify the interface 1/1.
  - To activate the row, mark the Active checkbox.
  - To temporarily save the settings, click the button.

<table>
<thead>
<tr>
<th>enable</th>
<th>Change to the Privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td>Change to the Configuration mode.</td>
</tr>
<tr>
<td>track add ping 1</td>
<td>Create a tracking object with track ID 1.</td>
</tr>
<tr>
<td>track modify ping 1</td>
<td>Modify the ping1 entry with the IP address 10.0.2.53.</td>
</tr>
<tr>
<td>address 10.0.2.53</td>
<td>Set the source interface number of the ping tracking instance to 1/2.</td>
</tr>
<tr>
<td>track modify ping 1</td>
<td>Activate the tracking object.</td>
</tr>
<tr>
<td>interface 1/2</td>
<td></td>
</tr>
<tr>
<td>track enable ping 1</td>
<td></td>
</tr>
</tbody>
</table>
track add ping 2
track modify ping 2 address 10.0.4.2
track modify ping 2 interface 1/1
track enable ping 2
exit
show track ping

Note: In order to activate the row, verify that the link on the interface is up.

Next enter the routes to the destination network 10.0.5.0/24 in the static routing table of router A.

Open the Routing > Routing Table dialog.

Click the button.
The dialog displays the Create window.

Enter the data for the first static route:
Network address: 10.0.5.0
Netmask: 255.255.255.0
Next hop IP address: 10.0.2.53
Preference: 1
Track name: ping-1

Click the Ok button.

Click the button.
The dialog displays the Create window.

Enter the data for the first static route:
Network address: 10.0.5.0
Netmask: 255.255.255.0
Next hop IP address: 10.0.4.2
Preference: 2
Track name: ping-2

Click the Ok button.

To temporarily save the settings, click the button.

Note: To make the configuration available even after a restart, save the settings permanently in the Basic Settings > Load/Save dialog.
On router B, create a ping tracking object with the track ID, for example 22, for IP address 10.0.2.1.

Enter the two routes to destination network 10.0.1.0/24 in the static routing table of router B.

Table 25: Static routing entries for router B

<table>
<thead>
<tr>
<th>Destination Network</th>
<th>Destination Netmask</th>
<th>Next Hop</th>
<th>Preference</th>
<th>Track ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.1.0</td>
<td>255.255.255.0</td>
<td>10.0.2.1</td>
<td>1</td>
<td>22</td>
</tr>
<tr>
<td>10.0.1.0</td>
<td>255.255.255.0</td>
<td>10.0.4.1</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>
13.4 NAT – Network Address Translation

The Network Address Translation (NAT) protocol describes a procedure for automatically and transparently changing IP address information in data packets while still transmitting the data packets to their precise destination.

When you do not want IP addresses of an internal network to be visible from outside, use NAT. The reasons for this can include, for example:

- Keeping the structure of the internal network hidden from the outside world.
- Keeping private IP addresses hidden.
- Using IP addresses multiple times – by forming identical production cells, for example.

Depending on your reason for using NAT, it offers you various procedures for using the IP address information. In the following sections, you will find additional information on this process.

13.4.1 Applying the NAT Rules

The device provides a multi-step approach to set up and apply the NAT rules:

- Create rule.
- Assign rule to a router interface.
  - Up to this step, changes have no effect on the behavior of the device and the data stream.
- Apply the rule to the data stream.

The data packets go through the filter functions of the device in the following sequence:

![Figure 44: Processing sequence of the data packets in the device](#)
13.4.2 1:1 NAT

The 1:1 NAT function lets you establish communication links within a local network to devices that are actually located in other networks. The NAT router virtually “shifts” the devices into the public network. To accomplish this, the NAT router replaces the virtual with the actual IP address in the data packet while sending it. A typical application is the connecting of several identically structured production cells with the same IP address to a server farm.

The prerequisite for the 1:1 NAT process is that the NAT router itself responds to ARP requests. To make this happen, activate the Proxy ARP function on the ingress interface.

**Figure 45: How the 1:1 NAT function works**

**Note:** With the 1:1 NAT function the device responds to ARP requests from the external network to addresses which it maps from the internal network. This is also the case where no device with the IP address exists in the internal network. Therefore, in the external network, only allocate to devices IP addresses located outside the area which the 1:1 NAT function maps from the internal network to the external network.

**Application example for 1:1 NAT**

You have multiple identical production cells and want to connect them with the host computer. As even the IP addresses used in the production cells are identical, you convert the IP addresses using the 1:1 NAT function.

**Figure 46: Connect identical production cells with the host computer (application example)**

**Prerequisites for further configuration:**
- You need two NAT routers.
- The Routing function is enabled in every device.
- Two router interfaces are configured in every device. One router interface is connected to the company network and one to the network of the production cell.
- The IP address and gateway are set in the devices of the production cell. The devices use the IP address of the egress interface of the NAT router as the gateway.

Perform the following steps:

- Open the **Routing > Interfaces > Configuration** dialog.
- On the router interface that is connected to the company network, mark the checkbox in the **Proxy ARP** field.
- Save the changes temporarily. To do this, click the **✓** button.

- Generate rule.

- Open the **Routing > NAT > 1:1 NAT > Rule** dialog.
- Add a table entry. To do this, click the **✓** button. The dialog displays the **Create** window.
- In the **Destination address** field, specify the virtual IP address of the device in the production cell. In the example this is **192.168.1.100** in NAT router 1 and **192.168.1.200** in NAT router 2.
- In the **New destination address** field, specify the IP address of the device in the production cell. In the example this is **192.168.2.100** in NAT router 1 and NAT router 2.
- Click the **Ok** button.
- In the **Rule name** column, specify the name of the NAT rule.
- In the **Priority** column, specify any value between 1 and 6500.
- In the **Ingress interface** column, select the router interface that is connected to the company network.
- In the **Egress interface** column, select the router interface connected with the production cell.
- Save the changes temporarily. To do this, click the **✓** button.

- Activate the rule.

- Mark the checkbox in the **Active** column.
- Save the changes temporarily. To do this, click the **✓** button.

- Apply the rule to the data stream.

- Open the **Routing > NAT > NAT Global** dialog.
- Click the **✓** button and then the **Commit changes** item.

When changes to the rules affect existing entries in the state table of the firewall, it helps to clear the state table. See the **Clear firewall table** button in the **Basic Settings > Restart** dialog. It is possible, that the device interrupts open communication connections.
13.4.3  Destination NAT

The Destination NAT function lets you divert the data stream of outgoing communication links to or through a server in a local network.

A special form of the Destination NAT function is port forwarding. You use port forwarding to hide the structure of a network from the outside while still allowing communication links from the outside into the network. A typical application is remote control of a PC in a production cell. The maintenance station establishes the communication link to the NAT router, and the Destination NAT function takes care of the routing to the production cell.

Figure 47: How the Destination NAT function works

Application example for port forwarding

You have a production cell. The network of the production cell is not visible on the company network. The NAT router establishes the connection between the production cell and the company network. To allow an administrator from the company network to manage a server in the production cell, use the port forwarding function.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Administrator PC</th>
<th>NAT router</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.2.55</td>
<td>192.168.2.8</td>
<td>192.168.1.8</td>
</tr>
<tr>
<td>Gateway</td>
<td>192.168.2.55</td>
<td>192.168.2.8</td>
<td>192.168.1.1</td>
</tr>
</tbody>
</table>
Prerequisites for further configuration:

- The *Routing* function is enabled in the device.
- In the device, a router interface is set up and connected to the company network.
- In the devices in the production cell, the IP address and gateway are defined. The devices use the IP address of port 1 of the NAT router as the gateway.
Perform the following steps:

☐ Generate rule.

☐ Open the **Routing > NAT > Destination NAT > Rule** dialog.

☐ Add a table entry. To do this, click the **Create** button. The dialog displays the **Create** window.

☐ In the **New destination address** field, specify the IP address of the server in the production cell. In the example this is **192.168.1.8**. The NAT router forwards the connection to this address.

☐ Click the **Ok** button.

☐ In the **Rule name** field, specify the name of the NAT rule.

☐ In the **Destination address** field, specify the IP address of the router interface in the company network. In the example this is **192.168.2.8**. The PC of the administrator establishes the connection to this address.

☐ In the **Destination port** field, specify the port number. In the example this is **8080**. The PC of the administrator establishes the connection to this port.

☐ In the **New destination port** field, specify the port number. In the example this is **80**. The NAT router forwards the connection to this port.

☐ To forward connections only from the PC of the administrator to the server in the production cell, change the value in the **Source address** field to the IP address of the PC. In the example this is **192.168.2.55**. Otherwise, leave the value **any**.

☐ To forward only TCP data packets to the server in the production cell, change the value in the **Protocol** field to **tcp**. Otherwise, leave the value **any**.

☐ Save the changes temporarily. To do this, click the **Ok** button.

☐ Activate the rule.

☐ Mark the checkbox in the **Active** column to enable the created rule.

☐ Save the changes temporarily. To do this, click the **Ok** button.

☐ Assign rule to a router interface.

☐ Open the **Routing > NAT > Destination NAT > Mapping** dialog.

☐ Click the **Assign** button.

☐ In the **Port** field, select the router interface that is connected to the company network.

☐ Select the created rule in the **Rule index** field.

☐ Click the **Ok** button.

☐ Activate assignment of the rule to the router interface.

☐ Mark the checkbox in the **Active** column to activate assignment of the rule to the router interface.

☐ Save the changes temporarily. To do this, click the **Ok** button.

☐ Apply the rule to the data stream.
13.4.4 Masquerading NAT

The Masquerading NAT function hides any number of devices behind the IP address of the NAT router and thus hides the structure of a network from other networks. To accomplish this, the NAT router replaces the sender address in the data packet with its own IP address. In addition, the NAT router replaces the source port in the data packet with its own value in order to send the response data packets back to the original sender at a later point.

Adding the port information also gave the IP Masquerading the name “Network Address Port Translation” (NAPT).

The devices establish communication links to the outside from the hidden network by converting the IP address. However, it is not possible to establish a connection in the other direction, because the devices outside only know the external IP address of the NAT router.

Note: If you enable the VRRP function on a router interface, then the Masquerading NAT function is ineffective on this router interface.
Double NAT

The Double NAT function lets you establish communication links between end devices located in different IP networks, which have no way to specify a default gateway or default route. The NAT router virtually "shifts" the devices into the other network. To accomplish this, the NAT router replaces the source address and the destination address in the data packet during sending. A typical application is the linking of controllers located in different networks.

The Double NAT function requires that the NAT router itself responds to ARP requests from the respective network. To make this happen, activate the Proxy ARP function on the ingress interface and on the egress interface.

The figure shows which IP addresses the devices use to communicate with each other and how the NAT router changes the IP addresses:

- The device on the left sends a data packet to the device on the right.
  - The data packet contains the source address 192.168.1.8 and the destination address 192.168.1.100.
  - The NAT router replaces both addresses.
  - The data packet that the device on the right receives contains the source address 192.168.2.8 and the destination address 192.168.2.100.

- In the reverse direction, the device on the right sends a data packet to the device on the left.
  - The data packet contains the source address 192.168.2.100 and the destination address 192.168.2.8.
  - The NAT router replaces both addresses.
  - The data packet that the device on the left receives contains the source address 192.168.1.100 and the destination address 192.168.1.8.

The NAT router changes the source and destination addresses in the data packets. Both devices communicate with each other in the same network, even though they are actually in different networks.
Application example for Double NAT

You want to connect the device on the left (a workstation in the company network, for example) with the device to the right (a robot controller in the production cell, for example). The robot controller only communicates with devices on the same logical network. When communicating between the networks, the NAT router translates the IP addresses.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Device on the left</th>
<th>Device on the right</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local internal IP address</strong></td>
<td>192.168.1.8</td>
<td></td>
</tr>
<tr>
<td><strong>Local external IP address</strong></td>
<td>192.168.2.8 (virtual)</td>
<td></td>
</tr>
<tr>
<td><strong>Remote internal IP address</strong></td>
<td>192.168.2.100</td>
<td></td>
</tr>
<tr>
<td><strong>Remote external IP address</strong></td>
<td>192.168.1.100 (virtual)</td>
<td></td>
</tr>
</tbody>
</table>

Prerequisites for further configuration:

- The Routing function is enabled in the device.
- Two router devices are configured in the device. One router interface is connected to the company network and one to the network of the production cell.
- The IP address is set in the device on the left and in the device on the right.
Perform the following steps:

- **Activate the Proxy ARP function on the router interfaces.**

- Open the Routing > Interfaces > Configuration dialog.
  - On the router interfaces that are connected to the company network and to the production cell, mark the checkbox in the Proxy ARP field.
  - Save the changes temporarily. To do this, click the ✅ button.

- **Generate rule.**

- Open the Routing > NAT > Double NAT > Rule dialog.
  - Add a table entry. To do this, click the ✪ button. The dialog displays the Create window.
  - In the Local internal IP address field, specify the IP address of the device on the left in the company network. In the example this is 192.168.1.8.
  - In the Local external IP address field, specify the virtual IP address of the device on the left in the production cell. In the example this is 192.168.2.8.
  - In the Remote internal IP address field, specify the IP address of the device on the right in the production cell. In the example this is 192.168.2.100.
  - In the Remote external IP address field, specify the virtual IP address of the device on the right in the company network. In the example this is 192.168.1.100.
  - Click the Ok button.
  - In the Rule name field, specify the name of the NAT rule.
  - Save the changes temporarily. To do this, click the ✅ button.

- **Activate the rule.**

- Mark the checkbox in the Active column to enable the created rule.
  - Save the changes temporarily. To do this, click the ✅ button.

- **Assign the rule to the ingress interface connected to the company network.**

- Open the Routing > NAT > Double NAT > Mapping dialog.
  - Click the Assign button.
  - In the Port field, select the router interface that is connected to the company network.
  - Select the value ingress in the Direction field.
  - Select the created rule in the Rule index field.
  - Click the Ok button.

- **Assign the rule to the egress interface connected to the production cell.**

- Open the Routing > NAT > Double NAT > Mapping dialog.
  - Click the Assign button.
  - In the Port field, select the router interface connected with the production cell.
- Select the value egress in the Direction field.
- Select the created rule in the Rule index field.
- Click the Ok button.

- Activate assignment of the rule to the router interface.

- Mark the checkbox in the Active column to activate assignment of the rule to the router interface.
- Save the changes temporarily. To do this, click the button.

- Apply the rule to the data stream.

- Open the Routing > NAT > NAT Global dialog.
- Click the button and then the Commit changes item.

When changes to the rules affect existing entries in the state table of the firewall, it helps to clear the state table. See the Clear firewall table button in the Basic Settings > Restart dialog. It is possible, that the device interrupts open communication connections.
13.5 **Tracking**

The tracking function lets you monitor certain objects, such as the availability of an interface or reachability of a network.

A special feature of this function is that it forwards an object status change to an application, for example VRRP, which previously registered as an interested party for this information.

Tracking can monitor the following objects:
- Link status of an interface (interface tracking)
- Accessibility of a device (ping tracking)
- Result of logical connections of tracking entries (logic tracking)

An object can have the following statuses:
- up (OK)
- down (not OK)
- notReady (not enabled)

The definition of "up" and "down" depends on the type of the tracking object (for example interface tracking).

Tracking can forward the state changes of an object to the following applications:
- VRRP
- Static routing

13.5.1 **Interface tracking**

With interface tracking the device monitors the link status of:
- physical ports
- Link Aggregation interfaces
- VLAN router interfaces

![Figure 50: Monitoring a line with interface tracking](image)

Ports/interfaces can have the following link statuses:
- interrupted physical link (link down)
- existing physical link (link up)

If the link to the participating ports is interrupted, then a Link Aggregation interface has link status "down".

If the link is interrupted from the physical ports/Link Aggregation interfaces that are members of the corresponding VLAN, then the VLAN router interface has the link status "down".

Setting a delay time enables you to insert a delay before informing the application about an object status change.
If the physical link interruption remains for longer than the “link down delay” delay time, then the interface tracking object has the status “down”.

When the physical link holds for longer than the “link up delay” delay time, the interface tracking object has the status “up”.

State on delivery: delay times = 0 seconds.

This means that in case where a status changes, the registered application is informed immediately.

You can set the “link down delay” and “link up delay” delay times independently of each other in the range from 0 to 255 seconds.

You can define an interface tracking object for each interface.

### 13.5.2 Ping tracking

With ping tracking, the device uses ping requests to monitor the link status to other devices.

The device sends ping requests to the device with the IP address that you entered in the IP address column.

The Ping interval [ms] column lets you define the frequency for sending ping requests, and thus the additional network load.

When the response comes back within the time entered in the Ping timeout [ms] column, this response is a valid Ping replies to receive.

When the response comes back after the time entered in the Ping timeout [ms] column, or not at all, this response is evaluated as Ping replies to lose.

