HIRSCHMANN
A BELDEN BRAND

Hirschmann Automation and Control GmbH

# DRAGON HiOS-3A-UR Rel. 08703

## Reference Manual

Graphical User Interface

## User Manual

Configuration

HIRSCHMANN
A BELDEN BRAND

# Reference Manual

## Graphical User Interface
## DRAGON Switch
## HiOS-3A-UR



Technical support
https://hirschmann-support.belden.com

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.

© 2021 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** . . . 9

**About this Manual** . . . 11

**Key** . . . 12

**Notes on the Graphical User Interface** . . . 13

**1 Basic Settings** . . . 19
1.1 System . . . 19
1.2 Modules . . . 24
1.3 Network . . . 28
1.3.1 Global . . . 29
1.3.2 IPv4 . . . 32
1.4 Out of Band . . . 34
1.5 Software . . . 38
1.6 Load/Save . . . 41
1.7 External Memory . . . 53
1.8 Port . . . 56
1.9 Power over Ethernet . . . 63
1.9.1 PoE Global . . . 64
1.9.2 PoE Port . . . 66
1.10 Restart . . . 68

**2 Time** . . . 71
2.1 Basic Settings . . . 71
2.2 SNTP . . . 75
2.2.1 SNTP Client . . . 76
2.2.2 SNTP Server . . . 80
2.3 PTP . . . 82
2.3.1 PTP Global . . . 83
2.3.2 PTP Boundary Clock . . . 85
2.3.2.1 PTP Boundary Clock Global . . . 86
2.3.2.2 PTP Boundary Clock Port . . . 91
2.3.3 PTP Transparent Clock . . . 95
2.3.3.1 PTP Transparent Clock Global . . . 96
2.3.3.2 PTP Transparent Clock Port . . . 100

**3 Device Security** . . . 103
3.1 User Management . . . 103
3.2 Authentication List . . . 109
3.3 LDAP . . . 111
3.3.1 LDAP Configuration . . . 112
3.3.2 LDAP Role Mapping . . . 118
3.4 Management Access . . . 120
3.4.1 Server . . . 121
3.4.2 IP Access Restriction . . . 135

3.4.3 Web . . . 138
3.4.4 Command Line Interface . . . 139
3.4.5 SNMPv1/v2 Community . . . 142
3.5 Pre-login Banner . . . 143

**4 Network Security** . . . 145
4.1 Network Security Overview . . . 145
4.2 Port Security . . . 147
4.3 802.1X Port Authentication . . . 152
4.3.1 802.1X Global . . . 153
4.3.2 802.1X Port Configuration . . . 156
4.3.3 802.1X Port Clients . . . 162
4.3.4 802.1X EAPOL Port Statistics . . . 164
4.3.5 802.1X Port Authentication History . . . 166
4.3.6 802.1X Integrated Authentication Server . . . 168
4.4 RADIUS . . . 169
4.4.1 RADIUS Global . . . 170
4.4.2 RADIUS Authentication Server . . . 172
4.4.3 RADIUS Accounting Server . . . 174
4.4.4 RADIUS Authentication Statistics . . . 176
4.4.5 RADIUS Accounting Statistics . . . 178
4.5 DoS . . . 179
4.5.1 DoS Global . . . 180
4.6 DHCP Snooping . . . 184
4.6.1 DHCP Snooping Global . . . 185
4.6.2 DHCP Snooping Configuration . . . 187
4.6.3 DHCP Snooping Statistics . . . 190
4.6.4 DHCP Snooping Bindings . . . 191
4.7 IP Source Guard . . . 192
4.7.1 IP Source Guard Port . . . 194
4.7.2 IP Source Guard Bindings . . . 195
4.8 Dynamic ARP Inspection . . . 196
4.8.1 Dynamic ARP Inspection Global . . . 198
4.8.2 Dynamic ARP Inspection Configuration . . . 200
4.8.3 Dynamic ARP Inspection ARP Rules . . . 203
4.8.4 Dynamic ARP Inspection Statistics . . . 204
4.9 ACL . . . 205
4.9.1 ACL IPv4 Rule . . . 206
4.9.2 ACL MAC Rule . . . 214
4.9.3 ACL Assignment . . . 220
4.9.4 ACL Time Profile . . . 222

**5 Switching** . . . 227
5.1 Switching Global . . . 227
5.2 Rate Limiter . . . 230
5.3 Filter for MAC Addresses . . . 233
5.4 IGMP Snooping . . . 235
5.4.1 IGMP Snooping Global . . . 236

5.4.2 IGMP Snooping Configuration . . . 238
5.4.3 IGMP Snooping Enhancements . . . 242
5.4.4 IGMP Snooping Querier . . . 245
5.4.5 IGMP Snooping Multicasts . . . 248
5.5 MRP-IEEE . . . 249
5.5.1 MRP-IEEE Configuration . . . 250
5.5.2 MRP-IEEE Multiple MAC Registration Protocol . . . 251
5.5.3 MRP-IEEE Multiple VLAN Registration Protocol . . . 256
5.6 GARP . . . 259
5.6.1 GMRP . . . 260
5.6.2 GVRP . . . 262
5.7 QoS/Priority . . . 263
5.7.1 QoS/Priority Global . . . 264
5.7.2 QoS/Priority Port Configuration . . . 265
5.7.3 802.1D/p Mapping . . . 267
5.7.4 IP DSCP Mapping . . . 269
5.7.5 Queue Management . . . 271
5.7.6 DiffServ . . . 272
5.7.6.1 DiffServ Overview . . . 273
5.7.6.2 DiffServ Global . . . 274
5.7.6.3 DiffServ Class . . . 275
5.7.6.4 DiffServ Policy . . . 282
5.7.6.5 DiffServ Assignment . . . 291
5.8 VLAN . . . 292
5.8.1 VLAN Global . . . 294
5.8.2 VLAN Configuration . . . 295
5.8.3 VLAN Port . . . 297
5.8.4 VLAN Voice . . . 299
5.8.5 MAC Based VLAN . . . 302
5.8.6 Subnet Based VLAN . . . 303
5.8.7 Protocol Based VLAN . . . 305
5.9 L2-Redundancy . . . 306
5.9.1 MRP . . . 307
5.9.2 HIPER Ring . . . 311
5.9.3 Spanning Tree . . . 312
5.9.3.1 Spanning Tree Global . . . 313
5.9.3.2 Spanning Tree MSTP . . . 320
5.9.3.3 Spanning Tree Port . . . 325
5.9.4 Link Aggregation . . . 334
5.9.5 Link Backup . . . 342
5.9.6 FuseNet . . . 345
5.9.6.1 Sub Ring . . . 347
5.9.6.2 Ring/Network Coupling . . . 352
5.9.6.3 Redundant Coupling Protocol . . . 358

**6 Routing** . . . 361
6.1 Routing Global . . . 361

6.2 Routing Interfaces . . . 365
6.2.1 Routing Interfaces Configuration . . . 366
6.2.2 Routing Interfaces Secondary Interface Addresses . . . 373
6.3 ARP . . . 374
6.3.1 ARP Global . . . 375
6.3.2 ARP Current . . . 377
6.3.3 ARP Static . . . 378
6.4 Router Discovery . . . 379
6.5 RIP . . . 382
6.6 Open Shortest Path First . . . 389
6.6.1 OSPF Global . . . 390
6.6.2 OSPF Areas . . . 398
6.6.3 OSPF Stub Areas . . . 400
6.6.4 OSPF Not So Stubby Areas . . . 402
6.6.5 OSPF Interfaces . . . 405
6.6.6 OSPF Virtual Links . . . 411
6.6.7 OSPF Ranges . . . 414
6.6.8 OSPF Diagnostics . . . 416
6.7 Routing Table . . . 427
6.8 Tracking . . . 431
6.8.1 Tracking Configuration . . . 432
6.8.2 Tracking Applications . . . 438
6.9 L3 Relay . . . 439
6.10 Loopback Interface . . . 444
6.11 Multicast Routing . . . 446
6.11.1 Multicast Routing Global . . . 447
6.11.2 Multicast Routing Boundary Configuration . . . 451
6.11.3 Multicast Routing Static . . . 453
6.11.4 IGMP . . . 454
6.11.4.1 IGMP Configuration . . . 455
6.11.4.2 IGMP Proxy Configuration . . . 463
6.11.4.3 IGMP Proxy Database . . . 465
6.12 L3-Redundancy . . . 467
6.12.1 VRRP . . . 467
6.12.1.1 VRRP Configuration . . . 468
6.12.1.2 VRRP Domains . . . 482
6.12.1.3 VRRP Statistics . . . 484
6.12.1.4 VRRP Tracking . . . 486

**7 Diagnostics** . . . 489
7.1 Status Configuration . . . 489
7.1.1 Device Status . . . 490
7.1.2 Security Status . . . 495
7.1.3 Signal Contact . . . 501
7.1.3.1 Signal Contact 1 / Signal Contact 2 . . . 502
7.1.4 MAC Notification . . . 507
7.1.5 Alarms (Traps) . . . 510

7.2 System . . . 512
7.2.1 System Information . . . 513
7.2.2 Hardware State . . . 514
7.2.3 Configuration Check . . . 515
7.2.4 IP Address Conflict Detection . . . 517
7.2.5 ARP . . . 523
7.2.6 Selftest . . . 524
7.3 Email Notification . . . 526
7.3.1 Email Notification Global . . . 527
7.3.2 Email Notification Recipients . . . 531
7.3.3 Email Notification Mail Server . . . 532
7.4 Syslog . . . 534
7.5 Ports . . . 537
7.5.1 SFP . . . 538
7.5.2 TP cable diagnosis . . . 540
7.5.3 Port Monitor . . . 542
7.5.4 Auto-Disable . . . 554
7.5.5 Port Mirroring . . . 558
7.6 LLDP . . . 562
7.6.1 LLDP Configuration . . . 563
7.6.2 LLDP Topology Discovery . . . 567
7.7 Loop Protection . . . 570
7.8 SFlow . . . 575
7.8.1 SFlow Configuration . . . 576
7.8.2 SFlow Receiver . . . 579
7.9 Report . . . 580
7.9.1 Report Global . . . 581
7.9.2 Persistent Logging . . . 586
7.9.3 System Log . . . 589
7.9.4 Audit Trail . . . 590

**8 Advanced** . . . 591
8.1 DHCP L2 Relay . . . 591
8.1.1 DHCP L2 Relay Configuration . . . 592
8.1.2 DHCP L2 Relay Statistics . . . 595
8.2 DHCP Server . . . 596
8.2.1 DHCP Server Global . . . 597
8.2.2 DHCP Server Pool . . . 599
8.2.3 DHCP Server Lease Table . . . 604
8.3 DNS . . . 605
8.3.1 DNS Client . . . 605
8.3.1.1 DNS Client Global . . . 606
8.3.1.2 DNS Client Current . . . 607
8.3.1.3 DNS Client Static . . . 608
8.3.1.4 DNS Client Static Hosts . . . 610
8.3.2 OPC UA Server . . . 611
8.4 Command Line Interface . . . 614

**A** **Index** . . . . . 615

**B** **Further support** . . . . . 621

**C** **Readers' Comments** . . . . . 622

# 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

# Key

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

# 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.

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.

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, *RAM test* 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 transfered 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
- Modules
- Network
- Out of Band
- Software
- Load/Save
- External Memory
- Port
- Power over Ethernet
- Restart

## 1.1 System

[ Basic Settings > 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.

- DHCP client
- *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 basic 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*

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.

| Parameters | Color | Meaning |
|---|---|---|
| *Status* | ● | There is currently no device status alarm. The device status is OK. |
| | ● | There is currently at least one device status alarm. Therefore, see the *Device status* frame above. |
| *Power* | ● | Device variant with 2 power supply units:<br>Only one supply voltage is active. |
| | ● | Device variant with 1 power supply unit:<br>The supply voltage is active.<br>Device variant with 2 power supply units:<br>Both supply voltages are active. |

| Parameters | Color | Meaning |
|---|---|---|
| *RM* | ● | The device is neither operating as a *MRP* ring manager nor as a *DLR* supervisor. |
| | ● | Loss of redundancy reserve.<br>The device is operating as a *MRP* ring manager. |
| | ● | Redundancy reserve is available.<br>The device is operating as a *MRP* ring manager. |
| *ACA* | ● | No external memory connected. |
| | ● | The external memory is connected, but not ready for operation. |
| | ● | The external memory is connected and ready for operation. |

### 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.

| Parameters | Status | Meaning |
|---|---|---|
| `<Port number>` | | The port is inactive.<br>The port does not send or receive any data. |
| | | The port is inactive.<br>The cable is connected. Active link. |
| | | The port is active.<br>No cable connected or no active link. |
| | | The port is active.<br>The cable is connected. Connection okay. Active link. Full-duplex mode |
| | | The half-duplex mode is enabled.<br>Verify the settings in the *Basic Settings > Ports* dialog, *Configuration* tab. |
| | | The port is in a blocking state due to a redundancy function. |
| | | The port operates as a router interface. |

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 1.2 Modules

[Basic Settings > Modules]

The device lets you install or remove the modules during operation (hot-plug).

The dialog contains the following tabs:
- [Ethernet module]
- [Fan module]
- [Power supply module]

## [Ethernet module]

As long as the *Ethernet module status* column displays the value `configurable` you can configure the module and save its preferences.
- When you replace the module with an identical module, the device applies the settings to the new module immediately.
- When you replace the module with a different type of module, the device applies the factory settings to the new module.
- When you plug a module in an empty slot, the device configures the module with its default settings. If the slot is inactive, then it remains inactive until you mark the checkbox in the *Active* column. With the port default settings loaded on the module, access to the network is possible.

### Install an Ethernet module

Perform the following steps:
- ☐ Plug the module in the slot.
  The device automatically configures the module with the default settings, and detects the module parameters.
- ☐ To update the Graphical User Interface, click the button.
  The *Ethernet module status* column displays the value `physical` for the installed Ethernet module.
- ☐ To temporarily save the changes, click the button.

### Activate/Deactivate a slot

On a deactivated slot, the device recognizes the installed module and port configuration is possible. The module establishes no network connections on a deactivated slot.

Perform the following steps:
- ☐ In the table highlight the module.
- ☐ To deactivate the slot and deny network access, unmark the *Active* checkbox.
- ☐ To activate the slot and allow network access, mark the *Active* checkbox.
- ☐ To temporarily save the changes, click the button.

### Remove an Ethernet module

Perform the following steps:
- ☐ Remove the module from the slot.
- ☐ To update the Graphical User Interface, click the button.
  The *Ethernet module status* column displays the value `configurable` for the removed module.
- ☐ In the table highlight the entry of the removed module.

- ☐ Click the ☰ button and then the *Remove Ethernet module* item.
  The *Ethernet module status* column displays the value `remove` for the removed module.
  The *Type* column and some other columns display the value `n/a`.
  The marked *Active* checkbox indicates that the slot is still active.
- ☐ To temporarily save the changes, click the ✔ button.

### Table

Ethernet module

Displays the number of the slot to which the entry refers.

Active

Activates/deactivates the slot.

Possible values:

- `marked` (default setting)
  The slot is active. The device recognizes a module installed in this slot.
- `unmarked`
  The slot is inactive.

Type

Displays the type of the installed module.

A value of `n/a` indicates that the slot is empty.

Description

Specifies a short description of the installed module.

Version

Displays the version of the installed module.

Ports

Displays how many ports are available on the installed module.

Serial number

Displays the serial number of the installed module.

A value of `n/a` indicates that the slot is empty.

Ethernet module status

Displays the status of the slot.

Possible values:

- *physical*
  A module is present in the slot.

- *configurable*
  The slot is empty and available for configuration.
- *remove*
  The slot is empty and deactivated.
- *fix*
  The module cannot be removed.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Remove Ethernet module

Removes the selected Ethernet module from the table.

## [Fan module]

Always operate the device with the fan module installed. Thus you help avoid unwanted effects on the operation and life span of the device. If the module or a fan inside is inoperable, then replace the module immediately.

### Install a module

Perform the following steps:

- ☐ Plug the module in the slot.
  The device automatically configures the module with the default settings, and detects the module parameters.
- ☐ To update the Graphical User Interface, click the button.
  The *Fan module status* column displays the value *ok* for the installed module.

### Uninstall a module

Perform the following steps:

- ☐ Remove the module from the slot.
- ☐ To update the Graphical User Interface, click the button.
  The *Fan module status* column displays the value *unavailable* for the removed module.

### Table

Fan module

Displays the number of the slot to which the entry refers.

Fan module status

Displays the status of the installed module.

Possible values:

- *unavailable*
  The module is not present in the slot.
- *ok*
  The module is present and functional.
- *failing*
  The module is present but an unexpected event occurred. For example, a fan in the module is inoperable.

### Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Remove Ethernet module

Removes the selected Ethernet module from the table.

## [Power supply module]

The device has 2 module slots for power supply units and thus operates with redundant power supplies.

### Install a module

Perform the following steps:

- ☐ Plug the module in the slot.
  The device automatically detects the module parameters.
- ☐ To update the Graphical User Interface, click the button.
  The *Power supply status* column displays the value *present* or *defective* for the installed module.

### Uninstall a module

Perform the following steps:

- ☐ Remove the module from the slot.
- ☐ To update the Graphical User Interface, click the button.
  The *Power supply status* column displays the value *not installed* for the removed module.

### Table

Power supply

Displays the number of the slot to which the entry refers.

Product code

Displays the product code of the installed module.

A value of `n/a` indicates that the slot is empty.

Version

Displays the version of the installed module.

A value of `0` indicates that the slot is empty.

Serial number

Displays the serial number of the installed module.

A value of `n/a` indicates that the slot is empty.

Power supply status

Displays the status of the installed module.

Possible values:

- *present*
  The module is present and functional.
- *defective*
  The module is present but an unexpected event occurred. For example, the module is not connected to the mains.
- *not installed*
  The module is not present in the slot.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Remove Ethernet module

Removes the selected Ethernet module from the table.

## 1.3 Network

[Basic Settings > Network]

The menu contains the following dialogs:

- Global
- IPv4

# 1.3.1 Global

[ Basic Settings > Network > 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.

MAC address conflict detection

Enables/disables the *MAC address conflict detection* function.

Possible values:

- `marked`
  The *MAC address conflict detection* function is enabled.
  The device verifies that its MAC address is unique in the network.
- `unmarked` (default setting)
  The *MAC address conflict detection* function is disabled.

### 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.

Relay status

Activates/deactivates the HiDiscovery relay function. This function lets the HiDiscovery software to find and display devices located in other subnets.

Possible values:

- `marked` (default setting)
  The HiDiscovery relay function is active.
  The device forwards the HiDiscovery request packets sent from the device management into directly connected subnets. The device also responds to requests with its IP parameters.
- `unmarked`
  The HiDiscovery relay function is inactive.
  The HiDiscovery software finds only the devices located in the same subnet as the device management.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 1.3.2 IPv4

[ Basic Settings > Network > 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.
- `BOOTP`
  The device receives its IP parameters from a BOOTP or DHCP server.
  The server evaluates the MAC address of the device, then assigns the IP parameters.
- `DHCP` (default setting)
  The device receives its IP parameters from a DHCP server.
  The server evaluates the MAC address, the DHCP name, or other parameters of the device, then assigns the IP parameters.
  When the server also provides the addresses of DNS servers, the device displays these addresses in the *Advanced > DNS > Cache > Current* dialog.

**Note:** If there is no response from the BOOTP or DHCP server, then the device sets the IP address to `0.0.0.0` and makes another attempt to obtain a valid IP address.

### BOOTP/DHCP

Client ID

Displays the DHCP client ID that the device sends to the BOOTP or DHCP server. If the server is configured accordingly, then it reserves an IP address for this DHCP client ID. Therefore, the device receives the same IP from the server every time it requests it.

The DHCP client ID that the device sends is the device name specified in the *System name* field in the *Basic Settings > System* dialog.

DHCP option 66/67/4/42

Enables/disables the *DHCP option 66/67/4/42* function in the device.

Possible values:

- `On` (default setting)
  The *DHCP option 66/67/4/42* function is enabled.
  The device loads the configuration profile and receives the time server information using the following DHCP options:
  - `Option 66: TFTP server name`
    `Option 67: Boot file name`
    The device automatically loads the configuration profile from the DHCP server into the volatile memory (`RAM`) using the TFTP protocol. The device uses the settings of the imported configuration profile in the `running-config`.
  - `Option 4: Time Server`
    `Option 42: Network Time Protocol Servers`
    The device receives the time server information from the DHCP server.
- `Off`
  The *DHCP option 66/67/4/42* function is disabled.
  - The device does not load a configuration profile using DHCP Options 66/67.
  - The device does not receive time server information using DHCP Options 4/42.

### 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
- *Out of Band* management port

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 of its own network.

Possible values:

- Valid IPv4 address

If the device does not use the specified gateway, then verify that another default gateway is specified. The setting in the following dialog has precedence:

- *Basic Settings > Out of Band* dialog, *Gateway address* field
- *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`

### Remaining lease time

Lease time [s]

Displays the remaining time in seconds during which the IP address that the DHCP server assigned to the device management is still valid.

To update the display, click the button.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 1.4 Out of Band

[ Basic Settings > Out of Band ]

The device comes with a Service Port that lets you access the device management out-of-band. When there is a high in-band load on the switching ports, you can still use the Service Port network interface to access the device management.

The device lets you access the device management through the Service Port network interface using the following protocols:

- HTTP
- HTTPS
- SSH
- Telnet
- SNMP

- FTP
- TFTP
- SFTP
- SCP

In this dialog the device lets you change the IP parameters and disable the Service Port network interface, if needed.

### Operation

Operation

Enables/disables the Service Port network interface.

Possible values:

- `On` (default setting)
  The device lets you access the device management through the Service Port network interface.
- `Off`
  The device prohibits access to the device management through the Service Port network interface.

### Management interface

IP address assignment

Specifies the source from which the device management receives its IP parameters for access through the Service Port network interface.

Possible values:

- `Local` (default setting)
  The device management uses the IP parameters specified in the *IP parameter* frame.
- `DHCP`
  The device management uses an external DHCP server to assign the IP parameters to the Service Port network interface.
  When the DHCP server also provides DNS server addresses, the device displays these addresses in the *Advanced > DNS > Client > Current* dialog.
  If there is no response from the DHCP server, then the device sets the IP address to `0.0.0.0` and makes another attempt to obtain a valid IP address.

MAC address

Displays the MAC address of the Service Port network interface.

Status

Displays the operating status of the Service Port network interface.

### IP parameter

Verify that the IP subnet of this network interface is not overlapping with any subnet connected to another interface of the device:

- management interface
- router interface
- loopback interface

IP address

Specifies the IP address of the device management for access through the Service Port network interface.

Possible values:

- Valid IPv4 address
  (default setting: `192.168.1.1`)

Netmask

Specifies the netmask.

Possible values:

- Valid IPv4 netmask
  (default setting: `255.255.255.0`)

Gateway address

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

Possible values:

- Valid IPv4 address
  (default setting: `0.0.0.0`)
  Verify that *IP address* and *Gateway address* are in the same network.

This setting takes precedence over the default gateway setting in the *Basic Settings > Network* dialog, *Gateway address* field.

If the device does not use the specified gateway, then verify that 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`

### Remaining lease time

Lease time [s]

Displays the remaining time in seconds during which the out-of-band IP address that the DHCP server assigned to the device management is still valid.

To update the display, click the button.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 1.5 Software

[ Basic Settings > 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.

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.

- Software update from an FTP server
  When the file is located on an FTP server, specify the URL for the file in the following form:
  `ftp://<user>:<password>@<IP address>:<port>/<file name>`
- Software update from a TFTP server
  When the file is located on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Software update from an SCP or SFTP server
  When the file is located on an SCP or SFTP server, specify the URL for the file in one of the following forms:
  - `scp://` or `sftp://<IP address>/<path>/<file name>`
    When you click the *Start* button, the device displays the *Credentials* window. There you enter *User name* and *Password*, to log in to the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

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 system

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
- *sd-card*
  External SD memory (ACA31)
- *usb*
  External USB memory (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.

### License

Packages allow you to extend the device with selected functions. This table displays the packages contained in the device software.

License ID

Displays the index number to which the table entry relates.

Description

Displays the purpose for the use of the package.

Status

Displays if the device uses the package.

Possible values:

- *active*
  The device uses the package.
- *inactive*
  The device does not use the package.
- *no-license*
  The device lacks the license to use the package.

Software level capabilities

Displays which software level the package belongs to.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 1.6 Load/Save

[ Basic Settings > 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.

**Note:** Upgrading from Classic to HiOS? Convert your device configuration files using our online tool: https://convert.hirschmann.com

### External memory

Selected external memory

Specifies the external memory that the device uses for file operations. On this external memory, the device stores for example copies of the device configuration.

Possible values:

- *sd*
  External SD memory (ACA31)
- *usb*
  External USB memory (ACA22)

Status

Displays the operating state of the selected 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

Active

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` or `second` 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*).

**Note:** The prerequisite for loading a configuration profile from the external memory is that in the *Basic Settings > External Memory* dialog the *Config priority* column displays the value `first` or `second`. This value is set as the default setting.

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.

### 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”.

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

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”.

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
- with a lower or the same level of the device software
  such as HiOS-2A or HiOS-3A on a device which runs HiOS-3A

**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 16.

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 selected external memory. See the *External memory* frame.

☐ 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.
- Import from an FTP server
  When the file is located on an FTP server, specify the URL for the file in the following form:
  `ftp://<user>:<password>@<IP address>:<port>/<file name>`
- Import from a TFTP server
  When the file is located on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Import from an SCP or SFTP server
  When the file is located on an SCP or SFTP server, specify the URL for the file in one of the following forms:
  `scp://` or `sftp://<IP address>/<path>/<file name>`
  When you click the *Start* button, the device displays the *Credentials* window. There you enter *User name* and *Password*, to log in to the server.
  `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

☐ 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.

▶ *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 device uses modules, then also read the help text of the *Basic Settings > Modules* dialog.
- 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:

- Export to an FTP server
  To save the file on an FTP server, specify the URL for the file in the following form:
  `ftp://<user>:<password>@<IP address>:<port>/<file name>`
- Export to a TFTP server
  To save the file on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Export to an SCP or SFTP server
  To save the file on an SCP or SFTP server, specify the URL for the file in one of the following forms:
  - `scp://` or `sftp://<IP address>/<path>/<file name>`
    When you click the *Ok* button, the device displays the *Credentials* window. There you enter *User name* and *Password*, to log in to the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

Load running-config as script

Imports a script file which modifies the current `running config` configuration profile.

The device gives you the following options to import a script file:

- 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.
- Import from an FTP server
  When the file is located on an FTP server, specify the URL for the file in the following form:
  `ftp://<user>:<password>@<IP address>:<port>/<file name>`
- Import from a TFTP server
  When the file is located on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Import from an SCP or SFTP server
  When the file is located on an SCP or SFTP server, specify the URL for the file in one of the following forms:
  `scp://` or `sftp://<IP address>/<path>/<file name>`

**Note:** The device applies script files additionally to the current settings. Verify that the script file does not contain any parts that conflict with the current settings.

Save running-config as script

Saves the `running config` configuration profile as a script file on the local PC. This lets you backup your current device settings or to use them on various devices.

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*).

# 1.7 External Memory

[ Basic Settings > 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:

- *sd*
  External SD memory (ACA31)
- *usb*
  External USB memory (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.

SSH key auto upload

Activates/deactivates the loading of the RSA key from an external memory upon restart.

Possible values:

- `marked` (default setting)
  The loading of the RSA key is activated.
  During a restart, the device loads the RSA key from the external memory when the following files are located in the external memory:
  - SSH RSA key file
  - a text file `startup.txt` with the content
    `autoUpdateRSA=<filename_of_the_SSH_RSA_key>`

  The device displays messages on the system console of the serial interface.
- `unmarked`
  The loading of the RSA key is deactivated.

**Note:** When loading the RSA key from the external memory (*ENVM*), the device overwrites the existing keys in the non-volatile memory (*NVM*).

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`, `second`
  The device loads the configuration profile from the external memory designated as `first`. When the device does not find a configuration profile there, it loads the configuration profile from the external memory designated as `second`, and so on.
  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` or `second` 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 16.

# 1.8 Port

[Basic Settings > 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]
- [Utilization]

## [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.
  When the *Port on* function is active, the *Auto-Disable* function has disabled the port.
  You specify the settings of the *Auto-Disable* function in the *Diagnostics > Ports > Auto-Disable* dialog.

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
- `2500 Mbit/s FDX`
  Full duplex connection
- `10000 Mbit/s FDX`
  Full duplex connection

**Note:** The operating modes of the port actually available depend on the device configuration and the media module used.

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
- `2500 Mbit/s FDX`
  Full duplex connection
- `10000 Mbit/s FDX`
  Full duplex connection

**Note:** The operating modes of the port actually available depend on the device configuration and the media module used.

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 a change 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.

MTU

Specifies the maximum allowed size of Ethernet packets on the port in bytes.

Possible values:

- `1518..12288` (default setting: `1518`)
  With the setting `1518`, the port transmits the Ethernet packets up to the following size:
  - 1518 bytes without VLAN tag
    (1514 bytes + 4 bytes CRC)
  - 1522 bytes with VLAN tag
    (1518 bytes + 4 bytes CRC)

This setting lets you increase the max. allowed size of Ethernet packets that this port can receive or transmit.

The following list contains possible applications:

- When you use the device in the transfer network with double VLAN tagging, it is possible that you require an *MTU* that is larger by 4 bytes.

On other interfaces, you specify the maximum permissible size of the Ethernet packets as follows:

- Router interfaces
  *Routing > Interfaces > Configuration* dialog, *MTU value* column
- *Link Aggregation* interfaces
  *Switching > L2-Redundancy > Link Aggregation* dialog, *MTU* column

Signal

Activates/deactivates the port LED flashing. This function lets you identify the port in the field.

Possible values:

- `marked`
  The flashing of the port LED is active.
  The port LED flashes until you disable the function again.
- `unmarked` (default setting)
  The flashing of the port LED is inactive.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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 16.

Clear port statistics

Resets the counter for the port statistics to `0`.

## [Utilization]

This tab displays the utilization (network load) for the individual ports.

### Table

Port

Displays the port number.

Utilization [%]

Displays the current utilization in percent in relation to the time interval specified in the *Control interval [s]* column.

The utilization is the relationship of the received data quantity to the maximum possible data quantity at the currently configured data rate.

Lower threshold [%]

Specifies a lower threshold for the utilization. If the utilization of the port falls below this value, then the *Alarm* column displays an alarm.

Possible values:

- `0.00..100.00` (default setting: `0.00`)

The value `0` deactivates the lower threshold.

Upper threshold [%]

Specifies an upper threshold for the utilization. If the utilization of the port exceeds this value, then the *Alarm* column displays an alarm.

Possible values:

- `0.00..100.00` (default setting: `0.00`)

The value `0` deactivates the upper threshold.

Control interval [s]

Specifies the interval in seconds.

Possible values:

- `1..3600` (default setting: `30`)

Alarm

Displays the utilization alarm status.

Possible values:

- `marked`
  The utilization of the port is below the value specified in the *Lower threshold [%]* column or above the value specified in the *Upper threshold [%]* column. The device sends an SNMP trap.
- `unmarked`
  The utilization of the port is above the value specified in the *Lower threshold [%]* column and below the value specified in the *Upper threshold [%]* column.
  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 16.

Clear port statistics

Resets the counter for the port statistics to `0`.

## 1.9 Power over Ethernet

[ Basic Settings > Power over Ethernet ]

In Power over Ethernet (PoE), the Power Source Equipment (PSE) supplies current to powered devices (PD) such as IP phones through the twisted pair cable.

The product code and the PoE-specific labeling on the PSE device housing indicates if your device supports *Power over Ethernet*. The PoE ports of the device support Power over Ethernet according to IEEE 802.3at.

The system provides an internal maximum power budget for the ports. When you connect a new powered device to the port, verify the difference between the *Configured power budget [W]* and *Delivered power [W]* columns. Verify that the difference is equal to or more than the maximum power class of the new powered device.

You manage the power output with the *Priority* parameter. When the sum of the power required by the connected devices exceeds the power available, the device turns off power supplied to the ports according to configured priority. The device turns off power supplied to the ports starting with ports configured as a low priority first. When several ports have a low priority, the device turns off power starting with the higher numbered ports.

**Note:** If some ports have the same priority, then the device also verifies the real power consumption on the ports. To maximize the number of powered devices, the device turns off the power for the ports with higher power consumption first. The device continues this process until it obtains the configured power budget.

The menu contains the following dialogs:

- PoE Global
- PoE Port

# 1.9.1 PoE Global

[ Basic Settings > Power over Ethernet > Global ]

Based on the settings specified in this dialog, the device provides power to the end-user devices. If the power consumption reaches the user-specified threshold, then the device sends an SNMP trap.

### Operation

Operation

Enables/disables the *Power over Ethernet* function.

Possible values:

- `On` (default setting)
  The *Power over Ethernet* function is enabled.
- `Off`
  The *Power over Ethernet* function is disabled.

### Table

Module

Device module to which the table entries relate.

Configured power budget [W]

Specifies the power of the modules for the distribution at the ports.

Possible values:

- `0..n` (default setting: n)
  Here, `n` corresponds to the value in the *Max. power budget [W]* column.

Max. power budget [W]

Displays the maximum power available for this module.

Delivered power [W]

Displays the actual power in watts delivered to powered devices connected to this port.

Delivered current [mA]

Displays the actual current in milliamperes delivered to powered devices connected to this port.

Power source

Displays the power sourcing equipment for the device.

Possible values:

- *internal*
  Internal power source
- *external*
  External power source

Threshold [%]

Specifies the threshold value for the power consumption of the module in percent. If the power output exceeds this threshold, then the device measures the total output power and sends an SNMP trap.

Possible values:

- `0..99` (default setting: `90`)

Send trap

Activates/deactivates the sending of SNMP traps if the device detects that the threshold value for the power consumption exceeds.

Possible values:

- `marked`
  The sending of SNMP traps is active.
  If the power consumption of the module exceeds the user-defined threshold, 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.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 1.9.2 PoE Port

[Basic Settings > Power over Ethernet > Port]

When power consumption is higher than deliverable power, the device turns off power to the powered devices (PD) according to the priority levels and port numbers. When the PDs connected require more power than the device provides, the device deactivates the *Power over Ethernet* function on the ports. The device disables the *Power over Ethernet* function on the ports with the lowest priority first. When multiple ports have the same priority, the device first disables the *Power over Ethernet* function on the ports with the higher port number. The device also turns off power to powered devices (PD) for a specified time period.

**Note:** If some ports have the same priority, then the device also verifies the real power consumption on the ports. To maximize the number of powered devices, the device turns off the power for the ports with higher power consumption first. The device continues this process until it obtains the configured power budget.

### Table

Port

Displays the port number.

PoE enable

Activates/deactivates the PoE power provided to the port.

When the function is activated or deactivated, the device logs an event in the log file (System Log).

Possible values:

- `marked` (default setting)
  Providing PoE power to the port is active.
- `unmarked`
  Providing PoE power to the port is inactive.

Priority

Specifies the port priority.

To help prevent current overloads, the device disables ports with low priority first. To help prevent that the device disables the ports supplying necessary devices, specify a high priority for these ports.

Possible values:

- *`critical`*
- *`high`*
- *`low`* (default setting)

Status

Displays the status of the port Powered Device (PD) detection.

Possible values:

- *disabled*
  The device is in the DISABLED state and is not delivering power to the powered devices.
- *deliveringPower*
  The device identified the class of the connected PD and is in the POWER ON state.
- *fault*
  The device is in the TEST ERROR state.
- *otherFault*
  The device is in the IDLE state.
- *searching*
  The device is in a state other than the listed states.
- *test*
  The device is in the TEST MODE.

Detected class

Displays the power class of the powered device connected to the port.

Possible values:

- *Class 0*
- *Class 1*
- *Class 2*
- *Class 3*
- *Class 4*

Consumption [W]

Displays the current power consumption of the port in watts.

Possible values:

- 0,0..30,0

Consumption [mA]

Displays the current delivered to the port in milliamperes.

Possible values:

- 0..600

Max. consumption [W]

Displays the maximum power in watts that the device has consumed so far.

You reset the value when you disable PoE on the port or terminate the connection to the connected device.

Name

Specifies the name of the port.

Specify the name of your choice.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters

Auto-shutdown power

Activates/deactivates the *Auto-shutdown power* function according to the settings.

Possible values:

- `marked`
- `unmarked` (default setting)

Disable power at [hh:mm]

Specifies the time at which the device disables the power for the port upon activation of the *Auto-shutdown power* function.

Possible values:

- `00:00..23:59` (default setting: `00:00`)

Re-enable power at [hh:mm]

Specifies the time at which the device enables the power for the port upon activation of the *Auto-shutdown power* function.

Possible values:

- `00:00..23:59` (default setting: `00:00`)

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 1.10 Restart

[ Basic Settings > Restart ]

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

### Restart

Restart in

Displays the remaining time until the device restarts.

To update the display of the remaining time, click the button.

Cancel

Aborts a delayed restart.

Cold start...

Opens the *Restart* dialog to initiate an immediate or delayed 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.
- In the *Restart in* field you specify the delay time for the delayed restart.
  Possible values:
  - `00:00:00..596:31:23` (default setting: `00:00:00`)

When the delay time elapsed, the device restarts and goes through the following phases:

- If you activate the function in the *Diagnostics > System > Selftest* dialog, then the device performs a RAM test.
- 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 16.

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.

Clear management access statistics

Resets the counters for statistics on device management access to `0`.

See the *Diagnostics > System > System Information* dialog, `Used Management Ports` table.

Reset IGMP snooping data

Removes the IGMP Snooping entries and resets the counter in the *Information* frame to `0`.

See the *Switching > IGMP Snooping > Global* dialog.

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 email notification statistics

Resets the counters in the *Information* frame to `0`.

See the *Diagnostics > Email Notification > Global* dialog.