Ping tracking objects can have the following statuses:

- the number of Ping replies to lose is greater than the number entered (down)
- the number of Ping replies to receive is greater than the number entered (up)
- the instance is inactive (notReady)

Entering a number for unreceived or received ping responses enables you to set the sensitivity of the ping behavior of the device. The device informs the application about an object status change.

Ping tracking enables you to monitor the accessibility of specified devices. As soon as a monitored device can no longer be accessed, the device can choose to use an alternative path.
13.5.3 **Logical tracking**

Logical tracking enables you to logically link multiple tracking objects with each other and thus perform relatively complex monitoring tasks.

You can use logical tracking, for example, to monitor the link status for a network node to which redundant paths lead (see on page 187 “Application example for logical tracking”).

The device provides the following options for a logical link:

- and
- or

For a logical link, you can combine up to 2 operands with one operator.

Logical tracking objects can have the following statuses:

- The result of the logical link is incorrect (down).
- The result of the logical link is correct (up).
- The monitoring of the tracking object is inactive (notReady).

When a logical link delivers the result down, the device can choose to use an alternative path.

13.5.4 **Configuring the tracking**

You configure the tracking by setting up tracking objects. The following steps are required to set up a tracking object:

- Enter the tracking object ID number (track ID).
- Select a tracking type, for example interface.
- Depending on the track type, enter additional options such as “port” or “link up delay” in the interface tracking.

**Note:** The registration of applications (for example VRRP) to which the tracking function reports status changes is performed in the application itself.

**Configuring interface tracking**

Set up interface tracking on port 1/1 with a link down delay of 0 seconds and a link up delay of 3 seconds. To do this, perform the following steps:

- Open the **Routing > Tracking > Configuration** dialog.
- Click the **Create** button. The dialog displays the **Create** window.

**Select type:**

- Enter the values you desire, for example:
  - **Type:** interface
  - **Track ID:** 11
- Click the **Ok** button.

**Properties:**

- Enter the values you desire, for example:
  - **Port:** 1/1
  - **Link up delay [s]:** 3
  - **Link down delay [s]:** 0
- To temporarily save the settings, click the **✓** button.
Application example for ping tracking

While the interface tracking monitors the directly connected link (see figure 50), the ping tracking monitors the entire link to device S2 (see figure 51).

Set up ping tracking at port 1/2 for IP address 10.0.2.53 with the preset parameters. To do this, perform the following steps:

- Open the Routing > Tracking > Configuration dialog.
- To add a table entry, click the button.
- Select type:
  - Enter the values you desire, for example:
    - **Type**: 21
    - **Track ID**: ping
  - Click **Ok**.
- Properties:
  - Enter the values you desire, for example:
    - **Port**: 1/2
    - **IP address**: 10.0.2.53
    - **Ping interval [ms]**: 500
    - **Ping replies to lose**: 3
    - **Ping replies to receive**: 2
    - **Ping timeout [ms]**: 100
  - To temporarily save the settings, click the button.
track enable ping 21

Activate the tracking object.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operand No. 1 (track ID)</td>
<td>21</td>
</tr>
<tr>
<td>Operand No. 2 (track ID)</td>
<td>22</td>
</tr>
</tbody>
</table>

The following is known:

Application example for logical tracking

The figure (see figure 52) displays an example of monitoring the connection to a redundant ring.

By monitoring lines L 2 and L 4, you can detect a line interruption from router A to the redundant ring.

With a ping tracking object on port 1/1 of router A, you monitor the connection to device S2.

With an additional ping tracking object on port 1/1 of router A, you monitor the connection to device S4.

Only the OR link of both ping tracking objects delivers the precise result that router A has no connection to the ring.

One ping tracking object for device S3 could indicate an interrupted connection to the redundant ring, but in this case there could be another reason for the lack of a ping response from device S3. For example, there could be a power failure at device S3.
Prerequisites for further configuration:

- The ping tracking objects for operands 1 and 2 are configured (see on page 186 “Application example for ping tracking”).

Figure 52: Monitoring the accessibility of a device in a redundant ring

- Set up a logical tracking object as an OR link. To do this, perform the following steps:

  1. Open the **Routing > Tracking > Configuration** dialog.
  2. Click the **button.**
      - The dialog displays the **Create** window.
  3. Select type:
      - Enter the values you desire, for example:
        - **Type:** 31
        - **Track ID:** logical
  4. Click the **Ok** button.
  5. Properties:
      - Enter the values you desire, for example:
        - **Logical operand A:** ping-21
        - **Logical operand B:** ping-22
        - **Operator:** or
  6. To temporarily save the settings, click the **button.

Enable
configure
track add logical 31
track modify logical 31 ping-21 or ping-22
track enable logical 31
Tracking ID logical-31 created Logical Instance ping-21 included
Logical Instance ping-22 included
Logical Operator set to or Tracking ID 31 activated
exit
show track ping 21

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Enter a tracking object in the table.
Enter the parameters for the tracking object.
Activate the tracking object.

Change to the Privileged EXEC mode.
Display the configured tracks.
Application example for logical tracking

The figure (see figure 52) displays an example of monitoring the connection to a redundant ring.

By monitoring lines L 2 and L 4, you can detect a line interruption from router A to the redundant ring.

With a ping tracking object on port 1/1 of router A, you monitor the connection to device S2.

With an additional ping tracking object on port 1/1 of router A, you monitor the connection to device S4.

Only the OR link of both ping tracking objects delivers the precise result that router A has no connection to the ring.
One ping tracking object for device S3 could indicate an interrupted connection to the redundant ring, but in this case there could be another reason for the lack of a ping response from device S3. For example, there could be a power failure at device S3.

The following is known:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operand No. 1 (track ID)</td>
<td>21</td>
</tr>
<tr>
<td>Operand No. 2 (track ID)</td>
<td>22</td>
</tr>
</tbody>
</table>

Prerequisites for further configuration:
- The ping tracking objects for operands 1 and 2 are configured (see on page 186 “Application example for ping tracking”).

Set up a logical tracking object as an OR link. To do this, perform the following steps:

1. Open the Routing > Tracking > Configuration dialog.
2. Click the button. The dialog displays the Create window.
   - Select type:
     - Enter the values you desire, for example:
       - Type: 31
       - Track ID: logical
     - Click the Ok button.
   - Properties:
     - Enter the values you desire, for example:
       - Logical operand A: ping-21
       - Logical operand B: ping-22
       - Operator: or
   - To temporarily save the settings, click the button.

Enable
configure
track add logical 31
track modify logical 31 ping-21 or ping-22
track enable logical 31

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Enter a tracking object in the table.
Enter the parameters for the tracking object.
Activate the tracking object.
Routing

13.5 Tracking

Tracking ID logical-31 created Logical Instance ping-21 included
Logical Instance ping-22 included
Logical Operator set to or
Tracking ID 31 activated

exit

show track ping 21

Ping Tracking Instance-----------------------------------
Name...........................................ping-21
Interface Number of outgoing ping packets......1/2
Target router network address....................10.0.2.53
Interval of missed repl. the state is down......3
Interval of received repl. the state is up......2
Maximal roundtrip-time ........................100
Time-To-Live for a transmitted ping request....128
Ifnumber which belongs to the best route......
State..........................................down
Send State Change trap.........................disabled
Number of state changes .......................0
Time of last change............................2014-06-18 14:23:22
Description....................................

show track ping 22

Ping Tracking Instance-----------------------------------
Name...........................................ping-22
Interface Number of outgoing ping packets......1/3
Target router network address....................10.0.2.54
Interval of missed repl. the state is down......3
Interval of received repl. the state is up......2
Maximal roundtrip-time ........................100
Time-To-Live for a transmitted ping request....128
Ifnumber which belongs to the best route......
State..........................................up
Send State Change trap.........................disabled
Number of state changes .......................0
Time of last change............................2014-06-18 14:23:55
Description....................................

show track logical 31

Logical Tracking Instance-----------------------------------
Name...........................................logical-31
Operand A......................................ping-21
Operand B......................................ping-22
Operator.......................................or
State..........................................up
Send State Change trap.........................disabled
Number of state changes .......................0
Time of last change............................2014-06-18 14:24:25
Description....................................

Change to the Privileged EXEC mode.
Display the configured tracks.

Display the configured tracks.

Display the configured tracks.
13.6 VRRP

End devices usually let you enter one default gateway for transmitting data packets in external subnetworks. Here the term “Gateway” applies to a router with which end devices communicate with other subnetworks.

If this router fails, then the end device cannot send any more data to the external subnetworks.

In this case, the Virtual Router Redundancy Protocol (VRRP) provides assistance.

VRRP is a type of “gateway redundancy”. VRRP describes a process that groups multiple routers into one virtual router. End devices constantly address the virtual router, and VRRP helps ensure that a physical router belonging to the virtual router transmits the data.

When a physical router fails, VRRP helps ensure that another physical router continues to route the data as part of the virtual router.

When a physical router fails, VRRP has a typical failover time of 3 to 4 seconds.

Note: The device supports only VRRP packets without authentication information. In order for the device to operate in conjunction with other devices that support VRRP authentication, verify that on those devices the VRRP authentication is not applied.

13.6.1 VRRP

The routers within a network on which VRRP is active specify among themselves which router is the master. The master router controls the IP and MAC address of the virtual router. The devices in the network that have entered this virtual IP address as the default gateway use the master as the default gateway.

When the master fails, then the remaining backup routers use VRRP to specify a new master. The backup router that wins the election process then controls the IP address and MAC address of the virtual router. Thus, the devices find the route through the default gateway, as before. The devices see only the master router with the virtual MAC and IP addresses, regardless of which physical router is actually behind this virtual address.

The administrator assigns the virtual router IP address.

VRRP specifies the virtual MAC address with: 00:00:5e:00:01:<VRID>.
The first 5 octets form the fixed part in accordance with RFC 3768. The last octet is the virtual router ID (VRID). The VRID is a number from 1 through 255. Based on the number of VRIDs, VRRP lets the administrator specify up to 255 virtual routers within a network.

In order to determine the master, a VRRP router sends IP Multicast messages to the IP Multicast address 224.0.0.18. The physical router with the higher VRRP priority becomes the master. The administrator specifies the VRRP priority of each physical router. When the VRRP priorities are the same, the physical router with higher IP interface address in the VRRP domain becomes the master. When the virtual IP address is the same as the IP address of a router interface, this router is the IP address owner. VRRP sets the VRRP priority of an IP address owner to the value of 255 and thus declares this router the master. When there is no IP address owner, VRRP declares the router with the higher VRRP priority the master.

In order to signal that the master router is ready for operation, the master router sends IP Multicast advertisements in regular intervals (default: 1 s) to the other VRRP routers (backup routers). When 3 intervals pass without the other VRRP routers receiving an advertisement, VRRP initiates the master router election process. The VRRP backup router with the higher VRRP priority declares itself the new master.

Table 26: Who shall be the master?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>The IP address owner as it has the higher VRRP priority (255) by definition.</td>
</tr>
<tr>
<td>2.</td>
<td>The VRRP router with the higher VRRP priority.</td>
</tr>
<tr>
<td>3.</td>
<td>When the priorities are the same, the VRRP router with the higher IP address.</td>
</tr>
</tbody>
</table>

VRRP terms:

- **Virtual router**
  A virtual router is a physical router or group of physical routers that act as the default gateway in a network using the Virtual Router Redundancy Protocol.

- **VRRP router**
  A VRRP router is a physical router with VRRP enabled. The VRRP router is part of one or more virtual routers.

- **Master router**
  The master router is the physical router within a virtual domain that is responsible for forwarding data packets and responding to ARP queries. The master router periodically sends messages (advertisements) to the backup routers in the virtual domain to inform them about its existence. The backup routers save the advertisement interval and VRRP priority contained in the master router advertisements to calculate the master down time and skew time.

- **IP address owner**
  The IP address owner is the VRRP router whose IP address is identical to the IP address of the virtual router. By definition, it has the VRRP priority of 255 and is thus automatically the master router.

- **Backup router**
  When the master router fails, the backup router is a VRRP router providing a stand-by route for the master router. The backup router is ready to take over the master role.

- **VRRP priority**
  The VRRP priority is a number from 1 through 255. VRRP uses the priority number to determine the master router. VRRP reserves the priority value 255 for the IP address owner.

- **VRID**
  The virtual router ID (VRID) uniquely identifies a virtual router. The VRID defines the last octet of the virtual router MAC address.
Routing
13.6 VRRP

- Virtual router MAC address
  The MAC address of the virtual router instance (see figure 55).
- Virtual router IP address
  The IP address of the virtual router instance.
- Advertisement interval
  The advertisement interval describes the frequency with which the master router sends
  advertisements to the backup routers within the same virtual router. The values for the
  advertisement interval are from 1 through 255 seconds. The default interval value for VRRP
  advertisements is 1 second.
- Skew time
  The skew time uses the VRRP priority of the master router to determine how long a backup
  router waits, after declaring the master down, until it initiates the master router election process.
  Skew time = ((256 - VRRP priority) / 256) * 1 second
- Master down interval
  The master down interval uses the advertisement interval of the master router to specify the time
  that elapses before a backup router declares the master down.
  Master down interval = 3 * advertisement interval + skew time

Configuration of VRRP

The configuration of VRRP requires the following steps:
- Enable the Routing function globally.
- Enable VRRP globally.
- Assign an IP address and subnet mask to the port.
- Enable VRRP on the port.
- Create the virtual router ID (VRID), because you have the option of activating multiple virtual
  routers on each port.
- Assign the virtual router IP address.
- Enable the virtual router.
- Assign the VRRP priority.
- You specify every active VRRP port the same way.
- You also perform the same configuration on the backup router.
13.6.2 VRRP with load sharing

With the simple configuration, a router performs the gateway function for the end devices. The capacity of the backup router lies idle. VRRP lets you also use the capacity of the backup router. Setting up a number of virtual routers lets you enter different default gateways on the connected end devices and thus steer the data flow.

When both routers are active, the data flows through the router on which the IP address of the default gateway has the higher VRRP priority. When a router fails, the data flows through the remaining routers.

Figure 56: Virtual router with load sharing

Configure load sharing. To do this, perform the following steps:

- Define a second VRID for the same router interface.
- Assign the router interface its own IP address for the second VRID.
- Assign the second virtual router a lower priority than the first virtual router.
- When configuring the backup router, verify that you assign the second virtual router a higher priority than the first.
- Give the end devices one of the virtual router IP addresses as a default gateway.

13.6.3 VRRP with Multinetting

The router lets you combine VRRP with Multinetting.

Figure 57: Virtual router with multinetting
Configure VRRP with multinetting on the basis of an existing VRRP configuration (see figure 54). To do this, perform the following steps:

- Assign a second (secondary) IP address to the port.
- Assign a second (secondary) IP address to the virtual router.

```plaintext
Interface 2/3

ip address secondary 10.0.2.1 255.255.255.0
ip vrrp virtual-address add 1 10.0.2.100
```

- Select the port at which you want to configure multinetting.
- Assign the second IP address to the port.
- Assign a second IP address to the virtual router with the VRID 1.

- Perform the same configuration on the backup router.
13.7 OSPF

Open Shortest Path First (OSPF) is a dynamic routing protocol based on the Link State Algorithm. This algorithm is based on the link states between the routers involved.

The significant metric in OSPF is the "OSPF costs", which is calculated from the available bit rate of a link.

OSPF was developed by IETF. OSPF is currently specified as OSPFv2 in RFC 2328. Along with many other advantages of OSPF, the fact that it is an open standard has contributed to the wide usage of this protocol. OSPF has replaced the Routing Information Protocol (RIP) as the standard Interior Gateway Protocol (IGP) in large networks.

OSPF has a number of significant advantages to offer:
- Cost-based routing metrics: In contrast to RIP, OSPF provides clear metrics based on the bandwidth of each individual network connection. OSPF provides major flexibility in designing a network, because you can change these costs.
- Routing using multiple paths (equal cost multiple path/ECMP): OSPF is able to support a number of equal paths to a given destination. OSPF thus provides efficient utilization of the network resources (load distribution) and improves the availability (redundancy).
- Hierarchical routing: By logically dividing the network into areas, OSPF shortens the time required to distribute routing information. The messages about changes in a subnetwork remain within the subnetwork, without putting any load on the rest of the network.
- Support of Classless Inter-Domain Routing (CIDR) and Variable Length Subnet Mask (VLSM): This lets the network administrator assign the IP address resources efficiently.
- Fast tuning time: OSPF supports the fast distribution of messages about route changes. This speeds up the tuning time for updating the network topology.
- Saving network resources / bandwidth optimization: Because OSPF, in contrast to RIP, does not exchange the routing tables at regular, short intervals, no bandwidth is unnecessarily "wasted" between the routers.
- Support of authentication: OSPF supports the authentication of nodes that send routing information.

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Every router calculates its routes independently of the other routers.</td>
<td>Complicated to implement</td>
</tr>
<tr>
<td>The routers have the same basic information.</td>
<td>Complex administration due to the large number of options.</td>
</tr>
<tr>
<td>Rapid detection of link interruptions and rapid calculation of alternative routes.</td>
<td></td>
</tr>
<tr>
<td>The data volume for router information is relatively small, because information is only sent in cases where it is required, and only the information that applies to the immediate neighbors.</td>
<td></td>
</tr>
<tr>
<td>Optimal path selection through evaluation of the link quality.</td>
<td></td>
</tr>
<tr>
<td>OSPF is a routing protocol based on the states of the links between the routers.</td>
<td></td>
</tr>
<tr>
<td>Using the link states collected from every router and the Shortest Path First algorithm, an OSPF router dynamically creates its routing table.</td>
<td></td>
</tr>
</tbody>
</table>
13.7.1 OSPF-Topology

OSPF is hierarchically structured in order to limit the scope of the OSPF information to be exchanged in large networks. You divide up your network using what are known as areas.

**Autonomous System**

An Autonomous System (AS) is a number of routers that are managed by a single administration and use the same Interior Gateway Protocol (IGP). Exterior Gateway Protocols (EGP), on the other hand, are used to connect a number of autonomous systems. OSPF is an Interior Gateway Protocol.

![Figure 58: Autonomous System](image)

An AS uses an “Autonomous System Boundary Router” (ASBR) to connect with the outside world. An ASBR understands multiple protocols and serves as a gateway to routers outside the areas. An ASBR is able to transfer routes from different protocols into OSPF. This process is known as redistribution.

**Router ID**

The router ID in the form of an IP address is used to uniquely identify every router within an autonomous system. To improve the transparency, it is necessary to manually configure the router ID of every OSPF router. Thus there is no automatic function that selects the router ID from the IP interfaces of the router.

```
   enable         Change to the Privileged EXEC mode.
   configure      Change to the Configuration mode.
   ip ospf router-id 192.168.1.2  Assign router ID, for example 192.168.1.2.
   ip ospf operation Enable OSPF globally.
```
Areas

Each area first forms its own database using the link states within the area. The data exchange required for this remains within the area. Each area uses an Area Border Router (ABR) to link to other areas. The routing information is summarized as much as possible between the areas (route summarization).

Every OSPF router has to be a member of at least one area.

An individual router interface can only be assigned to one area. By default, every router interface is assigned to the backbone area.

OSPF distinguishes between the following particular area types:

- **Backbone Area:**
  This is by definition the area 0.0.0.0. An OSPF network consists of at least the backbone area. It is the central area, which is linked to the other areas directly. The backbone area receives the routing information and is responsible for forwarding this information.

- **Stub Area:**
  When external LSAs are not to be flooded into the area, you define an area as a stub area. External means outside the autonomous system. These external LSAs are the yellow and orange links in the See figure 59 on page 199. illustration. Thus the routers within a stub area only learn internal routes (blue links – for example no routes that are exported into OSPF from another log / redistributing). The destinations outside the autonomous system are assigned to a default route. Stub areas are thus generally used in cases where only one router in the area has a link to outside the area. The use of stub areas keeps the routing table small within the stub area.

  Configuration notes:
  - For a stub area, the routers within the stub area have to be specified as stub routers.
  - A stub area does not allow passage for a virtual link.
  - The backbone area cannot be specified as a stub area.

- **Not So Stubby Area (NSSA):**
  You define an area as NSSA in cases where the external (yellow) routes of a system directly connected to the NSSA that is outside your autonomous system are to be led into the area (redistributed). These external (yellow) LSAs then also lead from the NSSA to other areas in your autonomous system. External (orange) LSAs within your own autonomous system do not, on the other hand, lead into an NSSA.

  By using NSSAs, you can integrate ASBRs into the area without foregoing the advantage of stub areas, namely that external routes from the backbone are not flooded into the corresponding area.

  Thus NSSAs have the advantage that external routes coming from the backbone are not entered in the routing tables of the internal routers. At the same time, however, a limited number of external networks, which can be reached across the boundaries of the NSSA, can be propagated into the backbone area.
Perform the following steps:

```markdown
enable
configure
ip ospf area 2.2.2.2 nssa add import-nssa
ip ospf area 3.3.3.3 stub add 0
ip ospf area 3.3.3.3 stub modify 0 default-cost 10
```

**Virtual Link**

OSPF requires that the backbone area to be connected to every area. However, when this is not actually possible, OSPF provides a virtual link (VL) to connect parts of the backbone area with each other [see figure 61 on page 200.](#) A VL even lets you connect an area that is connected with the backbone area via another area.

![Figure 60: Linking a remote area to the backbone area using a virtual link (VL)](image)

**Figure 60:** Linking a remote area to the backbone area using a virtual link (VL)

**Figure 61:** Expanding the backbone area using a virtual link (VL)

**Configuration for expanding the backbone area** (see figure 61):

Configure router 1. To do this, perform the following steps:

```markdown
enable
configure
ip ospf area 1.1.1.1 virtual-link add 2.2.2.2
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.

Enter the neighboring router ID for a virtual link in area 1.1.1.1.
Configure router 2. To do this, perform the following steps:

```plaintext
enable
configure
ip ospf area 1.1.1.1 virtual-link add 1.1.1.1
```

**OSPF Router**

OSPF distinguishes between the following router types:

- **Internal router:**
  The OSPF interfaces of an internal router are within the same area.

- **Area Border Router (ABR):**
  ABRs have OSPF interfaces in a number of areas, including the backbone area. The ABRs thus participate in multiple areas. Where possible, you summarize a number of routes and send “Summary LSAs” to the backbone area.

- **Autonomous System Area Border Router (ASBR):**
  An ASBR is located on the boundary of an autonomous system and links OSPF to other autonomous systems / routing protocols. These external routes are transferred into OSPF using what is known as redistribution and are then summarized as “AS-external LSAs” and flooded into the area.

  Enable the redistributing explicitly.
  When you want to use subnetting, you enter this explicitly.

  In OSPF, the following “routing protocols” can be exported:
  - connected (local subnetworks on which OSPF is not switched on)
  - static (static routes)

**Link State Advertisement**

As a basis for building up a database using the link states, OSPF uses Link State Advertisements (LSA).

An LSA contains the following information:

- the router,
- the connected subnets,
- the routes that can be reached,
- the network masks and
- the metric.

OSPF distinguishes between the following LSA types:

- **Router LSAs** (type 1 LSAs):
  Every router sends a router LSA to every other router in the same area. They describe the state and the costs of the router links (router interfaces) that the router has in the corresponding area. Router LSAs are only flooded within the area.

- **Network LSAs** (type 2 LSAs):
  These LSAs are generated by the designated router, DR (see on page 203 “Setting up the Adjacency”) and are sent for every connected network/subnet within an area.

- **Summary LSAs** (type 3 /type 4 LSAs)
  Summary LSAs are generated by ABRs and describe inter-area destinations, meaning destinations in different areas of the same autonomous system.
  Type 3 LSAs describe targets for IP networks (individual routes or summarized routes).
  Type 4 LSAs describe routes to ASBRs.
AS-external LSAs (type 5 LSAs):
These LSAs are generated by ASBRs and describe routes outside the autonomous system. These LSAs are flooded everywhere except for stub areas and NSSAs.

NSSA external LSAs (type 7 LSAs):
A stub area does not flood any external routes (represented by type 5 LSAs) and therefore does not support any Autonomous System Border Routers (ASBRs) at its boundaries. Thus an ASBR cannot carry any routes from other protocols into a stub area.

RFC 1587 specifies the NSSAs functions. According to RFC 1587, the ASBRs send type 7 LSAs instead of type 5 LSAs for the external routes within an NSSA. These type 7 LSAs are then converted into type 5 LSAs by an ABR and flooded into the backbone area. This “translator role” is negotiated among the ABRs in an NSSA (the router with the highest router ID), but it can also be configured manually.

13.7.2 General Operation of OSPF

OSPF was specially tailored to the needs of larger networks and provides a fast convergence and minimum usage of protocol messages.

The concept of OSPF is based on the creation, maintenance and distribution of what is called the link state database. This data base describes:
- every router within a routing domain (area) and
- their active interfaces and routes,
- how they are linked to each other and
- the costs of these links.

The routers within an area have an identical data base, which means that every router knows the exact topology within its area.

Every router plays its part in setting up the respective data base by propagating its local viewpoint as Link State Advertisements (LSAs). These LSAs are then flooded to the other routers within an area.

OSPF supports a range of different network types such as point-to-point networks (for example, packet over SONET/SDH), broadcast networks (Ethernet) or non-broadcast networks.

Broadcast networks are distinguished by the fact that a number of systems (end devices, switches, routers) are connected to the same segment and thus can be addressed simultaneously using broadcasts/multicasts.

OSPF generally performs the following steps in carrying out its tasks in the network:
- Setting up the Adjacencies using the Hello protocol
- Synchronizing the link state database
- Route calculation
13.7.3 Setting up the Adjacency

When a router boots, it uses what are called Hello packets to contact its neighboring routers. With these Hello packets, an OSPF router finds out which OSPF routers are near it and if they are suitable for setting up an adjacency.

In broadcast networks such as Ethernet, the number of neighbors increases with the number of routers connected, as does the information exchange for clarifying and maintaining the Adjacency. To reduce these volumes within an area, OSPF uses the “Hello” protocol to determine a designated router (DR) within the corresponding area. Thus every router in an area only sets up the Adjacency with its designated router, instead of with every neighbor. The designated router is responsible for the distribution of the link state information to its neighbor routers.

For security reasons, OSPF provides for the selection of a backup designated router (BDR), which takes over the tasks of the DR in case the DR fails. The OSPF router with the highest router priority is the DR. The router priority is specified by the administrator. When routers have the same priority, the router with the higher router ID is selected. The router ID is the smallest IP address of a router interface. You configure this router ID manually during booting of the OSPF router "Router ID" on page 198.

![Figure 62: LSA distribution with designated router and backup designated router](image)

To exchange information, OSPF uses reserved multicast addresses.

<table>
<thead>
<tr>
<th>Destination</th>
<th>Multicast IP address</th>
<th>Mapped Multicast MAC address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Every OSPF router</td>
<td>224.0.0.5</td>
<td>01:00:5E:00:00:05</td>
</tr>
<tr>
<td>Designated routers</td>
<td>224.0.0.6</td>
<td>01:00:5E:00:00:06</td>
</tr>
</tbody>
</table>

Hello packets are also used to check the configuration within an area (area ID, timer values, priorities) and to monitor the Adjacencies. Hello packets are sent cyclically (Hello interval). When Hello packets are not received for a specific period (Dead interval), the Adjacency is terminated and the corresponding routes are deleted.

The Hello interval (default setting: 10 seconds) and the Dead interval (default setting: 40 seconds) can be configured for each router interface. When reconfiguring the timers, verify that they are uniform within an area.

Perform the following steps:

```bash
enable
configure
interface 1/1
ip ospf hello-interval 20
ip ospf dead-interval 60
exit
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Change to the interface configuration mode of interface 1/1.
Specifies the Hello interval as 20 seconds.
Specifies the Dead interval as 60 seconds.
Change to the Configuration mode.
The following list contains the states of the Adjacencies:

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Down</td>
<td>No Hello packets received yet</td>
</tr>
<tr>
<td>Init</td>
<td>Receiving Hello packets</td>
</tr>
<tr>
<td>2-way</td>
<td>Bidirectional communication, determination of the DR and the BDR</td>
</tr>
<tr>
<td>Exstart</td>
<td>Determination of master/slave for LSA exchange</td>
</tr>
<tr>
<td>Exchange</td>
<td>LSAs are exchanged or flooded</td>
</tr>
<tr>
<td>Loading</td>
<td>Completion of the LSA exchange</td>
</tr>
<tr>
<td>Full</td>
<td>Data basis complete and uniform in the area. Routes can now be calculated</td>
</tr>
</tbody>
</table>

### 13.7.4 Synchronization of the LSDB

The central part of the OSPF is the link state database (LSDB). This database contains a description of the network and the states of every router. The LSDB is the source for calculating the routing table and reflects the topology of the network. The LSDB is set up after the designated router or the backup designated router has been determined within an area (Broadcast networks).

To set up the LSDB and update any topology changes, the OSPF router sends link status advertisements (LSA) to the directly accessible OSPF routers. These link state advertisements consist of the interfaces and the neighbors of the sending OSPF router reachable through these interfaces. OSPF routers put this information into their databases and flood the information to the ports.

When no topology changes occur, the routers send a LSA every 30 minutes.

You can view the content of the Link State Database with the command `show ip ospf database` using the Command Line Interface, whereby the entries are output in accordance with the areas. To do this, perform the following steps:

```
enable
show ip ospf database internal
```

Change to the Privileged EXEC mode.
Displays the internal Adjacencies of the router.
13.7.5 Route Calculation

After the LSDs are learned and the neighbor relationships go to the full state, every router calculates a path to every destination using the Shortest Path First (SPF) algorithm. After the optimal path to every destination has been determined, these routes are entered in the routing table. The route calculation is generally based on the accessibility of a hop and the metric (costs). The costs are added up for every hop to the destination.

The cost of individual router interfaces are based on the available bandwidth of this link. The calculation for the standard setting is based on the following formula:

\[ \text{Metric} = \frac{\text{Autocost reference bandwidth}}{\text{bandwidth (bits/sec)}} \]

For Ethernet, this leads to the following costs:

<table>
<thead>
<tr>
<th>Bandwidth</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Mbit</td>
<td>10</td>
</tr>
<tr>
<td>100 Mbit</td>
<td>1</td>
</tr>
<tr>
<td>1000 Mbit</td>
<td>1 (0.1 rounded up to 1)</td>
</tr>
</tbody>
</table>

The table displays that this form of calculation in the standard configuration does not permit any distinction between Fast Ethernet and Gigabit Ethernet.

You can change the standard configuration by assigning a different value for the costs to each OSPF interface. This enables you to differentiate between Fast Ethernet and Gigabit Ethernet. To do this, perform the following steps:

```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Change to the Privileged EXEC mode.</td>
</tr>
<tr>
<td>configure</td>
<td>Change to the Configuration mode.</td>
</tr>
<tr>
<td>interface 1/1</td>
<td>Change to the interface configuration mode of interface 1/1.</td>
</tr>
<tr>
<td>ip ospf cost 2</td>
<td>Assigns the value 1/1 to port 2 for the OSPF costs.</td>
</tr>
</tbody>
</table>
```
13.7.6 Configuring OSPF

In the delivery state, the default values are selected so that you can configure simple OSPF functions in a few steps. After the router interface is specified and OSPF is enabled, OSPF automatically enters the required routes in the routing table.

The example below displays a simple OSPF configuration. Area 0.0.0.0 is already specified by default. The end devices do not have an OSPF function, so you do not have to activate OSPF on the corresponding router interface. By activating the Redistribution function, you can inject the routes to the end devices into the OSPF.

Configure the OSPF functions. To do this, perform the following steps:

- Configure router interfaces – assign IP address and network mask.
- Activate OSPF on the port.
- Enable OSPF globally.
- Enable routing globally (if this has not already been done).
**Configuration for Router B**

Perform the following steps:

```plaintext
enable
configure
interface 2/2
ip address primary 10.0.3.1 255.255.255.0
ip routing
ip ospf operation
exit
interface 2/1
ip address primary 10.0.2.2 255.255.255.0
ip routing
ip ospf operation
exit
ip ospf router-id 10.0.2.2
ip ospf operation
ip ospf re-distribute connected
[subnets]
exit
exit
show ip ospf global
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Change to the interface configuration mode of interface 2/2.
Assign the IP parameters to the port.

Activate routing on this port.
Activate OSPF on this port.
Change to the Configuration mode.
Change to the interface configuration mode of interface 2/1.
Assign the IP parameters to the port.

Activate routing on this port.
Activate OSPF on this port.
Change to the Configuration mode.
Assign router ID 10.0.2.2 to router B.

Enable OSPF globally.
Specify the OSPF parameters for the following actions:
- send the routes of the locally connected interfaces
- include subnetworks without OSPF in OSPF (CIDR).

Change to the Configuration mode.
Change to the Privileged EXEC mode.
Display the settings for the global OSPF configuration.
Also perform the corresponding configuration on the other OSPF routers.

Display the settings for the OSPF interface configuration.