# 2 Time

The menu contains the following dialogs:
- Basic Settings
- SNTP
- PTP

## 2.1 Basic Settings

[ Time > Basic Settings ]

The device is equipped with a buffered hardware clock. This clock maintains the correct time if the power supply fails or you disconnect the device from the power supply. After the device is started, the current time is available to you, for example for log entries.

The hardware clock bridges a power supply downtime of 3 hours. The prerequisite is that the power supply of the device has been connected continually for at least 5 minutes beforehand.

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

The dialog contains the following tabs:
- [Global]
- [Daylight saving time]

### [Global]

In this tab you specify the system time in the device and the time zone.

#### 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.
- *sntp*
  The *SNTP* client is activated and the device is synchronized by an *SNTP* server.
- *ptp*
  PTP is activated and the clock of the device is synchronized with a *PTP* master clock.

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 16.

## [Daylight saving time]

In this tab you activate the automatic daylight saving time function. You specify the beginning and the end of summertime using a pre-defined profile, or you specify these settings individually. During summertime, the device puts the local time forward by 1 hour.

### Operation

Daylight saving time

Enables/disables the *Daylight saving time* mode.

Possible values:

- *On*
  The *Daylight saving time* mode is enabled.
  The device automatically changes between summertime and wintertime.
- *Off* (default setting)
  The *Daylight saving time* mode is disabled.

The times at which the device changes between summertime and wintertime are specified in the *Summertime begin* and *Summertime end* frames.

Profile...

Displays the *Profile...* dialog. There you select a pre-defined profile for the beginning and the end of summertime. This profile overwrites the settings in the *Summertime begin* and *Summertime end* frames.

### Summertime begin

In the first 3 fields you specify the day for the beginning of summertime, and in the last field the time.

When the time in the *System time* field reaches the value entered here, the device switches to summertime.

Week

Specifies the week in the current month.

Possible values:

- *none* (default setting)
- *first*
- *second*
- *third*
- *fourth*
- *last*

Day

Specifies the day of the week.

Possible values:

- *none* (default setting)
- *Sunday*
- *Monday*
- *Tuesday*
- *Wednesday*
- *Thursday*
- *Friday*
- *Saturday*

Month

Specifies the month.

Possible values:

- *none* (default setting)
- *January*
- *February*
- *March*
- *April*
- *May*
- *June*

- *July*
- *August*
- *September*
- *October*
- *November*
- *December*

System time

Specifies the time.

Possible values:

- `<HH:MM>` (default setting: `00:00`)

### Summertime end

In the first 3 fields you specify the day for the end of summertime, and in the last field the time.

When the time in the *System time* field reaches the value entered here, the device switches to wintertime.

Week

Specifies the week in the current month.

Possible values:

- *none* (default setting)
- *first*
- *second*
- *third*
- *fourth*
- *last*

Day

Specifies the day of the week.

Possible values:

- *none* (default setting)
- *Sunday*
- *Monday*
- *Tuesday*
- *Wednesday*
- *Thursday*
- *Friday*
- *Saturday*

Month

Specifies the month.

Possible values:

- *none* (default setting)
- *January*
- *February*
- *March*
- *April*
- *May*
- *June*
- *July*
- *August*
- *September*
- *October*
- *November*
- *December*

System time

Specifies the time.

Possible values:

- <HH:MM> (default setting: 00:00)

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 2.2 SNTP

[ Time > SNTP ]

The Simple Network Time Protocol (SNTP) is a procedure described in the RFC 4330 for time synchronization in the network.

The device lets you synchronize the system time in the device as an *SNTP* client. As the *SNTP* server, the device makes the time information available to other devices.

The menu contains the following dialogs:

- SNTP Client
- SNTP Server

# 2.2.1 SNTP Client

[ Time > SNTP > Client ]

In this dialog you specify the settings with which the device operates as an *SNTP* client.

As an *SNTP* client the device obtains the time information from both *SNTP* servers and *NTP* servers and synchronizes the local clock with the time of the time server.

### Operation

Operation

Enables/disables the *SNTP Client* function of the device.

Possible values:

- `On`
  The *SNTP Client* function is enabled.
  The device operates as an *SNTP* client.
- `Off` (default setting)
  The *SNTP Client* function is disabled.

### Configuration

Mode

Specifies if the device actively requests the time information from an *SNTP* server known and configured in the network (Unicast mode) or passively waits for the time information from a random *SNTP* server (Broadcast mode).

Possible values:

- `unicast` (default setting)
  The device takes the time information only from the configured *SNTP* server. The device sends Unicast requests to the *SNTP* server and evaluates its responses.
- `broadcast`
  The device obtains the time information from one or more *SNTP* or *NTP* servers. The device evaluates the Broadcasts or Multicasts only from these servers.

Request interval [s]

Specifies the interval in seconds at which the device requests time information from the *SNTP* server.

Possible values:

- `5..3600` (default setting: `30`)

Broadcast recv timeout [s]

Specifies the time in seconds a client in broadcast client mode waits before changing the value in the field from *`syncToRemoteServer`* to *`notSynchronized`* when the client receives no broadcast packets.

Possible values:

- `128..2048` (default setting: `320`)

Disable client after successful sync

Activates/deactivates the disabling of the *SNTP* client after the device has successfully synchronized the time.

Possible values:

- `marked`
  The disabling of the *SNTP* client is active.
  The device deactivates the *SNTP* client after successful time synchronization.
- `unmarked` (default setting)
  The disabling of the *SNTP* client is inactive.
  The *SNTP* client remains active after successful time synchronization.

### State

State

Displays the status of the *SNTP* client.

Possible values:

- *`disabled`*
  The *SNTP* client is disabled.
- *`notSynchronized`*
  The *SNTP* client is not synchronized with any *SNTP* or *NTP* server.
- *`synchronizedToRemoteServer`*
  The *SNTP* client is synchronized with an *SNTP* or *NTP* server.

### Table

In the table you specify the settings for up to 4 *SNTP* servers.

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.

After starting, the device sends requests to the *SNTP* server configured in the first table entry. When the server does not reply, the device sends its requests to the *SNTP* server configured in the next table entry.

If none of the configured *SNTP* servers responds in the meantime, then the *SNTP* client interrupts its synchronization. The device cyclically sends requests to each *SNTP* server until a server delivers a valid time. The device synchronizes itself with this *SNTP* server, even if the other servers can be reached again later.

Name

Specifies the name of the *SNTP* server.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters

Address

Specifies the IP address of the *SNTP* server.

Possible values:

- Valid IPv4 address (default setting: `0.0.0.0`)
- Hostname

Destination UDP port

Specifies the UDP Port on which the *SNTP* server expects the time information.

Possible values:

- `1..65535` (default setting: `123`)
  Exception: Port `2222` is reserved for internal functions.

Status

Displays the connection status between the *SNTP* client and the *SNTP* server.

Possible values:

- *`success`*
  The device has successfully synchronized the time with the *SNTP* server.

- *badDateEncoded*
  The time information received contains protocol errors - synchronization failed.
- *other*
  - The value 0.0.0.0 is entered for the IP address of the *SNTP* server - synchronization failed.
    or
  - The *SNTP* client is using a different *SNTP* server.
- *requestTimedOut*
  The device has not received a reply from the *SNTP* server - synchronization failed.
- *serverKissOfDeath*
  The *SNTP* server is overloaded. The device is requested to synchronize itself with another *SNTP* server. When no other *SNTP* server is available, the device checks at intervals longer than the setting in the *Request interval [s]* field, if the server is still overloaded.
- *serverUnsychronized*
  The *SNTP* server is not synchronized with either a local or an external reference time source - synchronization failed.
- *versionNotSupported*
  The *SNTP* versions on the client and the server are incompatible with each other - synchronization failed.

Active

Activates/deactivates the connection to the *SNTP* server.

Possible values:

- marked
  The connection to the *SNTP* server is activated.
  The *SNTP* client has access to the *SNTP* server.
- unmarked (default setting)
  The connection to the *SNTP* server is deactivated.
  The *SNTP* client has no access to the *SNTP* server.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 2.2.2 SNTP Server

[ Time > SNTP > Server ]

In this dialog you specify the settings with which the device operates as an *SNTP* server.

The *SNTP* server provides the Universal Time Coordinated (UTC) without considering local time differences.

If the setting is appropriate, then the *SNTP* server operates in the broadcast mode. In broadcast mode, the *SNTP* server automatically sends broadcast messages or multicast messages according to the broadcast send interval.

### Operation

Operation

Enables/disables the *SNTP Server* function of the device.

Possible values:

- `On`
  The *SNTP Server* function is enabled.
  The device operates as an *SNTP* server.
- `Off` (default setting)
  The *SNTP Server* function is disabled.

Note the setting in the *Disable server at local time source* checkbox in the *Configuration* frame.

### Configuration

UDP port

Specifies the number of the UDP port on which the *SNTP* server of the device receives requests from other clients.

Possible values:

- `1..65535` (default setting: `123`)
  Exception: Port `2222` is reserved for internal functions.

Broadcast admin mode

Activates/deactivates the Broadcast mode.

- `marked`
  The *SNTP* server replies to requests from *SNTP* clients in Unicast mode and also sends *SNTP* packets in Broadcast mode as Broadcasts or Multicasts.
- `unmarked` (default setting)
  The *SNTP* server replies to requests from *SNTP* clients in the Unicast mode.

Broadcast destination address

Specifies the IP address to which the *SNTP* server of the device sends the *SNTP* packets in Broadcast mode.

Possible values:

- Valid IPv4 address (default setting: `0.0.0.0`)

Broadcast and Multicast addresses are permitted.

Broadcast UDP port

Specifies the number of the UDP port on which the *SNTP* server sends the *SNTP* packets in Broadcast mode.

Possible values:

- `1..65535` (default setting: `123`)
  Exception: Port `2222` is reserved for internal functions.

Broadcast VLAN ID

Specifies the ID of the VLAN in which the *SNTP* server of the device sends the *SNTP* packets in Broadcast mode.

Possible values:

- `0`
  The *SNTP* server sends the *SNTP* packets in the same VLAN in which the access to the device management is possible. See the *Basic Settings > Network* dialog.
- `1..4042` (default setting: `1`)

Broadcast send interval [s]

Specifies the time interval at which the *SNTP* server of the device sends *SNTP* broadcast packets.

Possible values:

- `64..1024` (default setting: `128`)

Disable server at local time source

Activates/deactivates the disabling of the *SNTP* server when the device is synchronized to the local clock.

Possible values:

- `marked`
  The disabling of the *SNTP* server is active.
  If the device is synchronized to the local clock, then the device disables the *SNTP* server. The *SNTP* server continues to reply to requests from *SNTP* clients. In the *SNTP* packet, the *SNTP* server informs the clients that it is synchronized locally.
- `unmarked` (default setting)
  The disabling of the *SNTP* server is inactive.
  If the device is synchronized to the local clock, then the *SNTP* server remains active.

### State

State

Displays the state of the *SNTP* server.

Possible values:

- *disabled*
  The *SNTP* server is disabled.
- *notSynchronized*
  The *SNTP* server is not synchronized with either a local or an external reference time source.
- *syncToLocal*
  The *SNTP* server is synchronized with the hardware clock of the device.
- *syncToRefclock*
  The *SNTP* server is synchronized with an external reference time source, for example PTP.
- *syncToRemoteServer*
  The *SNTP* server is synchronized with an *SNTP* server that is higher than the device in a cascade.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 2.3 PTP

[ Time > PTP ]

The menu contains the following dialogs:

- PTP Global
- PTP Boundary Clock
- PTP Transparent Clock

# 2.3.1 PTP Global

[ Time > PTP > Global ]

In this dialog you specify basic settings for the *PTP* protocol.

The Precision Time Protocol (PTP) is a procedure described in the IEEE 1588-2008 standard that supplies the devices in the network with a precise time. The method synchronizes the clocks in the network with a precision of a few 100 ns. The protocol uses Multicast communication, so the load on the network due to the *PTP* synchronization messages is negligible.

PTP is significantly more accurate than SNTP. If the *SNTP* function and the *PTP* function are enabled in the device at the same time, then the *PTP* function has priority.

With the *Best Master Clock Algorithm*, the devices in the network determine which device has the most accurate time. The devices use the device with the most accurate time as the reference time source (*Grandmaster*). Subsequently the participating devices synchronize themselves with this reference time source.

If you want to transport PTP time accurately through your network, then use only devices with PTP hardware support on the transport paths.

The protocol differentiates between the following clocks:

- *Boundary Clock (BC)*
  This clock has any number of PTP ports and operates as both *PTP* master and *PTP* slave. In its respective network segment, the clock operates as an Ordinary Clock.
  - As *PTP* slave, the clock synchronizes itself with a *PTP* master that is higher than the device in the cascade.
  - As *PTP* master, the clock forwards the time information via the network to *PTP* slaves that are higher than the device in the cascade.
- *Transparent Clock (TC)*
  This clock has any number of PTP ports. In contrast to the *Boundary Clock*, this clock corrects the time information before forwarding it, without synchronizing itself.

### Operation IEEE1588/PTP

Operation IEEE1588/PTP

Enables/disables the *PTP* function.

Possible values:

- `On`
  The *PTP* function is enabled.
  The device synchronizes its clock with PTP.
  If the *SNTP* function and the *PTP* function are enabled in the device at the same time, then the *PTP* function has priority.
- `Off` (default setting)
  The *PTP* function is disabled.
  The device transmits the *PTP* synchronization messages without any correction on every port.

### Configuration IEEE1588/PTP

PTP mode

Specifies the PTP version and mode of the local clock.

Possible values:

- *v2-transparent-clock* (default setting)
- *v2-boundary-clock*

Sync lower bound [ns]

Specifies the lower threshold value in nanoseconds for the path difference between the local clock and the reference time source (*Grandmaster*). If the path difference falls below this value once, then the local clock is classed as synchronized.

Possible values:

- `0..999999999` (default setting: `30`)

Sync upper bound [ns]

Specifies the upper threshold value in nanoseconds for the path difference between the local clock and the reference time source (*Grandmaster*). If the path difference exceeds this value once, then the local clock is classed as unsynchronized.

Possible values:

- `31..1000000000` (default setting: `5000`)

PTP management

Activates/deactivates the PTP management defined in the PTP standard.

Possible values:

- `marked`
  PTP management is activated.
- `unmarked` (default setting)
  PTP management is deactivated.

### Status

Is synchronized

Displays if the local clock is synchronized with the reference time source (*Grandmaster*).

If the path difference between the local clock and the reference time source (*Grandmaster*) falls below the synchronization lower threshold one time, then the local clock is synchronized. This status is kept until the path difference exceeds the synchronization upper threshold one time.

You specify the synchronization thresholds in the *Configuration IEEE1588/PTP* frame.

Max. offset absolute [ns]

Displays the maximum path difference in nanoseconds that has occurred since the local clock was synchronized with the reference time source (*Grandmaster*).

PTP time

Displays the date and time for the PTP time scale when the local clock is synchronized with the reference time source (*Grandmaster*). Format: `Month Day, Year hh:mm:ss AM/PM`

#### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 2.3.2 PTP Boundary Clock

[ Time > PTP > Boundary Clock ]

With this menu you can configure the Boundary Clock mode for the local clock.

The menu contains the following dialogs:
- PTP Boundary Clock Global
- PTP Boundary Clock Port

# 2.3.2.1 PTP Boundary Clock Global

[ Time > PTP > Boundary Clock > Global ]

In this dialog you enter general, cross-port settings for the *Boundary Clock* mode for the local clock. The *Boundary Clock (BC)* operates according to PTP version 2 (IEEE 1588-2008).

The settings are effective when the local clock operates as the *Boundary Clock (BC)*. For this, you select in the *Time > PTP > Global* dialog in the *PTP mode* field the value `v2-boundary-clock`.

### Operation IEEE1588/PTPv2 BC

Priority 1

Specifies *priority 1* for the device.

Possible values:

- `0..255` (default setting: `128`)

The *Best Master Clock Algorithm* first evaluates *priority 1* among the participating devices in order to determine the reference time source (*Grandmaster*).

The lower you set this value, the more probable it is that the device becomes the reference time source (*Grandmaster*). See the *Grandmaster* frame.

Priority 2

Specifies *priority 2* for the device.

Possible values:

- `0..255` (default setting: `128`)

When the previously evaluated criteria are the same for multiple devices, the *Best Master Clock Algorithm* evaluates *priority 2* of the participating devices.

The lower you set this value, the more probable it is that the device becomes the reference time source (*Grandmaster*). See the *Grandmaster* frame.

Domain number

Assigns the device to a *PTP* domain.

Possible values:

- `0..255` (default setting: `0`)

The device transmits time information from and to devices only in the same domain.

### Status IEEE1588/PTPv2 BC

Two step

Displays that the clock is operating in Two-Step mode.

Steps removed

Displays the number of communication paths passed through between the local clock of the device and the reference time source (*Grandmaster*).

For a *PTP* slave, the value 1 means that the clock is connected with the reference time source (*Grandmaster*) directly through 1 communication path.

Offset to master [ns]

Displays the measured difference (offset) between the local clock and the reference time source (*Grandmaster*) in nanoseconds. The *PTP* slave calculates the difference from the time information received.

In Two-Step mode the time information consists of 2 *PTP* synchronization messages each, which the *PTP* master sends cyclically:

- The first synchronization message (sync message) contains an estimated value for the exact sending time of the message.
- The second synchronization message (follow-up message) contains the exact sending time of the first message.

The *PTP* slave uses the two *PTP* synchronization messages to calculate the difference (offset) from the master and corrects its clock by this difference. Here the *PTP* slave also considers the *Delay to master [ns]* value.

Delay to master [ns]

Displays the delay when transmitting the *PTP* synchronization messages from the *PTP* master to the *PTP* slave in nanoseconds.

The *PTP* slave sends a “Delay Request” packet to the *PTP* master and thus determines the exact sending time of the packet. When it receives the packet, the *PTP* master generates a time stamp and sends this in a “Delay Response” packet back to the *PTP* slave. The *PTP* slave uses the two packets to calculate the delay, and considers this starting from the next offset measurement.

The prerequisite is that the delay mechanism value of the slave ports is specified as *e2e*.

### Grandmaster

This frame displays the criteria that the *Best Master Clock Algorithm* uses when evaluating the reference time source (*Grandmaster*).

The algorithm first evaluates *priority 1* of the participating devices. The device with the lowest value for *priority 1* is designated as the reference time source (*Grandmaster*). When the value is the same for multiple devices, the algorithm takes the next criterion, and when this is also the same, the algorithm takes the next criterion after this one. When every value is the same for multiple devices, the lowest value in the *Clock identity* field decides which device is designated as the reference time source (*Grandmaster*).

The device lets you influence which device in the network is designated as the reference time source (*Grandmaster*). To do this, modify the value in the *Priority 1* field or the *Priority 2* field in the *Operation IEEE1588/PTPv2 BC* frame.

Priority 1

Displays *priority 1* for the device that is currently the reference time source (*Grandmaster*).

Clock class

Displays the class of the reference time source (*Grandmaster*). Parameter for the *Best Master Clock Algorithm*.

Clock accuracy

Displays the estimated accuracy of the reference time source (*Grandmaster*). Parameter for the *Best Master Clock Algorithm*.

Clock variance

Displays the variance of the reference time source (*Grandmaster*), also known as the *Offset scaled log variance*. Parameter for the *Best Master Clock Algorithm*.

Priority 2

Displays *priority 2* for the device that is currently the reference time source (*Grandmaster*).

### Local time properties

Time source

Specifies the time source from which the local clock gets its time information.

Possible values:

- *atomicClock*
- *gps*
- *terrestrialRadio*
- *ptp*
- *ntp*
- *handSet*
- *other*
- *internalOscillator* (default setting)

UTC offset [s]

Specifies the difference between the *PTP* time scale and the UTC.

See the *PTP timescale* checkbox.

Possible values:

- `-32768..32767`

**Note:** The default setting is the value valid on the creation date of the device software. You can find further information in the "Bulletin C" of the Earth Rotation and Reference Systems Service (IERS): http://www.iers.org/IERS/EN/Publications/Bulletins/bulletins.html

UTC offset valid

Specifies if the value specified in the *UTC offset [s]* field is correct.

Possible values:

- `marked`
- `unmarked` (default setting)

Time traceable

Displays if the device gets the time from a primary UTC reference, for example from an NTP server.

Possible values:

- `marked`
- `unmarked`

Frequency traceable

Displays if the device gets the frequency from a primary UTC reference, for example from an NTP server.

Possible values:

- `marked`
- `unmarked`

PTP timescale

Displays if the device uses the PTP time scale.

Possible values:

- `marked`
- `unmarked`

According to IEEE 1588, the PTP time scale is the TAI atomic time started on 01.01.1970.

In contrast to UTC, TAI does not use leap seconds.

As of July 1, 2020, the TAI time is 37 s ahead of the UTC time.

### Identities

The device displays the identities as byte sequences in hexadecimal notation.

The identification numbers (UUID) are made up as follows:

- The device identification number consists of the MAC address of the device, with the values `ff` and `fe` added between byte 3 and byte 4.
- The port UUID consists of the device identification number followed by a 16-bit port ID.

Clock identity

Displays the device's own identification number (UUID).

Parent port identity

Displays the port identification number (UUID) of the directly superior master device.

Grandmaster identity

Displays the identification number (UUID) of the reference time source (*Grandmaster*) device.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 2.3.2.2 PTP Boundary Clock Port

[ Time > PTP > Boundary Clock > Port ]

In this dialog you specify the *Boundary Clock (BC)* settings on each individual port.

The settings are effective when the local clock operates as the *Boundary Clock (BC)*. For this, you select in the *Time > PTP > Global* dialog in the *PTP mode* field the value `v2-boundary-clock`.

### Table

Port

Displays the port number.

PTP enable

Activates/deactivates *PTP* synchronization message transmission on the port.

Possible values:

- `marked` (default setting)
  The transmission is activated. The port forwards and receives *PTP* synchronization messages.
- `unmarked`
  The transmission is deactivated. The port blocks *PTP* synchronization messages.

PTP status

Displays the current status of the port.

Possible values:

- *`initializing`*
  Initialization phase
- *`faulty`*
  Faulty mode: error in the PTP protocol.
- *`disabled`*
  PTP is disabled on the port.
- *`listening`*
  Device port is waiting for *PTP* synchronization messages.
- *`pre-master`*
  *PTP* pre-master mode
- *`master`*
  *PTP* master mode
- *`passive`*
  *PTP* passive mode
- *`uncalibrated`*
  *PTP* uncalibrated mode
- *`slave`*
  *PTP* slave mode

Sync interval

Specifies the interval in seconds at which the port transmits *PTP* synchronization messages.

Possible values:

- `0.25`
- `0.5`
- `1` (default setting)
- `2`

Delay mechanism

Specifies the mechanism with which the device measures the delay for transmitting the *PTP* synchronization messages.

Possible values:

- *`disabled`*
  The measurement of the delay for the *PTP* synchronization messages for the connected PTP devices is inactive.
- *`e2e`* (default setting)
  End-to-End: As the *PTP* slave, the port measures the delay for the *PTP* synchronization messages to the *PTP* master.
  The device displays the measured value in the *Time > PTP > Boundary Clock > Global* dialog.
- *`p2p`*
  Peer-to-Peer: The device measures the delay for the *PTP* synchronization messages for the connected PTP devices, provided that these devices support P2P.
  This mechanism saves the device from having to determine the delay again in the case of a reconfiguration.

P2P delay

Displays the measured Peer-to-Peer delay for the *PTP* synchronization messages.

The prerequisite is that you select the value *`p2p`* in the *Delay mechanism* column.

P2P delay interval [s]

Specifies the interval in seconds at which the port measures the Peer-to-Peer delay.

The prerequisite is that you have specified the value *`p2p`* on this port and on the port of the remote device.

Possible values:

- `1` (default setting)
- `2`
- `4`
- `8`
- `16`
- `32`

Network protocol

Specifies which protocol the port uses to transmit the *PTP* synchronization messages.

Possible values:

- *IEEE 802.3* (default setting)
- *UDP/IPv4*

Announce interval [s]

Specifies the interval in seconds at which the port transmits messages for the PTP topology discovery.

Assign the same value to every device of a *PTP* domain.

Possible values:

- 1
- 2 (default setting)
- 4
- 8
- 16

Announce timeout

Specifies the number of announce intervals.

Example:

For the default setting (*Announce interval [s]* = 2 and *Announce timeout* = 3), the timeout is 3 × 2 s = 6 s.

Possible values:

- 2..10 (default setting: 3)
  Assign the same value to every device of a *PTP* domain.

E2E delay interval [s]

Displays the interval in seconds at which the port measures the End-to-End delay:

- When the port is operating as the *PTP* master, the device assigns to the port the value 8.
- When the port is operating as the *PTP* slave, the value is specified by the *PTP* master connected to the port.

V1 hardware compatibility

Specifies if the port adjusts the length of the *PTP* synchronization messages when you have set in the *Network protocol* column the value *udpIpv4*.

It is possible that other devices in the network expect the *PTP* synchronization messages to be the same length as PTPv1 messages.

Possible values:

- *auto* (default setting)
  The device automatically detects if other devices in the network expect the *PTP* synchronization messages to be the same length as PTPv1 messages. If this is the case, then the device extends the length of the *PTP* synchronization messages before transmitting them.

- *on*
  The device extends the length of the *PTP* synchronization messages before transmitting them.
- *off*
  The device transmits *PTP* synchronization messages without changing the length.

Asymmetry

Corrects the measured delay value corrupted by asymmetrical transmission paths.

Possible values:

- `-2000000000..2000000000` (default setting: `0`)

The value represents the delay symmetry in nanoseconds.

A measured delay value of y ns corresponds to an asymmetry of y × 2 ns.

The value is positive if the delay from the *PTP* master to the *PTP* slave is longer than in the opposite direction.

VLAN

Specifies the VLAN ID with which the device marks the *PTP* synchronization messages on this port.

Possible values:

- *none* (default setting)
  The device transmits *PTP* synchronization messages without a VLAN tag.
- `0..4042`
  You specify VLANs that you have already set up in the device from the list.

Verify that the port is a member of the VLAN.

See the *Switching > VLAN > Configuration* dialog.

VLAN priority

Specifies the priority with which the device transmits the *PTP* synchronization messages marked with a VLAN ID (Layer 2, IEEE 802.1D).

Possible values:

- `0..7` (default setting: `6`)

If you specified in the *VLAN* column the value *none*, then the device ignores the VLAN priority.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 2.3.3 PTP Transparent Clock

[ Time > PTP > Transparent Clock ]

With this menu you can configure the *Transparent Clock* mode for the local clock.

The menu contains the following dialogs:

- PTP Transparent Clock Global
- PTP Transparent Clock Port

# 2.3.3.1 PTP Transparent Clock Global

[ Time > PTP > Transparent Clock > Global ]

In this dialog you enter general, cross-port settings for the *Transparent Clock* mode for the local clock. The *Transparent Clock (TC)* operates according to PTP version 2 (IEEE 1588-2008).

The settings are effective when the local clock operates as the *Transparent Clock (TC)*. For this, you select in the *Time > PTP > Global* dialog in the *PTP mode* field the value `v2-transparent-clock`.

### Operation IEEE1588/PTPv2 TC

Delay mechanism

Specifies the mechanism with which the device measures the delay for transmitting the *PTP* synchronization messages.

Possible values:

- `e2e` (default setting)
  As the *PTP* slave, the port measures the delay for the *PTP* synchronization messages to the *PTP* master.
  The device displays the measured value in the *Time > PTP > Transparent Clock > Global* dialog.
- `p2p`
  The device measures the delay for the *PTP* synchronization messages for every connected PTP device, provided that the device supports P2P.
  This mechanism saves the device from having to determine the delay again in the case of a reconfiguration.
  If you specify this value, then the value `IEEE 802.3` is only available in the *Network protocol* field.
- `e2e-optimized`
  Like `e2e`, with the following special characteristics:
  - The device transmits the delay requests of the *PTP* slaves only to the *PTP* master, even though these requests are multicast messages. The device thus spares the other devices from unnecessary multicast requests.
  - If the master-slave topology changes, then the device relearns the port for the *PTP* master as soon as it receives a synchronization message from another *PTP* master.
  - If the device does not know a *PTP* master, then the device transmits delay requests to the ports.
- `disabled`
  The delay measuring is disabled on the port. The device discards messages for the delay measuring.

Primary domain

Assigns the device to a *PTP* domain.

Possible values:

- `0..255` (default setting: `0`)

The device transmits time information from and to devices only in the same domain.

Network protocol

Specifies which protocol the port uses to transmit the *PTP* synchronization messages.

Possible values:

- `ieee8023` (default setting)
- `udpIpv4`

Multi domain mode

Activates/deactivates the *PTP* synchronization message correction in every *PTP* domain.

Possible values:

- `marked`
  The device corrects *PTP* synchronization messages in every *PTP* domain.
- `unmarked` (default setting)
  The device corrects *PTP* synchronization messages only in the primary *PTP* domain. See the *Primary domain* field.

VLAN ID

Specifies the VLAN ID with which the device marks the *PTP* synchronization messages on this port.

Possible values:

- `none` (default setting)
  The device transmits *PTP* synchronization messages without a VLAN tag.
- `0..4042`
  You specify VLANs that you have already set up in the device from the list.

VLAN priority

Specifies the priority with which the device transmits the *PTP* synchronization messages marked with a VLAN ID (Layer 2, IEEE 802.1D).

Possible values:

- `0..7` (default setting: `6`)

If you specified the value `none` in the *VLAN ID* field, then the device ignores the specified value.

### Local synchronization

Syntonize

Activates/deactivates the frequency synchronization of the *Transparent Clock* with the *PTP* master.

Possible values:

- `marked` (default setting)
  The frequency synchronization is active.
  The device synchronizes the frequency.
- `unmarked`
  The frequency synchronization is inactive.
  The frequency remains constant.

Synchronize local clock

Activates/deactivates the synchronization of the local system time.

Possible values:

- `marked`
  The synchronization is active.
  The device synchronizes the local system time with the time received via PTP. The prerequisite is that the *Syntonize* checkbox is marked.
- `unmarked` (default setting)
  The synchronization is inactive.
  The local system time remains constant.

Current master

Displays the port identification number (UUID) of the directly superior master device on which the device synchronizes its frequency.

If the value contains only zeros, this is because:

- The *Syntonize* function is disabled.
  or
- The device cannot find a *PTP* master.

Offset to master [ns]

Displays the measured difference (offset) between the local clock and the *PTP* master in nanoseconds. The device calculates the difference from the time information received.

The prerequisite is that the *Synchronize local clock* function is enabled.

Delay to master [ns]

Displays the delay when transmitting the *PTP* synchronization messages from the *PTP* master to the *PTP* slave in nanoseconds.

Prerequisite:

- The *Synchronize local clock* function is enabled.
- In the *Delay mechanism* field, the value `e2e` is selected.

### Status IEEE1588/PTPv2 TC

Clock identity

Displays the device's own identification number (UUID).

The device displays the identities as byte sequences in hexadecimal notation.

The device identification number consists of the MAC address of the device, with the values `ff` and `fe` added between byte 3 and byte 4.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 2.3.3.2 PTP Transparent Clock Port

[ Time > PTP > Transparent Clock > Port ]

In this dialog you specify the *Transparent Clock (TC)* settings on each individual port.

The settings are effective when the local clock operates as the *Transparent Clock (TC)*. For this, you select in the *Time > PTP > Global* dialog in the *PTP mode* field the value `v2-transparent-clock`.

### Table

Port

Displays the port number.

PTP enable

Activates/deactivates the transmitting of *PTP* synchronization messages on the port.

Possible values:

- `marked` (default setting)
  The transmitting is active.
  The port forwards and receives *PTP* synchronization messages.
- `unmarked`
  The transmitting is inactive.
  The port blocks *PTP* synchronization messages.

P2P delay interval [s]

Specifies the interval in seconds at which the port measures the Peer-to-Peer delay.

The prerequisite is that you specify the value `p2p` on this port and on the port of the remote terminal. See the *Delay mechanism* option list in the *Time > PTP > Transparent Clock > Global* dialog.

Possible values:

- `1` (default setting)
- `2`
- `4`
- `8`
- `16`
- `32`

P2P delay

Displays the measured Peer-to-Peer delay for the *PTP* synchronization messages.

The prerequisite is that you select in the *Delay mechanism* option list the `p2p` radio button. See the *Delay mechanism* field in the *Time > PTP > Transparent Clock > Global* dialog.

Asymmetry

Corrects the measured delay value corrupted by asymmetrical transmission paths.

Possible values:

- `-2000000000..2000000000` (default setting: `0`)

The value represents the delay symmetry in nanoseconds.

A measured delay value of y ns corresponds to an asymmetry of y × 2 ns.

The value is positive if the delay from the *PTP* master to the *PTP* slave is longer than in the opposite direction.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 3 Device Security

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

## 3.1 User Management

[ Device Security > 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

Specifies the password that the user applies to access the device management using the Graphical User Interface or Command Line Interface.

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

When you specify the password for the first time, the device uses the same password in the *SNMP auth password* and *SNMP encryption password* columns.

- The device lets you specify different passwords in the *SNMP auth password* and *SNMP encryption password* columns.
- If you change the password in the current column, then the device also changes the passwords for the *SNMP auth password* and *SNMP encryption password* columns, but only if they are not individually specified previously.

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:

- *unauthorized*
  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 auth password

Specifies the password that the device applies for user access via SNMPv3.

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

By default, the device uses the same password that you specify in the *Password* column.

- For the current column, the device lets you specify a different password than in the *Password* column.
- If you change the password in the *Password* column, then the device also changes the password for the current column, but only if it is not individually specified.

Possible values:

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

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

SNMP encryption password

Specifies the password that the device applies to encrypt user access via SNMPv3.

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

By default, the device uses the same password that you specify in the *Password* column.

- For the current column, the device lets you specify a different password than in the *Password* column.
- If you change the password in the *Password* column, then the device also changes the password for the current column, but only if it is not individually specified.

Possible values:

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

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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

[ Device Security > Authentication List ]

In this dialog you manage the authentication lists. In an 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

With the port-based access control according to IEEE 802.1X, if connected end devices log in with valid login data, then the device lets them have access to the network. The device authenticates the end devices using the following methods:
- RADIUS
- IAS (Integrated Authentication Server)

In the default setting the following authentication lists are available:
- `defaultDot1x8021AuthList`
- `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.

Name

Displays the name of the list.

To create a new list, click the button.

Possible values:
- Alphanumeric ASCII character string with 1..32 characters

Policy 1
Policy 2
Policy 3
Policy 4
Policy 5

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.
- *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 polices.
  - 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 polices 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 devices immediately rejects the user login without attempting another policy.
  - Verify that the authentication list `defaultV24AuthList` contains at least one policy different from *reject*.
- *ias*
  The device authenticates the end devices logging in via 802.1X with the integrated authentication server (IAS). The integrated authentication server manages the login data in a separate database. See the *Network Security > 802.1X Port Authentication > Integrated Authentication Server* dialog.
  You can only assign this value to the authentication list `defaultDot1x8021AuthList`.
- *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 16.

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

[ Device Security > 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

[ Device Security > 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

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.
- Import from an FTP server
  When the certificate is on a FTP server, specify the URL for the file in the following form:
  `ftp://<user>:<password>@<IP address>:<port>/<path>/<file name>`
- Import from a TFTP server
  When the certificate is on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Import from an SCP or SFTP server
  When the certificate is on an SCP or SFTP server, specify the URL for the file in the following form:
  - `scp://` or `sftp://<IP address>/<path>/<file name>`
    When you click the *Start* button, the device displays the *Credentials* window. There you enter *User name* and *Password*, to log in to the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

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.
- *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 16.

Flush cache

Removes the cached login data of the successfully logged in users.

## 3.3.2 LDAP Role Mapping

[Device Security > 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 16.

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

[ Device Security > Management Access ]

The menu contains the following dialogs:

- Server
- IP Access Restriction
- Web
- Command Line Interface
- SNMPv1/v2 Community

# 3.4.1 Server

[Device Security > Management Access > 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]
- [Telnet]
- [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.

Telnet server

Displays if the server service is active or inactive, which authorizes access to the device using Telnet. See the *Telnet* 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 16.

## [SNMP]

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.

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.

SNMPover802

Activates/deactivates the access to the device through SNMP over IEEE-802.

Possible values:

- `marked`
  Access is activated.
- `unmarked` (default setting)
  Access is deactivated.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Telnet]

This tab lets you enable/disable the Telnet server in the device and specify its settings.

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

### Operation

Telnet server

Enables/disables the Telnet server.

Possible values:

- *On* (default setting)
  The Telnet server is enabled.
  The access to the device management is possible through the Command Line Interface using an unencrypted Telnet connection.
- *Off*
  The Telnet server is disabled.

**Note:** If the *SSH* server is disabled and you also disable the *Telnet* 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 Telnet requests from clients.

Possible values:

- `1..65535` (default setting: `23`)
  Exception: Port `2222` is reserved for internal functions.

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

Connections

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

Connections (max.)

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

Possible values:

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

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.

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`)

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [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.

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

SSH server

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 the *Telnet* server is disabled and you also 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.

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 *RSA fingerprint* field displays the fingerprint as Base64-coded SHA256 hash.

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.
- Import from an FTP server
  When the key is on an FTP server, specify the URL for the file in the following form:
  `ftp://<user>:<password>@<IP address>:<port>/<file name>`
- Import from a TFTP server
  When the key is on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Import from an SCP or SFTP server
  When the key is on an SCP or SFTP server, specify the URL for the file in the following form:
  - `scp://` or `sftp://<IP address>/<path>/<file name>`
    When you click the *Start* button, the device displays the *Credentials* window. There you enter *User name* and *Password*, to log in to the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

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 16.

## [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

HTTP server

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 16.

## [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

HTTPS server

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.
- Import from an FTP server
  When the certificate is on a FTP server, specify the URL for the file in the following form:
  `ftp://<user>:<password>@<IP address>:<port>/<path>/<file name>`
- Import from a TFTP server
  When the certificate is on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Import from an SCP or SFTP server
  When the certificate is on an SCP or SFTP server, specify the URL for the file in the following form:
  - `scp://` or `sftp://<IP address>/<path>/<file name>`
    When you click the *Start* button, the device displays the *Credentials* window. There you enter *User name* and *Password*, to log in to the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

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 16.