```
OSPF Admin Mode.............................. enabled
Router ID........................................ 10.0.2.2
ASBR Mode...................................... enabled
RFC 1583 Compatibility..................... enabled
ABR Status..................................... disabled
Exit Overflow Interval...................... 0
External LSA Count............................ 0
External LSA Checksum....................... 0
New LSAs Originated.......................... 0
LSAs Received................................ 0
External LSDB Limit........................... no limit
SFP delay time............................... 5
SFP hold time................................... 10
Auto cost reference bandwidth.............. 100
Default Metric............................... not configured
Default Route Advertise..................... disabled
Always.......................................... false
Metric.......................................... 0
Metric Type..................................... external-type2
Maximum Path................................. 4
Trap flags...................................... disabled
--More-- or (q)uit
show ip ospf interface 2/1
```

```
Display the OSPF Adjacencies.
```

```
Configure
ip routing
exit
```

Enable the Routing function globally.

Change to the Privileged EXEC mode.

Display the settings for the OSPF interface configuration.
13.7.7 Limiting the distribution of the routes using an ACL

With Redistributing enabled, OSPF distributes every static route configured in the device without further interference. The distribution of the rip routes and connected routes is analogous. You can restrict this behavior using Access Control Lists.

Using IP rules, you specify which routes the device distributes to other devices in OSPF:

- To distribute a few routes in OSPF, you use the explicit permit rules. Using the permit rules, you specify exactly which routes the device distributes in OSPF.
- To distribute many routes in OSPF, you use the explicit deny rules, combined with an explicit permit rule. The device then distributes every route except those specified with a deny rule.

In the following example, you restrict the distribution of static routes in OSPF using Access Control Lists.

The example contains the following sections:
- Setting up and distributing routes
- Explicitly enabling a route using a permit rule
- Explicitly disabling a route using a deny rule

Setting up and distributing routes

On Router A, you configure 2 static routes for the subnets 8.1.2.0/24 and 8.1.4.0/24. Router A distributes these routes in OSPF to Router B. On router B, you check the distribution of the routes configured on router A.
**Router A**
- Enable routing globally.
  ```
  enable
  configure
  ip routing
  ```
  Change to the Privileged EXEC mode.
  Change to the Configuration mode.
  Enable routing globally.

- Setting up the first router interface **10.0.1.1/24**.
  Activate routing.
  Activate OSPF on the router interface.
  ```
  interface 1/1
  ip address primary 10.0.1.1 255.255.255.0
  ip routing
  ip ospf operation
  exit
  ```
  Change to the interface configuration mode of interface 1/1.
  Specify the IP address and subnet mask.
  Activate routing.
  Activate OSPF on the router interface.
  Change to the Configuration mode.

- Setting up the second router interface **10.0.2.1/24**.
  Activate routing.
  Activate OSPF on the router interface.
  ```
  interface 1/2
  ip address primary 10.0.2.1 255.255.255.0
  ip routing
  ip ospf operation
  exit
  ```
  Change to the interface configuration mode of interface 1/2.
  Specify the IP address and subnet mask.
  Activate routing.
  Activate OSPF on the router interface.
  Change to the Configuration mode.

- Enable OSPF globally.
  ```
  ip ospf router-id 10.0.1.1
  ip ospf operation
  show ip route all
  ```
  Assign the router ID (for example 10.0.1.1).
  Enable OSPF globally.

- Configure and distribute static routes
  ```
  enable
  configure
  ```
  Change to the Privileged EXEC mode.
  Change to the Configuration mode.
ip route add 8.1.2.0 255.255.255.0 10.0.2.2
ip route add 8.1.4.0 255.255.255.0 10.0.2.4
ip ospf re-distribute static subnets enable

Configure the static route 8.1.2.0 through the gateway 10.0.2.2.
Configure the static route 8.1.4.0 through the gateway 10.0.2.4.
Distribute the configured routes in OSPF.
**Router B**

- Enable routing globally.

```plaintext
enable
configure
ip routing
```

- Setting up the router interface **10.0.1.2/24**.
  - Activate routing.
  - Activate OSPF on the router interface.

```plaintext
interface 2/2
ip address primary 10.0.1.2 255.255.255.0
ip routing
ip ospf operation
exit
show ip route all
```

- Enable OSPF globally.

```plaintext
ip ospf router-id 10.0.1.2
ip ospf operation
```

- Directly connect the port of the router interface **10.0.1.2** to the first router interface of router A.
  - Check the availability of the OSPF neighbors.

```plaintext
show ip ospf neighbor
```

- Check the distribution of the routes configured on router A.
  - Router A distributes both configured routes.

```plaintext
show ip route all
```
To explicitly enable a route with a permit rule, refer to the “Explicitly enabling a route using a permit rule” on page 213 section.

To explicitly disable a route with a deny rule, refer to the “Explicitly disabling a route using a deny rule” on page 215 section.

**Explicitly enabling a route using a permit rule**

The route for the **8.1.2.0/24** subnet is enabled for distribution in OSPF.

- Using a permit rule, you explicitly enable the route for the **8.1.2.0/24** subnet.
- Due to the implicit deny rule embedded in the device, every other route is disabled for distribution in OSPF.
**Router A**

- Set up an Access Control List with an explicit *permit* rule.

```bash
ip access-list extended name OSPF-rule
permit src 8.1.2.0-0.0.0.0 dst 255.255.255.0-0.0.0.0 proto ip
```

Create the *OSPF-rule* Access Control List and set up a *permit* rule for the 8.1.2.0 subnet.
- *src 8.1.2.0-0.0.0.0* = address of the destination network and inverse mask
- *dst 255.255.255.0-0.0.0.0* = mask of the destination network and inverse mask

The device lets you assign the address and mask of the destination network with bit-level accuracy using the inverse mask.

- Check the configured rules.

```bash
show access-list ip
```

Display the configured Access Control Lists and rules.

<table>
<thead>
<tr>
<th>Index</th>
<th>AclName</th>
<th>RuleNo</th>
<th>Action</th>
<th>SrcIP</th>
<th>DestIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>OSPF-rule</td>
<td>1</td>
<td>Permit</td>
<td>8.1.2.0</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

```bash
show access-list ip OSPF-rule 1
```

Display the rule 1 (explicit *permit* rule) in the *OSPF-rule* Access Control List.

```bash
ip ospf distribute-list out static OSPF-rule
```

Apply the *OSPF-rule* Access Control List to OSPF.
**Router B**

- Check the distribution of the routes configured on router A
- Router A only distributes the route for the subnet 8.1.2.0/24 due to the configured Access Control List.

```
show ip route all
```

<table>
<thead>
<tr>
<th>Network Address</th>
<th>Protocol</th>
<th>Next Hop IP</th>
<th>Next Hop If</th>
<th>Pref</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.2.0/24</td>
<td>OSPF</td>
<td>10.0.1.2</td>
<td>2/2</td>
<td>0</td>
<td>[x]</td>
</tr>
<tr>
<td>10.0.1.0/24</td>
<td>Local</td>
<td>10.0.1.2</td>
<td>2/2</td>
<td>0</td>
<td>[x]</td>
</tr>
<tr>
<td>10.0.2.0/24</td>
<td>OSPF</td>
<td>10.0.1.2</td>
<td>2/2</td>
<td>0</td>
<td>[x]</td>
</tr>
</tbody>
</table>

---

**Explicitly disabling a route using a deny rule**

The route for the 8.1.4.0/24 subnet is disabled for distribution in OSPF.

- Using an explicit *permit* rule, you enable every rule for distribution in OSPF.
- Using a *deny* rule, you explicitly disable the route for the 8.1.4.0/24 subnet.
**Router A**

- **Delete permit rule.**
  These steps are necessary only in case you have configured a **permit** rule, as described in section “Explicitly enabling a route using a permit rule” on page 213.

  ```
  no ip ospf distribute-list out static OSPF-rule
  ip access-list extended del OSPF-rule
  ```

- **Set up an Access Control List with an explicit deny rule.**

  ```
  ip access-list extended name OSPF-rule
deny src 8.1.4.0-0.0.0.0 dst 255.255.255.0-0.0.0.0 proto ip
  ```

- **Apply the Access Control List to OSPF.**

  ```
  ip ospf distribute-list out static OSPF-rule
  ```

**Router B**

- **Check the distribution of the routes configured on router A.**
  Due to the implicit **deny** rule embedded in the device, Router A does not distribute routes.

  ```
  show ip route all
  ```

<table>
<thead>
<tr>
<th>Network Address</th>
<th>Protocol</th>
<th>Next Hop IP</th>
<th>Next Hop If</th>
<th>Pref</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.2.0/24</td>
<td>OSPF</td>
<td>10.0.1.2</td>
<td>2/2</td>
<td>0</td>
<td>[x]</td>
</tr>
<tr>
<td>10.0.1.0/24</td>
<td>Local</td>
<td>10.0.1.2</td>
<td>2/2</td>
<td>0</td>
<td>[x]</td>
</tr>
<tr>
<td>10.0.2.0/24</td>
<td>OSPF</td>
<td>10.0.1.2</td>
<td>2/2</td>
<td>0</td>
<td>[x]</td>
</tr>
</tbody>
</table>

  Checking the router table:

  The route **10.0.2.0/24** remains available because the Access Control List helps prevent only the distribution of static routes.
**Router A**

- Adding the explicit **permit** rule to Access Control List.

```
ip access-list extended name OSPF-rule
permit src any dst any proto ip
```

Add a **permit** rule for every subnet to the **OSPF-rule** Access Control List.

- Check the configured rules.

```
show access-list ip
```

Display the configured Access Control Lists and rules.

<table>
<thead>
<tr>
<th>Index</th>
<th>AclName</th>
<th>RuleNo</th>
<th>Action</th>
<th>SrcIP</th>
<th>DestIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>OSPF-rule</td>
<td>1</td>
<td>Deny</td>
<td>8.1.4.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>1000</td>
<td>OSPF-rule</td>
<td>2</td>
<td>Permit</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

```
show access-list ip OSPF-rule 1
```

Display the rule 1 (explicit **deny** rule) in the **OSPF-rule** Access Control List.
IP access-list rule detail
--------------------------
IP access-list index.........................1000
IP access-list name..........................OSPF-rule
IP access-list rule index.......................1
Action......................................Deny
Match every ................................False
Protocol......................................IP
Source IP address..........................8.1.4.0
Source IP mask...............................0.0.0.0
Source L4 port operator......................eq
Source port..................................-1
Destination IP address.......................255.255.255.0
Destination IP mask..........................0.0.0.0
Source L4 port operator......................eq
Destination port................................-1
Flag Bits....................................-1
Flag Mask....................................-1
Established................................False
ICMP Type...................................0
ICMP Code...................................0
--More-- or (q)uit

show access-list ip OSPF-rule 2
Display the rule 2 (explicit permit rule) in the OSPF-rule Access Control List.

IP access-list rule detail
--------------------------
IP access-list index.........................1000
IP access-list name..........................OSPF-rule
IP access-list rule index.......................2
Action......................................Permit
Match every ................................False
Protocol......................................IP
Source IP address..........................0.0.0.0
Source IP mask...............................255.255.255.255
Source L4 port operator......................eq
Source port..................................-1
Destination IP address.......................0.0.0.0
Destination IP mask..........................255.255.255.255
Source L4 port operator......................eq
Destination port................................-1
Flag Bits....................................-1
Flag Mask....................................-1
Established................................False
ICMP Type...................................0
ICMP Code...................................0
--More-- or (q)uit
Router B

☐ Check the distribution of the routes configured on router A

Router A only distributes the route for the subnet 8.1.2.0/24 due to the configured Access Control List.