## 3.4.2 IP Access Restriction

[Device Security > Management Access > 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.
    and
  - 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.

Operation

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.

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.

Telnet

Activates/deactivates the Telnet 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 16.

## 3.4.3 Web

[Device Security > Management Access > 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 16.

## 3.4.4 Command Line Interface

[Device Security > Management Access > CLI]

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: `(DRAGON)`

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.

For the *Telnet* server and the *SSH* server, you specify the timeout in the *Device Security > Management Access > Server* dialog.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [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

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

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 16.

# 3.4.5 SNMPv1/v2 Community

[Device Security > Management Access > 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

Community

Displays the authorization for SNMPv1/v2 applications to the device:

- `Write`
  For requests with the community name entered, the application receives read and write authorization for the device.
- `Read`
  For requests with the community name entered, the application receives read authorization for the device.

Name

Specifies the community name for the adjacent authorization.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters
  `private` (default setting for read and write authorizations)
  `public` (default setting for read authorization)

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 3.5 Pre-login Banner

[ Device Security > 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

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

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 16.

# 4 Network Security

The menu contains the following dialogs:

- Network Security Overview
- Port Security
- 802.1X Port Authentication
- RADIUS
- DoS
- DHCP Snooping
- IP Source Guard
- Dynamic ARP Inspection
- ACL

## 4.1 Network Security Overview

[ 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.

ACL

Displays the *ACL* rules in the overview.

You edit *ACL* rules in the *Network Security > ACL* 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 16.

# 4.2 Port Security

[ Network Security > Port Security ]

The device lets you transmit only data packets from desired senders on one port. When this function is enabled, the device checks the VLAN ID and MAC address of the sender before it transmits a data packet. The device discards data packets from other senders and logs this event.

If the *Auto-Disable* function is activated, the device disables the port. This restriction makes MAC Spoofing attacks more difficult. The *Auto-Disable* function enables the relevant port again automatically when the parameters are no longer being exceeded.

In this dialog a *Wizard* window helps you to connect the ports with one or more desired sources. In the device, these addresses are known as *Static entries (x/y)*. To view the specified static addresses, highlight the relevant port and click the button.

To simplify the setup process, the device lets you record the desired senders automatically. The device “learns” the senders by evaluating the received data packets. In the device, these addresses are known as *Dynamic entries*. When a user-defined upper limit has been reached (*Dynamic limit*), the device stops the “learning” on the relevant port and transmits only the data packets of the senders already recorded. When you adapt the upper limit to the number of expected senders, you thus make MAC Flooding attacks more difficult.

**Note:** With the automatic recording of the *Dynamic entries*, the device constantly discards the 1st data packet from unknown senders. Using this 1st data packet, the device checks if the upper limit has been reached. The device records the sender until the upper limit is reached. Afterwards, the device transmits data packets that it receives on the relevant port from this sender.

### Operation

Operation

Enables/disables the *Port Security* function.

Possible values:

- `On`
  The *Port Security* function is enabled.
  The device checks the VLAN ID and the source MAC address before it transmits a data packet. The device transmits a received data packet only if the VLAN ID and the source MAC address of the data packet are allowed on the relevant port. For this setting to take effect, you also activate the checking of the source address on the relevant ports.
- `Off` (default setting)
  The *Port Security* function is disabled.
  The device transmits every received data packet without checking the source address.

### Configuration

Auto-disable

Activates/deactivates the *Auto-Disable* function for *Port Security*.

Possible values:

- `marked`
  The *Auto-Disable* function for *Port Security* is active.
  Also mark the checkbox in the *Auto-disable* column for the relevant ports.
- `unmarked` (default setting)
  The *Auto-Disable* function for *Port Security* is inactive.

### Table

Port

Displays the port number.

Active

Activates/deactivates the checking of the source address on the port.

Possible values:

- `marked`
  The device checks every data packet received on the port and transmits it only if the source address of the data packet is allowed. Also enable the *Port Security* function in the *Operation* frame.
- `unmarked` (default setting)
  The device transmits every data packet received on the port without checking the source address.

**Note:** When you operate the device as an active participant within an *MRP* ring or *HIPER Ring*, we recommend that you unmark the checkbox for the ring ports.

**Note:** When you operate the device as an active participant of a *Ring/Network Coupling* or *RCP*, we recommend that you unmark the checkbox for the relevant coupling ports.

Auto-disable

Activates/deactivates the *Auto-Disable* function for the parameters that the *Port Security* function is monitoring on the port.

Possible values:

- `marked` (default setting)
  The *Auto-Disable* function is active on the port.
  The prerequisite is that you mark the checkbox *Auto-disable* in the *Configuration* frame.
  - If the port registers source MAC addresses that are not allowed or more source MAC addresses than specified in the *Dynamic limit* column, then the device disables the port. The “Link status” LED for the port flashes 3× per period.
  - The *Diagnostics > Ports > Auto-Disable* dialog displays which ports are currently disabled due to the parameters being exceeded.
  - The *Auto-Disable* function reactivates the port automatically. For this you go to the *Diagnostics > Ports > Auto-Disable* dialog and specify a waiting period for the relevant port in the *Reset timer [s]* column.
- `unmarked`
  The *Auto-Disable* function on the port is inactive.

Send trap

Activates/deactivates the sending of SNMP traps when the device discards a data packet from an undesired sender on the port.

Possible values:

- `marked`
  The sending of SNMP traps is active.
  If the device discards data packets from a sender that is not allowed on the port, 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.

Trap interval [s]

Specifies the delay time in seconds that the device waits after sending an SNMP trap before sending the next SNMP trap.

Possible values:

- `0..3600` (default setting: `0`)

The value `0` deactivates the delay time.

Dynamic limit

Specifies the upper limit for the number of automatically registered sources (*Dynamic entries*). When the upper limit is reached, the device stops “learning” on this port.

Adjust the value to the number of expected sources.

If the port registers more senders than specified here, then the port disables the *Auto-Disable* function. The prerequisite is that you mark the checkbox in the *Auto-disable* column and the *Auto-disable* checkbox in the *Configuration* frame.

Possible values:

- `0`
  Deactivates the automatic registering of sources on this port.
- `1..600` (default setting: `600`)

Static limit

Specifies the upper limit for the number of sources connected to the port (*Static entries (x/y)*). The *Wizard* window, *MAC addresses* dialog, helps you to connect the port with one or more desired sources.

Possible values:

- `0..64` (default setting: `64`)

The value `0` helps prevent you from connecting a source with the port.

Dynamic entries

Displays the number of senders that the device has automatically determined.

See the *Wizard* window, *MAC addresses* dialog, *Dynamic entries* field.

Static MAC entries

Displays the number of senders that are linked with the port.

See the *Wizard* window, *MAC addresses* dialog, *Static entries (x/y)* field.

Last violating VLAN ID/MAC

Displays the VLAN ID and MAC address of an undesired sender whose data packets the device last discarded on this port.

Sent traps

Displays the number of discarded data packets on this port that caused the device to send an SNMP trap.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Port security (Wizard)]

The *Wizard* window helps you to connect the ports with one or more desired sources. After you specify the settings, click the *Finish* button.

**Note:** The device saves the sources connected with the port until you deactivate the checking of the source on the relevant port or in the *Operation* frame.

After closing the *Wizard* window, click the button to save your settings.

## [Port security (Wizard) – Select port]

Port

Specifies the port that you assign to the sender in the next step.

## [Port security (Wizard) – MAC addresses]

VLAN ID

Specifies the VLAN ID of the desired source.

Possible values:

- `1..4042`

To transfer the VLAN ID and the MAC address to the *Static entries (x/y)* field, click the *Add* button.

MAC address

Specifies the MAC address of the desired source.

Possible values:

- Valid Unicast MAC address
  Specify the value with a colon separator, for example `00:11:22:33:44:55`.

To transfer the VLAN ID and the MAC address to the *Static entries (x/y)* field, click the *Add* button.

Add

Transfers the values specified in the *VLAN ID* and *MAC address* fields to the *Static entries (x/y)* field.

Static entries (x/y)

Displays the VLAN ID and MAC address of desired senders connected to the port.

The device uses this field to display the number of senders connected to the port and the upper limit. You specify the upper limit for the number of entries in the table, *Static limit* field.

**Note:** You cannot assign a MAC address that you assign to this port to any other port.

Remove

Removes the entries highlighted in the *Static entries (x/y)* field.

Moves the entries highlighted in the *Dynamic entries* field to the *Static entries (x/y)* field.

Moves every entry from the *Dynamic entries* field to the *Static entries (x/y)* field.

When the *Dynamic entries* field contains more entries than are allowed in the *Static entries (x/y)* field, the device moves the foremost entries until the upper limit is reached.

Dynamic entries

Displays in ascending order the VLAN ID and MAC address of the senders automatically recorded on this port. The device transmits data packets from these senders when receiving the data packets on this port.

The prerequisites for the device to display MAC addresses are:

- The *Port Security* function is enabled. See the *Operation* frame.
- The device checks every data packet received on the port. The checkbox in the *Active* column is marked.

You specify the upper limit for the number of entries in the table, *Dynamic limit* field.

The and buttons allow you to transfer entries from this field into the *Static entries (x/y)* field. In this way, you connect the relevant senders with the port.

## 4.3 802.1X Port Authentication

[ Network Security > 802.1X Port Authentication ]

With the port-based access control according to IEEE 802.1X, the device monitors the access to the network from connected end devices. The device (authenticator) lets an end device (supplicant) have access to the network if it logs in with valid login data. The authenticator and the end devices communicate via the EAPoL (Extensible Authentication Protocol over LANs) authentication protocol.

The device supports the following methods to authenticate end devices:

- `radius`
  A RADIUS server in the network authenticates the end devices.
- `ias`
  The Integrated Authentication Server (IAS) implemented in the device authenticates the end devices. Compared to RADIUS, the IAS provides only basic functions.

The menu contains the following dialogs:

- 802.1X Global
- 802.1X Port Configuration
- 802.1X Port Clients
- 802.1X EAPOL Port Statistics
- 802.1X Port Authentication History
- 802.1X Integrated Authentication Server

# 4.3.1 802.1X Global

[ Network Security > 802.1X Port Authentication > Global ]

This dialog lets you specify basic settings for the port-based access control.

### Operation

Operation

Enables/disables the *802.1X Port Authentication* function.

Possible values:

- `On`
  The *802.1X Port Authentication* function is enabled.
  The device checks the access to the network from connected end devices.
  The port-based access control is enabled.
- `Off` (default setting)
  The *802.1X Port Authentication* function is disabled.
  The port-based access control is disabled.

### Configuration

VLAN assignment

Activates/deactivates the assigning of the relevant port to a VLAN. This function lets you provide selected services to the connected end device in this VLAN.

Possible values:

- `marked`
  The assigning is active.
  If the end device successfully authenticates itself, then the device assigns to the relevant port the VLAN ID transferred by the RADIUS authentication server.
- `unmarked` (default setting)
  The assigning is inactive.
  The relevant port is assigned to the VLAN specified in the *Network Security > 802.1X Port Authentication > Port Configuration* dialog, *Assigned VLAN ID* row.

Dynamic VLAN creation

Activates/deactivates the automatic creation of the VLAN assigned by the RADIUS authentication server if the VLAN does not exist.

Possible values:

- `marked`
  The automatic VLAN creation is active.
  The device creates the VLAN if it does not exist.
- `unmarked` (default setting)
  The automatic VLAN creation is inactive.
  If the assigned VLAN does not exist, then the port remains assigned to the original VLAN.

Monitor mode

Activates/deactivates the monitor mode.

Possible values:

- `marked`
  The monitor mode is active.
  The device monitors the authentication and helps with diagnosing detected errors. If an end device has not logged in successfully, then the device gives the end device access to the network.
- `unmarked` (default setting)
  The monitor mode is inactive.

### MAC authentication bypass format options

Group size

Specifies the size of the MAC address groups. The device splits the MAC address for authentication into groups. The size of the groups is specified in half bytes, each of which is represented as one character.

Possible values:

- *1*
  The device splits the MAC address into 12 groups of one character.
  Example: `A:A:B:B:C:C:D:D:E:E:F:F`
- *2*
  The device splits the MAC address into 6 groups of 2 characters.
  Example: `AA:BB:CC:DD:EE:FF`
- *4*
  The device splits the MAC address into 3 groups of 4 characters.
  Example: `AABB:CCDD:EEFF`
- *12* (default setting)
  The device formats the MAC address as one group of 12 characters.
  Example: `AABBCCDDEEFF`

Group separator

Specifies the character which separates the groups.

Possible values:

- *-*
  dash
- *:*
  colon
- *.*
  dot

Upper or lower case

Specifies if the device formats the authentication data in lowercase or uppercase letters.

Possible values:

- *lower-case*
- *upper-case*

Password

Specifies the optional password for the clients which use the authentication bypass.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters
  After entering the field displays ***** (asterisk) instead of the password.
- <empty>
  The device uses the user name of the client also as the password.

### Information

Monitor mode clients

Displays to how many end devices the device gave network access even though they did not log in successfully.

The prerequisite is that you activate the *Monitor mode* function. See the *Configuration* frame.

Non monitor mode clients

Displays the number of end devices to which the device gave network access after successful login.

Policy 1

Displays the method that the device currently uses to authenticate the end devices using IEEE 802.1X.

You specify the method used in the *Device Security > Authentication List* dialog.

- ☐ To authenticate the end devices through a RADIUS server, you assign the `radius` policy to the `8021x` list.
- ☐ To authenticate the end devices through the Integrated Authentication Server (IAS) you assign the `ias` policy to the `8021x` list.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 4.3.2 802.1X Port Configuration

[ Network Security > 802.1X Port Authentication > Port Configuration ]

This dialog lets you specify the access settings for every port.

When multiple end devices are connected to a port, the device lets you authenticate these individually (multi-client authentication). In this case, the device lets logged in end devices have access to the network. In contrast, the device blocks access for unauthenticated end devices, or for end devices whose authentication has elapsed.

### Table

Port

Displays the port number.

Port initialization

Activates/deactivates the port initialization in order to activate the access control on the port or reset it to its initial state. Use this function only on ports in which the *Port control* column contains the value `auto` or `multiClient`.

Possible values:

- `marked`
  The port initialization is active.
  When the initialization is complete, the device changes the value to `unmarked` again.
- `unmarked` (default setting)
  The port initialization is inactive.
  The device keeps the current port status.

Port reauthentication

Activates/deactivates the one-time reauthentication request.

Use this function only on ports in which the *Port control* column contains the value `auto` or `multiClient`.

The device also lets you periodically request the end device to log in again. See the *Periodic reauthentication* column.

Possible values:

- `marked`
  The one-time reauthentication request is active.
  The device requests the end device to log in again. Afterwards, the device changes the value to `unmarked` again.
- `unmarked` (default setting)
  The one-time reauthentication request is inactive.
  The device keeps the end device logged in.

Authentication activity

Displays the current status of the Authenticator (`Authenticator PAE state`).

Possible values:

- *initialize*
- *disconnected*
- *connecting*
- *authenticating*
- *authenticated*
- *aborting*
- *held*
- *forceAuth*
- *forceUnauth*

Backend authentication state

Displays the current status of the connection to the authentication server (`Backend Authentication state`).

Possible values:

- *request*
- *response*
- *success*
- *fail*
- *timeout*
- *idle*
- *initialize*

Authentication state

Displays the current status of the authentication on the port (`Controlled Port Status`).

Possible values:

- *authorized*
  The end device is logged in successfully.
- *unauthorized*
  The end device is not logged in.

Users (max.)

Specifies the upper limit for the number of end devices that the device authenticates on this port at the same time. This upper limit applies only to ports in which the *Port control* column contains the value `multiClient`.

Possible values:

- `1..16` (default setting: `16`)

Port control

Specifies how the device grants access to the network (`Port control mode`).

Possible values:

- *`forceUnauthorized`*
  The device blocks the access to the network. You use this setting if an end device is connected to the port that does not receive access to the network.
- *`auto`*
  The device grants access to the network if the end device logged in successfully. You use this setting if an end device is connected to the port that logs in at the authenticator.

**Note:** If other end devices are connected through the same port, then they get access to the network without additional authentication.

- *`forceAuthorized`* (default setting)
  When end devices do not support IEEE 802.1X, the device grants access to the network. You use this setting if an end device is connected to the port that receives access to the network without logging in.
- *`multiClient`*
  The device grants access to the network if the end device logs in successfully.
  If the end device does not send any EAPOL data packets, then the device grants or denies access to the network individually depending on the MAC address of the end device. See the *MAC authorized bypass* column.
  You use this setting if multiple end devices are connected to the port or if the *MAC authorized bypass* function is required.

Quiet period [s]

Specifies the time period in seconds in which the authenticator does not accept any more logins from the end device after an unsuccessful login attempt (*Quiet period [s]*).

Possible values:

- `0..65535` (default setting: `60`)

Transmit period [s]

Specifies the period in seconds after which the authenticator requests the end device to log in again. After this waiting period, the device sends an EAP request/identity data packet to the end device.

Possible values:

- `1..65535` (default setting: `30`)

Supplicant timeout period [s]

Specifies the period in seconds for which the authenticator waits for the login of the end device.

Possible values:

- `1..65535` (default setting: `30`)

Server timeout [s]

Specifies the period in seconds for which the authenticator waits for the response from the authentication server (RADIUS or IAS).

Possible values:

- `1..65535` (default setting: `30`)

Requests (max.)

Specifies how many times the authenticator requests the end device to log in until the time specified in the *Supplicant timeout period [s]* column has elapsed. The device sends an EAP request/identity data packet to the end device as often as specified here.

Possible values:

- `0..10` (default setting: `2`)

Assigned VLAN ID

Displays the ID of the VLAN that the authenticator assigned to the port. This value applies only on ports in which the *Port control* column contains the value *auto*.

Possible values:

- `0..4042` (default setting: `0`)

You find the VLAN ID that the authenticator assigned to the ports in the *Network Security > 802.1X Port Authentication > Port Clients* dialog.

For the ports in which the *Port control* column contains the value *multiClient*, the device assigns the VLAN tag based on the MAC address of the end device when receiving data packets without a VLAN tag.

Assignment reason

Displays the cause for the assignment of the VLAN ID. This value applies only on ports in which the *Port control* column contains the value `auto`.

Possible values:

- `notAssigned` (default setting)
- `radius`
- `guestVlan`
- `unauthenticatedVlan`

You find the VLAN ID that the authenticator assigned to the ports for a supplicant in the *Network Security > 802.1X Port Authentication > Port Clients* dialog.

Reauthentication period [s]

Specifies the period in seconds after which the authenticator periodically requests the end device to log in again.

Possible values:

- `1..65535` (default setting: `3600`)

Periodic reauthentication

Activates/deactivates periodic reauthentication requests.

Possible values:

- `marked`
  The periodic reauthentication requests are active.
  The device periodically requests the end device to log in again. You specify this time period in the *Reauthentication period [s]* column.
  If the authenticator assigned the ID of a Voice VLAN, Unauthenticated VLAN or Guest VLAN to the end device, then this setting becomes ineffective.
- `unmarked` (default setting)
  The periodic reauthentication requests are inactive.
  The device keeps the end device logged in.

Guest VLAN ID

Specifies the ID of the VLAN that the authenticator assigns to the port if the end device does not log in during the time period specified in the *Guest VLAN period* column. This value applies only on ports in which the *Port control* column contains the value `auto` or `multiClient`.

This function lets you grant end devices, without IEEE 802.1X support, access to selected services in the network.

Possible values:

- `0` (default setting)
  The authenticator does not assign a Guest VLAN to the port.
  When you enable the MAC-based authentication in the *MAC authorized bypass* column, the device automatically sets the value to `0`.
- `1..4042`

**Note:** The *MAC authorized bypass* function and the *Guest VLAN ID* function cannot be in use simultaneously.

Guest VLAN period

Specifies the period in seconds for which the authenticator waits for EAPOL data packets after the end device is connected. If this period elapses, then the authenticator grants the end device access to the network and assigns the port to the Guest VLAN specified in the *Guest VLAN ID* column.

Possible values:

- `1..300` (default setting: `90`)

Unauthenticated VLAN ID

Specifies the ID of the VLAN that the authenticator assigns to the port if the end device does not log in successfully. This value applies only on ports in which the *Port control* column contains the value `auto`.

This function lets you grant end devices without valid login data access to selected services in the network.

Possible values:

- `0..4042` (default setting: `0`)

The effect of the value `0` is that the authenticator does not assign a Unauthenticated VLAN to the port.

**Note:** Assign to the port a VLAN set up statically in the device.

MAC authorized bypass

Activates/deactivates the MAC-based authentication.

This function lets you authenticate end devices without IEEE 802.1X support on the basis of their MAC address.

Possible values:

- `marked`
  The MAC-based authentication is active.
  The device sends the MAC address of the end device to the RADIUS authentication server. The device assigns the supplicant by its MAC address to the corresponding VLAN as if the authentication was performed through IEEE 802.1X directly.
- `unmarked` (default setting)
  The MAC-based authentication is inactive.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 4.3.3 802.1X Port Clients

[Network Security > 802.1X Port Authentication > Port Clients]

This dialog displays information on the connected end devices.

**Table**

Port

Displays the port number.

User name

Displays the user name with which the end device logged in.

MAC address

Displays the MAC address of the end device.

Filter ID

Displays the name of the filter list that the RADIUS authentication server assigned to the end device after successful authentication.

The authentication server transfers the filter ID attributes in the Access Accept data packet.

Assigned VLAN ID

Displays the VLAN ID that the authenticator assigned to the port after the successful authentication of the end device.

If for the port in the *Network Security > 802.1X Port Authentication > Port Configuration* dialog, *Port control* column the value `multiClient` is specified, then the device assigns the VLAN tag based on the MAC address of the end device when receiving data packets without a VLAN tag.

Assignment reason

Displays the reason for the assignment of the VLAN.

Possible values:

- `default`
- `radius`
- `unauthenticatedVlan`
- `guestVlan`
- `monitorVlan`
- `invalid`

The field only displays a valid value as long as the client is authenticated.

Session timeout

Displays the remaining time in seconds until the login of the end device expires. This value applies only if for the port in the *Network Security > 802.1X Port Authentication > Port Configuration* dialog, *Port control* column the value `auto` or `multiClient` is specified.

The authentication server assigns the timeout period to the device through RADIUS. The value `0` means that the authentication server has not assigned a timeout.

Termination action

Displays the action performed by the device when the login has elapsed.

Possible values:

- `default`
- `reauthenticate`

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 4.3.4 802.1X EAPOL Port Statistics

[ Network Security > 802.1X Port Authentication > Statistics ]

This dialog displays which EAPOL data packets the end device has sent and received for the authentication of the end devices.

**Table**

Port

Displays the port number.

Received packets

Displays the total number of EAPOL data packets that the device received on the port.

Transmitted packets

Displays the total number of EAPOL data packets that the device sent on the port.

Start packets

Displays the number of EAPOL start data packets that the device received on the port.

Logoff packets

Displays the number of EAPOL logoff data packets that the device received on the port.

Response/ID packets

Displays the number of EAP response/identity data packets that the device received on the port.

Response packets

Displays the number of valid EAP response data packets that the device received on the port (without EAP response/identity data packets).

Request/ID packets

Displays the number of EAP request/identity data packets that the device received on the port.

Request packets

Displays the number of valid EAP request data packets that the device received on the port (without EAP request/identity data packets).

Invalid packets

Displays the number of EAPOL data packets with an unknown frame type that the device received on the port.

Received error packets

Displays the number of EAPOL data packets with an invalid packet body length field that the device received on the port.

Packet version

Displays the protocol version number of the EAPOL data packet that the device last received on the port.

Source of last received packet

Displays the sender MAC address of the EAPOL data packet that the device last received on the port.

The value `00:00:00:00:00:00` means that the port has not received any EAPOL data packets yet.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 4.3.5 802.1X Port Authentication History

[Network Security > 802.1X Port Authentication > Port Authentication History]

The device registers the authentication process of the end devices that are connected to its ports. This dialog displays the information recorded during the authentication.

### Table

Port

Displays the port number.

Authentification time stamp

Displays the time at which the authenticator authenticated the end device.

Result age

Displays since when this entry has been entered in the table.

MAC address

Displays the MAC address of the end device.

VLAN ID

Displays the ID of the VLAN that was assigned to the end device before the login.

Authentication status

Displays the status of the authentication on the port.

Possible values:

- *success*
  The authentication was successful.
- *failure*
  The authentication failed.

Access status

Displays if the device grants the end device access to the network.

Possible values:

- *granted*
  The device grants the end device access to the network.
- *denied*
  The device denies the end device access to the network.

Assigned VLAN ID

Displays the ID of the VLAN that the authenticator assigned to the port.

Assignment type

Displays the type of the VLAN that the authenticator assigned to the port.

Possible values:

- *default*
- *radius*
- *unauthenticatedVlan*
- *guestVlan*
- *monitorVlan*
- *notAssigned*

Assignment reason

Displays the reason for the assignment of the VLAN ID and the VLAN type.

### 802.1X Port Authentication History

Port

Simplifies the table and displays only the entries relating to the port selected here. This makes it easier for you to record the table and sort it as you desire.

Possible values:

- `all`
  The table displays the entries for every port.
- `<Port number>`
  The table displays the entries that apply to the port selected here.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 4.3.6 802.1X Integrated Authentication Server

[Network Security > 802.1X Port Authentication > Integrated Authentication Server]

The Integrated Authentication Server (IAS) lets you authenticate end devices using IEEE 802.1X. Compared to RADIUS, the IAS has a very limited range of functions. The authentication is based only on the user name and the password.

In this dialog you manage the login data of the end devices. The device lets you set up to 100 sets of login data.

To authenticate the end devices through the Integrated Authentication Server you assign in the *Device Security > Authentication List* dialog the `ias` policy to the 8021x list.

### Table

User name

Displays the user name of the end device.

To create a new user, click the button.

Password

Specifies the password with which the user authenticates.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters

The device differentiates between upper and lower case.

Active

Activates/deactivates the login data.

Possible values:

- `marked`
  The login data is active. An end device has the option of logging in through IEEE 802.1X using this login data.
- `unmarked` (default setting)
  The login data is inactive.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 4.4 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.
- Accounting
  The accounting server records the traffic data that has occurred during the port authentication according to IEEE 802.1X. This enables you to subsequently determine which services the users have used, and to what extent.

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 device also lets you authenticate end devices with IEEE 802.1X through an authentication server. To do this, you assign the `radius` policy to the `8021x` list in the *Device Security > Authentication List* dialog.

The menu contains the following dialogs:

- RADIUS Global
- RADIUS Authentication Server
- RADIUS Accounting Server
- RADIUS Authentication Statistics
- RADIUS Accounting Statistics

# 4.4.1 RADIUS Global

[ Network Security > 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`)

Accounting

Activates/deactivates the accounting.

Possible values:

- `marked`
  Accounting is active.
  The device sends the traffic data to an accounting server specified in the *Network Security* > RADIUS > *Accounting Server* dialog.
- `unmarked` (default setting)
  Accounting is inactive.

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.

**Note:** The device only includes the attribute 4 if the packet was triggered by the *802.1X* authentication request of an end device (supplicant).

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 16.

Reset

Deletes the statistics in the *Network Security > RADIUS > Authentication Statistics* dialog and in the *Network Security > RADIUS > Accounting Statistics* dialog.

# 4.4.2 RADIUS Authentication Server

[ Network Security > 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

Index

Displays the index number to which the table entry relates.

Name

Displays the name of the server.

To change the value, click the relevant field.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters
  (default setting: `Default-RADIUS-Server`)

Address

Specifies the IP address of the server.

Possible values:

- Valid IPv4 address

Destination UDP port

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.

Secret

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.

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 16.

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.

# 4.4.3 RADIUS Accounting Server

[Network Security > RADIUS > Accounting Server]

This dialog lets you specify up to 8 accounting servers. An accounting server records the traffic data that has occurred during the port authentication according to IEEE 802.1X. The prerequisite is that you activate in the *Network Security > RADIUS > Global* menu the *Accounting* function.

The device sends the traffic data to the first accounting server that can be reached. When the accounting server does not respond, the device contacts the next server in the table.

### Table

Index

Displays the index number to which the table entry relates.

Possible values:

- `1..8`

Name

Displays the name of the server.

To change the value, click the relevant field.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters
  (default setting: `Default-RADIUS-Server`)

Address

Specifies the IP address of the server.

Possible values:

- Valid IPv4 address

Destination UDP port

Specifies the number of the UDP port on which the server receives requests.

Possible values:

- `0..65535` (default setting: `1813`)
  Exception: Port `2222` is reserved for internal functions.

Secret

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..16 characters

You get the password from the administrator of the authentication server.

Active

Activates/deactivates the connection to the server.

Possible values:

- `marked` (default setting)
  The connection is active. The device sends traffic data to this server if the preconditions named above are fulfilled.
- `unmarked`
  The connection is inactive. The device does not send any traffic data to this server.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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.

# 4.4.4 RADIUS Authentication Statistics

[ Network Security > 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 ☰ button and then the *Reset* item.

### Table

Name

Displays the name of the server.

Address

Displays the IP address of the server.

Round trip time

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).

Access requests

Displays the number of access data packets that the device sent to the server. This value does not take repetitions into account.

Retransmitted access-request packets

Displays the number of access data packets that the device retransmitted to the server.

Access accepts

Displays the number of access accept data packets that the device received from the server.

Access rejects

Displays the number of access reject data packets that the device received from the server.

Access challenges

Displays the number of access challenge data packets that the device received from the server.

Malformed access responses

Displays the number of malformed access response data packets that the device received from the server (including data packets with an invalid length).

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 16.

# 4.4.5 RADIUS Accounting Statistics

[ Network Security > RADIUS > Accounting Statistics ]

This dialog displays information about the communication between the device and the accounting 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 ☰ button and then the *Reset* item.

### Table

Name

Displays the name of the server.

Address

Displays the IP address of the server.

Round trip time

Displays the time interval in hundredths of a second between the last response received from the server (Accounting Response) and the corresponding data packet sent (Accounting Request).

Accounting-request packets

Displays the number of accounting request data packets that the device sent to the server. This value does not take repetitions into account.

Retransmitted accounting-request packets

Displays the number of accounting request data packets that the device retransmitted to the server.

Received packets

Displays the number of accounting response data packets that the device received from the server.

Malformed packets

Displays the number of malformed accounting response data packets that the device received from the server (including data packets with an invalid length).

Bad authenticators

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

Pending requests

Displays the number of accounting 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 accounting port.

Packets dropped

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

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 4.5 DoS

[ Network Security > 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

[ Network Security > 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 device detects and discards incoming TCP packets with the following properties:
- No TCP flags are set.
- The TCP sequence number is 0.

Possible values:
- `marked`
  The filter is active.
- `unmarked` (default setting)
  The filter is inactive.

Xmas filter

Activates/deactivates the Xmas filter.

The device detects and discards incoming TCP packets with the following properties:
- The TCP flags *FIN*, *URG* and *PSH* are simultaneously set.
- The TCP sequence number is 0.

Possible values:
- `marked`
  The filter is active.
- `unmarked` (default setting)
  The filter is inactive.

SYN/FIN filter

Activates/deactivates the SYN/FIN filter.

The device 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 detects incoming data packets whose IP payload length in the IP header less the outer IP header size is smaller than the minimum TCP header size. If this is the first fragment that the device detects, then the device 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
- Broadcast pings

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.

Mark the *Filter by packet size* checkbox if you want the device to discard incoming data packets whose payload size exceeds the maximum allowed size for ICMP packets.

Possible values:

- `0..1472` (default setting: `512`)

Drop broadcast ping

Activates/deactivates the filter for Broadcast Pings. Broadcast Pings are a known evidence for Smurf Attacks.

Possible values:

- `marked`
  The filter is active.
  The device detects Broadcast Pings and drops them.
- `unmarked` (default setting)
  The filter is inactive.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 4.6 DHCP Snooping

[ Network Security > DHCP Snooping ]

DHCP Snooping is a function that supports the network security. DHCP Snooping monitors DHCP packets between the DHCP client and the DHCP server and acts like a firewall between the unsecured hosts and the secured DHCP servers.

In this dialog you configure and monitor the following device properties:
- Validate DHCP packets from untrusted sources and filter out invalid packets.
- Limit DHCP data traffic from trusted and untrusted sources.
- Set up and update the DHCP Snooping binding database. This database contains the MAC address, IP address, VLAN and port of DHCP clients at untrusted ports.
- Validate follow-up requests from untrusted hosts on the basis of the DHCP Snooping binding database.

You can activate DHCP Snooping globally and for a specific VLAN. You specify the security status (trusted or untrusted) on individual ports. Verify that the DHCP service can be reached via trusted ports. For DHCP Snooping you typically configure the user/client ports as untrusted and the uplink ports as trusted.

The menu contains the following dialogs:
- DHCP Snooping Global
- DHCP Snooping Configuration
- DHCP Snooping Statistics
- DHCP Snooping Bindings

# 4.6.1 DHCP Snooping Global

[ Network Security > DHCP Snooping > Global ]

This dialog lets you configure the global DHCP Snooping parameters for your device:
- Activate/deactivate *DHCP Snooping* globally.
- Activate/deactivate *Auto-Disable* globally.
- Enable/disable the checking of the source MAC address.
- Configure the name, storage location and storing interval for the binding database.

### Operation

Operation

Enables/disables the DHCP Snooping function globally.

Possible values:
- `On`
- `Off` (default setting)

### Configuration

Verify MAC

Activates/deactivates the source MAC address verification in the Ethernet packet.

Possible values:
- `marked`
  The source MAC address verification is active.
  The device compares the source MAC address with the MAC address of the client in the received DHCP packet.
- `unmarked` (default setting)
  The source MAC address verification is inactive.

Auto-disable

Activates/deactivates the *Auto-Disable* function for *DHCP Snooping*.

Possible values:
- `marked`
  The *Auto-Disable* function for *DHCP Snooping* is active.
  Also mark the checkbox in the *Auto-disable* column on the *Port* tab in the *Network Security > DHCP Snooping > Configuration* dialog for the relevant ports.
- `unmarked` (default setting)
  The *Auto-Disable* function for *DHCP Snooping* is inactive.

### Binding database

Remote file name

Specifies the name of the file in which the device saves the DHCP Snooping binding database.

**Note:**

The device saves only dynamic bindings in the persistent binding database. The device saves static bindings in the configuration profile.

Remote IP address

Specifies the remote IP address under which the device saves the persistent DHCP Snooping binding database. With the value `0.0.0.0` the device saves the binding database locally.

Possible values:

- Valid IPv4 address
- `0.0.0.0` (default setting)
  The device saves the DHCP Snooping binding database locally.

Store interval [s]

Specifies the time delay in seconds after which the device saves the DHCP Snooping binding database when the device identifies a change in the database.

Possible values:

- `15..86400` (default setting: `300`)

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 4.6.2 DHCP Snooping Configuration

[ Network Security > DHCP Snooping > Configuration ]

This dialog lets you configure DHCP Snooping for individual ports and for individual VLANs.

The dialog contains the following tabs:
- [Port]
- [VLAN ID]

### [Port]

In this tab you configure the *DHCP Snooping* function for individual ports.
- Configure a port as trusted/untrusted.
- Activate/deactivate the logging of invalid packets for individual ports.
- Limit the number of DHCP packets.
- Deactivate a port automatically if the DHCP data traffic exceeds the specified limit.

#### Table

Port

Displays the port number.

Trust

Activates/deactivates the security status (trusted, untrusted) of the port.

When this function is active, the port is configured as trusted. Typically, you have connected the trusted port to a DHCP server.

When this function is inactive, the port is configured as untrusted.

Possible values:
- `marked`
  The port is specified as trusted. DHCP Snooping forwards permissible client packets through trusted ports.
- `unmarked` (default setting)
  The port is configured as untrusted. On untrusted ports, the device compares the receiver port with the client port in the binding database.

Log

Activates/deactivates the logging of invalid packets that the device determines on this port.

Possible values:
- `marked`
  The logging of invalid packets is active.
- `unmarked` (default setting)
  The logging of invalid packets is inactive.

Rate limit

Specifies the maximum number of DHCP packets per burst interval for this port. If the number of incoming DHCP packets is currently exceeding the specified limit in a burst interval, then the device discards the additional incoming DHCP packets.

Possible values:

- `-1` (default setting)
  Deactivates the limitation of the number of DHCP packets per burst interval on this port.
- `0..150`packets per interval
  Limits the maximum number of DHCP packets per burst interval on this port.

You specify the burst interval in the *Burst interval* column.

If you activate the auto-disable function, then the device also disables the port. You find the auto-disable function in the *Auto-disable* column.

Burst interval

Specifies the length of the burst interval in seconds on this port. The burst interval is relevant for the rate limiting function.

You specify the maximum number of DHCP packets per burst interval in the *Rate limit* column.

Possible values:

- `1..15` (default setting: `1`)

Auto-disable

Activates/deactivates the *Auto-Disable* function for the parameters that the *DHCP Snooping* function is monitoring on the port.

Possible values:

- `marked` (default setting)
  The *Auto-Disable* function is active on the port.
  The prerequisite is that in the *Network Security > DHCP Snooping > Global* dialog the *Auto-disable* checkbox in the *Configuration* frame is marked.
  - If the port receives more DHCP packets than specified in the *Rate limit* field in the time specified in the *Burst interval* column, then the device disables the port. The “Link status” LED for the port flashes 3× per period.
  - The *Diagnostics > Ports > Auto-Disable* dialog displays which ports are currently disabled due to the parameters being exceeded.
  - The *Auto-Disable* function reactivates the port automatically. For this you go to the *Diagnostics > Ports > Auto-Disable* dialog and specify a waiting period for the relevant port in the *Reset timer [s]* column.
- `unmarked`
  The *Auto-Disable* function on the port is inactive.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [VLAN ID]

In this tab you configure the *DHCP Snooping* function for individual VLANs.