```
show ip route all
```

Checking the router table:

<table>
<thead>
<tr>
<th>Network Address</th>
<th>Protocol</th>
<th>Next Hop IP</th>
<th>Next Hop If</th>
<th>Pref</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.2.0/24</td>
<td>OSPF</td>
<td>10.0.1.2</td>
<td>2/2</td>
<td>0</td>
<td>[x]</td>
</tr>
<tr>
<td>10.0.1.0/24</td>
<td>Local</td>
<td>10.0.1.2</td>
<td>2/2</td>
<td>0</td>
<td>[x]</td>
</tr>
<tr>
<td>10.0.2.0/24</td>
<td>OSPF</td>
<td>10.0.1.2</td>
<td>2/2</td>
<td>0</td>
<td>[x]</td>
</tr>
</tbody>
</table>
To configure the Layer 3 function, you require access to the device management.

Depending on your own application, you will find many options for assigning IP addresses to the devices. The following example describes one option that often arises in practice. Although you have other prerequisites, this example shows the general method for entering the IP parameters and points out significant things that you should note.

The prerequisites for the following example are:
- All Layer 2 and Layer 3 devices have the IP address 0.0.0.0 (= default setting)
- The IP addresses of the devices and router interfaces and the gateway IP addresses are specified in the network plan.
The devices and their connections are installed.

Redundant connections are open (see VRRP). To help avoid loops in the configuration phase, close the redundant connections only after the configuration phase.

Perform the following steps:

- Assign the IP parameters to your configuration computer. During the configuration phase, the configuration computer is located in subnet 100. This is necessary, so that the configuration computer has access to the Layer 3 devices throughout the entire configuration phase.
- Start HiDiscovery on your configuration computer.
Assign the IP parameters to every Layer 2 and Layer 3 device in accordance with the network plan. When you have completed the following router configuration, you can access the devices in subnets 10 to 14 again.

Configure the Routing function for the Layer 3 devices.

Note the sequence:
First the Layer 3 device C.
Then the Layer 3 device B.
The sequence is necessary; you thus retain access to the devices.
When you assign an IP address from the subnetwork of the device management IP address (= SN 100) to a router interface, the device deletes the IP address of the device management. You access the device management via the IP address of the router interface.

Perform the following steps:
Configure the Routing function for Layer 3 device A.
You first configure the router interface at a port to which the configuration computer is connected. The result of this is that in future you will access the Layer 3 device via subnet 10.
Change the IP parameters of your configuration computer to the values for subnetwork 10. You thus access Layer 3 device A again, namely via the IP address of the router interface set up beforehand.
Finish the router configuration for Layer 3 device A (see figure 66).

After configuring the Routing function on every Layer 3 device, you have access to every device.
14 Operation diagnosis

The device provides you with the following diagnostic tools:
- Sending SNMP traps
- Monitoring the Device Status
- Out-of-Band signaling using the signal contact
- Port status indication
- Event counter at port level
- Detecting non-matching duplex modes
- Auto-Disable
- Displaying the SFP status
- Topology discovery
- Detecting IP address conflicts
- Detecting loops
- Reports
- Monitoring data traffic on a port (port mirroring)
- Syslog
- Event log
- Cause and action management during selftest

14.1 Sending SNMP traps

The device immediately reports unusual events which occur during normal operation to the network management station. This is done by messages called SNMP traps that bypass the polling procedure (“polling” means querying the data stations at regular intervals). SNMP traps allow you to react quickly to unusual events.

Examples of such events are:
- Hardware reset
- Changes to the configuration
- Segmentation of a port

The device sends SNMP traps to various hosts to increase the transmission reliability for the messages. The unacknowledged SNMP trap message consists of a packet containing information about an unusual event.

The device sends SNMP traps to those hosts entered in the trap destination table. The device lets you configure the trap destination table with the network management station using SNMP.
## 14.1 Sending SNMP traps

### 14.1.1 List of SNMP traps

The following table displays possible SNMP traps sent by the device.

<table>
<thead>
<tr>
<th>Name of the SNMP trap</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>authenticationFailure</td>
<td>When a station attempts to access an agent without authorisation, this trap is sent.</td>
</tr>
<tr>
<td>coldStart</td>
<td>Sent after a restart.</td>
</tr>
<tr>
<td>hm2DevMonSenseExtNvmRemoval</td>
<td>When the external memory has been removed, this trap is sent.</td>
</tr>
<tr>
<td>linkDown</td>
<td>When the connection to a port is interrupted, this trap is sent.</td>
</tr>
<tr>
<td>linkUp</td>
<td>When connection is established to a port, this trap is sent.</td>
</tr>
<tr>
<td>hm2DevMonSensePSState</td>
<td>When the status of a power supply unit changes, this trap is sent.</td>
</tr>
<tr>
<td>hm2SigConStateChange</td>
<td>When the status of the signal contact changes in the operation monitoring, this trap is sent.</td>
</tr>
<tr>
<td>newRoot</td>
<td>When the sending agent becomes the new root of the spanning tree, this trap is sent.</td>
</tr>
<tr>
<td>topologyChange</td>
<td>When the port changes from blocking to forwarding or from forwarding to blocking, this trap is sent.</td>
</tr>
<tr>
<td>alarmRisingThreshold</td>
<td>When the RMON input exceeds its upper threshold, this trap is sent.</td>
</tr>
<tr>
<td>alarmFallingThreshold</td>
<td>When the RMON input goes below its lower threshold, this trap is sent.</td>
</tr>
<tr>
<td>hm2AgentPortSecurityViolation</td>
<td>When a MAC address detected on this port does not match the current settings of the parameter hm2AgentPortSecurityEntry, this trap is sent.</td>
</tr>
<tr>
<td>hm2DiagSelftestActionTrap</td>
<td>When a self test for the four categories “task”, “resource”, “software”, and “hardware” is performed according to the configured settings, this trap is sent.</td>
</tr>
<tr>
<td>hm2MrpReconfig</td>
<td>When the configuration of the MRP ring changes, this trap is sent.</td>
</tr>
<tr>
<td>hm2DiagIfaceUtilizationTrap</td>
<td>When the threshold of the interface exceeds or undercuts the upper or lower threshold specified, this trap is sent.</td>
</tr>
<tr>
<td>hm2LogAuditStartNextSector</td>
<td>When the audit trail after completing one sector starts a new one, this trap is sent.</td>
</tr>
<tr>
<td>hm2ConfigurationSavedTrap</td>
<td>After the device has successfully saved its configuration locally, this trap is sent.</td>
</tr>
<tr>
<td>hm2ConfigurationChangedTrap</td>
<td>When you change the configuration of the device for the first time after it has been saved locally, this trap is sent.</td>
</tr>
<tr>
<td>hm2PlatformStpInstanceLoopInconsistentStartTrap</td>
<td>When the port in this STP instance changes to the “loop inconsistent” status, this trap is sent.</td>
</tr>
<tr>
<td>hm2PlatformStpInstanceLoopInconsistentEndTrap</td>
<td>When the port in this STP instance leaves the “loop inconsistent” status receiving a BPDU packet, this trap is sent.</td>
</tr>
</tbody>
</table>
14.1.2 SNMP traps for configuration activity

After you save a configuration in the memory, the device sends a `hm2ConfigurationSavedTrap`. This SNMP trap contains both the state variables of non-volatile memory (NVM) and external memory (ENVM) indicating if the running configuration is in sync with the non-volatile memory, and with the external memory. You can also trigger this SNMP trap by copying a configuration file to the device, replacing the active saved configuration.

Furthermore, the device sends a `hm2ConfigurationChangedTrap`, whenever you change the local configuration, indicating a mismatch between the running and saved configuration.

14.1.3 SNMP trap setting

The device lets you send an SNMP trap as a reaction to specific events. Create at least one trap destination that receives SNMP traps.

Perform the following steps:

- Open the `Diagnostics > Status Configuration > Alarms (Traps)` dialog.
- Click the `+` button. The dialog displays the `Create` window.
- In the `Name` frame, specify the name that the device uses to identify itself as the source of the SNMP trap.
- In the `Address` frame, specify the IP address of the trap destination to which the device sends the SNMP traps.
- In the `Active` column you select the entries that the device should take into account when it sends SNMP traps.
- Save the changes temporarily. To do this, click the `✓` button.

For example, in the following dialogs you specify when the device triggers an SNMP trap:
- `Basic Settings > Port` dialog
- `Network Security > Packet Filter > Rule` dialog
- `Routing > OSPF > Global` dialog
- `Routing > Tracking > Configuration` dialog
- `Routing > L3-Redundancy > VRRP > Configuration` dialog
- `Routing > NAT > 1:1 NAT > Rule` dialog
- `Routing > NAT > Destination NAT > Rule` dialog
- `Routing > NAT > Masquerading NAT > Rule` dialog
- `Routing > NAT > Double NAT > Rule` dialog
- `Diagnostics > Status Configuration > Device Status` dialog
- `Diagnostics > Status Configuration > Security Status` dialog
- `Diagnostics > Status Configuration > Signal Contact` dialog
- `Diagnostics > System > Selftest` dialog
14.1.4 **ICMP messaging**

The device lets you use the Internet Control Message Protocol (ICMP) for diagnostic applications, for example ping and trace route. The device also uses ICMP for time-to-live and discarding messages in which the device forwards an ICMP message back to the packet source device.

Use the ping network tool to test the path to a particular host across an IP network. The traceroute diagnostic tool displays paths and transit delays of packets across a network.
14.2 Monitoring the 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.

The device enables you to:
- Out-of-Band signalling using a signal contact
- signal the changed device status by sending an SNMP trap
- detect the device status in the *Basic Settings > System* dialog of the Graphical User Interface
- query the device status in the Command Line Interface

The *Global* tab of the *Diagnostics > Status Configuration > Device Status* dialog lets you configure the device to send a trap to the management station for the following events:
- Incorrect supply voltage
  - at least one of the 2 supply voltages is not operating
  - the internal supply voltage is not operating
- When the device is operating outside of the user-defined temperature threshold
- The interruption of link connection(s)
  Configure at least one port for this feature. When the link is down, you specify which ports the device signals in the *Port* tab of the *Diagnostics > Status Configuration > Device Status* dialog in the *Propagate connection error* row.
- The removal of the external memory.
- The configuration in the external memory is out-of-sync with the configuration in the device.

Select the corresponding entries to decide which events the device status includes.

**Note:** With a non-redundant voltage supply, the device reports the absence of a supply voltage. To disable this message, feed the supply voltage over both inputs or ignore the monitoring.

14.2.1 Events which can be monitored

<table>
<thead>
<tr>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>Monitors in case the temperature exceeds or falls below the value specified.</td>
</tr>
<tr>
<td>Connection errors</td>
<td>Enable this function to monitor every port link event in which the <em>Propagate connection error</em> checkbox is active.</td>
</tr>
<tr>
<td>External memory removal</td>
<td>Enable this function to monitor the presence of an external storage device.</td>
</tr>
<tr>
<td>External memory not in sync</td>
<td>The device monitors synchronization between the device configuration and the configuration stored in the external memory (<em>ENVM</em>).</td>
</tr>
<tr>
<td>Power supply</td>
<td>Enable this function to monitor the power supply.</td>
</tr>
</tbody>
</table>
14.2 Monitoring the Device Status

14.2.2 Configuring the Device Status

Perform the following steps:

- Open the Diagnostics > Status Configuration > Device Status dialog, Global tab.
- For the parameters to be monitored, mark the checkbox in the Monitor column.
- To send an SNMP trap to the management station, activate the Send trap function in the Traps frame.
- In the Diagnostics > Status Configuration > Alarms (Traps) dialog, create at least one trap destination that receives SNMP traps.
- Save the changes temporarily. To do this, click the button.
- Open the Basic Settings > System dialog.
- To monitor the temperature, at the bottom of the System data frame, you specify the temperature thresholds.
- Save the changes temporarily. To do this, click the button.

In order to enable the device to monitor an active link without a connection, first enable the global function, then enable the individual ports.

Perform the following steps:

- Open the Diagnostics > Status Configuration > Device Status dialog, Global tab.
- For the Connection errors parameter, mark the checkbox in the Monitor column.
14.2 Monitoring the Device Status

Perform the following steps:

- Open the Diagnostics > Status Configuration > Device Status dialog, Port tab.
- For the Propagate connection error parameter, mark the checkbox in the column of the ports to be monitored.
- Save the changes temporarily. To do this, click the button.

```
enable
configure
device-status monitor link-failure
  interface 1/1
device-status link-alarm
```

### Note:
The above commands activate monitoring and trapping for the supported components. When you want to activate or deactivate monitoring for individual components, you will find the corresponding syntax in the "Command Line Interface" reference manual or in the help of the Command Line Interface console. To display the help in Command Line Interface, insert a question mark `?` and press the <Enter> key.

14.2.3 Displaying the Device Status

Perform the following steps:

- Open the Basic Settings > System dialog.

```
show device-status all
```

In the EXEC Privilege mode: Displays the device status and the setting for the device status determination.
14.3 Security Status

The Security Status provides an overview of the overall security of the device. Many processes aid in system visualization by recording the security status of the device and then presenting its condition in graphic form. The device displays the overall security status in the Basic Settings > System dialog, Security status frame.

In the Global tab of the Diagnostics > Status Configuration > Security Status dialog the device displays its current status as error or ok in the Security status frame. The device determines this status from the individual monitoring results.

The device enables you to:
- Out-of-Band signalling using a signal contact
- signal the changed security status by sending an SNMP trap
- detect the security status in the Basic Settings > System dialog of the Graphical User Interface
- query the security status in the Command Line Interface

14.3.1 Events which can be monitored

Perform the following steps:
- Specify the events that the device monitors.
- For the corresponding parameter, mark the checkbox in the Monitor column.

Table 31: Security Status events

<table>
<thead>
<tr>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password default settings unchanged</td>
<td>After installation change the passwords to increase security. When active and the default passwords remain unchanged, the device displays an alarm.</td>
</tr>
<tr>
<td>Min. password length &lt; 8</td>
<td>Create passwords more than 8 characters long to maintain a high security posture. When active, the device monitors the Min. password length setting.</td>
</tr>
<tr>
<td>Password policy settings deactivated</td>
<td>The device monitors the settings located in the Device Security &gt; User Management dialog for password policy requirements.</td>
</tr>
<tr>
<td>User account password policy check deactivated</td>
<td>The device monitors the settings of the Policy check checkbox. When Policy check is inactive, the device sends an SNMP trap.</td>
</tr>
<tr>
<td>HTTP server active</td>
<td>The device monitors when you enable the HTTP function.</td>
</tr>
<tr>
<td>SNMP unencrypted</td>
<td>The device monitors when you enable the SNMPv1 or SNMPv2 function.</td>
</tr>
<tr>
<td>Access to system monitor with serial interface possible</td>
<td>The device monitors the System Monitor status.</td>
</tr>
<tr>
<td>Saving the configuration profile on the external memory possible</td>
<td>The device monitors the possibility to save configurations to the external non-volatile memory.</td>
</tr>
<tr>
<td>Link interrupted on enabled device ports</td>
<td>The device monitors the link status of active ports.</td>
</tr>
</tbody>
</table>
### 14.3 Security Status

#### 14.3.2 Configuring the Security Status

Perform the following steps:

- Open the **Diagnostics > Status Configuration > Security Status** dialog, **Global** tab.
- For the parameters to be monitored, mark the checkbox in the **Monitor** column.
- To send an SNMP trap to the management station, activate the **Send trap** function in the **Traps** frame.
- Save the changes temporarily. To do this, click the **✓** button.
- In the **Diagnostics > Status Configuration > Alarms (Traps)** dialog, create at least one trap destination that receives SNMP traps.

<table>
<thead>
<tr>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access with HiDiscovery possible</strong></td>
<td>The device monitors when you enable the HiDiscovery read/write access function.</td>
</tr>
<tr>
<td><strong>Load unencrypted config from external memory</strong></td>
<td>The device monitors the security settings for loading the configuration from the external NVM.</td>
</tr>
<tr>
<td><strong>Self-signed HTTPS certificate present</strong></td>
<td>The device monitors the HTTPS server for self-created digital certificates.</td>
</tr>
</tbody>
</table>

Table 31: **Security Status events (cont.)**

- **Security status**
- **Diagnostics**
- **Status Configuration**
- **Security Status**
- **Events (cont.)**
In order to enable the device to monitor an active link without a connection, first enable the global function, then enable the individual ports.

Perform the following steps:

1. Open the Diagnostics > Status Configuration > Security Status dialog, Global tab.
2. For the Link interrupted on enabled device ports parameter, mark the checkbox in the Monitor column.
3. Save the changes temporarily. To do this, click the button.
4. Open the Diagnostics > Status Configuration > Device Status dialog, Port tab.
5. For the Link interrupted on enabled device ports parameter, mark the checkbox in the column of the ports to be monitored.
6. Save the changes temporarily. To do this, click the button.

```
security-status monitor snmp-unsecure
Monitors the SNMP server.
When at least one of the following conditions applies, the value in the Security status frame changes to error:
- The SNMPv1 function is enabled.
- The SNMPv2 function is enabled.
- The encryption for SNMPv3 is disabled.
You enable the encryption in the Device Security > User Management dialog, in the SNMP encryption type field.
```

```
security-status monitor sysmon-enabled
To monitor the activation of System Monitor 1 in the device.
security-status monitor extnvm-upd-enabled
To monitor the activation of the external non volatile memory update.
security-status trap
When the device status changes, it sends an SNMP trap.
```

```
security-status monitor no-link-enabled
Monitors the link on active ports. When the link interrupts on an active port, the value in the Security status frame changes to error.
```

```
interface 1/1
Change to the interface configuration mode of interface 1/1.
```

```
security-status monitor no-link
Monitors the link on interface/port 1.
```

### 14.3.3 Displaying the Security Status

Perform the following steps:

1. Open the Basic Settings > System dialog.
show security-status all

In the EXEC Privilege mode, display the security status and the setting for the security status determination.
14.4 Out-of-Band signaling

The device uses the signal contact to control external devices and monitor device functions. Function monitoring enables you to perform remote diagnostics.

The device reports the operating status using a break in the potential-free signal contact (relay contact, closed circuit) for the selected mode. The device monitors the following functions:

- Incorrect supply voltage
  - at least one of the 2 supply voltages is not operating
  - the internal supply voltage is not operating
- When the device is operating outside of the user-defined temperature threshold
- The interruption of link connection(s)
  Configure at least one port for this feature. In the Propagate connection error frame, you specify which ports the device signals for a link interruption. In the default setting, link monitoring is inactive.
- The removal of the external memory.
- The configuration in the external memory does not match the configuration in the device.

Select the corresponding entries to decide which events the device status includes.

Note: With a non-redundant voltage supply, the device reports the absence of a supply voltage. To disable this message, feed the supply voltage over both inputs or ignore the monitoring.

14.4.1 Controlling the Signal contact

With the Manual setting mode you control this signal contact remotely.

Application options:

- Simulation of an error detected during SPS error monitoring
- Remote control of a device using SNMP, such as switching on a camera

Perform the following steps:

- Open the Diagnostics > Status Configuration > Signal Contact dialog, Global tab.
- To control the signal contact manually, in the Configuration frame, select the Manual setting item in the Mode drop-down list.
- To open the signal contact, you select the open radio button in the Configuration frame.
- To close the signal contact, you select the close radio button in the Configuration frame.
- Save the changes temporarily. To do this, click the enable button.

Enable
configure
signal-contact 1 mode manual
signal-contact 1 state open
signal-contact 1 state closed

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Select the manual setting mode for signal contact 1.
Open signal contact 1.
Close signal contact 1.
14.4.2 Monitoring the Device and Security Statuses

In the Configuration field, you specify which events the signal contact indicates.

- **Device status**
  Using this setting the signal contact indicates the status of the parameters monitored in the Diagnostics > Status Configuration > Device Status dialog.

- **Security status**
  Using this setting the signal contact indicates the status of the parameters monitored in the Diagnostics > Status Configuration > Security Status dialog.

- **Device/Security status**
  Using this setting the signal contact indicates the status of the parameters monitored in the Diagnostics > Status Configuration > Device Status and the Diagnostics > Status Configuration > Security Status dialog.

Configuring the operation monitoring

Perform the following steps:

- Open the Diagnostics > Status Configuration > Signal Contact dialog, Global tab.
- To monitor the device functions using the signal contact, in the Configuration frame, specify the value Monitoring correct operation in the Mode field.
- For the parameters to be monitored, mark the checkbox in the Monitor column.
- To send an SNMP trap to the management station, activate the Send trap function in the Traps frame.
- Save the changes temporarily. To do this, click the button.
- In the Diagnostics > Status Configuration > Alarms (Traps) dialog, create at least one trap destination that receives SNMP traps.
- Save the changes temporarily. To do this, click the button.
- You specify the temperature thresholds for the temperature monitoring in the Basic Settings > System dialog.

```
enable
configure
signal-contact 1 monitor temperature

signal-contact 1 monitor ring-redundancy

signal-contact 1 monitor link-failure

signal-contact 1 monitor envm-removal
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Change to the Privileged EXEC mode.</td>
</tr>
<tr>
<td><code>configure</code></td>
<td>Change to the Configuration mode.</td>
</tr>
<tr>
<td><code>signal-contact 1 monitor temperature</code></td>
<td>Monitors the temperature in the device. When the temperature exceeds / falls below the threshold values, the signal contact opens.</td>
</tr>
<tr>
<td><code>signal-contact 1 monitor ring-redundancy</code></td>
<td>Monitors the ring redundancy. The signal contact opens in the following situations:</td>
</tr>
<tr>
<td></td>
<td>- The redundancy function becomes active (loss of redundancy reserve).</td>
</tr>
<tr>
<td></td>
<td>- The device is a normal ring participant and detects an error in its settings.</td>
</tr>
<tr>
<td><code>signal-contact 1 monitor link-failure</code></td>
<td>Monitors the ports/interfaces link. When the link interrupts on a monitored port/interface, the signal contact opens.</td>
</tr>
<tr>
<td><code>signal-contact 1 monitor envm-removal</code></td>
<td>Monitors the active external memory. When you remove the active external memory from the device, the signal contact opens.</td>
</tr>
</tbody>
</table>
In order to enable the device to monitor an active link without a connection, first enable the global function, then enable the individual ports.

Perform the following steps:

- In the Monitor column, activate the Link interrupted on enabled device ports function.
- Open the Diagnostics > Status Configuration > Device Status dialog, Port tab.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Change to the Privileged EXEC mode.</td>
</tr>
<tr>
<td>configure</td>
<td>Change to the Configuration mode.</td>
</tr>
<tr>
<td>signal-contact 1 monitor link-failure</td>
<td>Monitors the ports/interfaces link. When the link interrupts on a monitored port/interface, the signal contact opens.</td>
</tr>
<tr>
<td>interface 1/1</td>
<td>Change to the interface configuration mode of interface 1/1.</td>
</tr>
<tr>
<td>signal-contact 1 link-alarm</td>
<td>Monitors the port/interface link. When the link interrupts on the port/interface, the signal contact opens.</td>
</tr>
</tbody>
</table>

**Events which can be monitored**

<table>
<thead>
<tr>
<th>Event</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>When the temperature exceeds or falls below the value specified.</td>
</tr>
<tr>
<td>Connection errors</td>
<td>Enable this function to monitor every port link event in which the Propagate connection error checkbox is active.</td>
</tr>
</tbody>
</table>
Displaying the signal contact's status

The device gives you additional options for displaying the status of the signal contact:

- Display in the Graphical User Interface
- Query in the Command Line Interface

Perform the following steps:

1. Open the Basic Settings > System dialog.
   
   The Signal contact status frame displays the signal contact status and informs you about alarms that have occurred. When an alarm currently exists, the frame is highlighted.

2. show signal-contact 1 all
   
   Displays signal contact settings for the specified signal contact.

<table>
<thead>
<tr>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>External memory not in sync with NVM</td>
<td>The device monitors synchronization between the device configuration and the configuration stored in the external memory (<strong>ENVM</strong>).</td>
</tr>
<tr>
<td>External memory removed</td>
<td>Enable this function to monitor the presence of an external storage device.</td>
</tr>
<tr>
<td>Power supply</td>
<td>Enable this function to monitor the power supply.</td>
</tr>
</tbody>
</table>

Table 32:  Device Status events (cont.)
14.5 Port status indication

To view the status of the ports, perform the following steps:

- Open the Basic Settings > System dialog.

The dialog displays the device with the current configuration. Furthermore, the dialog indicates the status of the individual ports with a symbol.

The following symbols represent the status of the individual ports. In some situations, these symbols interfere with one another. When you position the mouse pointer over the port icon, a bubble help displays a detailed description of the port state.

Table 33: Symbols identifying the status of the ports

<table>
<thead>
<tr>
<th>Criterion</th>
<th>Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth of the port</td>
<td>* 10 Mbit/s</td>
</tr>
<tr>
<td></td>
<td>Port activated, connection okay, full-duplex mode</td>
</tr>
<tr>
<td></td>
<td>* 100 Mbit/s</td>
</tr>
<tr>
<td></td>
<td>Port activated, connection okay, full-duplex mode</td>
</tr>
<tr>
<td></td>
<td>* 1000 Mbit/s</td>
</tr>
<tr>
<td></td>
<td>Port activated, connection okay, full-duplex mode</td>
</tr>
<tr>
<td>Operating state</td>
<td>§ Half-duplex mode enabled</td>
</tr>
<tr>
<td></td>
<td>See the Basic Settings &gt; Port dialog, Configuration tab, Automatic configuration checkbox, Manual configuration field and Manual cable crossing (Auto. conf. off) field.</td>
</tr>
<tr>
<td></td>
<td>¶ Autonegotiation enabled</td>
</tr>
<tr>
<td></td>
<td>See the Basic Settings &gt; Port dialog, Configuration tab, Automatic configuration checkbox.</td>
</tr>
<tr>
<td>AdminLink</td>
<td>-= The port is deactivated, connection okay</td>
</tr>
<tr>
<td></td>
<td>The port is deactivated, no connection set up</td>
</tr>
<tr>
<td></td>
<td>See the Basic Settings &gt; Port dialog, Configuration tab, Port on checkbox and Link/Current settings field.</td>
</tr>
</tbody>
</table>
14.6 Port event counter

The port statistics table lets experienced network administrators identify possible detected problems in the network.

This table displays the contents of various event counters. The packet counters add up the events sent and the events received. In the Basic Settings > Restart dialog, you can reset the event counters.

Table 34: Examples indicating known weaknesses

<table>
<thead>
<tr>
<th>Counter</th>
<th>Indication of known possible weakness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received fragments</td>
<td>• Non-functioning controller of the connected device</td>
</tr>
<tr>
<td></td>
<td>• Electromagnetic interference in the transmission medium</td>
</tr>
<tr>
<td>CRC Error</td>
<td>• Non-functioning controller of the connected device</td>
</tr>
<tr>
<td></td>
<td>• Electromagnetic interference in the transmission medium</td>
</tr>
<tr>
<td></td>
<td>• Inoperable component in the network</td>
</tr>
<tr>
<td>Collisions</td>
<td>• Non-functioning controller of the connected device</td>
</tr>
<tr>
<td></td>
<td>• Network over extended/lines too long</td>
</tr>
<tr>
<td></td>
<td>• Collision or a detected fault with a data packet</td>
</tr>
</tbody>
</table>

Perform the following steps:

☐ To display the event counter, open the Basic Settings > Port dialog, Statistics tab.
☐ To reset the counters, in the Basic Settings > Restart dialog, click the Clear port statistics button.

14.6.1 Detecting non-matching duplex modes

Problems occur when 2 ports directly connected to each other have mismatching duplex modes. These problems are difficult to track down. The automatic detection and reporting of this situation has the benefit of recognizing mismatching duplex modes before problems occur.

This situation arises from an incorrect configuration, for example, deactivation of the automatic configuration on the remote port.

A typical effect of this non-matching is that at a low data rate, the connection seems to be functioning, but at a higher bi-directional traffic level the local device records a lot of CRC errors, and the connection falls significantly below its nominal capacity.

The device lets you detect this situation and report it to the network management station. In the process, the device evaluates the error counters of the port in the context of the port settings.

Possible causes of port error events

The following table lists the duplex operating modes for TX ports, with the possible fault events. The meanings of terms used in the table are as follows:

- Collisions
  - In half-duplex mode, collisions mean normal operation.
- Duplex problem
  - Mismatching duplex modes.
Operation diagnosis
14.6 Port event counter

- **EMI**
  - Electromagnetic interference.

- **Network extension**
  - The network extension is too great, or too many cascading hubs.

- **Collisions, Late Collisions**
  - In full-duplex mode, no incrementation of the port counters for collisions or Late Collisions.

- **CRC Error**
  - The device evaluates these errors as non-matching duplex modes in the manual full duplex mode.

**Table 35: Evaluation of non-matching of the duplex mode**

<table>
<thead>
<tr>
<th>No.</th>
<th>Automatic configuration</th>
<th>Current duplex mode</th>
<th>Detected error events (≥ 10 after link up)</th>
<th>Duplex modes</th>
<th>Possible causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>marked</td>
<td>Half duplex</td>
<td>None</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>marked</td>
<td>Half duplex</td>
<td>Collisions</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>marked</td>
<td>Half duplex</td>
<td>Late Collisions</td>
<td>Duplex problem detected</td>
<td>Duplex problem, EMI, network extension</td>
</tr>
<tr>
<td>4</td>
<td>marked</td>
<td>Half duplex</td>
<td>CRC Error</td>
<td>OK</td>
<td>EMI</td>
</tr>
<tr>
<td>5</td>
<td>marked</td>
<td>Full duplex</td>
<td>None</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>marked</td>
<td>Full duplex</td>
<td>Collisions</td>
<td>OK</td>
<td>EMI</td>
</tr>
<tr>
<td>7</td>
<td>marked</td>
<td>Full duplex</td>
<td>Late Collisions</td>
<td>OK</td>
<td>EMI</td>
</tr>
<tr>
<td>8</td>
<td>marked</td>
<td>Full duplex</td>
<td>CRC Error</td>
<td>OK</td>
<td>EMI</td>
</tr>
<tr>
<td>9</td>
<td>unmarked</td>
<td>Half duplex</td>
<td>None</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>unmarked</td>
<td>Half duplex</td>
<td>Collisions</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>unmarked</td>
<td>Half duplex</td>
<td>Late Collisions</td>
<td>Duplex problem detected</td>
<td>Duplex problem, EMI, network extension</td>
</tr>
<tr>
<td>12</td>
<td>unmarked</td>
<td>Half duplex</td>
<td>CRC Error</td>
<td>OK</td>
<td>EMI</td>
</tr>
<tr>
<td>13</td>
<td>unmarked</td>
<td>Full duplex</td>
<td>None</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>unmarked</td>
<td>Full duplex</td>
<td>Collisions</td>
<td>OK</td>
<td>EMI</td>
</tr>
<tr>
<td>15</td>
<td>unmarked</td>
<td>Full duplex</td>
<td>Late Collisions</td>
<td>OK</td>
<td>EMI</td>
</tr>
<tr>
<td>16</td>
<td>unmarked</td>
<td>Full duplex</td>
<td>CRC Error</td>
<td>Duplex problem detected</td>
<td>Duplex problem, EMI</td>
</tr>
</tbody>
</table>
14.7 Displaying the SFP status

The SFP status display lets you look at the current SFP module connections and their properties. The properties include:

- module type
- serial number of media module
- temperature in °C
- transmission power in mW
- receive power in mW

Perform the following step:

☐ Open the Diagnostics > Ports > SFP dialog.
14.8 **Topology discovery**

IEEE 802.1AB defines the Link Layer Discovery Protocol (LLDP). LLDP lets you automatically detect the LAN network topology.

Devices with LLDP active:
- broadcast their connection and management information to neighboring devices on the shared LAN. When the receiving device has its LLDP function active, evaluation of the devices occur.
- receive connection and management information from neighboring devices on the shared LAN, provided these adjacent devices also have LLDP active.
- build a management information database and object definitions for storing information about adjacent devices with LLDP active.

As the main element, the connection information contains an exact, unique identifier for the connection end point: MAC (Service Access Point). This is made up of a device identifier which is unique on the entire network and a unique port identifier for this device.
- Chassis identifier (its MAC address)
- Port identifier (its port-MAC address)
- Description of port
- System name
- System description
- Supported system capabilities
- System capabilities currently active
- Interface ID of the management address
- VLAN-ID of the port
- Auto-negotiation status on the port
- Medium, half/full duplex setting and port speed setting
- Information about the VLANs installed in the device (VLAN-ID and VLAN name, irrespective of whether the port is a VLAN participant).

A network management station can call up this information from devices with activated LLDP. This information enables the network management station to map the topology of the network.

Non-LLDP devices normally block the special Multicast LLDP IEEE MAC address used for information exchange. Non-LLDP devices therefore discard LLDP packets. If you position a non-LLDP capable device between 2 LLDP capable devices, then the non-LLDP capable device prohibits information exchanges between the 2 LLDP capable devices.

The Management Information Base (MIB) for a device with LLDP capability holds the LLDP information in the lldp MIB and in the private HM2-LLDP-EXT-HM-MIB and HM2-LLDP-MIB.

### 14.8.1 Displaying the Topology discovery results

Display the topology of the network. To do this, perform the following step:

- Open the **Diagnostics > LLDP > Topology Discovery** dialog, **LLDP** tab.

When you use a port to connect several devices, for example via a hub, the table contains a line for each connected device.

Activating Display FDB Entries at the bottom of the table lets you display devices without active LLDP support in the table. In this case, the device also includes information from its FDB (forwarding database).
If you connect the port to devices with the topology discovery function active, then the devices exchange LLDP Data Units (LLDPDU) and the topology table displays these neighboring devices.

When a port connects only devices without an active topology discovery, the table contains a line for this port to represent the connected devices. This line contains the number of connected devices.

The FDB address table contains MAC addresses of devices that the topology table hides for the sake of clarity.
14.9 Reports

The following lists reports and buttons available for diagnostics:

- **System Log file**
  The log file is an HTML file in which the device writes device-internal events.

- **Audit Trail**
  Logs successful commands and user comments. The file also includes SNMP logging.

- **Persistent Logging**
  When the external memory is present, the device saves log entries in a file in the external memory. These files are available after power down. The maximum size, maximum number of retainable files, and the severity of logged events are configurable. After obtaining the user-defined maximum size or maximum number of retainable files, the device archives the entries and starts a new file. The device deletes the oldest file and renames the other files to maintain the configured number of files. To review these files use the Command Line Interface or copy them to an external server for future reference.

- **Download support information**
  This button lets you download system information as a ZIP archive.

In service situations, these reports provide the technician with the necessary information.

14.9.1 Global settings

Using this dialog you enable or disable where the device sends reports, for example, to a Console, a Syslog Server, or a connection to the Command Line Interface. You also set at which severity level the device writes events into the reports.

Perform the following steps:

- Open the **Diagnostics > Report > Global** dialog.
- To send a report to the console, specify the desired level in the **Console logging** frame, **Severity** field.
- To enable the function, select the **On** radio button in the **Console logging** frame.
- Save the changes temporarily. To do this, click the ✅ button.

The device buffers logged events in 2 separate storage areas so that the device keeps log entries for urgent events. Specify the minimum severity for events that the device logs to the buffered storage area with a higher priority.

Perform the following steps:

- To send events to the buffer, specify the desired level in the **Buffered logging** frame, **Severity** field.
- Save the changes temporarily. To do this, click the ✅ button.

When you activate the logging of SNMP requests, the device logs the requests as events in the Syslog. The **Log SNMP get request** function logs user requests for device configuration information. The **Log SNMP set request** function logs device configuration events. Specify the minimum level for events that the device logs in the Syslog.
Perform the following steps:

- Enable the *Log SNMP get request* function for the device in order to send SNMP Read requests as events to the Syslog server.
  
  To enable the function, select the *On* radio button in the *SNMP logging* frame.

- Enable the *Log SNMP set request* function for the device in order to send SNMP Write requests as events to the Syslog server.
  
  To enable the function, select the *On* radio button in the *SNMP logging* frame.

- Choose the desired severity level for the get and set requests.

- Save the changes temporarily. To do this, click the ✔️ button.

When active, the device logs configuration changes made using the Command Line Interface, to the audit trail. This feature is based on the IEEE 1686 standard for Substation Intelligent Electronic Devices.

Perform the following steps:

- Open the *Diagnostics > Report > Global* dialog.

  To enable the function, select the *On* radio button in the *CLI logging* frame.

- Save the changes temporarily. To do this, click the ✔️ button.

The device lets you save the following system information data in one ZIP file on your PC:

- `audittrail.html`
- `CLICommands.txt`
- `defaultconfig.xml`
- `script`
- `runningconfig.xml`
- `supportinfo.html`
- `systeminfo.html`
- `systemlog.html`

The device creates the file name of the ZIP archive automatically in the format `<IP_address>_system_name>.zip`.

Perform the following steps:

- Click the ☐️ button and then the *Download support information* item.

- Select the directory in which you want to save the support information.

- Save the changes temporarily. To do this, click the ✔️ button.
14.9.2 **Syslog**

The device enables you to send messages about device internal events to one or more Syslog servers (up to 8). Additionally, you also include SNMP requests to the device as events in the Syslog.

**Note:** To display the logged events, open the Diagnostics > Report > Audit Trail dialog or the Diagnostics > Report > System Log dialog.

Perform the following steps:

- Open the Diagnostics > Syslog dialog.
- To add a table entry, click the button.
- In the IP address column, enter the IP address or Hostname of the Syslog server.
- In the Destination UDP port column, specify the UDP port on which the Syslog server expects the log entries.
- In the Min. severity column, specify the minimum severity level that an event requires for the device to send a log entry to this Syslog server.
- Mark the checkbox in the Active column.
- To enable the function, select the On radio button in the Operation frame.
- Save the changes temporarily. To do this, click the button.

In the SNMP logging frame, configure the following settings for read and write SNMP requests:

Perform the following steps:

- Open the Diagnostics > Report > Global dialog.
- Enable the Log SNMP get request function for the device in order to send SNMP Read requests as events to the Syslog server.
  - To enable the function, select the On radio button in the SNMP logging frame.
- Enable the Log SNMP set request function for the device in order to send SNMP Write requests as events to the Syslog server.
  - To enable the function, select the On radio button in the SNMP logging frame.
- Choose the desired severity level for the get and set requests.
- Save the changes temporarily. To do this, click the button.

```
enable
configure
logging host add 1 addr 10.0.1.159 severity 3
logging syslog operation
exit
show logging host
```

<table>
<thead>
<tr>
<th>No.</th>
<th>Server IP</th>
<th>Port</th>
<th>Max. Severity</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.0.1.159</td>
<td>514</td>
<td>error</td>
<td>systemlog</td>
<td>active</td>
</tr>
</tbody>
</table>

Change to the Privileged EXEC mode.

Change to the Configuration mode.

Add a new recipient in the Syslog servers list. The value 3 specifies the severity level of the event that the device logs. The value 3 means error.

Enable the Syslog function.

Change to the Privileged EXEC mode.

Display the Syslog host settings.

```
show logging host
```
14.9.3 System Log

The device lets you call up a log file of the system events. The table in the Diagnostics > Report > System Log dialog lists the logged events.

Perform the following steps:

- To update the content of the log, click the button.
- To save the content of the log as an html file, click the button and then the Reset item.
- To delete the content of the log, click the button and then the Reset item.
- To search the content of the log for a key word, use the search function of your web browser.

Note: You have the option to also send the logged events to one or more Syslog servers.