### Table

VLAN ID

Displays the VLAN ID to which the table entry relates.

Active

Activates/deactivates the *DHCP Snooping* function in this VLAN.

The *DHCP Snooping* function forwards valid DHCP client messages to the trusted ports in VLANs without the *Routing* function.

Possible values:

- `marked`
  The *DHCP Snooping* function is active in this VLAN.
- `unmarked` (default setting)
  The *DHCP Snooping* function is inactive in this VLAN.
  The device forwards DHCP packets according to the switching settings without monitoring the packets. The binding database remains unchanged.

**Note:** To enable DHCP Snooping for a port, enable the *DHCP Snooping* function globally in the *Network Security > DHCP Snooping > Global* dialog. Verify that you assigned the port to a VLAN in which DHCP Snooping is enabled.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 4.6.3 DHCP Snooping Statistics

[ Network Security > DHCP Snooping > Statistics ]

With DHCP Snooping, the device logs detected errors and generates statistics. In this dialog you monitor the DHCP Snooping statistics for each port.

The device logs the following:
- Errors detected when validating the MAC address of the DHCP client
- DHCP client messages with a detected incorrect port
- DHCP server messages to untrusted ports

### Table

Port

Displays the port number.

MAC verify failures

Displays the number of discrepancies between the MAC address of the DHCP client in the ‘chaddr’ field of the DHCP data packet and the source address in the Ethernet packet.

Invalid client messages

Displays the number of incoming DHCP client messages received on the port for which the device expects the client on another port according to the DHCP Snooping binding database.

Invalid server messages

Displays the number of DHCP server messages the device received on the untrusted port.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset

Resets the entire table.

# 4.6.4 DHCP Snooping Bindings

[ Network Security > DHCP Snooping > Bindings ]

DHCP Snooping uses DHCP messages to set up and update the binding database.

- Static bindings
  The device lets you enter up to 2048 static DHCP Snooping bindings in the database.
- Dynamic bindings
  The dynamic binding database contains data for clients only on untrusted ports.

This menu lets you specify the settings for static and dynamic bindings.

- Set up new static bindings and set them to active/inactive.
- Display, activate/deactivate or delete static bindings that have been set up.

## Table

MAC address

Specifies the MAC address in the table entry that you bind to a *IP address* and *VLAN ID*.

Possible values:

- Valid Unicast MAC address
  Specify the value with a colon separator, for example `00:11:22:33:44:55`.

IP address

Specifies the IP address for the static DHCP Snooping binding.

Possible values:

- Valid Unicast IPv4 address smaller than `224.x.x.x` and outside the range `127.0.0.0/8` (default setting: `0.0.0.0`)

VLAN ID

Specifies the ID of the VLAN to which the table entry applies.

Possible values:

- `<ID of the VLANs that are set up>`

Port

Specifies the port for the static DHCP Snooping binding.

Possible values:

- Available ports

Remaining binding time

Displays the remaining time for the dynamic DHCP Snooping binding.

Active

Activates/deactivates the specified static DHCP Snooping binding.

Possible values:

- `marked`
  The static DHCP Snooping binding is active.
- `unmarked` (default setting)
  The static DHCP Snooping binding is inactive.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 16.

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

In the *MAC address* field, you specify the MAC address which you bind to an IP address and a VLAN ID.

Removes the highlighted table entry.

The prerequisite is that the checkbox in the *Active* column is unmarked.

Also, the device removes the dynamic bindings of this port created with the *IP Source Guard* function.

## 4.7 IP Source Guard

[Network Security > IP Source Guard]

*IP Source Guard* (IPSG) is a function that supports the network security. The function filters IP data packets based on the source ID (source IP address or source MAC address) of the subscriber. IPSG supports you in protecting the network against attacks through IP/MAC address spoofing.

**IPSG and DHCP Snooping**
IP Source Guard operates in combination with the port *DHCP Snooping* function.

*DHCP Snooping* discards IP data packets on untrusted ports, except DHCP messages. When the device receives DHCP responses and the DHCP Snooping binding database is set up, the device creates a VLAN Access Control List (VACL) for each port containing the source IDs of the subscribers.

You configure the parameters of the *DHCP Snooping* function for individual ports and individual VLANs in the *Network Security > DHCP Snooping > Configuration* dialog.

**IPSG and port security**

*IP Source Guard* cooperates with the *Port Security* function. See the *Network Security > Port Security* dialog. Upon request, IPSG informs the *Port Security* function on request if a MAC address belongs to a valid binding.

- If you deactivated IPSG on the ingress port, then IPSG identifies the data packet as valid.
- If you activated IPSG on the ingress port, then IPSG checks the MAC address using the bindings database. If the MAC address is entered in the bindings database, then IPSG identifies the data packet as valid, or otherwise invalid.

The *Port Security* function takes over the subsequent processing of invalid data packets. You specify the settings of the *Port Security* function in the *Network Security > Port Security* dialog.

**Note:** In order for the device to check the IP address and the MAC address of the data packets received on the port, enable the *Verify MAC* function.

In order for the device to check the VLAN ID and the MAC address of the source before forwarding the data packet, additionally enable the *Port Security* function. See the *Network Security > Port Security* dialog.

The menu contains the following dialogs:

- IP Source Guard Port
- IP Source Guard Bindings

# 4.7.1 IP Source Guard Port

[Network Security > IP Source Guard > Port]

This dialog lets you display and configure the following device properties for each port:
- Include/exclude source MAC addresses for the filtering.
- Activate/deactivate the *IP Source Guard* function.

### Table

Port

Displays the port number.

Verify MAC

Activates/deactivates the filtering based on the source MAC address if the *IP Source Guard* function is active. The device executes this filtering in addition to the filtering based on the source IP address.

Possible values:

- `marked`
  Filtering based on the source MAC address is active.
  To activate the function, mark the *Active* checkbox.
- `unmarked` (default setting)
  Filtering based on the source MAC address is inactive.
  To deactivate the function, also unmark the *Active* checkbox.

Active

Activates/deactivates the *IP Source Guard* function on the port.

Possible values:

- `marked`
  The *IP Source Guard* function is active.
  You also enable the *DHCP Snooping* function in the *Network Security > DHCP Snooping > Global* dialog.
- `unmarked` (default setting)
  The *IP Source Guard* function is inactive.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 4.7.2 IP Source Guard Bindings

[ Network Security > IP Source Guard > Bindings ]

This dialog displays static and dynamic IP Source Guard bindings.

- The device learns dynamic bindings through DHCP Snooping. See the *Network Security > DHCP Snooping > Configuration* dialog.
- Static bindings are IP Source Guard bindings manually set up by the user. The dialog lets you edit static bindings.

### Table

MAC address

Displays the MAC address of the binding.

IP address

Displays the IP address of the binding.

VLAN ID

Displays the VLAN ID of the binding.

Port

Displays the number of the port of the binding.

Hardware status

Displays the hardware status of the binding.

The device applies the binding to the hardware only if the settings are correct. Before the device applies the static IPSG binding to the hardware, it checks the following prerequisites:

- The *Active* checkbox is marked.
- The *IP Source Guard* function on the port is active, in the *Network Security > IP Source Guard > Port* dialog the *Active* checkbox is marked.

Possible values:

- `marked`
  The binding is active, the device applies the binding to the hardware.
- `unmarked`
  The binding is inactive.

Active

Activates/deactivates the specified static IPSG binding between the specified MAC address and the specified IP address, for the specified VLAN on the specified port.

Possible values:

- `marked`
  The static IPSG binding is active.
- `unmarked` (default setting)
  The static IPSG binding is inactive.

**Note:** To make the static binding effective, activate the *IP Source Guard* function on the corresponding port. In the *Network Security > IP Source Guard > Port* dialog, mark the *Active* checkbox.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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

- In the *MAC address* field, you specify the MAC address for the static binding.
- In the *IP address* field, you specify the IP address for the static binding.
- In the *VLAN ID* field, you specify the VLAN ID.
- In the *Port* field, you specify the ID of the VLAN.

Removes the highlighted table entry.

The prerequisite is that the checkbox in the *Active* column is unmarked.

## 4.8 Dynamic ARP Inspection

[ Network Security > Dynamic ARP Inspection ]

*Dynamic ARP Inspection* is a function that supports the network security. This function analyzes ARP packets, logs them, and discards invalid and hostile ARP packets.

The *Dynamic ARP Inspection* function helps prevent a range of man-in-the-middle attacks. With this kind of attack, a hostile station listens in on the data traffic from other subscribers by encroaching on the ARP cache of its unsuspecting neighbors. The hostile station sends ARP requests and ARP responses and enters the IP address of another subscriber for its own MAC address in the IP-to-MAC address relationship (binding).

Using the following measures, the *Dynamic ARP Inspection* function helps ensure that the device only forwards valid ARP requests and ARP responses.

- Listening in on ARP requests and ARP responses on untrusted ports.
- Verifying that the determined packets have a valid IP to MAC address relationship (binding) before the device updates the local ARP cache and before the device forwards the packets to the related destination address.
- Discarding invalid ARP packets.

The device lets you specify up to 100 active ARP ACLs (access lists). You can activate up to 20 rules for each ARP ACL.

The menu contains the following dialogs:

- Dynamic ARP Inspection Global
- Dynamic ARP Inspection Configuration
- Dynamic ARP Inspection ARP Rules
- Dynamic ARP Inspection Statistics

# 4.8.1 Dynamic ARP Inspection Global

[ Network Security > Dynamic ARP Inspection > Global ]

## Configuration

Verify source MAC

Activates/deactivates the source MAC address verification. The device executes the check in both ARP requests and ARP responses.

Possible values:

- `marked`
  The source MAC address verification is active.
  The device checks the source MAC address of the received ARP packets.
  - The device transmits ARP packets with a valid source MAC address to the related destination address and updates the local ARP cache.
  - The device discards ARP packets with an invalid source MAC address.
- `unmarked` (default setting)
  The source MAC address verification is inactive.

Verify destination MAC

Activates/deactivates the destination MAC address verification. The device executes the check in ARP responses.

Possible values:

- `marked`
  The destination MAC address verification is active.
  The device checks the destination MAC address of the incoming ARP packets.
  - The device transmits ARP packets with a valid destination MAC address to the related destination address and updates the local ARP cache.
  - The device discards ARP packets with an invalid destination MAC address.
- `unmarked` (default setting)
  The checking of the destination MAC address of the incoming ARP packets is inactive.

Verify IP address

Activates/deactivates the IP address verification.

In ARP requests, the device checks the source IP address. In ARP responses, the device checks the destination and source IP address.

The device designates the following IP addresses as invalid:

- `0.0.0.0`
- Broadcast addresses `255.255.255.255`
- Multicast addresses `224.0.0.0/4` (Class D)
- Class E addresses `240.0.0.0/4` (reserved for subsequent purposes)
- Loopback addresses in the range `127.0.0.0/8`.

Possible values:

- `marked`
  The IP address verification is active.
  The device checks the IP address of the incoming ARP packets. The device transmits ARP packets with a valid IP address to the related destination address and updates the local ARP cache. The device discards ARP packets with an invalid IP address.
- `unmarked` (default setting)
  The IP address verification is inactive.

Auto-disable

Activates/deactivates the *Auto-Disable* function for *Dynamic ARP Inspection*.

Possible values:

- `marked`
  The *Auto-Disable* function for *Dynamic ARP Inspection* is active.
  Also mark the checkbox in the *Port* column on the *Auto-disable* tab in the *Network Security* > Dynamic ARP Inspection > *Configuration* dialog for the relevant ports.
- `unmarked` (default setting)
  The *Auto-Disable* function for *Dynamic ARP Inspection* is inactive.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 4.8.2 Dynamic ARP Inspection Configuration

[Network Security > Dynamic ARP Inspection > Configuration]

The dialog contains the following tabs:

- [Port]
- [VLAN ID]

## [Port]

### Table

Port

Displays the port number.

Trust

Activates/deactivates the monitoring of ARP packets on untrusted ports.

Possible values:

- `marked`
  Monitoring is active.
  The device monitors ARP packets on untrusted ports.
  The device immediately forwards ARP packets on trusted ports.
- `unmarked` (default setting)
  Monitoring is inactive.

Rate limit

Specifies the maximum number of ARP packets per interval on this port. If the rate of incoming ARP packets is currently exceeding the specified limit in a burst interval, then the device discards the additional incoming ARP packets. You specify the burst interval in the *Burst interval* column.

Optionally, the device also deactivates the port if you activate the auto-disable function. You enable/disable the *Auto-Disable* function in the *Auto-disable* column.

Possible values:

- `-1` (default setting)
  Deactivates the limitation of the number of ARP packets per burst interval on this port.
- `0..300`packets per interval
  Limits the maximum number of ARP packets per burst interval on this port.

Burst interval

Specifies the length of the burst interval in seconds on this port. The burst interval is relevant for the rate limiting function.

You specify the maximum number of ARP packets per burst interval in the *Rate limit* column.

Possible values:

- `1..15` (default setting: `1`)

Auto-disable

Activates/deactivates the *Auto-Disable* function for the parameters that the *Dynamic ARP Inspection* function is monitoring on the port.

Possible values:

- `marked` (default setting)
  The *Auto-Disable* function is active on the port.
  The prerequisite is that in the *Network Security > Dynamic ARP Inspection > Global* dialog the *Auto-disable* checkbox in the *Configuration* frame is marked.
  - If the port receives more ARP packets than specified in the *Rate limit* field in the time specified in the *Burst interval* column, then the device disables the port. The “Link status” LED for the port flashes 3× per period.
  - The *Diagnostics > Ports > Auto-Disable* dialog displays which ports are currently disabled due to the parameters being exceeded.
  - The *Auto-Disable* function reactivates the port automatically. For this you go to the *Diagnostics > Ports > Auto-Disable* dialog and specify a waiting period for the relevant port in the *Reset timer [s]* column.
- `unmarked`
  The *Auto-Disable* function on the port is inactive.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [VLAN ID]

### Table

VLAN ID

Displays the VLAN ID to which the table entry relates.

Log

Activates/deactivates the logging of invalid ARP packets that the device determines in this VLAN. If the device detects an error when checking the IP, source MAC or destination MAC address, or when checking the IP-to-MAC address relationship (binding), then the device identifies an ARP packet as invalid.

Possible values:

- `marked`
  The logging of invalid packets is active.
  The device registers invalid ARP packets.
- `unmarked` (default setting)
  The logging of invalid packets is inactive.

Binding check

Activates/deactivates the checking of incoming ARP packets that the device receives on untrusted ports and on VLANs for which the *Dynamic ARP Inspection* function is active. For these ARP packets the device checks the ARP ACL and the DHCP Snooping relationship (bindings).

Possible values:

- `marked` (default setting)
  The binding check of ARP packets is active.
- `unmarked`
  The binding check of ARP packets is inactive.

ACL strict

Activates/deactivates the strict checking of incoming ARP packets based on the ARP ACL rules specified.

Possible values:

- `marked`
  The strict checking is active.
  The device checks the incoming ARP packets based on the ARP ACL rule specified in the *ARP ACL* column.
- `unmarked` (default setting)
  The strict checking is inactive.
  The device checks the incoming ARP packets based on the ARP ACL rule specified in the *ARP ACL* column and subsequently on the entries in the DHCP Snooping database.

ARP ACL

Specifies the ARP ACL that the device uses.

Possible values:

- `<rule name>`
  You create and edit the rules in the *Network Security > Dynamic ARP Inspection > ARP Rules* dialog.

Active

Activates/deactivates the *Dynamic ARP Inspection* function in this VLAN.

Possible values:

- `marked`
  The *Dynamic ARP Inspection* function is active in this VLAN.
- `unmarked` (default setting)
  The *Dynamic ARP Inspection* function is inactive in this VLAN.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 4.8.3 Dynamic ARP Inspection ARP Rules

[Network Security > Dynamic ARP Inspection > ARP Rules]

This dialog lets you specify rules for checking and filtering ARP packets.

### Table

Name

Displays the name of the ARP rule.

Source IP address

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

Possible values:

- Valid IPv4 address
  The device applies the rule to IP data packets with the specified source address.

Source MAC address

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

Possible values:

- Valid MAC address
  The device applies the rule to MAC data packets with the specified source address.

Active

Activates/deactivates the *ARP* 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 16.

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

- In the *Name* field, you specify the name of the ARP rule.
- In the *Source IP address* field, you specify the source IP address of the ARP rule.
- In the *Source MAC address* field, you specify the source MAC address of the ARP rule.

## 4.8.4 Dynamic ARP Inspection Statistics

[Network Security > Dynamic ARP Inspection > Statistics]

This window displays the number of discarded and forwarded ARP packets in an overview.

### Table

VLAN ID

Displays the VLAN ID to which the table entry relates.

Packets forwarded

Displays the number of ARP packets that the device forwards after checking them using the *Dynamic ARP Inspection* function.

Packets dropped

Displays the number of ARP packets that the device discards after checking them using the *Dynamic ARP Inspection* function.

DHCP drops

Displays the number of ARP packets that the device discards after checking the DHCP Snooping relationship (binding).

DHCP permits

Displays the number of ARP packets that the device forwards after checking the DHCP Snooping relationship (binding).

ACL drops

Displays the number of ARP packets that the device discards after checking them using the ARP ACL rules.

ACL permits

Displays the number of ARP packets that the device forwards after checking them using the ARP ACL rules.

Bad source MAC

Displays the number of ARP packets that the device discards after the *Dynamic ARP Inspection* function detected an error in the source MAC address.

Bad destination MAC

Displays the number of ARP packets that the device discards after the *Dynamic ARP Inspection* function detected an error in the destination MAC address.

Invalid IP address

Displays the number of ARP packets that the device discards after the *Dynamic ARP Inspection* function detected an error in the IP address.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset

Resets the entire table.

## 4.9 ACL

[ Network Security > ACL ]

In this menu, you specify the settings for the Access Control Lists (ACL). Access Control Lists contain rules which the device applies successively to the data stream on its ports or VLANs.

If a data packet complies with the criteria of one or more rules, then the device applies the action specified in the first rule that applies to the data stream. The device ignores the rules following. Possible actions include:

- *permit*: The device transmits the data packet to a port or to a VLAN.
  When necessary, the device transmits a copy of the data packets to a further port.
- *deny*: The device drops the data packet.

In the default setting, the device forwards every data packet. Once you assign an Access Control List to an interface or VLAN, there is changing this behavior. The device enters at the end of an Access Control List an implicit Deny-All rule. Consequently, the device discards data packets that do not meet any of the rules. If you want a different behavior, then add a "permit" rule at the end of your Access Control Lists.

Proceed as follows to set up Access Control Lists and rules:

- ☐ Make a time profile if necessary. See the *Network Security > ACL > Time Profile* dialog. The device applies Access Control Lists with a time profile at specified times instead of permanently.
- ☐ Make a rule and specify the rule settings. See the *Network Security > ACL > IPv4 Rule* dialog, or the *Network Security > ACL > MAC Rule* dialog.
- ☐ Assign the Access Control List to the Ports and VLANs of the device. See the *Network Security > ACL > Assignment* dialog.

The menu contains the following dialogs:

- ACL IPv4 Rule
- ACL MAC Rule
- ACL Assignment
- ACL Time Profile

# 4.9.1 ACL IPv4 Rule

[ Network Security > ACL > IPv4 Rule ]

In this dialog you specify the rules that the device applies to the IP data packets.

An Access Control List (group) contains one or more rules. The device applies the rules of an Access Control List successively, beginning with the rule with the lowest value in the *Index* column.

The device lets you filter according to the following criteria:
- Source or destination IP address of a data packet
- Type of the transmitting protocol
- Source or destination port of a data packet
- Classification according to DSCP
- Classification according to ToS

### Table

Group name

Displays the name of the Access Control List. The Access Control List contains the rules.

Index

Displays the number of the rule within the Access Control List.

If the Access Control List contains multiple rules, then the device processes the rule with the lowest value first.

Match every packet

Specifies to which IP data packets the device applies the rule.

Possible values:

- `marked` (default setting)
  The device applies the rule to every IP data packet.
- `unmarked`
  The device applies the rule to IP data packets depending on the value in the following fields:
  - *Source IP address*, *Destination IP address*, *Protocol*
  - *DSCP*, *TOS priority*, *TOS mask*
  - *ICMP type*, *ICMP code*
  - *IGMP type*
  - *Established*
  - *Packet fragmented*
  - *TCP flag*

Source IP address

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

Possible values:

- `?.?.?.?` (default setting)
  The device applies the rule to IP data packets with any source address.

- Valid IPv4 address
  The device applies the rule to IP data packets with the specified source address.
  You use the `?` character as a wild card.
  Example `192.?.?.32`: The device applies the rule to IP data packets whose source address begins with `192.` and ends with `.32`.
- Valid IPv4 address/bit mask
  The device applies the rule to IP data packets with the specified source address. The inverse bit mask lets you specify the address range with bit-level accuracy.
  Example `192.168.1.0/0.0.0.127`: The device applies the rule to IP data packets with a source address in the range from `192.168.1.0` to `….127`.

Destination IP address

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

Possible values:

- `?.?.?.?` (default setting)
  The device applies the rule to IP data packets with any destination address.
- Valid IPv4 address
  The device applies the rule to data packets with the specified destination address.
  You use the `?` character as a wild card.
  Example `192.?.?.32`: The device applies the rule to IP data packets whose source address begins with `192.` and ends with `.32`.
- Valid IPv4 address/bit mask
  The device applies the rule to data packets with the specified destination address. The inverse bit mask lets you specify the address range with bit-level accuracy.
  Example `192.168.1.0/0.0.0.127`: The device applies the rule to IP data packets with a destination address in the range from `192.168.1.0` to `….127`.

Protocol

Specifies the protocol type of the IP data packets to which the device applies the rule.

Possible values:

- `any` (default setting)
  The device applies the rule to every IP data packet without considering the protocol type.
- `icmp`
- `igmp`
- `ip-in-ip`
- `tcp`
- `udp`
- `ip`

Source TCP/UDP port

Specifies the source port of the IP data packets to which the device applies the rule. The prerequisite is that you specify in the *Protocol* column the value `TCP` or `UDP`.

Possible values:

- `any` (default setting)
  The device applies the rule to every IP data packet without considering the source port.
- `1..65535`
  The device applies the rule only to IP data packets containing the specified source port.
  To specify a port range, you can use one of the following operators:
  - `<`
    Range below the specified port number
  - `>`
    Range above the specified port number
  - `!=`
    Entire port range except the specified port
  These operators are allowed only in rules which the device applies to the received data packets.
  See the *Network Security > ACL > Assignment* dialog: *Direction* column = `inbound`.

Destination TCP/UDP port

Specifies the destination port of the IP data packets to which the device applies the rule. The prerequisite is that you specify in the *Protocol* column the value `TCP` or `UDP`.

Possible values:

- `any` (default setting)
  The device applies the rule to every IP data packet without considering the destination port.
- `1..65535`
  The device applies the rule only to IP data packets containing the specified destination port.
  To specify a port range, you can use one of the following operators:
  - `<`
    Range below the specified port number
  - `>`
    Range above the specified port number
  - `!=`
    Entire port range except the specified port
  These operators are allowed only in rules which the device applies to the received data packets.
  See the *Network Security > ACL > Assignment* dialog: *Direction* column = `inbound`.

DSCP

Specifies the Differentiated Service Code Point (DSCP value) in the header of the IP data packets to which the device applies the rule.

Possible values:

- `-` (default setting)
  The device applies the rule to every IP data packet without considering the DSCP value.
- `0..63`
  The device applies the rule only to IP data packets containing the specified DSCP value.

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:

- `any` (default setting)
  The device applies the rule to every IP data packet without considering the ToS value.
- `0..7`
  The device applies the rule only to IP data packets containing the specified ToS value.

TOS mask

Specifies the bit mask for the ToS value in the header of the IP data packets to which the device applies the rule. The prerequisite is that you specify in the *TOS priority* column a ToS value.

Possible values:

- `any` (default setting)
  The device applies the rule to IP data packets and considers the ToS value completely.
- `1..1f`
  The device applies the rule to IP data packets and considers the bits of the ToS value specified in the bit mask.

ICMP type

Specifies the ICMP type in the TCP header of the IP data packets to which the device applies the rule.

Possible values:

- `-1` (default setting)
  ICMP type matching is inactive.
- `0..255`
  The device applies the rule to every IP data packet and considers the specified ICMP type.

ICMP code

Specifies the ICMP code in the TCP header of the IP data packets to which the device applies the rule. The prerequisite is that, in the *ICMP type* field, you specify an ICMP value.

Possible values:

- `-1` (default setting)
  ICMP code matching is inactive.
- `0..255`
  The device applies the rule to every IP data packet and considers the specified ICMP code.

IGMP type

Specifies the IGMP type in the TCP header of the IP data packets to which the device applies the rule.

Possible values:

- `0` (default setting)
  IGMP type matching is inactive.
- `1..255`
  The device applies the rule to every IP data packet and considers the specified IGMP type.

Established

Activates/deactivates applying the ACL rule to TCP data packets which have either the RST bit, or the ACK bit set in the TCP header.

Possible values:

- `marked`
  The device applies the rule to every IP data packet in which the RST bit, or the ACK bit is set in the TCP header.
- `unmarked` (default setting)
  Matching is inactive.

Packet fragmented

Activates/deactivates applying the ACL rule to fragmented packets.

Possible values:

- `marked`
  The device applies the ACL rule to fragmented packets.
- `unmarked` (default setting)
  Matching is inactive.

TCP flag

Specifies the TCP flag and mask value.

The device lets you enter multiple values, by separating the values with a comma.

Specify the flags as either `+` or `-`.

Possible values:

- `-` (default setting)
  TCP flag matching is inactive.
- `-`
  When you use this value in combination with the following flags, the device considers packets in which the flag is not set.
- `+`
  When you use this value in combination with the following flags, the device considers packets in which the flag is set.
- `fin`
  Indicates that the sending device has finished its transmission.
- `syn`
  Indicates that the `Synchronize sequence` numbers are significant. Only the first packet sent from each end device has this flag set.
- `rst`
  Indicates a reset on the link.
- `psh`
  Indicates the push function, in which a device asks to push the buffered data to the receiving application.
- `ack`
  Indicates that the `Acknowledgment` field is significant. Every packet, after the initial syn packet sent by the client, has this flag set.
- `urg`
  Indicates that the `Urgent pointer` field is significant.

Action

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

Possible values:

- `permit` (default setting)
  The device transmits the IP data packets.
- *`deny`*
  The device drops the IP data packets.

Redirection port

Specifies the port on which the device transmits the IP data packets. The prerequisite is that you specify in the *Action* column the value *`permit`*.

Possible values:

- `-` (default setting)
  The *Redirection port* function is disabled.
- `<Port number>`
  The device transmits the IP data packets on the specified port.

The device does not provide the option of mirroring IP data packets across VLAN boundaries or to router interfaces.

Mirror port

Specifies the port on which the device transmits a copy of the IP data packets. The prerequisite is that you specify in the *Action* column the value *`permit`*.

Possible values:

- `-` (default setting)
  The *Mirror port* function is disabled.
- `<Port number>`
  The device transmits a copy of the IP data packets on the specified port.

The device does not provide the option of mirroring IP data packets across VLAN boundaries or to router interfaces.

Assigned queue ID

Specifies the priority queue to which the device assigns the IP data packets.

Possible values:

- `0..7` (default setting: `0`)

Log

Activates/deactivates the logging in the log file. See the *Diagnostics > Report > System Log* dialog.

Possible values:

- `marked`
  Logging is activated.
  The prerequisite is that you assign the Access Control List in the *Network Security > ACL > Assignment* dialog to a VLAN or port.
  The device registers in the log file, in an interval of 30 s, how many times it applied the deny rule to IP data packets.
- `unmarked` (default setting)
  Logging is deactivated.

The device lets you activate this function for up to 128 deny rules.

Time profile

Specifies if the device applies the rule permanently or time-controlled.

Possible values:

- `<empty>` (default setting)
  The device applies the rule permanently.
- `[Time Profile]`
  The device applies the rule only at the times specified in the time profile. You edit the time profile in the *Network Security > ACL > Time Profile* dialog.

Rate limit

Specifies the limit for the data transfer rate for the port specified in the *Redirection port* column. The limit applies to the summary of the data sent and received.

This function limits the data stream on the port or in the VLAN:

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.

Unit

Specifies the measurement unit for the data transfer rate specified in the *Rate limit* column.

Possible values:

- *kbps*
  kByte per second

Burst size

Specifies the limit in KByte for the data volume during temporary bursts.

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. The prerequisite is that you specify in the *Rate limit* column a value >`0`.

Recommendation:

- If the bandwidth is known:
  *Burst size* = bandwidth × allowed duration of a burst / 8.
- If the bandwidth is unknown:
  *Burst size* = 10 × MTU (*Maximum Transmission Unit*) of the port.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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

- In the *Group name* field, you specify the name of the Access Control List to which the rule belongs.
- In the *Index* field, you specify the number of the rule within the Access Control List. If the Access Control List contains multiple rules, then the device processes the rule with the lowest value first.

## 4.9.2 ACL MAC Rule

[ Network Security > ACL > MAC Rule ]

In this dialog you specify the rules that the device applies to the MAC data packets.

An Access Control List (group) contains one or more rules. The device applies the rules of an Access Control List successively, beginning with the rule with the lowest value in the *Index* column.

The device lets you filter according to the following criteria:
- Source or destination MAC address of a data packet
- Type of the transmitting protocol
- Membership of a specific VLAN
- Service class of a data packet

### Table

Group name

Displays the name of the Access Control List. The Access Control List contains the rules.

Index

Displays the number of the rule within the Access Control List.

If the Access Control List contains multiple rules, then the device processes the rule with the lowest value first.

Match every packet

Specifies to which MAC data packets the device applies the rule.

Possible values:

- `marked` (default setting)
  The device applies the rule to every MAC data packet.
  The device ignores the value in the *Source MAC address*, *Destination MAC address*, *Ethertype*, *Ethertype custom value*, *VLAN ID*, and *COS* fields.
- `unmarked`
  The device applies the rule to MAC data packets depending on the value in the *Source MAC address*, *Destination MAC address*, *Ethertype*, *Ethertype custom value*, *VLAN ID*, and *COS* fields.

Source MAC address

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

Possible values:

- `??:??:??:??:??:??` (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.
  You use the `?` character as a wild card.
  Example `00:11:??:??:??:??`: The device applies the rule to MAC data packets whose source address begins with `00:11`.
- Valid MAC address/bit mask
  The device applies the rule to MAC data packets with the specified source address. The bit mask lets you specify the address range with bit-level accuracy.
  Example `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`: The device applies the rule to MAC data packets with a source address in the range from `00:11:22:33:44:54` to `…:57`.

Destination MAC address

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

Possible values:

- `??:??:??:??:??:??` (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.
  You use the `?` character as a wild card.
  Example `00:11:??:??:??:??`: The device applies the rule to MAC data packets whose destination address begins with `00:11`.
- Valid MAC address/bit mask
  The device applies the rule to MAC data packets with the specified source address. The bit mask lets you specify the address range with bit-level accuracy.
  Example `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`: The device applies the rule to MAC data packets with a destination address in the range from `00:11:22:33:44:54` to `…:57`.

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*
- *rarp*
- *pppoe*

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 considering the *Ethertype* value.
- `600..ffff`
  The device applies the rule only to MAC data packets containing the *Ethertype* value specified here.

VLAN ID

Specifies the VLAN ID of the MAC data packets to which the device applies the rule.

Possible values:

- `0` (default setting)
  The device applies the rule to every MAC data packet without considering the VLAN ID.
- `1..4042`

COS

Specifies the Class of Service (COS) value of the MAC data packets to which the device applies the rule.

Possible values:

- `0..7`
- `any` (default setting)
  The device applies the rule to every MAC data packet without considering the Class of Service value.

**Note:** For data packets without a VLAN tag, the device uses the port priority instead of the *COS* value.

Action

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

Possible values:

- *permit* (default setting)
  The device transmits the MAC data packets.
- *deny*
  The device discards the MAC data packets.

Redirection port

Specifies the port on which the device transmits the MAC data packets. The prerequisite is that in the *Action* column the value `permit` is specified.

Possible values:

- `-` (default setting)
  The *Redirection port* function is disabled.
- `<Port number>`
  The device transmits the MAC data packets on the specified port.

The device does not provide the option of mirroring IP data packets across VLAN boundaries or to router interfaces.

Mirror port

Specifies the port on which the device transmits a copy of the MAC data packets. The prerequisite is that in the *Action* column the value `permit` is specified.

Possible values:

- `-` (default setting)
  The *Mirror port* function is disabled.
- `<Port number>`
  The device transmits a copy of the MAC data packets on the specified port.

The device does not provide the option of mirroring IP data packets across VLAN boundaries or to router interfaces.

Assigned queue ID

Specifies the ID of the priority queue on which the device transmits the MAC data packets.

Possible values:

- `0..7` (default setting: `0`)

Log

Activates/deactivates the logging in the log file. See the *Diagnostics > Report > System Log* dialog.

Possible values:

- `marked`
  Logging is activated.
  The prerequisite is that you assign the Access Control List in the *Network Security > ACL > Assignment* dialog to a VLAN or port.
  The device registers in the log file, in an interval of 30 s, how many times it applied the deny rule to MAC data packets.
- `unmarked` (default setting)
  Logging is deactivated.

The device lets you activate this function for up to 128 deny rules.

Time profile

Specifies if the device applies the rule permanently or time-controlled.

Possible values:

- `<empty>` (default setting)
  The device applies the rule permanently.
- `[Time Profile]`
  The device applies the rule only at the times specified in the time profile. You edit the time profile in the *Network Security > ACL > Time Profile* dialog.

Rate limit

Specifies the limit for the data transfer rate for the port specified in the *Redirection port* column. The limit applies to the summary of the data sent and received.

This function limits the data stream on the port or in the VLAN:

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 MAC 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.

Unit

Specifies the unit of measurement for the data transfer rate specified in the *Rate limit* column.

Possible values:

- *kbps*
  kByte per second

Burst size

Specifies the limit in KByte for the data volume during temporary bursts.

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. The prerequisite is that you specify in the *Rate limit* column a value > `0`.

Recommendation:

- If the bandwidth is known:
  *Burst size* = bandwidth × allowed duration of a burst / 8.
- If the bandwidth is unknown:
  *Burst size* = 10 × MTU (*Maximum Transmission Unit*) of the port.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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

- In the *Group name* field, you specify the name of the Access Control List to which the rule belongs.
- In the *Index* field, you specify the number of the rule within the Access Control List. If the Access Control List contains multiple rules, then the device processes the rule with the lowest value first.

## 4.9.3 ACL Assignment

[ Network Security > ACL > Assignment ]

This dialog lets you assign one or more Access Control Lists to the ports and VLANs of the device. By assigning a priority you specify the processing sequence, provided you assign one or more Access Control Lists to a port or VLAN.

The device applies rules successively, namely in the sequence specified by the rule index. You specify the priority of a group in the *Priority* column. The lower the number, the higher the priority. In this process, the device applies the rules with a high priority before the rules with a low priority.

The assignment of Access Control Lists to ports and VLANs results in the following different types of ACL:

- Port-based IPv4-ACLs
- Port-based MAC ACLs
- VLAN-based IPv4 ACLs
- VLAN-based MAC ACLs

The device lets you apply the Access Control Lists to data packets received (`inbound`) or sent (`outbound`).

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

**Note:** You cannot apply IP ACL rules and DiffServ rules together in the same direction on a port.

### Table

Group name

Displays the name of the Access Control List. The Access Control List contains the rules.

Type

Displays if the Access Control List contains MAC rules or IPv4 rules.

Possible values:

- *mac*
  The Access Control List contains MAC rules.
- *ip*
  The Access Control List contains IPv4 rules.

You edit Access Control Lists with IPv4 rules in the *Network Security > ACL > IPv4 Rule* dialog. You edit Access Control Lists with MAC rules in the *Network Security > ACL > MAC Rule* dialog.

Port

Displays the port to which the Access Control List is assigned. The field remains empty when the Access Control List is assigned to a VLAN.

VLAN ID

Displays the VLAN to which the Access Control List is assigned. The field remains empty when the Access Control List is assigned to a port.

Direction

Displays if the device applies the Access Control List to data packets received or sent.

Possible values:

- *inbound*
  The device applies the Access Control List to data packets received on the port or in the VLAN.
- *outbound*
  The device applies the Access Control List to data packets sent on the port or in the VLAN.

Priority

Displays the priority of the Access Control List.

Using the priority, you specify the sequence in which the device applies the Access Control Lists to the data stream. The device applies the rules in ascending order which starts with priority `1`.

Possible values:

- `1..4294967295`

If an Access Control List is assigned to a port and to a VLAN with the same priority, then the device applies the rules to the port first.

Active

Displays if the Access Control List on the port or in the VLAN is active.

Possible values:

- `marked` (default setting)
  The Access Control List is active.
- `unmarked`
  The Access Control List is inactive.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Opens the *Create* dialog to assign a rule to a port or a VLAN.

- In the *Port/VLAN* field, you specify the port or the VLAN ID.
- In the *Priority* field, you specify the source MAC address of the ARP rule.
- In the *Direction* field, you specify the data packets to which the device applies the rule.
- In the *Group name* filed, you specify which rule the device assigns to the port or VLAN.

# 4.9.4 ACL Time Profile

[Network Security > ACL > Time Profile]

This dialog lets you create and edit time profiles. If you assign a time profile to an ACL rule, then the device applies the rule at the times specified in the time profile. If no time profile is assigned, the device applies the rule permanently.

The device lets you create up to 100 time profiles. Each time profile can contain:
- One *Absolute* time period and up to 9 *Periodic* time periods
  or
- Up to 10 *Periodic* time periods

The device applies the ACL rules during the time specified within the time period.
- If you specify the time periods using the *Absolute* option, then the device applies the rule once.
- If you specify the time periods using the *Periodic* option, then the device applies the rule recurrently.

The implied Deny-All rule of the ACLs is permanently valid independently of the time control.

### Table

**Note:** If you reconfigure a time period, then first specify the end time and then the start time. Otherwise, the dialog displays an error message.