14.9.4 Audit Trail

The Diagnostics > Report > Audit Trail dialog contains system information and changes to the device configuration performed through the Command Line Interface and SNMP. In the case of device configuration changes, the dialog displays Who changed What and When.

The Diagnostics > Syslog dialog lets you specify up to 8 Syslog servers to which the device sends Audit Trails.

The following list contains log events:

- changes to configuration parameters
- Commands (except show commands) using the Command Line Interface
- Command logging audit-trail <string> using the Command Line Interface which logs the comment
- Automatic changes to the System Time
- watchdog events
- locking a user after several unsuccessful login attempts
- User login, either locally or remote, using the Command Line Interface
Operation diagnosis
14.9 Reports

- Manual, user-initiated, logout
- Timed logout after a user-defined period of inactivity in the Command Line Interface
- file transfer operation including a Firmware Update
- Configuration changes using HiDiscovery
- Automatic configuration or firmware updates using the external memory
- Blocked access to the device management due to invalid login
- Rebooting
- Opening and closing SNMP over HTTPS tunnels
- Detected power failures
15 Advanced functions of the device

15.1 Using the device as a DNS client

The Domain Name System (DNS) client queries DNS servers to resolve host names and IP addresses of network devices. Much like a telephone book, the DNS client converts names of devices into IP addresses. When the DNS client receives a request to resolve a new name, the DNS client first queries its internal static database, then the assigned DNS servers for the information. The DNS client saves the queried information in a cache for future requests.

The device lets you assign host names to IP addresses statically.

The DNS client provides the following user functions:
- DNS server list, with space for 4 domain name server IP addresses
- host cache, with space for 128 entries

15.1.1 Configuring a DNS server example

Name the DNS client and configure it to query a DNS server to resolve host names. To do this, perform the following steps:

- Open the Advanced > DNS > Client > Static dialog.
- In the Configuration frame, Configuration source field, specify the value user.
- In the Configuration frame, Domain name field, specify the value device1.
- To add a table entry, click the button.
- In the Address column, specify the value 192.168.3.5 as the IPv4 address of the DNS server.
- Mark the checkbox in the Active column.
- Open the Advanced > DNS > Client > Global dialog.
- To enable the function, select the On radio button in the Operation frame.
- Save the changes temporarily. To do this, click the button.

```
enable
configure
dns client source user

dns client domain-name device1

dns client servers add 1 ip 192.168.3.5

dns client adminstate
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Specifying that the user manually configures the DNS client settings.
Specifying the string device1 as a unique domain name for the device.
To add a DNS name server with an IPv4 address of 192.168.3.5 as index 1.
Enable the DNS Client function globally.
Advanced functions of the device

15.1 Using the device as a DNS client
A Setting up the configuration environment

A.1 Preparing access via SSH

You can connect to the device using SSH. To do this, perform the following steps:

- Generate a key in the device.
- or
- Transfer your own key onto the device.
- Prepare access to the device in the SSH client program.

Note: In the default setting, the key is already existing and access using SSH is enabled.

A.1.1 Generating a key in the device

The device lets you generate the key directly in the device. To do this, perform the following steps:

- Open the Device Security > Management Access > Server dialog, SSH tab.
- To disable the SSH server, select the off radio button in the Operation frame.
- To enable the SSH server, select the on radio button in the Operation frame.
- Save the changes temporarily. To do this, click the button.
- To create a RSA key, in the Signature frame, click the Create button.
- To create a RSA key, in the Signature frame, click the Create button.
- Save the changes temporarily. To do this, click the button.

```
enable
configure
ssh key rsa generate
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Generate a new RSA key.

A.1.2 Loading your own key onto the device

OpenSSH gives experienced network administrators the option of generating an own key. To generate the key, enter the following commands on your PC:

```
ssh-keygen.exe -q -t rsa -f rsa.key -C '' -N ''
rhoparam -out rsaparam.pem 2048
```

The device lets you transfer your own SSH key onto the device. To do this, perform the following steps:

- Open the Device Security > Management Access > Server dialog, SSH tab.
- To disable the SSH server, select the off radio button in the Operation frame.
- Save the changes temporarily. To do this, click the button.
Setting up the configuration environment
A.1 Preparing access via SSH

Perform the following steps:
- Copy the self-generated key from your PC to the external memory.
- Copy the key from the external memory into the device.

```
enable
```

Change to the Privileged EXEC mode.

```
copy sshkey envm <file name>
```

Load your own key onto the device from the external memory.

A.1.3 Preparing the SSH client program

The PuTTY program lets you access the device using SSH. This program is provided on the product CD.

Perform the following steps:
- Start the program by double-clicking on it.

```
In the Host Name (or IP address) field you enter the IP address of your device. The IP address (a.b.c.d) consists of 4 decimal numbers with values from 0 to 255. The 4 decimal numbers are separated by points.
- To select the connection type, select the SSH radio button in the Connection type option list.
- Click the Open button to set up the data connection to your device.

Figure 67: PuTTY input screen

Select the SSH option in the Connection type option list.
```

In the Host Name (or IP address) field you enter the IP address of your device. The IP address (a.b.c.d) consists of 4 decimal numbers with values from 0 to 255. The 4 decimal numbers are separated by points.
- To select the connection type, select the SSH radio button in the Connection type option list.
- Click the Open button to set up the data connection to your device.

Figure 67: PuTTY input screen
Before the connection is established, the PuTTY program displays a security alarm message and lets you check the key fingerprint.

![PuTTY Security Alert](image)

**Figure 68: Security alert prompt for the fingerprint**

Before the connection is established, the PuTTY program displays a security alarm message and lets you check the key fingerprint.

- Check the fingerprint of the key to help ensure that you have actually connected to the desired device.
- When the fingerprint matches your key, click the Yes button.

For experienced network administrators, another way of accessing your device through an SSH is by using the OpenSSH Suite. To set up the data connection, enter the following command:

```
ssh admin@10.0.112.53
```

**admin** is the user name.

**10.0.112.53** is the IP address of your device.
A.2 HTTPS certificate

Your web browser establishes the connection to the device using the HTTPS protocol. The prerequisite is that you enable the HTTPS server function in the Device Security > Management Access > Server dialog, HTTPS tab.

**Note:** Third-party software such as web browsers validate certificates based on criteria such as their expiration date and current cryptographic parameter recommendations. Old certificates can cause errors for example, an expired certificate or cryptographic recommendations change. To solve validation conflicts with third-party software, transfer your own up-to-date certificate onto the device or regenerate the certificate with the latest firmware.

A.2.1 HTTPS certificate management

A standard certificate according to X.509/PEM (Public Key Infrastructure) is required for encryption. In the default setting, a self-generated certificate is already present in the device. To do this, perform the following steps:

- Open the Device Security > Management Access > Server dialog, HTTPS tab.
- To create a X509/PEM certificate, in the Certificate frame, click the Create button.
- Save the changes temporarily. To do this, click the button.
- Restart the HTTPS server to activate the key. Restart the server using the Command Line Interface.

```
enable
configure
https certificate generate
no https server
https server
```

- The device also enables you to transfer an externally generated X.509/PEM certificate onto the device:

```
enable
configure
https certificate generate
no https server
https server
```

- Open the Device Security > Management Access > Server dialog, HTTPS tab.
- When the certificate is located on your PC or on a network drive, drag and drop the certificate in the area. Alternatively click in the area to select the certificate.
- Click on the Start button to copy the certificate to the device.
- Save the changes temporarily. To do this, click the button.

```
enable
copy https-cert envm <file name>
```

Change to the Privileged EXEC mode.
Change to the Configuration mode.
Generate a https X.509/PEM Certificate.
Disable the HTTPS function.
Enable the HTTPS function.
Copy HTTPS certificate from external non-volatile memory device.
### A.2 HTTPS certificate

#### Note:
To activate the certificate after you created or transferred it, reboot the device or restart the HTTPS server. Restart the HTTPS server using the Command Line Interface.

#### A.2.2 Access through HTTPS

The default setting for HTTPS data connection is TCP port **443**. If you change the number of the HTTPS port, then reboot the device or the HTTPS server. Thus the change becomes effective. To do this, perform the following steps:

- Open the **Device Security > Management Access > Server** dialog, **HTTPS** tab.
- To enable the function, select the **On** radio button in the **Operation** frame.
- To access the device by HTTPS, enter HTTPS instead of HTTP in your browser, followed by the IP address of the device.

When you make changes to the HTTPS port number, disable the HTTPS server and enable it again in order to make the changes effective.

The device uses HTTPS protocol and establishes a new data connection. When you log out at the end of the session, the device terminates the data connection.
Setting up the configuration environment
A.2 HTTPS certificate
Appendix

B.1 Literature references

A small selection of books on network topics, ordered by publication date (newest first):

- **TSN – Time-Sensitive Networking (in German)**
  Wolfgang Schulte
  VDE Verlag, 2020
  ISBN 978-3-8007-5078-8

- **Time-Sensitive Networking For Dummies, Belden/Hirschmann Special Edition (in English)**
  Oliver Kleineberg and Axel Schneider
  Wiley, 2018
  Get your free PDF copy on [https://www.belden.com/resources/knowledge/ebooks/time-sensitive-networking-for-dummies-lp](https://www.belden.com/resources/knowledge/ebooks/time-sensitive-networking-for-dummies-lp)

- **IPv6: Grundlagen - Funktionalität - Integration (in German)**
  Silvia Hagen
  Sunny Connection, 3rd edition, 2016
  ISBN 978-3-9522942-3-9 (Print), ISBN 978-3-9522942-8-4 (eBook)

- **IPv6 Essentials (in English)**
  Silvia Hagen
  O’Reilly, 3rd edition, 2014

- **TCP/IP Illustrated, Volume 1: The Protocols (2nd Edition) (in English)**
  W. R. Stevens and Kevin R. Fall
  Addison Wesley, 2011

- **Measurement, Control and Communication Using IEEE 1588 (in English)**
  John C. Eidson
  Springer, 2006

- **TCP/IP: Der Klassiker. Protokollanalyse. Aufgaben und Lösungen (in German)**
  W. R. Stevens
  Hüthig-Verlag, 2008
  ISBN 978-3-7785-4036-7

- **Optische Übertragungstechnik in der Praxis (in German)**
  Christoph Wrobel
  Hüthig-Verlag, 3rd edition, 2004
  ISBN 978-3-8266-5040-6
B.2 Maintenance

Hirschmann is continually working on improving and developing their software. Check regularly if there is an updated version of the software that provides you with additional benefits. You find information and software downloads on the Hirschmann product pages on the Internet at www.hirschmann.com.
B.3 Management Information Base (MIB)

The Management Information Base (MIB) is designed in the form of an abstract tree structure. The branching points are the object classes. The "leaves" of the MIB are called generic object classes.

When this is required for unique identification, the generic object classes are instantiated, that means the abstract structure is mapped onto reality, by specifying the port or the source address.

Values (integers, time ticks, counters or octet strings) are assigned to these instances; these values can be read and, in some cases, modified. The object description or object ID (OID) identifies the object class. The subidentifier (SID) is used to instantiate them.

Example:

The generic object class `hm2PSState (OID = 1.3.6.1.4.1.248.11.11.1.1.1.1.2)` is the description of the abstract information power supply status. However, it is not possible to read any value from this, as the system does not know which power supply is meant.

Specifying the subidentifier 2 maps this abstract information onto reality (instantiates it), thus identifying it as the operating status of power supply 2. A value is assigned to this instance and can be read. The instance `get 1.3.6.1.4.1.248.11.11.1.1.1.1.2.1` returns the response 1, which means that the power supply is ready for operation.

### Definition of the syntax terms used:

<table>
<thead>
<tr>
<th>Syntax Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integer</td>
<td>An integer in the range $-2^{31} - 2^{31} - 1$</td>
</tr>
<tr>
<td>IP address</td>
<td>xxx.xxx.xxx.xxx (xxx = integer in the range 0..255)</td>
</tr>
<tr>
<td>MAC address</td>
<td>12-digit hexadecimal number in accordance with ISO/IEC 8802-3</td>
</tr>
<tr>
<td>Object Identifier</td>
<td>x.x.x.x… (for example 1.3.6.1.1.4.1.248...)</td>
</tr>
<tr>
<td>Octet String</td>
<td>ASCII character string</td>
</tr>
<tr>
<td>PSID</td>
<td>Power supply identifier (number of the power supply unit)</td>
</tr>
<tr>
<td>TimeTicks</td>
<td>Stopwatch, Elapsed time = numerical value / 100 (in seconds) numerical value = integer in the range 0-2^{32}-1</td>
</tr>
<tr>
<td>Timeout</td>
<td>Time value in hundredths of a second time value = integer in the range 0-2^{32}-1</td>
</tr>
<tr>
<td>Type field</td>
<td>4-digit hexadecimal number in accordance with ISO/IEC 8802-3</td>
</tr>
<tr>
<td>Counter</td>
<td>Integer (0-2^{32}-1), when certain events occur, the value increases by 1.</td>
</tr>
</tbody>
</table>
A description of the MIB can be found on the product CD provided with the device.
## B.4 List of RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>768</td>
<td>UDP</td>
</tr>
<tr>
<td>791</td>
<td>IP</td>
</tr>
<tr>
<td>792</td>
<td>ICMP</td>
</tr>
<tr>
<td>793</td>
<td>TCP</td>
</tr>
<tr>
<td>826</td>
<td>ARP</td>
</tr>
<tr>
<td>1157</td>
<td>SNMPv1</td>
</tr>
<tr>
<td>1155</td>
<td>SMIv1</td>
</tr>
<tr>
<td>1191</td>
<td>Path MTU Discovery</td>
</tr>
<tr>
<td>1212</td>
<td>Concise MIB Definitions</td>
</tr>
<tr>
<td>1213</td>
<td>MIB2</td>
</tr>
<tr>
<td>1493</td>
<td>Dot1d</td>
</tr>
<tr>
<td>1643</td>
<td>Ethernet-like -MIB</td>
</tr>
<tr>
<td>1757</td>
<td>RMON</td>
</tr>
<tr>
<td>1812</td>
<td>Requirements for IP Version 4 Routers</td>
</tr>
<tr>
<td>1867</td>
<td>Form-Based File Upload in HTML</td>
</tr>
<tr>
<td>1901</td>
<td>Community based SNMP v2</td>
</tr>
<tr>
<td>1905</td>
<td>Protocol Operations for SNMP v2</td>
</tr>
<tr>
<td>1906</td>
<td>Transport Mappings for SNMP v2</td>
</tr>
<tr>
<td>1945</td>
<td>HTTP/1.0</td>
</tr>
<tr>
<td>2068</td>
<td>HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03</td>
</tr>
<tr>
<td>2233</td>
<td>The Interfaces Group MIB using SMI v2</td>
</tr>
<tr>
<td>2246</td>
<td>The TLS Protocol, Version 1.0</td>
</tr>
<tr>
<td>2328</td>
<td>OSPF v2</td>
</tr>
<tr>
<td>2346</td>
<td>AES Ciphersuites for Transport Layer Security</td>
</tr>
<tr>
<td>2365</td>
<td>Administratively Scoped IP Multicast</td>
</tr>
<tr>
<td>2578</td>
<td>SMIv2</td>
</tr>
<tr>
<td>2579</td>
<td>Textual Conventions for SMI v2</td>
</tr>
<tr>
<td>2580</td>
<td>Conformance statements for SMI v2</td>
</tr>
<tr>
<td>2618</td>
<td>RADIUS Authentication Client MIB</td>
</tr>
<tr>
<td>2620</td>
<td>RADIUS Accounting MIB</td>
</tr>
<tr>
<td>2663</td>
<td>IP Network Address Translator (NAT) Terminology and Considerations</td>
</tr>
<tr>
<td>2674</td>
<td>Dot1p/Q</td>
</tr>
<tr>
<td>2818</td>
<td>HTTP over TLS</td>
</tr>
<tr>
<td>2851</td>
<td>Internet Addresses MIB</td>
</tr>
<tr>
<td>2863</td>
<td>The Interfaces Group MIB</td>
</tr>
<tr>
<td>2865</td>
<td>RADIUS Client</td>
</tr>
<tr>
<td>3022</td>
<td>Traditional IP Network Address Translator</td>
</tr>
<tr>
<td>3164</td>
<td>The BSD Syslog Protocol</td>
</tr>
<tr>
<td>3410</td>
<td>Introduction and Applicability Statements for Internet Standard Management Framework</td>
</tr>
<tr>
<td>3412</td>
<td>Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)</td>
</tr>
</tbody>
</table>
### Appendix

#### B.4 List of RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3413</td>
<td>Simple Network Management Protocol (SNMP) Applications</td>
</tr>
<tr>
<td>RFC 3414</td>
<td>User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)</td>
</tr>
<tr>
<td>RFC 3415</td>
<td>View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)</td>
</tr>
<tr>
<td>RFC 3418</td>
<td>Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)</td>
</tr>
<tr>
<td>RFC 3584</td>
<td>Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework</td>
</tr>
<tr>
<td>RFC 3768</td>
<td>VRRP</td>
</tr>
<tr>
<td>RFC 4022</td>
<td>Management Information Base for the Transmission Control Protocol (TCP)</td>
</tr>
<tr>
<td>RFC 4113</td>
<td>Management Information Base for the User Datagram Protocol (UDP)</td>
</tr>
<tr>
<td>RFC 4188</td>
<td>Definitions of Managed Objects for Bridges</td>
</tr>
<tr>
<td>RFC 4251</td>
<td>SSH protocol architecture</td>
</tr>
<tr>
<td>RFC 4252</td>
<td>SSH authentication protocol</td>
</tr>
<tr>
<td>RFC 4253</td>
<td>SSH transport layer protocol</td>
</tr>
<tr>
<td>RFC 4254</td>
<td>SSH connection protocol</td>
</tr>
<tr>
<td>RFC 4293</td>
<td>Management Information Base for the Internet Protocol (IP)</td>
</tr>
<tr>
<td>RFC 4318</td>
<td>Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol</td>
</tr>
<tr>
<td>RFC 4363</td>
<td>Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions</td>
</tr>
<tr>
<td>RFC 4836</td>
<td>Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)</td>
</tr>
<tr>
<td>RFC 5905</td>
<td>NTPv4</td>
</tr>
</tbody>
</table>
## B.5 Underlying IEEE Standards

<table>
<thead>
<tr>
<th>IEEE Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.1AB</td>
<td>Station and Media Access Control Connectivity Discovery</td>
</tr>
<tr>
<td>IEEE 802.1D</td>
<td>MAC Bridges (switching function)</td>
</tr>
<tr>
<td>IEEE 802.1Q</td>
<td>Virtual LANs (VLANs, MRP, Spanning Tree)</td>
</tr>
<tr>
<td>IEEE 802.3</td>
<td>Ethernet</td>
</tr>
<tr>
<td>IEEE 802.3ac</td>
<td>VLAN Tagging</td>
</tr>
<tr>
<td>IEEE 802.3x</td>
<td>Flow Control</td>
</tr>
<tr>
<td>IEEE 802.3af</td>
<td>Power over Ethernet</td>
</tr>
</tbody>
</table>
B.6 Underlying ANSI Norms

ANSI/TIA-1057  Link Layer Discovery Protocol for Media Endpoint Devices, April 2006
## B.7 Technical Data

### Switching

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size of the MAC address table (incl. static filters)</td>
<td>16384</td>
</tr>
<tr>
<td>Max. number of statically configured MAC address filters</td>
<td>100</td>
</tr>
<tr>
<td>Number of priority queues</td>
<td>8 Queues</td>
</tr>
<tr>
<td>Port priorities that can be set</td>
<td>0..7</td>
</tr>
<tr>
<td>MTU (Max. allowed length of packets a port can receive or transmit)</td>
<td>1518 Bytes</td>
</tr>
</tbody>
</table>

### VLAN

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID range</td>
<td>1..4042</td>
</tr>
<tr>
<td>Number of VLANs max.</td>
<td>64 simultaneously per device</td>
</tr>
<tr>
<td></td>
<td>max. 64 simultaneously per port</td>
</tr>
</tbody>
</table>

### Routing/Switching

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU (Max. allowed length of over-long packets a router interface can receive or transmit)</td>
<td>1500</td>
</tr>
<tr>
<td>Number of loopback interfaces</td>
<td>8</td>
</tr>
<tr>
<td>Max. number of Secondary IP addresses (Multinetting)</td>
<td>1</td>
</tr>
<tr>
<td>Max. number of VLAN router interfaces</td>
<td>64</td>
</tr>
<tr>
<td>Max. number of static routing entries</td>
<td>256</td>
</tr>
</tbody>
</table>

### Firewall

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. number of L3 firewall rules</td>
<td>2048</td>
</tr>
</tbody>
</table>

### NAT

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. number of 1:1 NAT rules</td>
<td>255</td>
</tr>
<tr>
<td>Max. number of Destination NAT rules</td>
<td>255</td>
</tr>
<tr>
<td>Max. number of Double NAT rules</td>
<td>255</td>
</tr>
<tr>
<td>Max. number of Masquerading NAT rules</td>
<td>128</td>
</tr>
<tr>
<td>Max. number of Connection Tracking entries</td>
<td>7768</td>
</tr>
</tbody>
</table>
B.8 Copyright of integrated Software

The product contains, among other things, Open Source Software files developed by third parties and licensed under an Open Source Software license.

You can find the license terms in the Graphical User Interface in the Help > Licenses dialog.
## B.9 Abbreviations used

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACA</td>
<td>Name of the external memory</td>
</tr>
<tr>
<td>BOO TP</td>
<td>Bootstrap Protocol</td>
</tr>
<tr>
<td>CLI</td>
<td>Command Line Interface</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>EUI</td>
<td>Extended Unique Identifier</td>
</tr>
<tr>
<td>FDB</td>
<td>Forwarding Database</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>LED</td>
<td>Light Emitting Diode</td>
</tr>
<tr>
<td>LLDP</td>
<td>Link Layer Discovery Protocol</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>NMS</td>
<td>Network Management System</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RFC</td>
<td>Request For Comment</td>
</tr>
<tr>
<td>RM</td>
<td>Redundancy Manager</td>
</tr>
<tr>
<td>SCP</td>
<td>Secure Copy</td>
</tr>
<tr>
<td>SFP</td>
<td>Small Form-factor Pluggable</td>
</tr>
<tr>
<td>SFTP</td>
<td>SSH File Transfer Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TP</td>
<td>Twisted Pair</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>UTC</td>
<td>Coordinated Universal Time</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
</tbody>
</table>
## Index

### 0-9
- 1to1 NAT ............................................. 173

### A
- ABR .............................................. 199, 201
- Access roles ...................................... 55
- Access security ................................... 95
- Address Resolution Protocol .................. 157
- Adjacency ......................................... 203
- Advertisement ..................................... 193
- Advertisement interval ........................... 194
- Alarm .............................................. 225
- Alarm messages ................................... 223
- APNIC ............................................. 39
- Area Border Router ............................... 199, 201
- ARIN .............................................. 39
- ARP .............................................. 42, 157, 158
- ASBR .............................................. 198, 201
- Authentication .................................... 69
- Authentication list ................................ 51
- Automatic configuration .......................... 96
- Autonomous System Area Border Router ... 201
- Autonomous System Boundary Router ....... 198

### B
- Backbone Area .................................... 199
- Backup Designated Router ..................... 203, 204
- Backup router .................................... 193
- Bandwidth ........................................ 142
- BDR .............................................. 203
- Broadcast ........................................ 156

### C
- CA .................................................. 69
- Certificate ........................................ 69
- Certification authority (CA) ................... 69
- CIDR ............................................... 42, 159, 197
- Classless inter domain routing ............... 42
- Classless Inter-Domain Routing ............... 159, 197
- Closed circuit .................................... 234
- Command Line Interface ........................ 16
- Command tree .................................... 25
- Confidentiality .................................... 67
- Configuration modifications .................... 223
### Index

**D**
- Data traffic .................................................. 107
- Daylight saving time ........................................ 130
- Deep Packet Inspection ...................................... 121
- Default gateway ............................................. 192, 193
- Denial of Service ............................................ 107
- Denial of service ............................................ 120
- Designated Router .......................................... 203, 204
- Destination NAT ............................................. 175
- Destination table ........................................... 223
- Device status ................................................ 227
- Distance ......................................................... 166, 167
- DoS ............................................................... 107, 120
- Double NAT ................................................... 179
- DPI ............................................................... 121
- DR ............................................................... 203

**E**
- Event log ......................................................... 247

**F**
- FAQ ............................................................... 275
- Faulty device replacement .................................. 13
- First installation ............................................. 39
- Flow control .................................................. 142

**G**
- Gateway ......................................................... 40, 44
- Generic object classes ...................................... 259
- Global Config mode .......................................... 22

**H**
- Hardware reset .............................................. 223
- Hello ............................................................ 203
- HiDiscovery ................................................... 39
- HiView .......................................................... 50
- Host address .................................................. 40

**I**
- IANA ............................................................. 39
- IEEE MAC Adresse ........................................... 242
- IKE ............................................................. 69
- Importance ..................................................... 168
- Industrial HiVision .......................................... 11
- Instantiation ................................................... 259
- Integrity ......................................................... 67
- Interface tracking .......................................... 183, 185, 186
- Interface tracking object .................................. 184
- Internal router ................................................ 201
- Internet Key Exchange ...................................... 69
- Internet key exchange protocol ......................... 69
- Internet Protocol Security ................................ 67
- IP ............................................................... 157
- IP address ....................................................... 39, 44, 192
- IP address owner ............................................. 193
- IP Masquerading ............................................. 178
- IPsec ............................................................ 67, 69
- ISO/OSI layer model ......................................... 42
- ISO/OSI reference model .................................... 156
### L
- LACNIC ................................................................. 40
- LDAP ................................................................. 51
- Link Aggregation interface ........................................ 183
- Link down delay .................................................... 184
- Link monitoring ..................................................... 227, 234
- Link State Advertisement .......................................... 201
- Link State Database ................................................ 204
- Link up delay ......................................................... 184
- Load sharing .......................................................... 167
- Logical tracking ...................................................... 183, 185, 187, 189
- Login dialog .......................................................... 15
- LSA ...................................................................... 201, 204
- LSD ...................................................................... 204

### M
- MAC address ............................................................ 192
- MAC address filter .................................................. 135
- MAC destination address .......................................... 42
- Masquerading NAT .................................................. 178
- Master router ........................................................... 193
- Memory (RAM) ......................................................... 77
- Message ................................................................. 223
- Mode ..................................................................... 96
- Multicast ................................................................. 156
- Multicast address ..................................................... 203
- Multinetting ............................................................. 160

### N
- NAPT .................................................................... 178
- NAT .................................................................... 172
- NAT (1) NAT) .......................................................... 173
- NAT (Double NAT) .................................................. 179
- NAT (Masquerading NAT) ........................................ 178
- Netmask ................................................................. 40, 44
- Network Address Port Translation ............................... 178
- Network Address Translation .................................... 172
- Network plan .......................................................... 155
- Network Time Protocol ............................................ 129
- Non-volatile memory (NVM) ..................................... 77
- Not So Stubby Area .................................................. 199
- NSSA .................................................................... 199
- NTP .................................................................... 129
- NVM (non-volatile memory) ..................................... 77

### O
- Object classes .......................................................... 259
- Object description ................................................... 259
- Object ID ................................................................. 259
- Open Shortest Path First .......................................... 197
- OpenSSH-Suite ....................................................... 17
- OpenSSL ................................................................. 70
- Operand ................................................................... 188, 190
- Operation monitoring .............................................. 234
- Operators ................................................................. 185
- OSI reference model ............................................... 156
- OSPF .................................................................... 155, 197
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
</tr>
<tr>
<td>Packet filter .......................................................... 107</td>
</tr>
<tr>
<td>Packet filter (Routed Firewall Mode) .................................. 108</td>
</tr>
<tr>
<td>Packet filter (Transparent Firewall Mode) ........................... 112</td>
</tr>
<tr>
<td>Password ................................................................. 18, 20</td>
</tr>
<tr>
<td>Ping response .............................................................. 184</td>
</tr>
<tr>
<td>Ping tracking .............................................................. 168, 183, 184</td>
</tr>
<tr>
<td>Polling ....................................................................... 223</td>
</tr>
<tr>
<td>Port forwarding ............................................................ 175</td>
</tr>
<tr>
<td>Port-based router interface .............................................. 161</td>
</tr>
<tr>
<td>Pre-shared key ............................................................. 69</td>
</tr>
<tr>
<td>Priority ..................................................................... 140</td>
</tr>
<tr>
<td>Priority tagged frames ................................................... 140</td>
</tr>
<tr>
<td>Privileged Exec mode ....................................................... 22</td>
</tr>
<tr>
<td>Proxy ARP ................................................................. 158</td>
</tr>
<tr>
<td>PuTTY ................................................................. 16</td>
</tr>
<tr>
<td>Q</td>
</tr>
<tr>
<td>QoS ................................................................. 139</td>
</tr>
<tr>
<td>R</td>
</tr>
<tr>
<td>RADIUS ............................................................... 51</td>
</tr>
<tr>
<td>RAM (memory) .............................................................. 77</td>
</tr>
<tr>
<td>Real time ................................................................. 139</td>
</tr>
<tr>
<td>Redistributing ............................................................ 199</td>
</tr>
<tr>
<td>Redistribution ........................................................... 198</td>
</tr>
<tr>
<td>Redundant static route ................................................... 166</td>
</tr>
<tr>
<td>Reference clock ......................................................... 132</td>
</tr>
<tr>
<td>Reference time source .................................................... 129</td>
</tr>
<tr>
<td>Relay contact ............................................................. 234</td>
</tr>
<tr>
<td>Remote diagnostics ....................................................... 234</td>
</tr>
<tr>
<td>Report ................................................................. 244</td>
</tr>
<tr>
<td>RFC ................................................................. 261</td>
</tr>
<tr>
<td>RIPE NCC .............................................................. 40</td>
</tr>
<tr>
<td>Route Summarization ..................................................... 199</td>
</tr>
<tr>
<td>Route tracking ........................................................... 198</td>
</tr>
<tr>
<td>Routed Firewall Mode (Packet filter) .................................. 108</td>
</tr>
<tr>
<td>Router ................................................................. 40</td>
</tr>
<tr>
<td>Router ID ............................................................... 203</td>
</tr>
<tr>
<td>Router priority ........................................................... 203</td>
</tr>
<tr>
<td>Routing table ......................................................... 162, 168</td>
</tr>
</tbody>
</table>
Index

S
Secure shell ................................................................. 16, 17
Segmentation .............................................................. 223
Serial interface .......................................................... 16, 19
Service ................................................................. 244
Service shell ............................................................ 22
Service Shell deactivation .............................................. 35
Setting the time ......................................................... 129
SFP module ............................................................... 241
Shortest Path First ...................................................... 205
Signal contact ............................................................ 234
Signal runtime ........................................................... 131
Skew time ................................................................. 194
SNMP ................................................................. 223
SNMP trap ............................................................... 223, 225
Software version ......................................................... 89
SPF ................................................................. 205
SSH ................................................................. 16, 17
Starting the graphical user interface .................................. 15
Static route tracking .................................................... 168
Static routes ............................................................. 155
Static routing ........................................................... 183
Store-and-forward ...................................................... 135
Stub Area ................................................................. 199
Subidentifier ............................................................. 259
Subnet ................................................................. 44
System requirements (Graphical User Interface) .................... 15
System time ........................................................... 132

T
Tab Completion .......................................................... 32
Technical questions .................................................... 275
Tracking ................................................................. 168
Tracking (VRRP) ........................................................ 183
Traffic flow confidentiality ............................................ 67
Training courses ......................................................... 275
Transmission reliability ................................................. 223
Transparent Firewall Mode (Packet filter) .......................... 112
Trap ................................................................. 223, 225
Trap destination table .................................................. 223
Tunnel mode .............................................................. 68

U
Update ................................................................. 37
User Exec mode ........................................................ 22
User name ............................................................... 18, 20
### Index

#### V
- Variable Length Subnet Mask ................................................................. 197
- virtual link ......................................................................................... 200
- Virtual MAC address ................................................................. 193
- Virtual router ..................................................................................... 193
- Virtual router ID ............................................................................... 193
- Virtual router IP address ............................................................. 194
- Virtual router MAC address .......................................................... 194
- VLAN ......................................................................................... 145
- VLAN priority ............................................................................... 141
- VLAN router interface ................................................................. 183
- VLAN tag ......................................................................................... 140, 145
- VLSM ......................................................................................... 197
- VPN .................................................................................................. 67
- VRID ............................................................................................. 193
- VRRP .............................................................................................. 183, 192
- VRRP priority .............................................................................. 193
- VRRP router ..................................................................................... 193
- VRRP Tracking ............................................................................... 183
- VT100 ............................................................................................... 20

#### X
- X.509 rsa .......................................................................................... 69
D  Further support

Technical questions

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

You find the addresses of our partners on the Internet at www.hirschmann.com.

A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at hirschmann-support.belden.com.

This site also includes a free of charge knowledge base and a software download section.

Technical Documents

The current manuals and operating instructions for Hirschmann products are available at doc.hirschmann.com.

Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors on three counts with its complete range of innovative services:

▶ Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.

▶ Training offers you an introduction to the basics, product briefing and user training with certification.

You find the training courses on technology and products currently available at www.hicomcenter.com.

▶ Support ranges from the first installation through the standby service to maintenance concepts.

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

<table>
<thead>
<tr>
<th></th>
<th>Very Good</th>
<th>Good</th>
<th>Satisfactory</th>
<th>Mediocre</th>
<th>Poor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precise description</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Readability</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Understandability</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Examples</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Structure</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Comprehensive</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Graphics</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Drawings</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Tables</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>

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

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

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
  Germany