Profile name

Displays the name of the time profile. The time profile contains the time periods.

Operational status

Displays whether the status of the time profile is currently *active*/*inactive*.

Index

Displays the number of the time period within the time profile. The device automatically assigns this number.

Absolute

Start date

Specifies the date at which the device starts to apply the one-time rule.

Possible values:
- `YYYY-MM-DD` or `DD.MM.YY`
  (depending on the language preferences of your web browser)

Start time

Specifies the time at which the device starts to apply the one-time rule.

Possible values:

- `hh:mm`
  Hour:Minute

End date

Specifies the date at which the device terminates the one-time rule.

Possible values:

- `YYYY-MM-DD` or `DD.MM.YY`
  (depending on the language preferences of your web browser)

The device also allows you to specify time periods that span several days. Example:

- *Start date*: *Sat*
- *Start time*: `12:00 PM`
- *End date*: *Sun*
- *End time*: `11:00 AM`

End time

Specifies the time at which the device terminates the one-time rule.

Possible values:

- `hh:mm`
  Hour:Minute

Periodic

Starting days

Specifies the days of the week on which the device periodically starts to apply the rule.

The device allows you to specify multiple values in the *Starting days* column, for example a list of the weekdays *Mon*,*Tue*,*Wed*,*Thu*,*Fri*. In this case, verify that the *Starting days* and *Ending days* fields contain identical values. The device then applies the rule every weekday at the times specified in the *Start time* and *End time* fields.

Possible values:

- *Sun*
- *Mon*
- *Tue*
- *Wed*
- *Thu*
- *Fri*
- *Sat*

Start time

Specifies the time at which the device periodically starts to apply the rule.

Possible values:

- `hh:mm`
  Hour:Minute

Ending days

Specifies the days of the week on which the device periodically terminates the rule.

The device allows you to specify multiple values in the *Ending days* column, for example a list of the weekdays *Mon*,*Tue*,*Wed*,*Thu*,*Fri*. In this case, verify that the *Starting days* and *Ending days* fields contain identical values. The device then applies the rule every weekday at the times specified in the *Start time* and *End time* fields.

The device also allows you to specify time periods that span several days. In this case, verify that the *Starting days* and *Ending days* fields each contain a single value. Example: *Starting days*: *Sat*, *Start time*: `12:00 PM`, *Ending days*: *Sun*, *End time*: `11:00 AM`.

Possible values:

- *Sun*
- *Mon*
- *Tue*
- *Wed*
- *Thu*
- *Fri*
- *Sat*

End time

Specifies the time at which the device periodically terminates the rule.

Possible values:

- `hh:mm`
  Hour:Minute

## Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Opens the *Create* dialog to create a new time period.

- In the *Profile name* field, you specify the name of the time profile to which the time period belongs.
- In the *Type* field, you specify the type of time period.
  - With the *Periodic* radio button, you specify a time period at which the device activates the recurring rule.
  - With the *Absolute* radio button, you specify a time period at which the device activates the rule one time. Within every time profile, exactly one such time period is allowed.

- In the *Start* frame, you specify the time at which the device starts to apply the rule.
- In the *End* frame, you specify the time at which the device terminates to apply the rule.

# 5 Switching

The menu contains the following dialogs:

- Switching Global
- Rate Limiter
- Filter for MAC Addresses
- IGMP Snooping
- MRP-IEEE
- GARP
- QoS/Priority
- VLAN
- L2-Redundancy

## 5.1 Switching Global

[ 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
- Enable the VLAN Unaware Mode

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”).

According to standard IEEE 802.1Q, the device forwards data packets with a VLAN tag in a VLAN ≥1. However, a small number of applications on connected end devices send or receive data packets with a VLAN ID=0. When the device receives one of these data packets, before forwarding it the device overwrites the original value in the data packet with the VLAN ID of the receiving port. If you activate the VLAN Unaware Mode, then this deactivates the VLAN settings in the device. The device then transparently forwards the data packets and evaluates the priority information contained only in the data packet.

### 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.

If you are using a redundancy function, then 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.

VLAN unaware mode

Activates/deactivates the VLAN unaware mode.

Possible values:

- `marked`
  The VLAN unaware mode is active.
  The device works in the VLAN Unaware bridging mode (IEEE 802.1Q):
  - The device ignores the VLAN settings in the device and the VLAN tags in the data packets. The device transmits the data packets based on their destination MAC address or destination IP address in VLAN `1`.
  - The device ignores the VLAN settings specified in the *Switching > VLAN > Configuration* and *Switching > VLAN > Port* dialogs. Every port is assigned to VLAN `1`.
  - The device evaluates the priority information contained in the data packet.

**Note:** You specify the VLAN ID `1` for every function in the device which uses VLAN settings. Among other things, this applies to static filters, MRP and IGMP Snooping.

- `unmarked` (default setting)
  The VLAN unaware mode is inactive.
  The device works in the VLAN-aware bridging mode (IEEE 802.1Q):
  - The device evaluates the VLAN tags in the data packets.
  - The device transmits the data packets based on their destination MAC address or destination IP address in the corresponding VLAN.
  - The device evaluates the priority information contained in the data packet.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 5.2 Rate Limiter

[ Switching > 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]
- [Egress]

## [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

Port

Displays the port number.

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 *`percent`* in the *Threshold unit* column, then enter a percentage value from `1` to `100`.
  - If you select the value *`pps`* in the *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:

- `marked`
- `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 *`percent`* in the *Threshold unit* column, 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.

Unknown unicast mode

Activates/deactivates the rate limiter function for received unicast data packets with an unknown destination address.

Possible values:

- `marked`
- `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 16.

## [Egress]

In this tab you specify the egress transmission rate on the port.

### Table

Port

Displays the port number.

Bandwidth [%]

Specifies the egress transmission rate.

Possible values:

- `0` (default setting)
  The bandwidth limitation is disabled.
- `1..100`
  The bandwidth limitation is enabled.
  This value specifies the percentage of overall link speed for the port in 1% increments.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 5.3 Filter for MAC Addresses

[ Switching > 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.
- *IGMP*
  Address filter automatically set up by IGMP Snooping.
- *mgmt*
  MAC address of the device. The address filter is protected against changes.
- *MRP-MMRP*
  Multicast address filter automatically set up by MMRP.
- *GMRP*
  Multicast address filter automatically set up by GMRP.

<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.
- `IGMP learned`
  The port transmits data packets to the destination address. The device created the filter automatically based on IGMP.
- `unicast static`
  The port transmits data packets to the destination address. A user created the filter.
- `multicast static`
  The port transmits data packets to the destination address. A user created the filter.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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

- In the *Address* field, you specify the destination MAC address.
- In the *VLAN ID* field, you specify the ID of the VLAN.
- In the *Port* field, you specify the port.
  - Select one port if the destination MAC address is a unicast address.
  - Select one or more ports if the destination MAC address is a multicast address.
  - Select no port to create a discard filter. The device discards data packets with the destination MAC address specified in the table entry.

Reset MAC address table

Removes the MAC addresses from the forwarding table that have the value `learned` in the *Status* column.

# 5.4 IGMP Snooping

[ Switching > IGMP Snooping ]

The Internet Group Management Protocol (IGMP) is a protocol for dynamically managing Multicast groups. The protocol describes the distribution of Multicast data packets between routers and end devices on Layer 3.

The device lets you use the IGMP Snooping function to also use the IGMP mechanisms on Layer 2:
- Without IGMP Snooping, the device transmits the Multicast data packets to every port.
- With the activated IGMP Snooping function, the device transmits the Multicast data packets only on ports to which Multicast receivers are connected. This reduces the network load. The device evaluates the IGMP data packets transmitted on Layer 3 and uses the information on Layer 2.

Activate the IGMP Snooping function not until the following conditions are fulfilled:
- There is a Multicast router in the network that creates IGMP queries (periodic queries).
- The devices participating in IGMP Snooping forward the IGMP queries.

The device links the IGMP reports with the entries in its address table. When a multicast receiver joins a multicast group, the device creates a table entry for this port in the *Switching > Filter for MAC Addresses* dialog. When the multicast receiver leaves the multicast group, the device removes the table entry.

The menu contains the following dialogs:
- IGMP Snooping Global
- IGMP Snooping Configuration
- IGMP Snooping Enhancements
- IGMP Snooping Querier
- IGMP Snooping Multicasts

# 5.4.1 IGMP Snooping Global

[ Switching > IGMP Snooping > Global ]

This dialog lets you enable the *IGMP Snooping* protocol in the device and also configure it for each port and each VLAN.

### Operation

Operation

Enables/disables the *IGMP Snooping* function in the device.

Possible values:

- `On`
  The *IGMP Snooping* function is enabled in the device according to RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches).
- `Off` (default setting)
  The *IGMP Snooping* function is disabled in the device.
  The device transmits received query, report, and leave data packets without evaluating them. Received data packets with a Multicast destination address are transmitted to every port by the device.

### Information

Multicast control packets processed

Displays the number of Multicast control data packets processed.

This statistic encompasses the following packet types:

- IGMP Reports
- IGMP Queries version V1
- IGMP Queries version V2
- IGMP Queries version V3
- IGMP Queries with an incorrect version
- PIM or DVMRP packets

The device uses the Multicast control data packets to create the address table for transmitting the Multicast data packets.

Possible values:

- `0..2^31-1`

You use the *Reset IGMP snooping data* button in the *Basic Settings > Restart* dialog or the command `clear igmp-snooping` using the Command Line Interface to reset the IGMP Snooping entries, including the counter for the processed multicast control data packets.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset IGMP snooping counters

Removes the IGMP Snooping entries and resets the counter in the *Information* frame to `0`.

## 5.4.2 IGMP Snooping Configuration

[ Switching > IGMP Snooping > Configuration ]

This dialog lets you enable the *IGMP Snooping* function in the device and also configure it for each port and each VLAN.

The dialog contains the following tabs:
- [VLAN ID]
- [Port]

### [VLAN ID]

In this tab you configure the *IGMP Snooping* function for every VLAN.

#### Table

VLAN ID

Displays the ID of the VLAN to which the table entry applies.

Active

Activates/deactivates the *IGMP Snooping* function for this VLAN.

The prerequisite is that the *IGMP Snooping* function is globally enabled.

Possible values:
- `marked`
  IGMP Snooping is activated for this VLAN. The VLAN has joined the Multicast data stream.
- `unmarked` (default setting)
  IGMP Snooping is deactivated for this VLAN. The VLAN has left the Multicast data stream.

Group membership interval

Specifies the time in seconds for which a VLAN from a dynamic Multicast group remains entered in the address table when the device does not receive any more report data packets from the VLAN.

Specify a value larger than the value in the *Max. response time* column.

Possible values:
- `2..3600` (default setting: `260`)

Max. response time

Specifies the time in seconds in which the members of a multicast group should respond to a query data packet. For their response, the members specify a random time within the response time. You thus help prevent the multicast group members from responding to the query at the same time.

Specify a value smaller than the value in the *Group membership interval* column.

Possible values:

- `1..25` (default setting: `10`)

Fast leave admin mode

Activates/deactivates the Fast Leave function for this VLAN.

Possible values:

- `marked`
  When the Fast Leave function is active and the device receives an IGMP Leave message from a multicast group, the device immediately removes the entry from its address table.
- `unmarked` (default setting)
  When the Fast Leave function is inactive, the device first sends MAC-based queries to the members of the multicast group and removes an entry when a VLAN does not send any more report messages.

MRP expiration time

Multicast Router Present Expiration Time. Specifies the time in seconds for which the device waits for a query on this port that belongs to a VLAN. When the port does not receive a query data packet, the device removes the port from the list of ports with connected multicast routers.

You have the option of configuring this parameter only if the port belongs to an existing VLAN.

Possible values:

- `0`
  unlimited timeout - no expiration time
- `1..3600` (default setting: `260`)

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Port]

In this tab you configure the *IGMP Snooping* function for every port.

### Table

Port

Displays the port number.

Active

Activates/deactivates the *IGMP Snooping* function for this port.

The prerequisite is that the *IGMP Snooping* function is globally enabled.

Possible values:

- `marked`
  IGMP Snooping is active on this port. The device includes the port in the multicast data stream.
- `unmarked` (default setting)
  IGMP Snooping is inactive on this port. The port left the multicast data stream.

Group membership interval

Specifies the time in seconds for which a port, from a dynamic multicast group, remains entered in the address table when the device does not receive any more report data packets from the port.

Possible values:

- `2..3600` (default setting: `260`)

Specify the value larger than the value in the *Max. response time* column.

Max. response time

Specifies the time in seconds in which the members of a multicast group should respond to a query data packet. For their response, the members specify a random time within the response time. You thus help prevent the multicast group members from responding to the query at the same time.

Possible values:

- `1..25` (default setting: `10`)

Specify a value lower than the value in the *Group membership interval* column.

MRP expiration time

Specifies the Multicast Router Present Expiration Time. The MRP expiration time is the time in seconds for which the device waits for a query packet on this port. When the port does not receive a query data packet, the device removes the port from the list of ports with connected multicast routers.

Possible values:

- `0`
  unlimited timeout - no expiration time
- `1..3600` (default setting: `260`)

Fast leave admin mode

Activates/deactivates the Fast Leave function for this port.

Possible values:

- `marked`
  When the Fast Leave function is active and the device receives an IGMP Leave message from a multicast group, the device immediately removes the entry from its address table.
- `unmarked` (default setting)
  When the Fast Leave function is inactive, the device first sends MAC-based queries to the members of the multicast group and removes an entry when a port does not send any more report messages.

Static query port

Activates/deactivates the *Static query port* mode.

Possible values:

- `marked`
  The *Static query port* mode is active.
  The port is a static query port in the VLANs that are set up.
  If you use the *Redundant Coupling Protocol* function and the device operates as slave, then do not activate the *Static query port* mode for the ports on the secondary ring/network.
- `unmarked` (default setting)
  The *Static query port* mode is inactive.
  The port is not a static query port. The device transmits IGMP report messages to the port only if it receives IGMP queries.

VLAN IDs

Displays the ID of the VLANs to which the table entry applies.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 5.4.3 IGMP Snooping Enhancements

[ Switching > IGMP Snooping > Snooping Enhancements ]

This dialog lets you select a port for a VLAN ID and to configure the port.

### Table

VLAN ID

Displays the ID of the VLAN to which the table entry applies.

<Port number>

Displays for every VLAN set up in the device if the relevant port is a query port. Additionally, the field displays if the device transmits every Multicast stream in the VLAN to this port.

Possible values:

- `-`
  The port is not a query port in this VLAN.
- `L`= Learned
  The device detected the port as a query port because the port received IGMP queries in this VLAN. The port is not a statically configured query port.
- `A`= Automatic
  The device detected the port as a query port. The prerequisite is that you configure the port as *`Learn by LLDP`*.
- `S`= Static (manual setting)
  A user specified the port as a static query port. The device transmits IGMP reports only to ports on which it previously received IGMP queries – and to statically configured query ports.
  To assign this value, perform the following steps:
  - ☐ Open the *Wizard* window.
  - ☐ In the *Configuration* dialog, mark the *`Static`* checkbox.
- `P`= Learn by LLDP (manual setting)
  A user specified the port as *`Learn by LLDP`*.
  With the Link Layer Discovery Protocol (LLDP), the device detects Hirschmann devices connected directly to the port. The device denotes the detected query ports with `A`.
  To assign this value, perform the following steps:
  - ☐ Open the *Wizard* window.
  - ☐ In the *Configuration* dialog, mark the *`Learn by LLDP`* checkbox.
- `F`= Forward All (manual setting)
  A user specified the port so that the device transmits every received Multicast stream in the VLAN to this port. Use this setting for diagnostics purposes, for example.
  To assign this value, perform the following steps:
  - ☐ Open the *Wizard* window.
  - ☐ In the *Configuration* dialog, mark the *`Forward all`* checkbox.

Display categories

Enhances the clarity of the display. The table emphasizes the cells which contain the specified value. This helps to analyze and sort the table according to your needs.

- *`Learned (L)`*
  The table displays cells which contain the value `L` and possibly further values. Cells which contain other values than `L` only, the table displays with the “`-`“ symbol.

- *Static (S)*
  The table displays cells which contain the value S and possibly further values. Cells which contain other values than S only, the table displays with the "-" symbol.
- *Automatic (A)*
  The table displays cells which contain the value A and possibly further values. Cells which contain other values than A only, the table displays with the "-" symbol.
- *Learned by LLDP (P)*
  The table displays cells which contain the value P and possibly further values. Cells which contain other values than P only, the table displays with the "-" symbol.
- *Forward all (F)*
  The table displays cells which contain the value F and possibly further values. Cells which contain other values than F only, the table displays with the "-" symbol.

### Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Opens the *Wizard* window that helps you to select and configure the ports.

## [Selection VLAN/Port (Wizard)]

In the *Selection VLAN/Port* dialog you assign a VLAN ID to port.

In the *Configuration* dialog you specify the settings for the port.

After closing the *Wizard* window, click the button to save your settings.

## [Selection VLAN/Port (Wizard) – Selection VLAN/Port]

VLAN ID

Select the ID of the VLAN.

Possible values:

- `1..4042`

Port

Select the port.

Possible values:

- `<Port number>`

## [Selection VLAN/Port (Wizard) – Configuration]

VLAN ID

Displays the ID of the selected VLAN.

Port

Displays the number of the selected port.

Static

Specifies the port as a static query port in the VLANs that are set up. The device transmits IGMP report messages to the ports at which it receives IGMP queries. This lets you also transmit IGMP report messages to other selected ports (enable) or connected Hirschmann devices (`Automatic`).

Learn by LLDP

Specifies the port as *`Learn by LLDP`*. Lets the device detect directly connected Hirschmann devices using LLDP and learn the related ports as a query port.

Forward all

Specifies the port as *`Forward all`*. With the *`Forward all`* setting, the device transmits at this port every data packet with a Multicast address in the destination address field.

# 5.4.4 IGMP Snooping Querier

[ Switching > IGMP Snooping > Querier ]

The device lets you send a Multicast stream only to those ports to which a Multicast receiver is connected.

To determine which ports Multicast receivers are connected to, the device sends query data packets to the ports at a definable interval. When a Multicast receiver is connected, it joins the Multicast stream by responding to the device with a report data packet.

This dialog lets you configure the Snooping Querier settings globally and for the VLANs that are set up.

### Operation

Operation

Enables/disables the IGMP Querier function globally in the device.

Possible values:

- *On*
- *Off* (default setting)

### Configuration

In this frame you specify the IGMP Snooping Querier settings for the general query data packets.

Protocol version

Specifies the IGMP version of the general query data packets.

Possible values:

- 1
  IGMP v1
- 2 (default setting)
  IGMP v2
- 3
  IGMP v3

Query interval [s]

Specifies the time in seconds after which the device generates general query data packets itself when it has received query data packets from the Multicast router.

Possible values:

- `1..1800` (default setting: `60`)

Expiry interval [s]

Specifies the time in seconds after which an active querier switches from the passive state back to the active state if it has not received any query packets for longer than specified here.

Possible values:

- `60..300` (default setting: `125`)

### Table

In the table you specify the Snooping Querier settings for the VLANs that are set up.

VLAN ID

Displays the ID of the VLAN to which the table entry applies.

Active

Activates/deactivates the IGMP Snooping Querier function for this VLAN.

Possible values:

- `marked`
  The IGMP Snooping Querier function is active for this VLAN.
- `unmarked` (default setting)
  The IGMP Snooping Querier function is inactive for this VLAN.

Current state

Displays if the Snooping Querier is active for this VLAN.

Possible values:

- `marked`
  The Snooping Querier is active for this VLAN.
- `unmarked`
  The Snooping Querier is inactive for this VLAN.

Address

Specifies the IP address that the device adds as the source address in generated general query data packets. You use the address of the multicast router.

Possible values:

- Valid IPv4 address (default setting: `0.0.0.0`)

Protocol version

Displays the IGMP protocol version of the general query data packets.

Possible values:

- 1
  IGMP v1
- 2
  IGMP v2
- 3
  IGMP v3

Max. response time

Displays the time in seconds in which the members of a Multicast group should respond to a query data packet. For their response, the members specify a random time within the response time. This helps prevent every Multicast group member to respond to the query at the same time.

Last querier address

Displays the IP address of the Multicast router from which the last received IGMP query was sent out..

Last querier version

Displays the IGMP version that the Multicast router used when sending out the last IGMP query received in this VLAN.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 5.4.5 IGMP Snooping Multicasts

[ Switching > IGMP Snooping > Multicasts ]

The device lets you specify how it transmits data packets with unknown Multicast addresses: Either the device discards these data packets, floods them to every port, or transmits them only to the ports that previously received query packets.

The device also lets you transmit the data packets with known Multicast addresses to the query ports.

### Configuration

Unknown multicasts

Specifies how the device transmits the data packets with unknown Multicast addresses.

Possible values:

- *discard*
  The device discards data packets with an unknown MAC/IP Multicast address.
- *flood* (default setting)
  The device forwards data packets with an unknown MAC/IP Multicast address to every port.
- *query ports*
  The device forwards data packets with an unknown MAC/IP Multicast address to the query ports.

### Table

In the table you specify the settings for known Multicasts for the VLANs that are set up.

VLAN ID

Displays the ID of the VLAN to which the table entry applies.

Known multicasts

Specifies how the device transmits the data packets with known Multicast addresses.

Possible values:

- *send to query and registered ports*
  The device forwards data packets with an unknown MAC/IP Multicast address to the query ports and to the registered ports.
- *send to registered ports* (default setting)
  The device forwards data packets with an unknown MAC/IP Multicast address to registered ports.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 5.5 MRP-IEEE

[ Switching > MRP-IEEE ]

The IEEE 802.1ak amendment to the IEEE 802.1Q standard introduced the Multiple Registration Protocol (MRP) to replace the Generic Attribute Registration Protocol (GARP). The IEEE also modified and replaced the GARP applications, GARP Multicast Registration Protocol (GMRP) and GARP VLAN Registration Protocol (GVRP). The Multiple MAC Registration Protocol (MMRP) and the Multiple VLAN Registration Protocol (MVRP) replace these protocols.

MRP-IEEE helps confine traffic to the required areas of the LAN. To confine traffic, the MRP-IEEE applications distribute attribute values to participating MRP-IEEE devices across a LAN registering and de-registering multicast group membership and VLAN identifiers.

Registering group participants lets you reserve resources for specific traffic transversing a LAN. Defining resource requirements regulates the level of traffic, allowing the devices to determine the required resources and provides for dynamic maintenance of the allocated resources.

The menu contains the following dialogs:

- MRP-IEEE Configuration
- MRP-IEEE Multiple MAC Registration Protocol
- MRP-IEEE Multiple VLAN Registration Protocol

## 5.5.1 MRP-IEEE Configuration

[ Switching > MRP-IEEE > Configuration ]

This dialog lets you set the various MRP timers. By maintaining a relationship between the various timer values, the protocol operates efficiently and with less likelihood of unnecessary attribute withdraws and re-registrations. The default timer values effectively maintain these relationships.

When you reconfigure the timers, maintain the following relationships:
- To allow for re-registration after a Leave or LeaveAll event, even if there is a lost message, specify the LeaveTime to: ≥ (2x JoinTime) + 60.
- To minimize the volume of rejoining traffic generated following a LeaveAll event, specify the value for the LeaveAll timer larger than the LeaveTime value.

### Table

Port

Displays the port number.

Join time [1/100s]

Specifies the Join timer which controls the interval between transmit opportunities applied to the Applicant state machine.

Possible values:
- 10..100 (default setting: 20)

Leave time [1/100s]

Specifies the Leave timer which controls the period that the Registrar state machine waits in the leave (LV) state before transiting to the empty (MT) state.

Possible values:
- 20..600 (default setting: 60)

Leave all time [1/100s]

Specifies the LeaveAll timer which controls the frequency with which the LeaveAll state machine generates LeaveAll PDUs.

Possible values:
- 200..6000 (default setting: 1000)

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 5.5.2 MRP-IEEE Multiple MAC Registration Protocol

[ Switching > MRP-IEEE > MMRP ]

The Multiple MAC Registration Protocol (MMRP) lets end devices and MAC switches register and de-register group membership and individual MAC address information with switches located in the same LAN. The switches within the LAN disseminate the information through switches that support extended filtering services. Using the MAC address information, MMRP lets you confine multicast traffic to the required areas of a Layer 2 network.

For an example of how MMRP works, consider a security camera mounted on a mast overlooking a building. The camera sends multicast packets onto a LAN. You have 2 end devices installed for surveillance in separate locations. You register the MAC addresses of the camera and the 2 end devices in the same multicast group. You then specify the MMRP settings on the ports to send the multicast group packets to the 2 end devices.

The dialog contains the following tabs:
- [Configuration]
- [Service requirement]
- [Statistics]

## [Configuration]

In this tab you select active MMRP port participants and set the device to transmit periodic events. The dialog also lets you enable VLAN registered MAC address broadcasting.

A periodic state machine exists for each port and transmits periodic events regularly to the applicant state machines associated with active ports. Periodic events contain information indicating the status of the devices associated with the active port.

### Operation

Operation

Enables/disables the global *MMRP* function in the device. The device participates in MMRP message exchanges.

Possible values:

- *On*
  The device is a normal participant in MMRP message exchanges.
- *Off* (default setting)
  The device ignores MMRP messages.

### Configuration

Periodic state machine

Enables/disables the global periodic state machine in the device.

Possible values:

- *On*
  With MMRP *Operation* enabled globally, the device transmits MMRP messages in one-second intervals, on MMRP participating ports.
- *Off* (default setting)
  Disables the periodic state machine in the device.

### Table

Port

Displays the port number.

Active

Activates/deactivates the port MMRP participation.

Possible values:

- `marked` (default setting)
  With MMRP enabled globally and on this port, the device sends and receives MMRP messages on this port.
- `unmarked`
  Disables the port MMRP participation.

Restricted group registration

Activates/deactivates the restriction of dynamic MAC address registration using MMRP on the port.

Possible values:

- `marked`
  If enabled and a static filter entry for the MAC address exists on the VLAN concerned, then the device registers the MAC address attributes dynamically.
- `unmarked` (default setting)
  Activates/deactivates the restriction of dynamic MAC address registration using MMRP on the port.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Service requirement]

This tab contains forwarding parameters for each active VLAN, specifying the ports on which multicast forwarding applies. The device lets you statically setup VLAN ports as *Forward all* or Forbidden. You set the Forbidden MMRP service requirement statically only through the Graphical User Interface or Command Line Interface.

A port is setup only as ForwardAll or Forbidden.

### Table

VLAN ID

Displays the ID of the VLAN.

<Port number>

Specifies the service requirement handling for the port.

Possible values:

- FA
  Specifies the ForwardAll traffic setting on the port. The device forwards traffic destined to MMRP registered multicast MAC addresses on the VLAN. The device forwards traffic to ports which MMRP has dynamically setup or ports which the administrator has statically setup as ForwardAll ports.
- F
  Specifies the Forbidden traffic setting on the port. The device blocks dynamic MMRP ForwardAll service requirements. With ForwardAll requests blocked on this port in this VLAN, the device blocks traffic destined to MMRP registered multicast MAC addresses on this port. Furthermore, the device blocks MMRP service request for changing this value on this port.
- \- (default setting)
  Disables the forwarding functions on this port.
- Learned
  Displays values setup by MMRP service requests.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Statistics]

Devices on a LAN exchange Multiple MAC Registration Protocol Data Units (MMRPDU) to maintain statuses of devices on an active MMRP port. This tab lets you monitor the MMRP traffic statistics for each port.

### Information

Transmitted MMRP PDU

Displays the number of MMRPDUs transmitted in the device.

Received MMRP PDU

Displays the number of MMRPDUs received in the device.

Received bad header PDU

Displays the number of MMRPDUs received with a bad header in the device.

Received bad format PDU

Displays the number of MMRPDUs with a bad data field that were not transmitted in the device.

Transmission failed

Displays the number of MMRPDUs not transmitted in the device.

### Table

Port

Displays the port number.

Transmitted MMRP PDU

Displays the number of MMRPDUs transmitted on the port.

Received MMRP PDU

Displays the number of MMRPDUs received on the port.

Received bad header PDU

Displays the number of MMRPDUs with a bad header that were received on the port.

Received bad format PDU

Displays the number of MMRPDUs with a bad data field that were not transmitted on the port.

Transmission failed

Displays the number of MMRPDUs not transmitted on the port.

Last received MAC address

Displays the last MAC address from which the port received MMRPPDUs.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset

Resets the port statistics counters and the values in the *Last received MAC address* column.

# 5.5.3 MRP-IEEE Multiple VLAN Registration Protocol

[ Switching > MRP-IEEE > MVRP ]

The Multiple VLAN Registration Protocol (MVRP) provides a mechanism that lets you distribute VLAN information and configure VLANs dynamically. For example, when you configure a VLAN on an active MVRP port, the device distributes the VLAN information to other MVRP enabled devices. Using the information received, an MVRP enabled device dynamically creates the VLAN trunks on other MVRP enabled devices as needed.

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

## [Configuration]

In this tab you select active MVRP port participants and set the device to transmit periodic events.

A periodic state machine exists for each port and transmits periodic events regularly to the applicant state machines associated with active ports. Periodic events contain information indicating the status of the VLANs associated with the active port. Using the periodic events, MVRP enabled switches dynamically maintain the VLANs.

### Operation

Operation

Enables/disables the global Applicant Administrative Control which specifies if the Applicant state machine participates in MMRP message exchanges.

Possible values:
- *On*
  Normal Participant. The Applicant state machine participates in MMRP message exchanges.
- *Off* (default setting)
  Non-Participant. The Applicant state machine ignores MMRP messages.

### Configuration

Periodic state machine

Enables/disables the periodic state machine in the device.

Possible values:

- `On`
  The periodic state machine is enabled.
  With MVRP *Operation* enabled globally, the device transmits MVRP periodic events in 1 second intervals, on MVRP participating ports.
- `Off` (default setting)
  The periodic state machine is disabled.
  Disables the periodic state machine in the device.

### Table

Port

Displays the port number.

Active

Activates/deactivates the port MVRP participation.

Possible values:

- `marked` (default setting)
  With MVRP enabled globally and on this port, the device distributes VLAN membership information to MVRP-aware devices connected to this port.
- `unmarked`
  Disables the port MVRP participation.

Restricted VLAN registration

Activates/deactivates the *Restricted VLAN registration* function on this port.

Possible values:

- `marked`
  If enabled and a static VLAN registration entry exists, then the device lets you create a dynamic VLAN for this entry.
- `unmarked` (default setting)
  Disables the *Restricted VLAN registration* function on this port.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Statistics]

Devices on a LAN exchange Multiple VLAN Registration Protocol Data Units (MVRPDU) to maintain statuses of VLANs on active ports. This tab lets you monitor the MVRP traffic.

### Information

Transmitted MVRP PDU

Displays the number of MVRPDUs transmitted in the device.

Received MVRP PDU

Displays the number of MVRPDUs received in the device.

Received bad header PDU

Displays the number of MVRPDUs received with a bad header in the device.

Received bad format PDU

Displays the number of MVRPDUs with a bad data field that the device blocked.

Transmission failed

Displays the number of failures while adding a message into the MVRP queue.

Message queue failures

Displays the number of MVRPDUs that the device blocked.

### Table

Port

Displays the port number.

Transmitted MVRP PDU

Displays the number of MVRPDUs transmitted on the port.

Received MVRP PDU

Displays the number of MVRPDUs received on the port.

Received bad header PDU

Displays the number of MVRPDUs with a bad header that the device received on the port.

Received bad format PDU

Displays the number of MVRPDUs with a bad data field that the device blocked on the port.

Transmission failed

Displays the number of MVRPDUs that the device blocked on the port.

Registrations failed

Displays the number of failed registration attempts on the port.

Last received MAC address

Displays the last MAC address from which the port received MMRPDUs.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset

Resets the port statistics counters and the values in the *Last received MAC address* column.

## 5.6 GARP

[ Switching > GARP ]

The Generic Attribute Registration Protocol (GARP) is defined by the IEEE to provide a generic framework so switches can register and deregister attribute values, such as VLAN identifiers and multicast group membership.

When an attribute for a participant is registered or deregistered according to GARP, the participant is modified according to specific rules. The participants are a set of reachable end stations and network devices. The defined set of participants at any given time, along with their attributes, is the reachability tree for the subset of the network topology. The device forwards the data frames only to the registered end stations. The station registration helps prevent attempts to send data to the end stations that are unreachable.

**Note:** Before you enable the *GMRP* function, verify that the *MMRP* function is disabled.

The menu contains the following dialogs:

- GMRP
- GVRP

# 5.6.1 GMRP

[ Switching > GARP > GMRP ]

The GARP Multicast Registration Protocol (GMRP) is a Generic Attribute Registration Protocol (GARP) that provides a mechanism allowing network devices and end stations to dynamically register group membership. The devices register group membership information with the devices attached to the same LAN segment. GARP also lets the devices distribute the information across the network devices that support extended filtering services.

GMRP and GARP are industry-standard protocols defined by the IEEE 802.1P.

### Operation

Operation

Enables/disables the global *GMRP* function in the device. The device participates in GMRP message exchanges.

Possible values:

- *On*
  GMRP is enabled.
- *Off* (default setting)
  The device ignores GMRP messages.

### Multicasts

Unknown multicasts

Enables/disables the unknown multicast data to be either flooded or discarded.

Possible values:

- *discard*
  The device discards unknown multicast data.
- *flood* (default setting)
  The device forwards unknown multicast data to every port.

### Table

Port

Displays the port number.

GMRP active

Activates/deactivates the port *GMRP* participation.

The prerequisite is that the *GMRP* function is globally enabled.

Possible values:

- `marked` (default setting)
  The port *GMRP* participation is active.
- `unmarked`
  The port *GMRP* participation is inactive.

Service requirement

Specifies the ports on which multicast forwarding applies.

Possible values:

- *`Forward all unregistered groups`* (default setting)
  The device forwards data destined to *GMRP*-registered multicast MAC addresses on the VLAN.
  The device forwards data to the unregistered groups.
- *`Forward all groups`*
  The device forwards data destined to every group, registered or unregistered.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 5.6.2 GVRP

[ Switching > GARP > GVRP ]

The GARP VLAN Registration Protocol (GVRP) or Generic VLAN Registration Protocol is a protocol that facilitates control of Virtual Local Area Networks (VLANs) within a larger network. GVRP is a Layer 2 network protocol, used to automatically configure devices in a VLAN network.

GVRP is a GARP application that provides IEEE 802.1Q-compliant VLAN pruning, and creating dynamic VLAN on 802.1Q trunk ports. With GVRP, the device exchanges VLAN configuration information with other GVRP devices. Thus, the device reduces the unnecessary broadcast and unknown unicast traffic. Exchanging VLAN configuration information also lets you dynamically create and manage VLANs connected through the 802.1Q trunk ports.

## Operation

Operation

Enables/disables the *GVRP* function globally in the device. The device participates in *GVRP* message exchanges. If the function is disabled, then the device ignores *GVRP* messages.

Possible values:

- `On`
  The *GVRP* function is enabled.
- `Off` (default setting)
  The *GVRP* function is disabled.

## Table

Port

Displays the port number.

GVRP active

Activates/deactivates the port *GVRP* participation.

The prerequisite is that the *GVRP* function is globally enabled.

Possible values:

- `marked` (default setting)
  The port *GVRP* participation is active.
- `unmarked`
  The port *GVRP* participation is inactive.

## Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 5.7 QoS/Priority

[ Switching > 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`.

The menu contains the following dialogs:
- QoS/Priority Global
- QoS/Priority Port Configuration
- 802.1D/p Mapping
- IP DSCP Mapping
- Queue Management
- DiffServ

# 5.7.1 QoS/Priority Global

[ Switching > 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.

In the *Switching > QoS/Priority > IP DSCP Mapping* dialog you assign a traffic class to every IP DSCP value.

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 16.

## 5.7.2 QoS/Priority Port Configuration

[ Switching > 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

Port

Displays the port number.

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`)

Trust mode

Specifies how the device handles a received data packet if the data packet contains QoS/priority information.

Possible values:

- *untrusted*
  The device transmits the data packet according to the priority specified in the *Port priority* column.
  The device ignores the priority information contained in the data packet.
  In the *Switching > QoS/Priority > 802.1D/p Mapping* dialog, you assign a traffic class to every VLAN priority.
- *trustDot1p* (default setting)
  The device transmits the data packet according to the priority information in the VLAN tag.
  In the *Switching > QoS/Priority > 802.1D/p Mapping* dialog, you assign a traffic class to every VLAN priority.
- *trustIpDscp*
  - If the data packet is an IP packet, then:
    The device transmits the data packet according to the IP DSCP value contained in the data packet.
    In the *Switching > QoS/Priority > IP DSCP Mapping* dialog you assign a traffic class to every IP DSCP value.
  - If the data packet is not an IP packet, then:
    The device transmits the data packet according to the priority specified in the *Port priority* column.
    In the *Switching > QoS/Priority > 802.1D/p Mapping* dialog, you assign a traffic class to every VLAN priority.

Untrusted traffic class

Displays the traffic class assigned to the VLAN priority information specified in the *Port priority* column. In the *Switching > QoS/Priority > 802.1D/p Mapping* dialog, you assign a traffic class to every VLAN priority.

Possible values:

- `0..7`

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 5.7.3 802.1D/p Mapping

[ Switching > QoS/Priority > 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 assign a traffic class to every VLAN priority. You assign the traffic classes to the priority queues of the ports.

### Table

VLAN priority

Displays the VLAN priority.

Traffic class

Specifies the traffic class assigned to the VLAN priority.

Possible values:

- `0..7`
  `0` assigned to the priority queue with the lowest priority.
  `7` assigned to the priority queue with the highest priority.

**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 16.

### Default assignment of the VLAN priority to traffic classes

| VLAN Priority | Traffic class | Content description according to IEEE 802.1D |
|---|---|---|
| `0` | 2 | `Best Effort`<br>Normal data without prioritizing |
| `1` | 0 | `Background`<br>Non-time-sensitive data and background services |
| `2` | 1 | `Standard`<br>Normal data |
| `3` | 3 | `Excellent Effort`<br>Crucial data |
| `4` | 4 | `Controlled Load`<br>Time-sensitive data with a high priority |

| VLAN Priority | Traffic class | Content description according to IEEE 802.1D |
|---|---|---|
| 5 | 5 | Video<br>Video transmission with delays and jitter < 100 ms |
| 6 | 6 | Voice<br>Voice transmission with delays and jitter < 10 ms |
| 7 | 7 | Network Control<br>Data for network management and redundancy mechanisms |

# 5.7.4 IP DSCP Mapping

[ Switching > QoS/Priority > IP DSCP Mapping ]

The device transmits IP data packets according to the DSCP value contained in the data packet with a higher or lower priority.

In this dialog you assign a traffic class to every DSCP value. You assign the traffic classes to the priority queues of the ports.

### Table

DSCP value

Displays the DSCP value.

Traffic class

Specifies the traffic class which is assigned to the DSCP value.

Possible values:

- `0..7`
  `0` assigned to the priority queue with the lowest priority.
  `7` assigned to the priority queue with the highest priority.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

### Default assignment of the DSCP values to traffic classes

| DSCP Value | DSCP Name | Traffic class |
|---|---|---|
| 0 | Best Effort /CS0 | 2 |
| 1-7 | | 2 |
| 8 | CS1 | 0 |
| 9,11,13,15 | | 0 |
| 10,12,14 | AF11,AF12,AF13 | 0 |
| 16 | CS2 | 1 |
| 17,19,21,23 | | 1 |
| 18,20,22 | AF21,AF22,AF23 | 1 |
| 24 | CS3 | 3 |
| 25,27,29,31 | | 3 |
| 26,28,30 | AF31,AF32,AF33 | 3 |
| 32 | CS4 | 4 |
| 33,35,37,39 | | 4 |
| 34,36,38 | AF41,AF42,AF43 | 4 |

| DSCP Value | DSCP Name | Traffic class |
|---|---|---|
| 40 | CS5 | 5 |
| 41,42,43,44,45,47 | | 5 |
| 46 | EF | 5 |
| 48 | CS6 | 6 |
| 49-55 | | 6 |
| 56 | CS7 | 7 |
| 57-63 | | 7 |

# 5.7.5 Queue Management

[ Switching > QoS/Priority > Queue Management ]

This dialog lets you enable and disable the *Strict priority* function for the traffic classes. When you disable the *Strict priority* function, the device processes the priority queues of the ports with "Weighted Fair Queuing".

You also have the option of assigning a minimum bandwidths to every traffic classes which the device uses to process the priority queues with "Weighted Fair Queuing"

### Table

Traffic class

Displays the traffic class.

Strict priority

Activates/deactivates the processing of the port priority queue with *Strict priority* for this traffic class.

Possible values:

- `marked` (default setting)
  The processing of the port priority queue with *Strict priority* is active.
  - The port forwards only data packets that are in the priority queue with the highest priority. When this priority queue is empty, the port forwards data packets that are in the priority queue with the next lower priority.
  - The port forwards data packets with a lower traffic class after the priority queues with a higher priority are empty. In unfavorable situations, the port does not send these data packets.
  - When you select this setting for a traffic class, the device also enables the function for traffic classes with a higher priority.
  - Use this setting for applications such as VoIP or video that require the least possible delay.
- `unmarked`
  The processing of the port priority queue with *Strict priority* is inactive. The device uses "Weighted Fair Queuing"/"Weighted Round Robin" (WRR) to process the port priority queue.
  - The device assigns a minimum bandwidth to each traffic class.
  - Even under a high network load the port transmits data packets with a low traffic class.
  - When you select this setting for a traffic class, the device also disables the function for traffic classes with a lower priority.

Min. bandwidth [%]

Specifies the minimum bandwidth for this traffic class when the device is processing the priority queues of the ports with "Weighted Fair Queuing".

Possible values:

- `0..100` (default setting: `0` = the device does not reserve any bandwidth for this traffic class)

The value specified in percent refers to the available bandwidth on the port. When you disable the *Strict priority* function for every traffic class, the maximum bandwidth is available on the port for the "Weighted Fair Queuing".

The maximum total of the assigned bandwidths is 100 %.

Max. bandwidth [%]

Specifies the shaping rate at which a Traffic Class transmits packets (Queue Shaping).

Possible values:

- `0` (default setting)
  The device does not reserve any bandwidth for this traffic class.
- `1..100`
  The device reserves the specified bandwidth for this traffic class. The specified value in percent refers to the maximum available bandwidth on this port.

For example, using queue shaping lets you limit the rate of a strict-high priority queue. Limiting a strict-high priority queue lets the device also process low-priority queues. To use queue shaping, you set the maximum bandwidth for a particular queue.

#### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 5.7.6 DiffServ

[ Switching > QoS/Priority > DiffServ ]

Differentiated Services (DiffServ) filter data packets in order to prioritize or limit the data stream.
- In a class, you specify the filter criteria.
- In a policy, you link the class with actions.

The device applies the actions of the policy to those data packets that meet the filter criteria of the assigned class.

To configure DiffServ, perform the following steps:
- ☐ Create a class with the filter criteria.
- ☐ Create a policy.
- ☐ Assign a class with the filter criteria to the policy.
- ☐ Specify the actions of the policy.
- ☐ Assign the policy to a port.
- ☐ Activate the DiffServ function.

The device lets you use the following per class and per instance configurations:
- 13 rules per class
- 28 instances per policy
- 3 attributes per instance

The menu contains the following dialogs:
- DiffServ Overview
- DiffServ Global
- DiffServ Class
- DiffServ Policy
- DiffServ Assignment

# 5.7.6.1 DiffServ Overview

[ Switching > QoS/Priority > DiffServ > Overview ]

This dialog displays the configured DiffServ settings.

### Port

Port

Simplifies the table and displays the entries relating to a specific port. Displaying the table in this fashion makes it easier for you to sort the table as you desire.

Possible values:

- `All` (default setting)
  The table displays the entries for every port.
- `<Port number>`
  The table displays the entries that apply to the selected port.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 5.7.6.2 DiffServ Global

[ Switching > QoS/Priority > DiffServ > Global ]

In this dialog you enable the DiffServ function.

### Operation

Operation

Enables/disables the *DiffServ* function.

Possible values:

- `On`
  The *DiffServ* function is enabled.
  The device processes traffic according to the DiffServ rules.
- `Off` (default setting)
  The *DiffServ* function is disabled.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 5.7.6.3 DiffServ Class

[ Switching > QoS/Priority > DiffServ > Class ]

In this dialog you specify the data packets to which the device executes the actions specified in the *Policy* dialog. This assignment is called a class.

Only one class can be assigned to a policy. This means each class can contain multiple filter criteria.

### Table

Class name

Specifies the name of the DiffServ class. The device lets you change the class name directly in the table.

Possible values:

- Alphanumeric ASCII character string with 1..31 characters

Criteria

Displays the specified criteria for this rule.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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

### Create

Class name

Specifies the name of the DiffServ class.

Possible values:

- Alphanumeric ASCII character string with 1..31 characters

Type

Specifies the type of Class Rule for matching; this determines the individual match conditions for the present class rule.

Depending on which value you select, the following visible parameters change.

To match every packet regardless of content, select the value `every`.

Possible values:

- *cos* (default setting)
- *dstip*
- *dstl4port*
- *dstmac*
- *every*
- *ipdscp*
- *ipprecedence*
- *iptos*
- *protocol*
- *refclass*
- *srcip*
- *srcl4port*
- *srcmac*
- *cos2*
- *etype*
- *vlanid*
- *vlanid2*

Type = cos

COS

Specifies the class of service as the match value for the class.

Possible values:

- 0..7 (default setting: 0)

Type = dstip

Destination IP address

Specifies the destination IP address as the match value for the class.

Possible values:

- Valid IP address

Destination IP address mask

Specifies the mask for the destination IP address.

Possible values:

- Valid netmask

Type = dstl4port

Destination port

Specifies the destination Layer 4 port as the match value for the class.

Possible values:

- Valid TCP or UDP port number

Type = dstmac

Destination MAC address

Specifies the destination MAC address as the match value for the class.

Possible values:

- Valid MAC address

Destination MAC address mask

Specifies the mask for the destination MAC address.

Possible values:

- Valid netmask

Type = ipdscp

DSCP

Specifies the IP DiffServ Code Point (DSCP) as the match value for the class.

Possible values:

- `0..63` (default setting: `0(be/cs0)`)

Type = `ipprecedence`

TOS priority

Specifies the IP Precedence as the match value for the class. The precedence bits are the high-order 3 bits of the Service Type octet in the IPv4 header.

Possible values:

- `0..7` (default setting: `0`)

Type = `iptos`

TOS mask

Specifies the IP TOS bits and mask as the match value for the class. The TOS bits are the 8 bits of the Service Type octet in the IPv4 header.

Possible values:

- `0x00..0xFF`

Type = `protocol`

Protocol number

Specifies the value of the IPv4 header protocol field as the match value for the class.

Possible values:

- `0..255`
  Some common values are listed here:
  - `1`
    ICMP
  - `2`
    IGMP
  - `4`
    IPv4 (IPv4 in IPv4 encapsulation)
  - `6`
    TCP
  - `17`
    UDP
  - `41`
    IPv6 (IPv6 in IPv4 encapsulation)
  - `255`
    A rule with this value matches every protocol in the list.

The IANA defined the “Assigned Internet Protocol Numbers” that you enter here.

To find a list of the assigned numbers use the following link: www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.

Type = refclass

Ref class

Specifies the parent class as a corresponding reference class. This reference class uses the set of match rules specified in a parent class as the match value.

Possible values:

- <Name of the DiffServ Class>

Conditions:

- If the reference class refers only to the parent class, then the parent class to which you bind this rule and the reference class produce the same results.
- Any attempt to delete the parent class while still referenced to by another class fails.
- If the reference class uses the parent class as the match value, then any subsequent change to the parent class rules changes the reference class rules only.
- You add subsequent rules to the parent class compatible with the rules existing in the reference class.

Type = srcip

Source IP address

Specifies the source IP address as the match value for the class.

Possible values:

- Valid IP address

Source IP address mask

Specifies the mask for the source IP address.

Possible values:

- Valid netmask

Type = srcl4port

Source port

Specifies the source Layer 4 port as the match value for the class.

Possible values:

- Valid TCP or UDP port number

Type = srcmac

Source MAC address

Specifies the source MAC address as the match value for the class.

Possible values:

- Valid MAC address and mask

Source MAC address mask

Specifies the mask for the source MAC address.

Possible values:

- Valid netmask

Type = cos2

COS 2

Specifies a secondary class of service as the match value for the class.

Possible values:

- 0..7 (default setting: 0)

Type = etype

Etype

Specifies the Ethertype as the match value for the class.

Possible values:

- *custom* (default setting)
  You specify the Ethertype in the *Etype value* field.
- *appletalk*
- *arp*
- *ibmsna*
- *ipv4*
- *ipv6*
- *ipx*
- *mplsmcast*
- *mplsucast*
- *netbios*
- *novell*
- *pppoe*
- *rarp*

Etype value

Specifies the user-defined Ethertype value.

The prerequisite is that in the *Etype* field you specify the value *custom*.

Possible values:

- 0x0600..0xFFFF

Type = vlanid

VLAN ID

Specifies the VLAN ID as the match value for the class.

Possible values:

- 1..4042

Type = vlanid2

VLAN2 ID

Specifies the secondary VLAN ID as the match value for the class.

Possible values:

- 1..4042

# 5.7.6.4 DiffServ Policy

[ Switching > QoS/Priority > DiffServ > Policy ]

In this dialog you specify which actions the device performs on data packets which fulfill the filter criteria specified in the *Class* dialog. This assignment is called a policy.

Only one policy can be assigned to a port. Each policy can contain multiple actions.

### Table

Policy name

Displays the name of the policy.

To change the value, click the relevant field.

Possible values:

- Alphanumeric ASCII character string with 1..31 characters

Direction

Displays the data packets (receiving or sending) to which the device applies the policy.

Possible values:

- *in*
  The device applies the policy to data packets that it receives.
- *out*
  The device applies the policy to data packets that it sends.

Class name

Displays the name of the class that is assigned to the policy.

The filter criteria are specified in the class.

Attribute

Displays the action that the device performs on the data packets.

- ☐ To change an existing action, select the affected row, click the button and then the *Modify attribute* item.
- ☐ To add additional actions to a policy, click the button.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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

Modify attribute

Specifies the action that the device performs on the data packets.

### Create

In this dialog you create a new policy or add further actions to an existing policy.

Policy name

Specifies the name of the policy.

- ☐ To create a new policy, add a new name.
- ☐ To add more actions to an existing policy, select a name in the list.

Possible values:

- Alphanumeric ASCII character string with 1..31 characters

Direction

Specifies the data packets (receiving or sending) to which the device applies the policy.

Possible values:

- *in* (default setting)
  The device applies the policy to data packets that it receives.
- *out*
  The device applies the policy to data packets that it sends.

Class name

Assigns the class to the policy.

The filter criteria are specified in the class.

Type

Specifies the policy type.

Depending on which value you select, the following visible parameters change.

Possible values:

- *markCosVal* (default setting)
- *markIpDscpVal*
- *markIpPrecedenceVal*
- *policeSimple*
- *policeTworate*
- *assignQueue*
- *drop*
- *redirect*
- *mirror*
- *markCosAsSecCos*

Type = markCosVal

Overwrites the priority field in the VLAN tag of the Ethernet packets:

- In the VLAN tag, the device overwrites the priority value in the *COS* parameter.
- With QinQ-tagged (IEEE 802.1ad) Ethernet packets, the device writes the value to the outer tag (*Service tag* or *S tag*).
- With data packets without VLAN tags, the device adds a priority tag.

Can be combined with *Type* = *redirect* and *mirror*.

COS

Specifies the priority value that the device writes to the priority field of the VLAN tag of the Ethernet packets.

Possible values:

▶ 0..7

Type = markIpDscpVal

Overwrites the DS field of the IP packets.

The device writes the value specified in the *DSCP* parameter to the DS field. Subsequent devices in the network to which the device forwards the IP packets, prioritize the IP packets according to this setting. For making the device prioritize the IP packets, also enter the IP packets with *Type* = *assignQueue* into the desired queue.

Can be combined with *Type* = *assignQueue*, *redirect* and *mirror*.

DSCP

Specifies the value that the device writes to the DS field of the IP packets.

Possible values:

▶ 0..63

Type = markIpPrecedenceVal

Overwrites the TOS field of the IP packets.

The device writes the value specified in the *TOS priority* parameter to the TOS field.

Can be combined with *Type* = *assignQueue*, *redirect* and *mirror*.

TOS priority

Specifies the value that the device writes to the TOS field of the IP packets.

Possible values:

▶ 0..7

Type = policeSimple

Limits the classified data stream to the values specified in the *Simple C rate* and *Simple C burst* fields:

- If the transfer rate and burst size of the data stream are below the specified values, then the

device applies the action specified in the *Conform action* field.

- If the transfer rate and burst size of the data stream are above the specified values, then the device applies the action specified in the *Non conform action* field.

Can be combined with *Type* = `assignQueue`, `redirect` and `mirror`.

Simple C rate

Specifies the committed rate in kbit/s.

Upper limit

Possible values:

▶ `1..4294967295`

Simple C burst

Specifies the committed burst size in kBytes.

Possible values:

▶ `0..128`

Conform action, Non conform action

In the *Conform action* field, you specify the action that the device applies to the compliant data stream. Compliant means that the data stream is under the limits specified in the parameters *Simple C rate* and *Simple C burst*.

In the *Non conform action* field, you specify the action that the device applies to the non-compliant data stream. Non-compliant means that the data stream is over the limits specified in the parameters *Simple C rate* and *Simple C burst*.

Possible values:

▶ *drop*
Discards the data packets.

▶ *markDscp*
Overwrites the DS field of the IP packets.
The device writes the value specified in the adjacent field [`0..63`] to the DS field.

▶ *markPrec*
Overwrites the TOS field of the IP packets.
The device writes the value specified in the adjacent field [`0..7`] to the TOS field.

▶ *send*
Sends the data packets.

▶ *markCos*
Overwrites the priority field in the VLAN tag of the Ethernet packets:
  – in the VLAN tag, the device overwrites the priority value in the *COS* parameter.
  – With QinQ-tagged (IEEE 802.1ad) Ethernet packets, the device writes the value to the outer tag (*Service tag* or *S tag*).
  – With Ethernet packets without VLAN tags, the device adds a priority tag.

- *markCos2*
  With QinQ-tagged Ethernet packets, overwrites the priority field in the inner tag (*Customer tag* or *C tag*) with the value specified in the adjacent field [0..7].
- *markCosAsSecCos*
  Overwrites the priority field in the outer tag (*Service tag* or *S tag*) with the priority value of the inner tag (*C tag*).

Color conform class

Specifies the class of the received data stream that the devices designates as conform (green).

Possible values:

- *blind*
  The device operates in the color-blind mode. The devices designates the complete data stream received as conform (green).
- <Name of the DiffServ Class>
  The devices designates only this class of the received data stream as conform (green). Those classes are selectable for which in the *Switching > QoS/Priority > DiffServ > Class* dialog, *Criteria* column a rule of the type *cos*, *ipdscp*, *ipprec*, *cos2* is specified.

Verify that the filter criteria of the class selected in the *Class name* drop-down list above and of the class selected in this drop-down list, is neither identical nor exclude each other. Exclusion criteria are:

- The filter criteria have the same rule type, for example *cos* and *cos*. Use classes with a different rule type, for example *cos* and *ipdscp*.
- One of the classes references with the rule type *refclass* another class that conflicts with the used classes.

Type = policeTworate

Limits the classified data stream to the values specified in the *Two rate C rate*, *Two rate C burst*, *Two rate P rate*, and *Two rate P burst* fields.

- If the transfer rate and burst size are below *Two rate C rate* and *Two rate C burst*, then the device applies the *Conform action* action to the data stream.
- If the transfer rate and burst size are between *Two rate C rate* and *Two rate P rate* as well as *Two rate C burst* and *Two rate P burst*, then the device applies the *Exceed action* action to the data stream.
- If the transfer rate and burst size are above *Two rate P rate* and *Two rate P burst*, then the device applies the *Non conform action* action to the data stream.

Can be combined with *Type* = `assignQueue`, `redirect` and `mirror`.

Two rate C rate

Specifies the committed rate in kbit/s.

Possible values:

▶ `1..4294967295`

Two rate C burst

Specifies the committed burst size in kBytes.

Possible values:

▶ `0..128`

Two rate P rate

Specifies the peak rate (max. allowable transfer rate of the data stream) in kbit/s.

Possible values:

▶ `1..4294967295`

Two rate P burst

Specifies the peak burst size (max. allowable burst size) in kBytes.

Possible values:

▶ `1..128`

Conform action
Conform value
Exceed action
Exceed value
Non conform action
Non conform value

In the *Conform action* field, you specify the action that the device applies to the compliant data stream. Compliant means that transfer rate and burst size are below *Two rate C rate* and *Two rate C burst*.

In the *Exceed action* field, you specify the action that the device applies to the data stream. The prerequisite is that the transfer rate and burst size are between *Two rate C rate* and *Two rate P rate*

as well as *Two rate C burst* and *Two rate P burst*.

In the *Non conform action* field, you specify the action that the device applies to the non-compliant data stream. Non-compliant means that the transfer rate and burst size are above *Two rate P rate* and *Two rate P burst*.

Possible values:

- `drop`
  Discards the data packets.
- `markDscp`
  Overwrites the DS field of the IP packets.
  The device writes the value specified in the adjacent field [`0..63`] to the DS field.
- `markPrec`
  Overwrites the TOS field of the IP packets.
  The device writes the value specified in the adjacent field [`0..7`] to the TOS field.
- `send`
  Sends the data packets.
- `markCos`
  Overwrites the priority field in the VLAN tag of the Ethernet packets:
  - in the VLAN tag, the device overwrites the priority value in the *COS* parameter.
  - With QinQ-tagged (IEEE 802.1ad) Ethernet packets, the device writes the value to the outer tag (*Service tag* or *S tag*).
  - With Ethernet packets without VLAN tags, the device adds a priority tag.
- `markCos2`
  With QinQ-tagged Ethernet packets, overwrites the priority field in the inner tag (*Customer tag* or *C tag*) with the value specified in the adjacent field [`0..7`].
- `markCosAsSecCos`
  Overwrites the priority field in the outer tag (*S tag*) with the priority value of the inner tag (*C tag*).

Color conform class

Specifies the class of the received data stream that the devices designates as conform (green).

Possible values:

- `0 - blind`
  The device operates in the color blind mode. The devices designates the complete data stream received as conform (green).
- `<Name of the DiffServ Class>`
  The devices designates only this class of the received data stream as conform (green).
  Those classes are selectable for which in the *Switching > QoS/Priority > DiffServ > Class* dialog, *Criteria* column a rule of the type `cos`, `ipdscp`, `ipprec`, `cos2` is specified.

Verify that the filter criteria of the class selected in the *Class name* drop-down list above and of the class selected in this drop-down list, is neither identical nor exclude each other. Exclusion criteria are:

- The filter criteria have the same rule type, for example `cos` and `cos`. Use classes with a different rule type, for example `cos` and `ipdscp`.
- One of the classes references with the rule type `refclass` another class that conflicts with the used classes.

Type = assignQueue

Changes the priority queue into which the device adds the data packets.

The device enqueues the data packets into the priority queue with the ID specified in the *Queue ID* parameter.

Apply this action only to data packets that the device receives.

Can be combined with *Type* = *drop*, *markCosVal* and *markCosAsSecCos*.

Queue ID

Specifies the ID of the priority queue into which the device adds the data packets. See the *Traffic class* field and the *Switching > QoS/Priority > 802.1D/p Mapping* dialog.

Possible values:

- 0..7

Type = drop

Discards the data packets.

Can be combined with *Type* = *mirror* if *mirror* is set up first.

Type = redirect

The device forwards the received data stream to the port specified in the *Redirection interface* field.

Apply this action only to data packets that the device receives.

Can be combined with *Type* = *markCosVal*, *markIpDscpVal*, *markIpPrecedenceVal*, *policeSimple*, *policeTworate*, *assignQueue* and *markCosAsSecCos*.

Redirection interface

Specifies the destination port.

Possible values:

- <Port number>
  Number of the destination port. The device forwards the data packets to this port.

**Note:** The destination port needs sufficient bandwidth to absorb the data stream. If the copied data stream exceeds the bandwidth of the destination port, then the device discards surplus data packets on the destination port.

Type = mirror

The device copies the received data stream and also transfers it to the port specified in the *Mirror interface* field.

Apply this action only to data packets that the device receives.

Can be combined with *Type* = *markCosVal*, *markIpDscpVal*, *markIpPrecedenceVal*, *policeSimple*, *policeTworate*, *assignQueue* and *markCosAsSecCos*.

Mirror interface

Specifies the destination port.

Possible values:

- <Port number>
  Number of the destination port. The device copies the data packets to this port.

**Note:** The destination port needs sufficient bandwidth to absorb the data stream. If the copied data stream exceeds the bandwidth of the destination port, then the device discards surplus data packets on the destination port.

Type = markCosAsSecCos

Overrides the priority field in the outer VLAN tag of the Ethernet packets with the priority value of the inner VLAN tag.

Apply this action only to data packets that the device receives.

Can be combined with *Type* = *assignQueue*, *redirect* and *mirror*.

# 5.7.6.5 DiffServ Assignment

[ Switching > QoS/Priority > DiffServ > Assignment ]

In this dialog you assign the policy to a port.

**Note:** You cannot apply IP ACL rules and DiffServ rules together in the same direction on a port.

### Table

Port

Displays the port number.

Direction

Displays the interface direction to which you assigned the policy.

Policy name

Displays the name of the policy assigned to the interface.

Status

Displays the port status.

Active

Activates/deactivates the DiffServ parameters associated with this row.

Possible values:

- `marked`
  The device forwards traffic according to the specified DiffServ settings.
- `unmarked`
  The device forwards traffic without regarding the specified DiffServ settings.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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

**Create**

Port

Specifies the port to which the table entry relates.

Possible values:
- Available ports

Direction

Specifies the direction in which the device applies the policy.

Possible values:
- *In* (default setting)
- *Out*

Policy

Specifies the policy assigned to the port.

Possible values:
- Available policies

## 5.8 VLAN

[ Switching > VLAN ]

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 device prioritizes the received data stream in the following sequence:

- Voice VLAN
- MAC-based VLAN
- IP subnet-based VLAN
- Protocol-based VLAN
- Port-based VLAN

The menu contains the following dialogs:

- VLAN Global
- VLAN Configuration
- VLAN Port
- VLAN Voice
- MAC Based VLAN
- Subnet Based VLAN
- Protocol Based VLAN

## 5.8.1 VLAN Global

[ Switching > 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 16.

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.

## 5.8.2 VLAN Configuration

[ Switching > 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:
  - *MRP*: If you assign to the ring ports a non-existing VLAN, then the device creates this VLAN.
  - *MVRP*: The device creates a VLAN based on the messages of neighboring devices.
  - *Routing*: The device creates a VLAN for every router interface.

**Note:** The settings are effective only if the VLAN Unaware Mode is disabled. See the *Switching* > Global dialog.

### Table

VLAN ID

ID of the VLAN.

The device supports up to 512 VLANs simultaneously set up.

Possible values:
- `1..4042`

Status

Displays how the VLAN is set up.

Possible values:
- *`other`*
  VLAN `1`
  or
  VLAN set up using the *802.1X Port Authentication* function. See the *Network Security > 802.1X Port Authentication* dialog.
- *`permanent`*
  VLAN set up by the user.
  or
  VLAN set up using the *MRP* function. See the *Switching > L2-Redundancy > MRP* dialog.
  If you save the changes in the non-volatile memory, then the VLANs with this setting remain set up after a restart.
- *`dynamicMvrp`*
  VLAN set up using the *MVRP* function. See the *Switching > MRP-IEEE > MVRP* dialog.
  VLANs with this setting are write-protected. The device removes a VLAN from the table as soon as the last port leaves the VLAN.

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.
  Additionally, the device helps prevent the port from becoming a VLAN member through the *MVRP* function.
- `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 16.

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

In the *VLAN ID* field, you specify the ID of the VLAN.

## 5.8.3 VLAN Port

[ Switching > 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 if the VLAN Unaware mode is disabled 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.

**Note:** The settings are effective only if the VLAN Unaware Mode is disabled. See the *Switching > Global* dialog.

### Table

Port

Displays the port number.

Port-VLAN ID

Specifies the ID of the VLAN which the device assigns to data packets without a VLAN tag.

Prerequisites:
- In the *Acceptable packet types* column, you specify the value `admitAll`.

Possible values:
- ID of a VLAN you set up (default setting: `1`)

If you use the *MRP* function and you did not assign a VLAN to the ring ports, then you specify the value `1` here for the ring ports. Otherwise, the device assigns the value to the ring ports automatically.

Acceptable packet types

Specifies if the port transmits or discards received data packets without a VLAN tag.

Possible values:
- `admitAll` (default setting)
  The port accepts data packets both with and without a VLAN tag.
- `admitOnlyVlanTagged`
  The port accepts only data packets tagged with a VLAN ID ≥ `1`.

Ingress filtering

Activates/deactivates the ingress filtering.

Possible values:

- `marked`
  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` (default setting)
  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 16.

# 5.8.4 VLAN Voice

[ Switching > VLAN > Voice ]

Use the Voice VLAN feature to separate voice and data traffic on a port, by VLAN and/or priority. A primary benefit of Voice VLAN is safeguarding the quality of voice traffic when data traffic on the port is high.

The device detects VoIP phones using the Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED). The device then adds the appropriate port to the member set of the configured Voice VLAN. The member set is either tagged or untagged. Tagging depends on the Voice VLAN interface mode (VLAN ID, Dot1p, None, Untagged).

Another benefit of the Voice VLAN feature is that the VoIP phone obtains VLAN ID or priority information via LLDP-MED from the device. As a result, the VoIP phone sends voice data tagged as priority, or untagged. This depends on the configured Voice VLAN Interface mode. You activate Voice VLAN on the port which is connecting to the VoIP phone.

### Operation

Operation

Enables/disables the *VLAN Voice* function of the device globally.

Possible values:

- *On*
- *Off* (default setting)

### Table

Port

Displays the port number.

Voice VLAN mode

Specifies if the port transmits or discards received data packets without voice VLAN tagging or with voice VLAN priority information.

Possible values:

- *disabled* (default setting)
  Deactivates the *VLAN Voice* function for this table entry.
- *none*
  Lets the IP telephone use its own configuration for sending untagged voice traffic.
- *vlan/dot1p-priority*
  The port filters data packets of the voice VLAN using the vlan and dot1p priority tags.
- *untagged*
  The port filters data packets without a voice VLAN tag.

- *vlan*
  The port filters data packets of the voice VLAN using the vlan tag.
- *dot1p-priority*
  The port filters data packets of the voice VLAN using the dot1p priority tags. If you select this value, then additionally specify a proper value in the *Priority* column.

Data priority mode

Specifies the trust mode for the data traffic on the particular port.

The device uses this mode for data traffic on the voice VLAN, when it detects a VoIP telephone and a PC and when these devices use the same cable for transmitting and receiving data.

Possible values:

- *trust* (default setting)
  If voice traffic is present on the interface, then the data traffic uses the normal priority with this setting.
- *untrust*
  If voice traffic is present and the *Voice VLAN mode* is set to *dot1p-priority*, then the data has the priority 0. If the interface only transmits data, then the data has the normal priority.

Status

Displays the status of the Voice VLAN on the port.

Possible values:

- marked
  The Voice VLAN is enabled.
- unmarked
  The Voice VLAN is disabled.

VLAN ID

Specifies the ID of the VLAN to which the table entry applies.

To forward traffic to this VLAN ID using this filter, select in the *Voice VLAN mode* column the value *vlan*.

Possible values:

- 0..4042

Priority

Specifies the Voice VLAN Priority of the port.

Prerequisites:

- In the *Voice VLAN mode* column, you specify the value *dot1p-priority*.

Possible values:

- *0..7*
- *none*
  Deactivates the Voice VLAN Priority of the port.

Bypass authentication

Activates the Voice VLAN Authentication mode.

If you deactivate the function and set the value in the *Voice VLAN mode* column to `dot1p-priority`, then voice devices require an authentication.

Possible values:

- `marked` (default setting)
  If you activated the function in the *Network Security > 802.1X Port Authentication > Global* dialog, then set the *Port control* parameter for this port to the `multiClient` value before activating this function. You find the *Port control* parameter in the *Network Security > 802.1X Port Authentication > Global* dialog.
- `unmarked`

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 5.8.5 MAC Based VLAN

[ Switching > VLAN > MAC Based VLAN ]

In a MAC-based VLAN, the device forwards traffic based on the source MAC address associated with a VLAN. User-defined filters determine if a packet belongs to a particular VLAN.

MAC-based VLANs specify the filtering criteria only for untagged or priority-tagged packets. Assign a port to a MAC-based VLAN for a specific source MAC address. The device then forwards untagged packets received with the configured MAC address to the MAC-based VLAN ID. Other untagged packets are subject to normal VLAN classification rules.

### Table

MAC address

Displays the MAC address to which the table entry relates.

The device supports up to 256 simultaneous MAC-based VLAN assignments.

Possible values:

- Valid MAC address

VLAN ID

Displays the ID of the VLAN to which the table entry applies.

Possible values:

- `1..4042` (set up VLAN IDs)

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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

- In the *MAC address* field, you specify the MAC address.
- In the *VLAN ID* field, you specify the ID of the VLAN.

# 5.8.6 Subnet Based VLAN

[ Switching > VLAN > Subnet Based VLAN ]

In IP subnet-based VLANs, the device forwards traffic based on the source IP address and subnet mask associated with the VLAN. User-defined filters determine if a packet belongs to a particular VLAN.

IP subnet-based VLANs specify the filtering criteria only for untagged packets or priority tagged packets. Assign a port to an IP subnet-based VLAN for a specific source address. The device then forwards untagged packets received with the configured address to the IP subnet-based VLAN ID.

To configure an IP subnet based VLAN, specify an IP address, a subnet mask, and the corresponding VLAN identifier. When multiple entries apply, the device uses the entry with the longest prefix first.

### Table

IP address

Displays the IP address to which you assign the subnetwork based VLAN.

The device supports up to 256 VLANs set up simultaneously to subnetwork based VLANs.

Possible values:

- Valid IP address

Netmask

Displays the netmask to which you assign the subnetwork based VLAN.

Possible values:

- Valid IP netmask

VLAN ID

Displays the VLAN ID.

Possible values:

- `1..4042`

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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

- In the *IP address* field, you specify the IP address.
- In the *Netmask* field, you specify the netmask.
- In the *VLAN ID* field, you specify the ID of the VLAN.

# 5.8.7 Protocol Based VLAN

[ Switching > VLAN > Protocol Based VLAN ]

In a protocol-based VLAN, specified ports bridge traffic based on the L3 protocol (Ethertype) associated with the VLAN. User-defined packet filters determine if a packet belongs to a particular VLAN.

Protocol-based VLANs specify the filtering criteria only for untagged packets. Assign a port to a protocol-based VLAN for a specific protocol. The device then forwards untagged packets received with the configured protocol to the protocol-based VLAN ID. The device assigns other untagged packets with the port VLAN ID.

**Table**

Group ID

Displays the group identifier of the protocol-based VLAN entry.

The device supports up to 128 protocol-based VLAN associations simultaneously.

Possible values:

- `1..128`

Name

Specifies the group name of the protocol-based VLAN entry.

Possible values:

- Alphanumeric ASCII character string with 1..16 characters

VLAN ID

Specifies the ID of the VLAN.

Possible values:

- `1..4042`

Port

Specifies the ports that are assigned to the group.

Possible values:

- `<Port number>`
  In the drop-down list, select the ports.

Ethertype

Specifies the Ethertype value assigned to the VLAN.

The Ethertype is a two-octet field in an Ethernet packet to indicate which protocol the payload contains.

Possible values:

- `0x0600..0xFFFF`
  Ethertype as a hexadecimal number sequence
  When you enter a decimal value, the device converts the value into a hexadecimal number sequence when you click the *Add* button.
- `ip`
  Ethertype keyword for IPv4 (equivalent to `0x0800`)
- `arp`
  Ethertype keyword for ARP (equivalent to `0x0806`)
- `ipx`
  Ethertype keyword for IPX (equivalent to `0x8137`)

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 5.9 L2-Redundancy

[ Switching > L2-Redundancy ]

The menu contains the following dialogs:

- MRP
- HIPER Ring
- Spanning Tree
- Link Aggregation
- Link Backup
- FuseNet

# 5.9.1 MRP

[ Switching > L2-Redundancy > MRP ]

The Media Redundancy Protocol (MRP) is a protocol that lets you set up high-availability, ring-shaped network structures. An MRP ring with Hirschmann devices is made up of up to 100 devices that support the MRP protocol according to IEC 62439.

If a section fails, then the ring structure of an MRP ring changes back into a line structure. The maximum recovery time can be configured.

The Ring Manager function of the device closes the ends of a backbone in a line structure to a redundant ring.

**Note:** *Spanning Tree* and Ring Redundancy have an effect on each other. Deactivate the *Spanning Tree* protocol for the ports connected to the MRP ring. See the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.

When you work with oversized Ethernet packets (the value in the *MTU* column for the port is > `1518`, see the *Basic Settings > Port* dialog), the switching time of the MRP ring reconfiguration depends on the following parameters:

- Bandwidth of the ring line
- Size of the Ethernet packets
- Number of devices in the ring

Set the recovery time sufficiently large to help avoid delays in the MRP packages due to latencies in the devices. You can find the formula for calculating the switching time in IEC 62439-2, section 9.5.

### Operation

Operation

Enables/disables the *MRP* function.

After you configured the parameters for the MRP ring, enable the function here.

Possible values:

- `On`
  The *MRP* function is enabled.
  After you configured the devices in the MRP ring, the redundancy is active.
- `Off` (default setting)
  The *MRP* function is disabled.

### Ring port 1/Ring port 2

Port

Specifies the number of the port that is operating as a ring port.

Possible values:

- `<Port number>`
  Number of the ring port

Operation

Displays the operating status of the ring port.

Possible values:

- *forwarding*
  The port is enabled, connection exists.
- *blocked*
  The port is blocked, connection exists.
- *disabled*
  The port is disabled.
- *not-connected*
  No connection exists.

Fixed backup

Activates/deactivates the backup port function for the *Ring port 2*.

**Note:** The switch over to the primary port can exceed the maximum ring recovery time.

Possible values:

- `marked`
  The *Ring port 2* backup function is active. When the ring is closed, the ring manager reverts back to the primary ring port.
- `unmarked` (default setting)
  The *Ring port 2* backup function is inactive. When the ring is closed, the ring manager continues to send data on the secondary ring port.

### Configuration

Ring manager

Enables/disables the *Ring manager* function.

If there is one device at each end of the line, then you activate this function.

Possible values:

- *On*
  The *Ring manager* function is enabled.
  The device operates as a ring manager.
- *Off* (default setting)
  The *Ring manager* function is disabled.
  The device operates as a ring client.

Advanced mode

Activates/deactivates the advanced mode for fast recovery times.

Possible values:

- `marked` (default setting)
  Advanced mode active.
  MRP-capable Hirschmann devices support this mode.
- `unmarked`
  Advanced mode inactive.
  Select this setting if another device in the ring does not support this mode.

Ring recovery

Specifies the maximum recovery time in milliseconds for reconfiguration of the ring. This setting is effective if the device operates as a ring manager.

Possible values:

- *500ms*
- *200ms* (default setting)

Shorter switching times make greater demands on the response time of every individual device in the ring. Use values lower than *500ms* if the other devices in the ring also support this shorter recovery time.

When you are working with oversized Ethernet packets, the number of devices in the ring is limited. Note that the switching time depends on several parameters. See the description above.

VLAN ID

Specifies the ID of the VLAN which you assign to the ring ports.

Possible values:

- `0` (default setting)
  No VLAN assigned.
  Assign in the *Switching > VLAN > Configuration* dialog to the ring ports for VLAN `1` the value `U`.
- `1..4042`
  VLAN assigned.
  If you assign to the ring ports a non-existing VLAN, then the device creates this VLAN. In the *Switching > VLAN > Configuration* dialog, the device creates an entry in the table for the VLAN and assigns the value `T` to the ring ports.

### Information

Information

Displays messages for the redundancy configuration and the possible causes of errors.

When the device operates as a ring client or a ring manager, the following messages are possible:

- *Redundancy available*
  The redundancy is set up. When a component of the ring is down, the redundant line takes over its function.
- *Configuration error: Error on ringport link.*
  Error in the cabling of the ring ports.

When the device operates as a ring manager, the following messages are possible:

- *Configuration error: Packets from another ring manager received.*
  Another device exists in the ring that operates as the ring manager.
  Enable the *Ring manager* function only on one device in the ring.
- *Configuration error: Ring link is connected to wrong port.*
  A line in the ring is connected with a different port instead of with a ring port. The device only receives test data packets on one ring port.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Delete ring configuration

Disables the redundancy function and resets the settings in the dialog to the default setting.

## 5.9.2 HIPER Ring

[ Switching > L2-Redundancy > HIPER Ring ]

The concept of HIPER ring redundancy enables the construction of high-availability, ring-shaped networks. This device provides a HIPER ring client. This function lets you extend an existing HIPER ring or to replace a device already participating as a client in a HIPER ring.

A HIPER ring contains a Ring Manager (RM) which controls the ring. The RM sends watchdog packets into the ring on both the primary and secondary ports. When the RM receives the watchdog packets on both ports, the primary port remains in the forwarding state and the secondary port remains in the discarding state.

The device operates only in the ring client mode. This means that the device is able to recognize and forward the watchdog packets on the ring ports and can also forward the change in link status to the RM for example, LinkDown and LinkUp packets.

The device only supports Fast Ethernet and Gigabit Ethernet ports as ring ports. Furthermore, the device only supports HIPER ring in VLAN `1`.

**Note:** *Spanning Tree* and Ring Redundancy have an effect on each other. Deactivate the *Spanning Tree* protocol for the ports connected to the HIPER ring. See the *Switching* > *L2-Redundancy* > Spanning Tree > *Port* dialog.

**Note:** Configure the devices of the HIPER ring individually. Before you connect the redundant link, complete the configuration of every device of the HIPER ring. You thus help avoid loops during the configuration phase.

### Operation

Operation

Enables/disables the *HIPER Ring* client.

Possible values:

- `On`
  The *HIPER Ring* client is enabled.
- `Off` (default setting)
  The *HIPER Ring* client is disabled.

### Ring port 1/Ring port 2

Port

Specifies the port number of the primary/secondary ring port.

Possible values:

- `-` (default setting)
  No primary/secondary ring port selected.
- `<Port number>`
  Number of the ring port

State

Displays the state of the primary/secondary ring port.

Possible values:

- *not-available*
  The *HIPER Ring* client is disabled.
  or
  No primary or secondary ring port selected.
- *active*
  The ring port is enabled and logically up.
- *inactive*
  The ring port is logically down.
  As soon as the link goes down on a ring port, the device sends a LinkDown packet to the Ring Manager on the other ring port.

**Information**

Mode

Displays that the device is able to operate in the ring client mode.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 16.

## 5.9.3 Spanning Tree

[ Switching > L2-Redundancy > Spanning Tree ]

The Spanning Tree Protocol (STP) is a protocol that deactivates redundant paths of a network in order to help avoid loops. If a network component becomes inoperable on the path, then the device calculates the new topology and reactivates these paths.

The Rapid Spanning Tree Protocol (RSTP) enables fast switching to a newly calculated topology without interrupting existing connections. RSTP gets average reconfiguration times of less than a second. When you use RSTP in a ring with 10 to 20 devices, you can get reconfiguration times in the order of milliseconds.

The device supports the Multiple Spanning Tree Protocol (MSTP) standardized in IEEE 802.1, which is a further development of the Spanning Tree Protocol (STP).

**Note:** When you connect the device to the network through twisted pair SFPs instead of through usual twisted pair ports, the reconfiguration of the network takes slightly longer.

The menu contains the following dialogs:

- Spanning Tree Global
- Spanning Tree MSTP
- Spanning Tree Port

# 5.9.3.1 Spanning Tree Global

[ Switching > L2-Redundancy > Spanning Tree > Global ]

In this dialog you enable/disable the *Spanning Tree* function and specify the bridge settings.

### Operation

Operation

Enables/disables the Spanning Tree function in the device.

Possible values:

- `On` (default setting)
- `Off`
  The device behaves transparently. The device floods received Spanning Tree data packets like multicast data packets to the ports.

### Variant

Variant

Specifies the protocol used for the *Spanning Tree* function:

Possible values:

- `rstp` (default setting)
  The protocol `RSTP` is active.
  With RSTP (IEEE 802.1Q-2005), the *Spanning Tree* function operates for the underlying physical layer.
- `mstp`
  The protocol `MSTP` is active.
  To help avoid longer recovery times, specify the maximum value `40` in the *Tx holds* field.

### Traps

Send trap

Activates/deactivates the sending of SNMP traps for the following events:

- Another bridge takes over the root bridge role.
- The topology changes. A port changes its *Port state* from *forwarding* into *discarding* or from *discarding* into *forwarding*.

Possible values:

- `marked`
  The sending of SNMP traps is active.
- `unmarked` (default setting)
  The sending of SNMP traps is inactive.

### Ring only mode

Active

Activates/deactivates the *Ring only mode* function, in which the device does not verify the age of the BPDUs.

Possible values:

- `marked`
  The *Ring only mode* function is active. Use this setting for applications for RSTP rings with diameters greater than 40.
- `unmarked` (default setting)
  The *Ring only mode* function is inactive.

First port

Specifies the port number of the first interface.

Possible values:

- `<Port number>` (default setting: `-`)

Second port

Specifies the port number of the second interface.

Possible values:

- `<Port number>` (default setting: `-`)

### Bridge configuration

Bridge ID

Displays the bridge ID of the device.

The device with the lowest bridge ID numerical value takes over the role of the root bridge in the network.

Possible values:

- `<Bridge priority> / <MAC address>`
  Value in the *Priority* field / MAC address of the device

Priority

Specifies the bridge priority of the device.

Possible values:

- `0..61440` in steps of 4096 (default setting: `32768`)

To make this device the root bridge, assign the lowest numeric priority value in the network to the device.

Hello time [s]

Specifies the time in seconds between the sending of two configuration messages (Hello data packets).

Possible values:

- `1..2` (default setting: `2`)

If the device takes over the role of the root bridge, then the other devices in the network use the value specified here.

Otherwise, the device uses the value specified by the root bridge. See the *Root information* frame.

Due to the interaction with the *Tx holds* parameter, we recommend that you do not change the default setting.

Forward delay [s]

Specifies the delay time for the status change in seconds.

Possible values:

- `4..30` (default setting: `15`)

If the device takes over the role of the root bridge, then the other devices in the network use the value specified here.

Otherwise, the device uses the value specified by the root bridge. See the *Root information* frame.

In the RSTP protocol, the bridges negotiate a status change without a specified delay.

The *Spanning Tree* protocol uses the parameter to delay the status change between the statuses *disabled*, *discarding*, *learning*, *forwarding*.

The parameters *Forward delay [s]* and *Max age* have the following relationship:

*Forward delay [s]* ≥ (*Max age*/2) + 1

If you enter values in the fields that contradict this relationship, then the device replaces these values with the last valid values or with the default value.

Max age

Specifies the maximum permitted branch length for example, the number of devices to the root bridge.

Possible values:

- `6..40` (default setting: `20`)

If the device takes over the role of the root bridge, then the other devices in the network use the value specified here.

Otherwise, the device uses the value specified by the root bridge. See the *Root information* frame.

The *Spanning Tree* protocol uses the parameter to specify the validity of STP-BPDUs in seconds.

Tx holds

Limits the maximum transmission rate for sending BPDUs.

Possible values:

- `1..40` (default setting: `10`)
  To help avoid longer recovery times when using the `MSTP` protocol, set the maximum value to `40`.

When the device sends a BPDU, the device increments a counter on this port.

If the counter reaches the value specified here, then the port stops sending BPDUs. On the one hand, this reduces the load generated by RSTP, and on the other when the device does not receive BPDUs, a communication interruption can be caused.

The device decrements the counter by `1` every second. In the following second, the device sends a maximum of `1` new BPDU.

BPDU guard

Activates/deactivates the BPDU Guard function in the device.

With this function, the device helps protect your network from incorrect configurations, attacks with STP-BPDUs, and unwanted topology changes.

Possible values:

- `marked`
  The *BPDU guard* is active.
  - The device applies the function to manually specified edge ports. For these ports, in the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *CIST* tab the checkbox in the *Admin edge port* column is marked.
  - If an edge port receives an STP-BPDU, then the device disables the port. For this port, in the *Basic Settings > Port* dialog, *Configuration* tab the checkbox in the *Port on* column is `unmarked`.
- `unmarked` (default setting)
  The *BPDU guard* is inactive.

To reset the status of the port to the value *`forwarding`*, you proceed as follows:

- ☐ If the port is still receiving BPDUs, then:
  - In the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *CIST* tab unmark the checkbox in the *Admin edge port* column.
    or
  - In the *Switching > L2-Redundancy > Spanning Tree > Global* dialog, unmark the *BPDU guard* checkbox.
- ☐ To re-enable the port again you use the *Auto-Disable* function. Alternatively, proceed as follows:
  - Open the *Basic Settings > Port* dialog, *Configuration* tab.
  - Mark the checkbox in the *Port on* column.

BPDU filter (all admin edge ports)

Activates/deactivates the STP-BPDU filter on every manually specified edge port. For these ports, in the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *CIST* tab the checkbox in the *Admin edge port* column is marked.

Possible values:

- `marked`
  The BPDU filter is active on every edge port.
  The function does not use these ports in *Spanning Tree* operations.
  - The device does not send STP-BPDUs on these ports.
  - The device drops any STP-BPDUs received on these ports.
- `unmarked` (default setting)
  The global BPDU filter is inactive.
  You have the option to explicitly activate the BPDU filter for single ports. See the *Port BPDU filter* column in the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.

Auto-disable

Activates/deactivates the *Auto-Disable* function for the parameters that *BPDU guard* is monitoring on the port.

Possible values:

- `marked`
  The *Auto-Disable* function for the *BPDU guard* is active.
  - When the port receives an STP-BPDU, the device disables an edge port. The “Link status” LED for the port flashes 3× per period.
  - The *Diagnostics > Ports > Auto-Disable* dialog displays which ports are currently disabled due to the parameters being exceeded.
  - The *Auto-Disable* function reactivates the port automatically. For this you go to the *Diagnostics > Ports > Auto-Disable* dialog and specify a waiting period for the relevant port in the *Reset timer [s]* column.
- `unmarked` (default setting)
  The *Auto-Disable* function for the *BPDU guard* is inactive.

### Root information

Bridge ID

Displays the bridge ID of the current root bridge.

Possible values:

- `<Bridge priority> / <MAC address>`

Priority

Displays the bridge priority of the current root bridge.

Possible values:

- `0..61440` in steps of 4096

Hello time [s]

Displays the time in seconds that the root bridge specifies between the sending of two configuration messages (Hello data packets).

Possible values:

- `1..2`

The device uses this specified value. See the *Bridge configuration* frame.

Forward delay [s]

Specifies the delay time in seconds set up by the root bridge for status changes.

Possible values:

- `4..30`

The device uses this specified value. See the *Bridge configuration* frame.

In the RSTP protocol, the bridges negotiate a status change without a specified delay.

The *Spanning Tree* protocol uses the parameter to delay the status change between the statuses *disabled*, *discarding*, *learning*, *forwarding*.

Max age

Specifies the maximum permitted branch length that the root bridge sets up for example, the number of devices to the root bridge.

Possible values:

- `6..40` (default setting: `20`)

The *Spanning Tree* protocol uses the parameter to specify the validity of STP-BPDUs in seconds.

### Topology information

Bridge is root

Displays if the device currently has the role of the root bridge.

Possible values:

- `marked`
  The device currently has the role of the root bridge.
- `unmarked`
  Another device currently has the role of the root bridge.

Root port

Displays the number of the port from which the current path leads to the root bridge.

If the device takes over the role of the root bridge, then the field displays the value `0`.

Root path cost

Specifies the path cost for the path that leads from the root port of the device to the root bridge of the layer 2 network.

Possible values:

- `0..200000000`
  If the value `0` is specified, then the device takes over the role of the root bridge.

Topology changes

Displays how many times the device has put a port into the *`forwarding`* status using the *Spanning Tree* function since the *Spanning Tree* instance was started.

Time since topology change

Displays the time since the last topology change.

Possible values:

- `<days, hours:minutes:seconds>`

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 5.9.3.2 Spanning Tree MSTP

[ Switching > L2-Redundancy > Spanning Tree > MSTP ]

In this dialog you manage the settings of the global and local MST instances.

In contrast to the local MST instances, the global MST instance is configured permanently in the device. The global MST instance contains the VLANs that are not explicitly allocated to a local MST instance.

The device supports up to 31 local MST instances. To create a local MST instance, click the button.

While STP has a single Spanning Tree spanning the network, MSTP lets you set up one Spanning Tree per VLAN or group of VLANs. Thus it is possible to specify several smaller Spanning Trees covering one network.

How to help avoid longer convergence times:
- Only use devices in the network that support RSTP or MSTP.
- Adjust the following parameters to the topology and number of bridges:
  - Maximum allowed number of devices to the root bridge
    *Switching > L2-Redundancy > Spanning Tree > Global* dialog, *Max age* field
  - Maximum allowed number of bridges within the MST region in a branch to the root bridge
    *Switching > L2-Redundancy > Spanning Tree > MSTP* dialog, *Global CIST parameter* frame, *Hops (max.)* field

For bridges in an MST region, specify identical values for the following parameters:
- *Name* of the MST region
- *Revision level* of the MST region
- Allocation of the VLANs to the MST instances
  - Include ports connecting the bridges of an MST region as members in the VLANs set up on the bridges. The ports are to transmit the data packets with a VLAN tag. You thus help avoid potential connection breaks within the MST region when the topology is changed.
  - Include ports connecting an MST region with other MST regions or with the CST region (boundary ports) as members in the VLANs set up in both regions. The ports are to transmit the data packets with a VLAN tag. You thus help avoid potential connection breaks when topology changes affecting the boundary ports are made.

### MST region identifier

Name

Specifies the name of the MST region to which the device belongs.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters

Revision level

Specifies the version number of the MST region to which the device belongs.

Possible values:

- `0..65535` (default setting: `1`)

Checksum

Displays the MD5 checksum of the MST configuration.

### Global CIST parameter

Hops (max.)

Specifies the maximum number of bridges within the MST region in a branch to the root bridge.

Possible values:

- `6..40` (default setting: `20`)

Attached VLANs

Displays the IDs of the VLANs that are assigned only to the global MST instance and to no other local MST instance.

Possible values:

- `ID of the statically configured VLANs`
  (default setting: `1`)

Bridge ID

Displays the bridge ID of the device.

Possible values:

- `<Bridge priority> / <MAC address>`
  The value is made up as follows:
  - Value in the *Priority* field. See the *Switching > L2-Redundancy > Spanning Tree > Global* dialog, *Bridge configuration* frame.
  - MAC address of the device.

Root ID

Displays the bridge ID of the current CIST root bridge of the whole Layer 2 network.

Possible values:

- `<Bridge priority> / <MAC address>`

The device with the numerically lowest bridge ID takes over the role of the CIST root bridge in the network. The following devices are able to take over the role of the root bridge:

- Bridges not belonging to any MST region
- Bridges belonging to the global instance of an MST region

In the whole Layer 2 network, the bridges use the time settings of the CIST root bridge, for example *Hello time [s]*.

Regional root ID

Displays the Bridge ID of the current root bridge that belongs to the global instance of the MST region to which this device belongs.

Possible values:

- `<Bridge priority> / <MAC address>`

The values in the *Regional root ID* and *Root ID* fields are identical when the regional root bridge has the lowest bridge ID in the whole Layer 2 network.

Root port

Displays the port of the device from which the path leads to the current CIST root bridge of the whole Layer 2 network.

Possible values:

- `no Port`
  The device currently has the role of the root bridge.
- `<Port number>`
  The path to the current CIST root bridge of the whole Layer 2 network leads over this port.

Root path cost

Displays the path cost for the path that leads from the regional root bridge of the MST region to the current CIST root bridge of the whole Layer 2 network.

Possible values:

- `0..200000000`
  If the value `0` is specified, then the regional root bridge simultaneously has the role of the CIST root bridge.
  For the devices within an MST region, the *Root path cost* values are identical.

If you do not use MSTP, then the *Root path cost* values are identical to the root path costs of Spanning Tree or Rapid Spanning Tree. In this case, every device considers itself as an own region.

Internal root path cost

Displays the internal path cost for the path that leads from the root port of the device to the current regional root bridge of the MST region.

Possible values:

- `0..200000000`
  If the value `0` is specified, then the local bridge simultaneously has the role of the current regional root bridge.

**Table**

MSTI

Displays the instance number of the local MST instance.

Attached VLANs

Displays the IDs of the VLANs that are allocated to this local MST instance.

Priority

Specifies the bridge priority of the local MST instance.

Possible values:

- `0..61440` in steps of 4096 (default setting: `32768`)

Assign the lowest numeric priority in this local MST instance to the device to make this device the root bridge.

Bridge ID

Displays the bridge ID.

The device with the numerically lowest bridge ID takes over the role of the MSTI (regional) root bridge in the instance.

Possible values:

- `<Bridge priority + Number of the instance> / <MAC address>`
  Sum of the value in the *Priority* and *MSTI* fields / MAC address of the device.

Time since topology change

Displays the time that has elapsed since the last topology change within this instance.

Topology changes

Displays how many times the device has put a port into the *`forwarding`* status using the *Spanning Tree* function since the *Spanning Tree* instance was started.

Topology change

Displays if the device has detected a topology change within the instance.

Possible values:

- `marked`
  The device has detected a topology change.
- `unmarked`
  The device has not detected a topology change.

Root ID

Displays the bridge ID of the current root bridge in this instance.

Possible values:

- `<Bridge ID> / <MAC address>`

Root path cost

Displays the path cost for the path that leads from the root port of the device to the root bridge of the instance.

Possible values:

- `0..200000000`
  If the value `0` is specified, then the bridge is simultaneously the root bridge of the instance.

Root port

Displays the port of the device from which the current path leads to the root bridge of the instance.

Possible values:

- `no Port`
  The device currently has the role of the root bridge.
- `<Port number>`
  The path to the current root bridge of the instance leads over this port.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Adds a new table entry.

The device supports up to local 16 instances.

Configure VLANs

Opens the *Configure VLANs* dialog to allocate VLANs to the local MST instance which is highlighted in the table.

# 5.9.3.3 Spanning Tree Port

[ Switching > L2-Redundancy > Spanning Tree > Port ]

In this dialog you activate the Spanning Tree function on the ports, specify edge ports, and specify the settings for various protection functions.

The dialog contains the following tabs:
- [CIST]
- [Guards]
- [MSTI<MSTI>]

## [CIST]

In this tab you have the option to activate the Spanning Tree function on the ports individually, specify the settings for edge ports, and view the current values. The abbreviation CIST stands for Common and Internal Spanning Tree.

**Note:** Deactivate the *Spanning Tree* function on the ports that are participating in other Layer 2 redundancy protocols. Otherwise, it is possible that the redundancy protocols operate differently than intended. This can cause loops.

### Table

Port

Displays the port number.

STP active

Activates/deactivates the Spanning Tree function on the port.

Possible values:

- `marked` (default setting)
  The *Spanning Tree* function is active on the port.
- `unmarked`
  The *Spanning Tree* function is inactive on the port.
  If the *Spanning Tree* function is enabled in the device and inactive on the port, then the port does not send STP-BPDUs and drops any STP-BPDUs received.

Port state

Displays the transmission status of the port.

Possible values:

- *discarding*
  The port is blocked and forwards only STP-BPDUs.
- *learning*
  The port is blocked, but it learns the MAC addresses of received data packets.
- *forwarding*
  The port forwards data packets.

- *disabled*
  The port is inactive. See the *Basic Settings > Port* dialog, *Configuration* tab.
- *manualFwd*
  The *Spanning Tree* function is disabled on the port. The port forwards STP-BPDUs.
- *notParticipate*
  The port is not participating in STP.

Port role

Displays the current role of the port in CIST.

Possible values:

- *root*
  Port with the cheapest path to the root bridge.
- *alternate*
  Port with the alternative path to the root bridge (currently blocking).
- *designated*
  Port for the side of the tree averted from the root bridge (currently blocking).
- *backup*
  Port receives STP-BPDUs from its own device.
- *master*
  Port with the cheapest path to the CIST. The port is the CIST root port of the CIST Regional Root. The port is unique in an MST region.
- *disabled*
  The port is inactive. See the *Basic Settings > Port* dialog, *Configuration* tab.

Port path cost

Specifies the path costs of the port.

Possible values:

- `0..200000000` (default setting: `0`)

When the value is `0`, the device automatically calculates the path costs depending on the data rate of the port.

Port priority

Specifies the priority of the port.

Possible values:

- `16..240` in steps of 16 (default setting: `128`)

This value represents the first 4 bits of the port ID.

Received bridge ID

Displays the bridge ID of the device from which this port last received an STP-BPDU.

Possible values:

- For ports with the *designated* role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the possible STP problems in the network.
- For the *alternate*, *backup*, *master*, and *root* port roles, in the stationary condition (static topology) this information is identical to the information of the *designated* port role.
- If a port has no connection or if it did not receive any STP-BDPUs yet, then the device displays the values that the port can send with the *designated* role.

Received port ID

Displays the port ID of the device from which this port last received an STP-BPDU.

Possible values:

- For ports with the *designated* role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the possible STP problems in the network.
- For the *alternate*, *backup*, *master*, and *root* port roles, in the stationary condition (static topology) this information is identical to the information of the *designated* port role.
- If a port has no connection or if it did not receive any STP-BDPUs yet, then the device displays the values that the port can send with the *designated* role.

Received path cost

Displays the path cost that the higher-level bridge has from its root port to the root bridge.

Possible values:

- For ports with the *designated* role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the possible STP problems in the network.
- For the *alternate*, *backup*, *master*, and *root* port roles, in the stationary condition (static topology) this information is identical to the information of the *designated* port role.
- If a port has no connection or if it did not receive any STP-BDPUs yet, then the device displays the values that the port can send with the *designated* role.

Received path cost

Displays the path cost that the higher-level bridge has from its root port in the local MST instance to the root bridge.

Admin edge port

Activates/deactivates the *Admin edge port* mode. If the port is connected to an end device, then use the *Admin edge port* mode. This setting lets the edge port change faster to the forwarding state after linkup and thus a faster accessibility of the end device.

Possible values:

- `marked`
  The *Admin edge port* mode is active.
  The port is connected to an end device.
  - After the connection is set up, the port changes to the *`forwarding`* status without changing to the *`learning`* status beforehand.
  - If the port receives an STP-BPDU and the BPDU Guard function is active, then the device deactivates the port. See the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- `unmarked` (default setting)
  The *Admin edge port* mode is inactive.
  The port is connected to another STP bridge.
  After the connection is set up, the port changes to the *`learning`* status before changing to the *`forwarding`* status, if applicable.

Auto edge port

Activates/deactivates the automatic detection of whether you connect an end device to the port. The prerequisite is that the checkbox in the *Admin edge port* column is `unmarked`.

Possible values:

- `marked` (default setting)
  The automatic detection is active.
  After the installation of the connection and after 1.5 × *Hello time [s]*, the device sets the port to the *`forwarding`* status (default setting 1.5 × 2 s) if the port did not receive any STP-BPDUs during this time.
- `unmarked`
  The automatic detection is inactive.
  After the installation of the connection, and after *Max age* the device sets the port to the *`forwarding`* status.
  (default setting: 20 s)

Oper edge port

Displays if an end device or an STP bridge is connected to the port.

Possible values:

- `marked`
  An end device is connected to the port. The port does not receive any STP-BPDUs.
- `unmarked`
  An STP bridge is connected to the port. The port receives STP-BPDUs.

Oper PointToPoint

Displays if the port is connected to an STP device via a direct full-duplex link.

Possible values:

- `marked`
  The port is connected directly to an STP device via a full-duplex link. The direct, decentralized communication between 2 bridges enables short reconfiguration times.
- `unmarked`
  The port is connected in another way, for example via a half-duplex link or via a hub.

Port BPDU filter

Activates/deactivates the filtering of STP-BPDUs on the port explicitly.

The prerequisite is that the port is a manually specified edge port. For these ports, the checkbox in the *Admin edge port* column is marked.

Possible values:

- `marked`
  The BPDU filter is active on the port.
  The function excludes the port from *Spanning Tree* operations.
  - The device does not send STP-BPDUs on the port.
  - The device drops any STP-BPDUs received on the port.
- `unmarked` (default setting)
  The BPDU filter is inactive on the port.
  You have the option to globally activate the BPDU filter for every edge port. See the *Switching* > L2-Redundancy > *Spanning Tree* > *Global* dialog, *Bridge configuration* frame.
  If the *BPDU filter (all admin edge ports)* checkbox is marked, then the BPDU filter is still active on the port.

BPDU filter status

Displays if the BPDU filter is active on the port.

Possible values:

- `marked`
  The BPDU filter is active on the port as a result of the following settings:
  - The checkbox in the *Port BPDU filter* column is marked.
    and/or
  - The checkbox in the *BPDU filter (all admin edge ports)* column is marked. See the *Switching* > L2-Redundancy > *Spanning Tree* > *Global* dialog, *Bridge configuration* frame.
- `unmarked`
  The BPDU filter is inactive on the port.

BPDU flood

Activates/deactivates the *BPDU flood* mode on the port even if the *Spanning Tree* function is inactive on the port. The device floods STP-BPDUs received on the port to the ports for which the *Spanning Tree* function is inactive and the *BPDU flood* mode is active too.

Possible values:

- `marked`
  The *BPDU flood* mode is active.

- `unmarked` (default setting)
  The *BPDU flood* mode is inactive.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Guards]

This tab lets you specify the settings for various protection functions on the ports.

### Table

Port

Displays the port number.

Root guard

Activates/deactivates the monitoring of STP-BPDUs on the port. The prerequisite is that the *Loop guard* function is inactive.

With this setting the device helps you protect your network from incorrect configurations or attacks with STP-BPDUs that try to change the topology. This setting is relevant only for ports with the STP role *designated*.

Possible values:

- `marked`
  The monitoring of STP-BPDUs is active.
  - If the port receives an STP-BPDU with better path information to the root bridge, then the device discards the STP-BPDU and sets the status of the port to the value *discarding* instead of *root*.
  - If there are no STP-BPDUs with better path information to the root bridge, then the device resets the status of the port after 2 × *Hello time [s]*.
- `unmarked` (default setting)
  The monitoring of STP-BPDUs is inactive.

TCN guard

Activates/deactivates the monitoring of "Topology Change Notifications" on the port. With this setting the device helps you protect your network from attacks with STP-BPDUs that try to change the topology.

Possible values:

- `marked`
  The monitoring of "Topology Change Notifications" is enabled.
  - The port ignores the Topology Change flag in received STP-BPDUs.
  - If the received BPDU contains other information that causes a topology change, then the device processes the BPDU even if the TCN guard is enabled.
    Example: The device receives better path information for the root bridge.
- `unmarked` (default setting)
  The monitoring of "Topology Change Notifications" is disabled.
  If the device receives STP-BPDUs with a Topology Change flag, then the device deletes the address table of the port and forwards the Topology Change Notifications.

Loop guard

Activates/deactivates the monitoring of loops on the port. The prerequisite is that the *Root guard* function is inactive.

With this setting the device helps prevent loops if the port does not receive any more STP-BPDUs. Use this setting only for ports with the STP role *alternate*, *backup* or *root*.

Possible values:

- `marked`
  The monitoring of loops is active. This helps prevent loops for example, if you disable the Spanning Tree function on the remote device or if the connection is interrupted only in the receiving direction.
  - If the port does not receive any STP-BPDUs for a while, then the device sets the status of the port to the value *`discarding`* and marks the checkbox in the *Loop state* column.
  - If the port receives STP-BPDUs again, then the device sets the status of the port to a value according to *Port role* and unmarks the checkbox in the *Loop state* column.
- `unmarked` (default setting)
  The monitoring of loops is inactive.
  If the port does not receive any STP-BPDUs for a while, then the device sets the status of the port to the value *`forwarding`*.

### Loop state

Displays if the loop state of the port is inconsistent.

Possible values:

- `marked`
  The loop state of the port is inconsistent:
  - The port is not receiving any STP-BPDUs and the *Loop guard* function is enabled.
  - The device sets the state of the port to the value *`discarding`*. The device thus helps prevent any potential loops.
- `unmarked`
  The loop state of the port is consistent. The port receives STP-BPDUs.

### Trans. into loop

Displays how many times the loop state of the port became inconsistent (marked checkbox in the *Loop state* column).

### Trans. out of loop

Displays how many times the loop state of the port became consistent (unmarked checkbox in the *Loop state* column).

### BPDU guard effect

Displays if the port received an STP-BPDU as an edge port.

Prerequisite:

- The port is a manually specified edge port. In the *Port* dialog, the checkbox for this port in the *Admin edge port* column is `marked`.
- In the *Switching > L2-Redundancy > Spanning Tree > Global* dialog, the BPDU Guard function is active.

Possible values:

- `marked`
  The port is an edge port and received an STP-BPDU.
  The device deactivates the port. For this port, in the *Basic Settings > Port* dialog, *Configuration* tab the checkbox in the *Port on* column is `unmarked`.
- `unmarked`
  The port is an edge port and has not received any STP-BPDUs, or the port is not an edge port.

To reset the status of the port to the value *forwarding*, you proceed as follows:

- ☐ If the port is still receiving BPDUs, then:
  - In the *CIST* tab, unmark the checkbox in the *Admin edge port* column.
    or
  - In the *Switching > L2-Redundancy > Spanning Tree > Global* dialog, unmark the *BPDU guard* checkbox.
- ☐ To activate the port, proceed as follows:
  - Open the *Basic Settings > Port* dialog, *Configuration* tab.
  - Mark the checkbox in the *Port on* column.

### Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

## [MSTI<MSTI>]

This tab lets you specify the settings on the ports for path costs and priority in the local MST instance, and to view current values.

### Table

Port

Displays the port number.

Port state

Displays the transmission status of the port.

Possible values:

- *discarding*
  The port is blocked and forwards only STP-BPDUs.
- *learning*
  The port is blocked, but it learns the MAC addresses of received data packets.
- *forwarding*
  The port forwards data packets.
- *disabled*
  The port is inactive. See the *Basic Settings > Port* dialog, *Configuration* tab.
- *manualFwd*
  The *Spanning Tree* function is disabled on the port.
  The port forwards STP-BPDUs.
- *notParticipate*
  The port is not participating in STP.

Port role

Specifies the current role of the port in the local instance.

Possible values:

- *root*
  Port with the cheapest path to the root bridge.
- *alternate*
  Port with the alternative path to the root bridge (currently interrupted).
- *designated*
  Port for the side of the tree averted from the root bridge.
- *backup*
  Port which receives STP-BPDUs from its own device.
- *master*
  Port with the cheapest path to the CIST. The port is the CIST root port of the CIST Regional Root. The port is unique in an MST region.
- *disabled*
  The port is inactive. See the *Basic Settings > Port* dialog, *Configuration* tab.

Port path cost

Specifies the path costs of the port in the local instance.

Possible values:

- `0..200000000` (default setting: `0`)
  When the value is `0`, the device automatically calculates the path costs depending on the data rate of the port.

Port priority

Specifies the priority of the port in the local instance.

Possible values:

- `16..240` in steps of 16 (default setting: `128`)

Received bridge ID

Displays the bridge ID of the device from which this port last received an STP-BPDU in the local instance.

Received port ID

Displays the port ID of the device from which this port last received an STP-BPDU.

Possible values:

- For ports with the *designated* role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the possible STP problems in the network.
- For the *alternate*, *backup*, *master*, and *root* port roles, in the stationary condition (static topology) this information is identical to the information of the *designated* port role.
- If a port has no connection or if it did not receive any STP-BDPUs yet, then the device displays the values that the port can send with the *designated* role.

Received path cost

Displays the path cost that the higher-level bridge has from its root port to the root bridge.

Possible values:

- For ports with the *designated* role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the possible STP problems in the network.
- For the *alternate*, *backup*, *master*, and *root* port roles, in the stationary condition (static topology) this information is identical to the information of the *designated* port role.
- If a port has no connection or if it did not receive any STP-BDPUs yet, then the device displays the values that the port can send with the *designated* role.

### Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

## 5.9.4 Link Aggregation

[ Switching > L2-Redundancy > Link Aggregation ]

The *Link Aggregation* function lets you aggregate multiple parallel links. The prerequisite is that the links have the same speed and are full duplex. The advantages compared to conventional connections using a single line are higher availability and a higher transmission bandwidth.

The criteria for distributing the load to the parallel links are based on the *Hashing option* function.

The Link Aggregation Control Protocol (LACP) makes it possible to monitor the packet-based continuous link status on the physical ports. LACP also helps ensure that the link partners meet the aggregation prerequisites.

If the remote side does not support the Link Aggregation Control Protocol (LACP), then you can use the *Static link aggregation* function. In this case, the device aggregates the links based on the link, link speed and duplex setting.

### Configuration

Hashing option

Specifies which information the device uses to distribute the packets to the physical ports of the LAG interface. The device transmits packets containing the same distribution-relevant information over the same physical port to keep the packet order.

This setting overwrites the value specified in the *Hashing option* column for the port.

Possible values:

- *sourceMacVlan*
  The device uses the `Source MAC address`, `VLAN ID`, `EtherType` fields of the packet, and the physical ingress port.

- *destMacVlan*
  The device uses the Destination MAC address, VLAN ID, EtherType fields of the packet, and the physical ingress port.
- *sourceDestMacVlan* (default setting)
  The device uses the Source MAC address, Destination MAC address, VLAN ID, EtherType fields of the packet, and the physical ingress port.
- *sourceIPsourcePort*
  The device uses the Source IP address and Source TCP/UDP port fields of the packet.
- *destIPdestPort*
  The device uses the Destination IP address and Destination TCP/UDP port fields of the packet.
- *sourceDestIPPort*
  The device uses the Source IP address, Destination IP address, Source TCP/UDP port, and Destination TCP/UDP port fields of the packet.

### Table

Trunk port

Displays the LAG interface number.

Name

Specifies the name of the LAG interface.

Possible values:

- Alphanumeric ASCII character string with 1..15 characters

Link/Status

Displays the current operating state of the LAG interface and the physical ports.

Possible values:

- *up* (lag/… row)
  The LAG interface is operational.
  The prerequisites are:
  – The *Static link aggregation* function is active on this LAG interface.
    or
  – LACP is active on the physical ports assigned to the LAG interface, see the *LACP active* column.
    and
    The key specified for the LAG interface in the *LACP admin key* column matches the keys specified for the physical ports in the *LACP port actor admin key* column.
    and
    The number of operational physical ports assigned to the LAG interface is greater than or equal to the value specified in the *Active ports (min.)* column.
- *up*
  The physical port is operational.

- *down* (lag/… row)
  The LAG interface is down.
- *down*
  The physical port is disabled.
  or
  No cable connected or no active link.

Active

Activates/deactivates the LAG interface.

Possible values:

- marked (default setting)
  The LAG interface is active.
  Consider that the following protocols do not work properly on the physical ports when you activate the LAG interface:
  – *PTP*
- unmarked
  The LAG interface is inactive.

STP active

Activates/deactivates the *Spanning Tree* protocol on this LAG interface. The prerequisite is that you enable the *Spanning Tree* function globally in the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.

You can also activate/deactivate the *Spanning Tree* protocol on the LAG interfaces in the *Switching* > L2-Redundancy > *Spanning Tree* > *Port* dialog.

Possible values:

- marked (default setting)
  The *Spanning Tree* protocol is active on this LAG interface.
- unmarked
  The *Spanning Tree* protocol is inactive on this LAG interface.

Static link aggregation

Activates/deactivates the *Static link aggregation* function on the LAG interface. The device aggregates the assigned physical ports to the LAG interface, even if the remote site does not support LACP.

Possible values:

- marked
  The *Static link aggregation* function is active on this LAG interface. The device aggregates an assigned physical port to the LAG interface as soon as the physical port gets a link. The device does not send LACPDUs and discards received LACPDUs.
- unmarked (default setting)
  The *Static link aggregation* function is inactive on this LAG interface. If the connection was successfully negotiated using LACP, then the device aggregates an assigned physical port to the LAG interface.

Hashing option

Specifies which information the device uses to distribute the packets to the individual physical ports of the LAG interface. This setting has priority over the value selected in the *Configuration* frame, *Hashing option* drop-down list.

For further information on the values, see the description of the *Hashing option* drop-down list in the *Configuration* frame.

MTU

Specifies the maximum allowed size of Ethernet packets on the LAG interface in bytes. Any present VLAN tag is not taken into account.

This setting lets you increase the size of the Ethernet packets for specific applications.

Possible values:

- `1518..12288` (default setting: `1518`)
  With the value `1518`, the LAG interface transmits the Ethernet packets up to the following size:
  - 1518 bytes without VLAN tag
    (1514 bytes + 4 bytes CRC)
  - 1522 bytes with VLAN tag
    (1518 bytes + 4 bytes CRC)

Active ports (min.)

Specifies the minimum number of physical ports to be active for the LAG interface to stay active. If the number of active physical ports is lower than the specified value, then the device deactivates the LAG interface.

If a redundancy function like *Spanning Tree* or *MRP* over LAG is active in the device, then you use this function to force the device to switch automatically to the redundant line.

Possible values:

- `1` (default setting)
- `2`
- Depending on the hardware:
  `4`
  `8`
  `32`

Type

Displays if the LAG interface is based on the *Static link aggregation* function or on LACP.

Possible values:

- *`static`*
  The LAG interface is based on the *Static link aggregation* function.
- *`dynamic`*
  The LAG interface is based on LACP.

Send trap (Link up/down)

Activates/deactivates the sending of SNMP traps when the device detects a change in the link up/down status for this interface.

Possible values:

- `marked` (default setting)
  The sending of SNMP traps is active.
  If the device detects a link up/down status change, 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.

LACP admin key

Specifies the LAG interface key. The device uses this key to identify the ports that can be aggregated to the LAG interface.

Possible values:

- `0..65535`
  You specify the corresponding value for the physical ports in the *LACP port actor admin key* column.

Port

Displays the physical ports number assigned to the LAG interface.

Aggregation port status

Displays if the LAG interface aggregates the physical port.

Possible values:

- *`active`*
  The LAG interface aggregates the physical port.
- *`inactive`*
  The LAG interface does not aggregate the physical port.

LACP active

Activates/deactivates LACP on the physical port.

Possible values:

- `marked` (default setting)
  LACP is active on the physical port.
- `unmarked`
  LACP is inactive on the physical port.

LACP port actor admin key

Specifies the physical port key. The device uses this key to identify the ports that can be aggregated to the LAG interface.

Possible values:

- `0`
  The device ignores the key on this physical port when deciding to aggregate the port into the LAG interface.
- `1..65535`
  If this value matches the value of the LAG interface specified in the *LACP admin key* column, then the device only aggregates this physical port to the LAG interface.

LACP actor admin state

Specifies the actor state values that the LAG interface transmits in the LACPDUs. This lets you control the LACPDU parameters.

The device lets you mix the values. In the drop-down list, select one or more values.

Possible values:

- *ACT*
  (`LACP_Activity` state)
  When selected, the link transmits the LACPDUs cyclically, otherwise when requested.
- *STO*
  (`LACP_Timeout` state)
  When selected, the link transmits the LACPDUs cyclically using the short timeout, otherwise using the long timeout.
- *AGG*
  (`Aggregation` state)
  When selected, the device interprets the link as a candidate for aggregation, otherwise as an individual link.

For further information on the values, see the standard IEEE 802.1AX-2014.

LACP actor oper state

Displays the actor state values that the LAG interface transmits in the LACPDUs.

Possible values:

- *ACT*
  (`LACP_Activity` state)
  When visible, the link transmits the LACPDUs cyclically, otherwise when requested.
- *STO*
  (`LACP_Timeout` state)
  When visible, the link transmits the LACPDUs cyclically using the short timeout, otherwise using the long timeout.
- *AGG*
  (`Aggregation` state)
  When visible, the device interprets the link as a candidate for aggregation, otherwise as an individual link.
- *SYN*
  (`Synchronization` state)
  When visible, the device interprets the link as `IN_SYNC`, otherwise as `OUT_OF_SYNC`.

- *COL*
  (`Collecting` state)
  When visible, collection of incoming frames is enabled on this link, otherwise disabled.
- *DST*
  (`Distributing` state)
  When visible, distribution of outgoing frames is enabled on this link, otherwise disabled.
- *DFT*
  (`Defaulted` state)
  When visible, the link uses defaulted operational information, administratively specified for the Partner. Otherwise the link uses the operational information received from a LACPDU.
- *EXP*
  (`Expired` state)
  When visible, the link receiver is in the `EXPIRED` state.

LACP partner oper SysID

Displays the MAC address of the remote device connected to this physical port.

The LAG interface has received this information in a LACPDU from the partner.

LACP partner oper port

Displays the port number of the remote device connected to this physical port.

The LAG interface has received this information in a LACPDU from the partner.

LACP partner oper port state

Displays the partner state values that the LAG interface receives in the LACPDUs.

Possible values:

- *ACT*
- *STO*
- *AGG*
- *SYN*
- *COL*
- *DST*
- *DFT*
- *EXP*

For further information on the values, see the description of the *LACP actor oper state* column and the standard IEEE 802.1AX-2014.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Opens the *Create* window to add a new LAG interface entry to the table or to assign a physical port to a LAG interface.

- In the *Trunk port* drop-down list, you select the LAG interface number.
- In the *Port* drop-down list, you select the number of a physical port to assign to the LAG interface.

After you create a LAG interface, the device adds the LAG interface to the table in the *Basic Settings > Port* dialog, *Statistics*tab.

## 5.9.5 Link Backup

[ Switching > L2-Redundancy > Link Backup ]

With Link Backup, you configure pairs of redundant links. Each pair has a primary port and a backup port. The primary port forwards traffic until the device detects an error. If the device detects an error on the primary port, then the Link Backup function transfers traffic over to the backup port.

The dialog also lets you set a fail back option. If you enable the fail back function and the primary port returns to normal operation, then the device first blocks traffic on the backup port and then forwards traffic on the primary port. This process helps protect the device from causing loops in the network.

### Operation

Operation

Enables/disables the Link Backup function globally in the device.

Possible values:

- *On*
  Enables the Link Backup function.
- *Off* (default setting)
  Disables the Link Backup function.

### Table

Primary port

Displays the primary port of the interface pair. When you enable the Link Backup function, this port is responsible for forwarding traffic.

Possible values:

- Physical ports

Backup port

Displays the backup port on which the device forwards traffic if the device detects an error on the primary port.

Possible values:

- Physical ports except for the port you set as the primary port.

Description

Specifies the Link Backup pair. Enter a name to identify the Backup pair.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

Primary port status

Displays the status of the primary port for this Link Backup pair.

Possible values:

- *forwarding*
  The link is up, no shutdown, and forwarding traffic.
- *blocking*
  The link is up, no shutdown, and blocking traffic.
- *down*
  The port is either link down, cable unplugged, or disabled in software, shutdown.
- *unknown*
  The Link Backup feature is globally disabled, or the port pair is inactive. Therefore, the device ignores the port pair settings.

Backup port status

Displays the status of the Backup port for this Link Backup pair.

Possible values:

- *forwarding*
  The link is up, no shutdown, and forwarding traffic.
- *blocking*
  The link is up, no shutdown, and blocking traffic.
- *down*
  The port is either link down, cable unplugged, or disabled in the software, shutdown.
- *unknown*
  The Link Backup feature is globally disabled, or the port pair is inactive. Therefore, the device ignores the port pair settings.

Fail back

Activates/deactivates the automatic fail back.

Possible values:

- `marked` (default setting)
  The automatic fail back is active.
  After the delay timer expires, the backup port changes to *`blocking`* and the primary port changes to *`forwarding`*.
- `unmarked`
  The automatic fail back is inactive.
  The backup port continues forwarding traffic even after the primary port re-establishes a link or you manually change the admin status of the primary port from `shutdown` to `no shutdown`.

Fail back delay [s]

Specifies the delay time in seconds that the device waits after the primary port re-establishes a link. Furthermore, this timer also applies when you manually set the admin status of the primary port from `shutdown` to `no shutdown`. After the delay timer expires, the backup port changes to *`blocking`* and the primary port changes to *`forwarding`*.

Possible values:

- `0..3600` (default setting: `30`)
  When set to `0`, immediately after the primary port re-establishes a link, the backup port changes to *`blocking`* and the primary port changes to *`forwarding`*. Furthermore, immediately after you manually set the admin status of from `shutdown` to `no shutdown`, the backup port changes to *`blocking`* and the primary port changes to *`forwarding`*.

Active

Activates/deactivates the Link Back up pair configuration.

Possible values:

- `marked`
  The Link Backup pair is active. The device senses the link and administration status and forwards traffic according to the pair configuration.
- `unmarked` (default setting)
  The Link Backup pair is inactive. The ports forward traffic according to standard switching.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

**Create**

Primary port

Specifies the primary port of the backup interface pair. During normal operation this port is responsible for forwarding the traffic.

Possible values:

- Physical ports

Backup port

Specifies the backup port to which the device transfers the traffic to if the device detects an error on the primary port.

Possible values:

- Physical ports except for the port you set as the primary port.

## 5.9.6 FuseNet

[ Switching > L2-Redundancy > FuseNet ]

The *FuseNet* protocols let you couple rings that are operating with one of the following redundancy protocols:

- MRP
- HIPER Ring
- RSTP

**Note:** If you use the *Ring/Network Coupling* protocol to couple networks, then verify that the networks only contain Hirschmann devices.

Use the following table to select the *FuseNet* coupling protocol to be used in your network:

| Main Ring | Connected Network | | |
|---|---|---|---|
| | **MRP** | **HIPER ring** | **RSTP** |
| **MRP** | *Sub Ring*[1)] | *Redundant Coupling Protocol*<br>*Ring/Network Coupling* | *Redundant Coupling Protocol*<br>*Ring/Network Coupling* |
| **HIPER ring** | *Sub Ring* | *Ring/Network Coupling* | *Redundant Coupling Protocol*<br>*Ring/Network Coupling* |
| **RSTP** | *Redundant Coupling Protocol* | *Redundant Coupling Protocol* | – |

– no suitable coupling protocol

1) with *MRP* configured on different VLANs

The menu contains the following dialogs:

- Sub Ring
- Ring/Network Coupling
- Redundant Coupling Protocol

# 5.9.6.1 Sub Ring

[ Switching > L2-Redundancy > FuseNet > Sub Ring ]

This dialog lets you set up the device as a subring manager.

The *Sub Ring* function enables you to easily couple network segments to existing redundancy rings. The subring manager (SRM) couples a subring to an existing ring (base ring).

In the subring you can use any devices that support MRP as ring participants. These devices do not require a subring manager function.

When setting up subrings, remember the following rules:
- The device supports *Link Aggregation* in the subring
- No spanning tree on subring ports
- Same *MRP domain* on devices within a subring
- Different VLANs for base ring and subring

Specify the VLAN settings as follows:
- VLAN `X` for base ring
  - on the ring ports of the base ring participants
  - on the base ring ports of the subring manager
- VLAN `Y` for subring
  - on the ring ports of the subring participants
  - on the subring ports of the subring manager

**Note:** To help avoid loops, only close the redundant line when the settings are specified in every device participating in the ring.

### Operation

Operation

Enables/disables the *Sub Ring* function.

Possible values:

- `On`
  The *Sub Ring* function is enabled.
- `Off` (default setting)
  The *Sub Ring* function is disabled.

### Information

Table entries (max.)

Displays the maximum number of subrings supported by the device.

### Table

Sub ring ID

Displays the unique identifier of this subring.

Possible values:

- `1..20`

Name

Specifies the optional name of the subring.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

Active

Activates/deactivates the subring.

Activate the subring when the configuration of every subring device is complete. Close the subring only after activating the *Sub Ring* function.

Possible values:

- `marked`
  The subring is active.
- `unmarked` (default setting)
  The subring is inactive.

Configuration status

Displays the operational state of the subring configuration.

Possible values:

- *`noError`*
  The device detects an acceptable subring configuration.
- *`ringPortLinkError`*
  - The ring port has no link.
  - One of the subring lines is connected to one more port of the device. But the subring line is not connected to one of the ring ports of the device.
- *`multipleSRM`*
  The subring manager receives packets from more than one subring manager in the subring.
- *`noPartnerManager`*
  The subring manager receives its own frames.
- *`concurrentVLAN`*
  The MRP protocol in the base ring uses the VLAN of the subring manager domain.
- *`concurrentPort`*
  One more redundancy protocol uses the ring port of the subring manager domain.
- *`concurrentRedundancy`*
  The subring manager domain is inactive because of one more active redundancy protocol.

- *trunkMember*
  The ring port of the subring manager domain is member of a *Link Aggregation* connection.
- *sharedVLAN*
  The subring manager domain is inactive because shared VLAN is active and the main ring also uses the MRP protocol.

Redundancy available

Displays the operational state of the ring redundancy in the subring.

Possible values:

- *redGuaranteed*
  Redundancy reserve is available.
- *redNotGuaranteed*
  Loss of redundancy reserve.

Port

Specifies the port that connects the device to the subring.

Possible values:

- <Port number>

SRM mode

Specifies the mode of the subring manager.

A subring has 2 managers simultaneously that couple the subring to the base ring. As long as the subring is physically closed, one manager blocks its subring port.

Possible values:

- *manager* (default setting)
  The subring port forwards data packets.
  When this value is set on both devices that couple the subring to the base ring, the device with the higher MAC address functions as the *redundantManager*.
- *redundantManager*
  The subring port is blocked while the subring is physically closed. If the subring is interrupted, then the subring port transmits the data packets.
  When this value is set on both devices that couple the subring to the base ring, the device with the higher MAC address functions as the *redundantManager*.
- *singleManager*
  Use this value when the subring is coupled to the base ring via one single device. The prerequisite is that there are 2 instances of the subring in the table. Assign this value to both instances. The subring port of the instance with the higher port number is blocked while the subring is physically closed.

SRM status

Displays the current mode of the subring manager.

Possible values:

- *manager*
  The subring port forwards data packets.

- *redundantManager*
  The subring port is blocked while the subring is physically closed. If the subring is interrupted, then the subring port transmits the data packets.
- *singleManager*
  The subring is coupled to the base ring via one single device. The subring port of the instance with the higher port number is blocked while the subring is physically closed.
- *disabled*
  The subring is inactive.

Port status

Displays the connection status of the subring port.

Possible values:

- *forwarding*
  The port is passing frames according to the forwarding behavior of IEEE 802.1D.
- *disabled*
  The port is dropping every frame.
- *blocked*
  The port is dropping every frame with the exception of the following cases:
  - The port passes frames used by the selected ring protocol specified to pass blocked ports.
  - The port passes frames from other protocols specified to pass blocked ports.
- *not-connected*
  The port link is down.

VLAN

Specifies the VLAN to which this subring is assigned. If no VLAN exists under the VLAN ID entered, then the device automatically creates it.

Possible values:

- Available configured VLANs (default setting: `0`)
  If you do not want to use a separate VLAN for this subring, then you leave the entry as 0.

Partner MAC

Displays the MAC address of the subring manager at the other end of the subring.

MRP domain

Specifies the MRP domain of the subring manager. Assign the same MRP domain name to every member of a subring. If you only use Hirschmann devices, then you use the default value for the MRP domain; otherwise adjust this value if necessary. With multiple subrings, the function lets you use the same MRP domain name for the subrings.

Possible values:

- Permitted MRP domain names (default setting: 255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255)

Protocol

Specifies the protocol.

Possible values:

- *iec-62439-mrp*

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 5.9.6.2 Ring/Network Coupling

[ Switching > L2-Redundancy > FuseNet > Ring/Network Coupling ]

You use the *Ring/Network Coupling* function to redundantly couple an existing HIPER ring, MRP ring, or Fast HIPER ring to another network or another ring. Verify that the coupling partners are Hirschmann devices.

**Note:** With two-switch coupling, verify that you have configured a HIPER ring, MRP ring, or Fast HIPER ring before configuring the *Ring/Network Coupling* function.

In the *Ring/Network Coupling* dialog, you can perform the following tasks:
- display an overview of the existing *Ring/Network Coupling*
- configure a *Ring/Network Coupling*
- create a new *Ring/Network Coupling*
- delete *Ring/Network Coupling*
- enable/disable *Ring/Network Coupling*

When configuring the coupling ports, specify the following settings in the *Basic Settings > Port* dialog:

| Port type | Bit rate | Port on | Automatic configuration | Manual configuration |
|---|---|---|---|---|
| TX | 100 Mbit/s | `marked` | `unmarked` | *`100 Mbit/s FDX`* |
| TX | 1 Gbit/s | `marked` | `marked` | – |
| Optical | 100 Mbit/s | `marked` | `unmarked` | *`100 Mbit/s FDX`* |
| Optical | 1 Gbit/s | `marked` | `marked` | – |
| Optical | 2.5 Gbit/s | `marked` | – | *`2.5 Gbit/s FDX`* |
| Optical | 10 Gbit/s | `marked` | – | *`10 Gbit/s`* |

**Note:** The operating modes of the port actually available depend on the device configuration and the media module used.

If you configured VLANs, then note the VLAN configuration of the coupling and partner coupling ports. In the *Ring/Network Coupling* configuration, select the following values for the coupling and partner coupling ports:
- `VLAN ID 1` and *Ingress filtering* disabled in the port table
- VLAN membership `T` in the *VLAN Configuration* table

Independently of the VLAN settings, the device sends the ring coupling frames with `VLAN ID 1` and priority `7`. Verify that the device sends VLAN 1 frames tagged in the local ring and in the connected network. Tagging the VLAN frames maintains the priority of the ring coupling frames.

The *Ring/Network Coupling* function operates with test packets. The devices send their test packets with a VLAN tag, including the VLAN ID `1` and the highest VLAN priority `7`. If the forwarding port is a member in VLAN `1` and transmits the data packets without a VLAN tag, then the device also sends test packets.

### Operation

Operation

Enables/disables the *Ring/Network Coupling* function.

Possible values:

- *On*
  The *Ring/Network Coupling* function is enabled.
- *Off* (default setting)
  The *Ring/Network Coupling* function is disabled.

### Mode

Type

Specifies the method used to couple the networks together.

Possible values:

- *one-switch coupling*
  Lets you specify the port settings in the *Coupling port* and *Partner coupling port* frames.
- *two-switch coupling, master*
  Lets you specify the port settings in the *Coupling port* frame.
- *two-switch coupling, slave*
  Lets you specify the port settings in the *Coupling port* frame.
- *two-switch coupling with control line, master*
  Lets you specify the port settings in the *Coupling port* and *Control port* frames.
- *two-switch coupling with control line, slave*
  Lets you specify the port settings in the *Coupling port* and *Control port* frames.

### Coupling port

Port

Specifies the port to which you connect the redundant link.

Possible values:

- *-*
  No port selected.
- *<Port number>*

If you also have configured ring ports, then specify the coupling and ring ports on different ports.

To help prevent continuous loops, the device disables the coupling port in the following cases:

- disabling the function
- changing the configuration while the connections are operating on the ports

When the device has disabled the coupling port, the *Port on* checkbox is unmarked in the *Basic Settings > Port* dialog, *Configuration* tab.

State

Displays the status of the selected port.

Possible values:

- *active*
  The port is active.
- *standby*
  The port is in stand-by mode.
- *not-connected*
  The port is not connected.
- *not-applicable*
  The port is incompatible with the configured control mode.

### Partner coupling port

Port

Specifies the port on which you connect the partner port.

Possible values:

- -
  No port selected.
- <Port number>

If you also have configured ring ports, then specify the coupling and ring ports on different ports.

State

Displays the status of the selected port.

Possible values:

- *active*
  The port is active.
- *standby*
  The port is in stand-by mode.
- *not-connected*
  The port is not connected.
- *not-applicable*
  The port is incompatible with the configured control mode.

IP address

Displays the IP address of the partner, when the devices are connected.

The prerequisite is that you select a two-switch coupling method and enable the partner in the network.

### Control port

Port

Displays the port on which you connect the control line.

Possible values:

- `-`
  No port selected.
- `<Port number>`

State

Displays the status of the selected port.

Possible values:

- *`active`*
  The port is active.
- *`standby`*
  The port is in stand-by mode.
- *`not-connected`*
  The port is not connected.
- *`not-applicable`*
  The port is incompatible with the configured control mode.

### Configuration

Redundancy mode

Enables/disables the device to respond to a failure in the remote ring or network.

Possible values:

- *`redundant ring/network coupling`*
  Either the main line or the redundant line is active. Both lines are not active simultaneously. If the device detects that the link is down between the devices in the connected network, then the standby device keeps the redundant port in the standby mode.
- *`extended redundancy`*
  The main line and the redundant line are active simultaneously. If the device detects a problem in the connection between the devices in the connected network, then the standby device forwards data on the redundant port. With the setting you can maintain continuity in the remote network.

**Note:** During the reconfiguration period, package duplications can occur. Therefore, if your application is able to detect package duplications, then you can select this setting.

Coupling mode

The settings in this frame allow you to couple a specific type of network.

Possible values:

- *ring coupling*
  The device couples redundant rings. The device lets you couple rings that use the following redundancy protocols:
  - HIPER ring
  - Fast HIPER ring
  - MRP ring
- *network coupling*
  The device couples network segments. The function lets you couple mesh and bus networks together.

### Information

Redundancy available

Displays if the redundancy is available.

When a component of the ring is down, the redundant line takes over its function.

Possible values:

- *redGuaranteed*
  The redundancy is available.
- *redNotGuaranteed*
  The redundancy is unavailable.

Configuration failure

You have configured the function incorrectly, or there is no ring port connection.

Possible values:

- *noError*
- *slaveCouplingLinkError*
  The coupling line is not connected to the coupling port of the slave device. Instead, the coupling line is connected to another port of the slave device.
- *slaveControlLinkError*
  The control port of the slave device has no data link.
- *masterControlLinkError*
  The control line is not connected to the control port of the master device. Instead, the control line is connected to another port of the master device.
- *twoSlaves*
  The control line connects two slave devices.
- *localPartnerLinkError*
  The partner coupling line is not connected to the partner coupling port of the slave device. Instead, the partner coupling line is connected to another port of the slave device in *one-switch coupling* mode.
- *localInvalidCouplingPort*
  In *one-switch coupling* mode, the coupling line is not connected on the same device as the partner line. Instead, the coupling line is connected to another device.

- *couplingPortNotAvailable*
  The coupling port is not available because the module to which the port refers is not available or the port does not exist on this module.
- *controlPortNotAvailable*
  The control port is not available because the module to which the port refers is not available or the port does not exist on this module.
- *partnerPortNotAvailable*
  The partner coupling port is not available because the module to which the port refers is not available or the port does not exist on this module.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset

Disables the redundancy function and resets the parameters in the dialog to the default setting.

# 5.9.6.3 Redundant Coupling Protocol



A ring topology provides short transition times with a minimal use of resources. However, to couple these rings redundantly to a higher-level network is more of a challenge.

When you want to use a standard protocol such as MRP for the ring redundancy and RSTP to couple the rings together, the *Redundant Coupling Protocol* helps provide options for you.

Do not use the following redundancy protocols on the ports of the *RCP* primary ring and the *RCP* secondary rings:

- *Sub Ring*
- *Ring/Network Coupling*

On a device in the *slave* role, do not use the port-based *Routing* function on the ports of the *RCP* primary ring and the *RCP* secondary rings.

**Note:** On a device in the *master* role, you can use the port-based *Routing* function on the ports of the *RCP* primary ring and the *RCP* secondary rings. The prerequisite is that you explicitly set up the device's *master* role.

### Operation

Operation

Enables/disables the *RCP* function.

Possible values:

- `On`
  The *RCP* function is enabled.
- `Off` (default setting)
  The *RCP* function is disabled.

### Primary ring/network / Secondary ring/network

If the device operates as slave (value in the *Role* field is `slave`), then do not activate the *Static query port* mode for the ports on the secondary ring/network.

Inner port

Specifies the inner port number in the primary ring/secondary ring. The port is directly connected to the partner bridge.

Possible values:

- `-` (default setting)
  No port selected.
- `<Port number>`

Outer port

Specifies the outer port number in the primary ring/secondary ring.

Possible values:

- `-` (default setting)
  No port selected.
- `<Port number>`

Primary Ring protocol/Secondary Ring protocol

Displays the protocol that is active on the redundant coupling port in the devices in the primary/secondary ring.

### Coupler configuration

Role

Specifies the role of the local device.

Possible values:

- *`master`*
  The device operates as master.
- *`slave`*
  The device operates as slave.
- *`auto`* (default setting)
  The device automatically selects its role as *master* or *slave*.

Current role

Displays the current role of the local device. The value can be different from the configured role:

- If you configured both partner bridges as *`auto`*, then the partner bridge that is currently coupling the instances takes the *`master`* role. The other partner bridge takes the *`slave`* role.
- If both partner bridges are configured as *`master`* or both as *`slave`*, then the partner bridge with the smaller Basis MAC address takes the *`master`* role.
  The other partner bridge takes the *`slave`* role.
- If the protocol is started and the partner bridge cannot be found for a bridge in the configured role *`master`*, *`slave`* or *`auto`*, then the bridge sets its own role to *`listening`*.
- If the device detects a configuration problem for example, the inner ring ports are connected crosswise, then the device sets its role to *`error`*.

Timeout [ms]

Specifies the maximum time, in milliseconds, during which the slave device waits for test packets from the master device on the outer ports before the slave device takes over the coupling. This only applies in the state in which both inner ports of the slave device have lost the connection to the master device.

Configure the timeout longer than the longest assumable interruption time for the redundancy protocol of the faster instance. Otherwise, loops can occur.

Possible values:

- `5..60000` (default setting: `250`)

Partner MAC address

Displays the basic MAC address of the partner device.

Partner IP address

Displays the IP address of the partner device.

Coupling state

Displays the coupling state of the local device.

Possible values:

- *forwarding*
  The coupling state of the port is forwarding.
- *blocking*
  The coupling state of the port is blocking.

Redundancy state

Displays if the redundancy is available.

For a master-slave configuration, both bridges display this information.

Possible values:

- *redAvailable*
  The redundancy is available.
- *redNotAvailable*
  The redundancy is unavailable.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 6 Routing

The menu contains the following dialogs:

- Routing Global
- Routing Interfaces
- ARP
- Router Discovery
- RIP
- Open Shortest Path First
- Routing Table
- Tracking
- L3 Relay
- Loopback Interface
- Multicast Routing
- L3-Redundancy

## 6.1 Routing Global

[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:

- 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

Operation

Enables/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.

### Routing profile

In the *Routing profile* frame, you have the option of selecting a routing profile containing specific router settings.

Next routing profile

Specifies the routing profile that the device loads and applies upon the next restart.

A routing profile contains association settings for the internal resources (unicast routes, multicast routes, next-hop table / ARP table). By selecting a preset routing profile you have the option of operating the router with settings especially adapted to your intended use.

Possible values:

- *default*
  Sets the preset value for the device.
- *ipv4RoutingDefault* (default setting)
- *ipv4DataCenter*
- *ipv4RoutingUnicast*

When you position the mouse pointer over one of the values, a bubble help displays the association settings used in the routing profile.

Current routing profile

Displays the routing profile that the device loaded during the last restart and is currently applied.

### 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 time window in milliseconds in which the device sends the number of “ICMP error message” type data packets specified in the *Rate limit burst size* field.

Possible values:

- `0..2147483647` (default setting: `1000`)

Rate limit burst size

Specifies the number of “ICMP Error” messages that the device sends in the time window specified in the *Rate limit interval [ms]* field.

The limitation contains every “ICMP Error” message on the router interfaces that are set up.

Possible values:

- `1..200` (default setting: `100`)

The device lets you specify the limitation for a time window of any size desired. In the default setting, the device sends 100 data packets per 1000 ms. You obtain the same result but with a finer granularity using the following settings:

- *Rate limit interval [ms]*=`100`
  *Rate limit burst size*=`10`
  or
- *Rate limit interval [ms]*=`10`
  *Rate limit burst size*=`1`

### Configuration

File transfer source interface

Specifies the interface whose IP address the device uses as source IP address for the following file transfers:

- FTP
- SCP
- SFTP
- TFTP

This setting does not apply to data packets that the device sends on the *Out of Band* management port.

Possible values:

- `none` (default setting)
- `<Port number>`

Source routing

Activates/deactivates the *Source routing* function.

The *Source routing* function lets the sender of a data packet determine its route through the network. This can lead to an unavoidable security issue. If a sniffer inserts its IP address into the data packets, then he can redirect the data packets to his host.

Possible values:

- `marked`
  The *Source routing* function is active.
  The device forwards packets which contain *Source routing* information. If the device is the receiver specified in a packet, the device accepts the packet.
- `unmarked` (default setting)
  The *Source routing* function is inactive.
  The device neither forwards nor accepts packets which contain *Source routing* information.

### 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 16.

## 6.2 Routing Interfaces

[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

## 6.2.1 Routing Interfaces Configuration

[ 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

Port

Displays the number of the port or VLAN belonging to the router interface.

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.

Port status

Displays the operating state of the port.

Possible values:

- `marked`
  The port is enabled.
- `unmarked`
  The port is disabled.

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
- *Out of Band* management port

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.

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.

Netdirected broadcasts

Activates/deactivates the forwarding of netdirected broadcasts to the connected subnet on the router interface.

Possible values:

- `marked`
  Forwarding is active.
  The router interface forwards netdirected broadcasts to the connected subnet. If the subnet has a direct connection to the Internet, then this setting increases the vulnerability to Denial of Service (DoS) attacks.
- `unmarked` (default setting)
  Forwarding is inactive.

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..12266` (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 unreachables

Activates/deactivates the sending of *ICMP Destination Unreachable* messages on the router interface.

Possible values:

- `marked` (default setting)
  The router interface sends *ICMP Destination Unreachable* messages.
- `unmarked`
  The router interface does not send *ICMP Destination Unreachable* messages.

ICMP redirects

Activates/deactivates the sending of “ICMP Redirect” messages on the router interface.

Possible values:

- `marked` (default setting)
  The router interface sends “ICMP Redirect” messages.
  The prerequisite is that you activate the *Send redirects* function in the device. See the *Routing > Global* dialog.
- `unmarked`
  The router interface does not send “ICMP Redirect” messages.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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 32 IP addresses (1 primary, 31 secondary) for a router interface and a total of up to 1024 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`)

# 6.2.2 Routing Interfaces Secondary Interface Addresses

[ 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 32 IP addresses (1 primary, 31 secondary) for a router interface and a total of up to 1024 IP addresses.

### Table

Port

Displays the number of the port or VLAN belonging to the router interface.

IP address

Displays the primary IP address of the router interface. See the *Routing > Interfaces > Configuration* dialog.

Netmask

Displays the primary netmask of the router interface. See the *Routing > Interfaces > Configuration* dialog.

Additional IP address

Displays further IP addresses assigned to the router interface.

Additional netmask

Displays further netmasks assigned to the router interface.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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
- *Out of Band* management port

## 6.3 ARP

[ Routing > 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

# 6.3.1 ARP Global

[ Routing > ARP > Global ]

This dialog lets you set the ARP parameters and view statistical values.

### Configuration

Aging time [s]

Specifies the time in seconds, after which the device removes an entry from the ARP table.

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`)

Dynamic renew

Activates/deactivates the query to a device if the aging time is exceeded.

Possible values:

- `marked`
  The query is activated.
  The device sends a new query to a device when its entry has exceeded the aging time. When the query remains unanswered, the device removes the entry from the ARP table.
- `unmarked` (default setting)
  The query is deactivated.

Selective learning

Activates or deactivates the learning of the IP/MAC address assignment of the sender.

Possible values:

- `marked` (default setting)
  Learning is activated.
  The device learns the IP/MAC address assignment of transmitting equipment only if the ARP query was addressed to the address of the device itself.
- `unmarked`
  Learning is deactivated.
  The device learns the IP/MAC address assignment of transmitting devices by evaluating the received ARP queries.
  This does away with time-consuming ARP queries before the device forwards data packets to unknown devices.
  On the other hand, the device is vulnerable to “ARP cache poisoning” and also learns unnecessary ARP entries, such as from devices that communicate only in the local network.

### Information

Current entries total

Displays the number of entries that the ARP table currently contains.

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 16.

## 6.3.2 ARP Current

[ Routing > 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 16.

Reset ARP table

Removes the dynamically set up addresses from the ARP table.

# 6.3.3 ARP Static

[Routing > ARP > Static]

This dialog lets you add to the ARP table IP/MAC address assignments that you have specified yourself.

### Table

IP address

Displays the IP address that the device assigns to the adjacent MAC address.

MAC address

Displays the MAC address that the device assigns to the adjacent IP address.

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 16.

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.

### [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

IP address

Specifies the IP address.

Possible values:

- ▶ Valid IPv4 address

MAC address

Specifies the MAC address.

Possible values:

- ▶ Valid MAC address

## 6.4 Router Discovery

[ Routing > Router Discovery ]

The ICMP Router Discovery Protocol (IRDP), described in RFC 1256, lets end devices determine the addresses of the routers available in a subnet.

The router sends advertisements to identify itself as a router to the end devices.

End devices that support IRDP update their routing table after receiving an advertisement. If a standard gateway was previously entered, then the address learned with the advertisement has a lower priority in the routing table.

#### Table

Port

Displays the router interface to which the setting applies.

Advertise mode

Activates/deactivates the router discovery function on the router interface.

Possible values:

- `marked`
  The router discovery function is active. The device sends advertisements on the router interface.
- `unmarked` (default setting)
  The router discovery function is inactive.

Advertise address

Specifies the destination to which the device sends advertisements.

Possible values:

- `Broadcast`
  The device sends advertisements to the broadcast address `255.255.255.255`.
- `Multicast` (default setting)
  The device sends advertisements to the multicast address `224.0.0.1`.

Min. advertisement interval [s]

Specifies the minimum period in seconds after which the device sends another advertisement.

Possible values:

- `3..1800` (default setting: `450`)

Max. advertisement interval [s]

Specifies the maximum period in seconds after which the device sends another advertisement. The prerequisite is that the value is greater than or equal to the value specified in the *Min. advertisement interval [s]* column.

Possible values:

- `4..1800` (default setting: `600`)

Advertisement lifetime [s]

Specifies the validity period for the advertisements in seconds. The prerequisite is that the value is greater than or equal to the value specified in the *Max. advertisement interval [s]* column.

Possible values:

- `4..9000` (default setting: `1800`)

Preference level

Specifies the key figure that an end device uses to decide which gateway to the destination network to use when multiple routers in the subnet identify themselves through IRDP.

Possible values:

- `0..2147483647` (default setting: `0`)
  The higher the specified value, the greater the probability that an end device will use the device as a gateway.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 6.5 RIP

[ Routing > RIP ]

The Routing Information Protocol (RIP) as specified in RFC 2453 is a routing protocol based on the distance vector algorithm using a hop count as the metric to determine the path from source to destination. You use RIP for the dynamic creation of the routing table.

RIP uses 2 types of packets to communicate with its neighbor, request packets and response packets. When you first start RIP, the router transmits a request packet out of the RIP enabled interfaces. Routers on which RIP is active transmit response packets back to the request originator. The response packets contain the routing table of each router. The routes transmitted in the response packets include the network address and metric.

RIP uses routing by rumor to update the routing tables. Routing by rumor means that the router only exchanges routing information with its neighbors.

The dialog contains the following tabs:
- [Configuration]
- [Route redistribution]
- [Statistics]

## [Configuration]

In this tab you enter both general settings and settings for each port for the routing information protocol.

### Operation

Operation

Enables/disables the *RIP* function on this router.

Possible values:

- `On`
  The *RIP* function is enabled.
- `Off` (default setting)
  The *RIP* function is disabled.

### Configuration

Auto-summary mode

Activates/deactivates the auto summary mode.

Possible values:

- `marked` (default setting)
  The device combines or summarizes, routes advertised by a RIP router whenever possible into aggregates. Summarizing the routes reduces the amount of routing information in the routing table.
- `unmarked`
  The function is inactive.

Host routes accept mode

Activates/deactivates the host routes accept mode. When you activate the function, RIP lets you specify the host routes.

Possible values:

- `marked` (default setting)
  The device enters (learns) the host routes with a 32-bit netmask advertised to this RIP router into its routing table.
- `unmarked`
  The function is inactive.

Advertise default route

Activates/deactivates the propagation of the default routes learned from other protocols.

Possible values:

- `marked`
  The device advertises the default routes learned from other protocols to its neighbors.
- `unmarked` (default setting)
  The function is inactive.

Split horizon

Activates/deactivates the split horizon mode. You use the split horizon mode to help avoid the count-to-infinity issue.

Possible values:

- *`none`*
  Disables split horizon.
- *`simple`* (default setting)
  Simple split horizon omits the entries known by a neighbor when sending the routing table to this neighbor.
- *`poisonReverse`*
  The Poison Reverse split horizon sends the routing table to a neighbor with the entries known by this neighbor, but denotes these entries with the infinity metric.

Default metric

Specifies the default metric of redistributed routes.

Possible values:

- `0` (default setting)
  No default metric. RIP propagates the route with metric `1`.
- `1..15`

Update interval [s]

Specifies the time interval at which the router transfers the entire content of the routing table to the RIP neighbors.

The router sets other RIP timers accordingly:

- Timeout
  6 × update interval
- Garbage Collection
  10 × update interval

Possible values:

- `0..1000` (default setting: `30`)
  Values below 10 seconds cause an increased network load in larger networks.

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:

- `1..254` (default setting: `120`)
  In routing decisions, the device gives preference to the route with the smallest value.
- `255`
  In routing decisions, the device ignores the route.

### Table

Port

Displays the router interface number.

Active

Activates/deactivates RIP on this router interface.

Send version

Specifies the RIP version that the router uses on this router interface to send RIP information.

Possible values:

- *`doNotSend`*
  RIP does not send any routing information.

- *ripVersion1*
  RIP sends information with version 1 as a broadcast.
- *rip1Compatible*
  RIP sends information with version 2 as a broadcast.
- *ripVersion2* (default setting)
  RIP sends information with version 2 as a multicast.

Receive version

Specifies the RIP version that the device accepts on the receiver side.

Possible values:

- *rip1*
  RIP accepts RIP V1 packets.
- *rip2*
  RIP accepts RIP V2 packets.
- *rip1OrRip2* (default setting)
  RIP accepts RIP V1 and V2 packets.
- *doNotRecieve*
  The device rejects RIP information.

Authentication

Specifies the type of authentication used on this interface.

Possible values:

- *noAuthentication* (default setting)
  The routers exchange RIP information without authentication.
- *simplePassword*
  The routers exchange RIP information with plain text password authentication.
- *MD5*
  The routers exchange RIP information with password authentication, whereby the devices transfer the password with md5 encryption.

Key

Specifies the password for authentication. For communication purposes, the port on the other end requires the same authentication settings.

The prerequisite is that, in the *Authentication* column, you specify the value *simplePassword* or *MD5*.

Possible values:

- 0..16 (octets in a string)
  If you supply a string shorter than 16 octets, then RIP left-justifies and pads the string, on the right with nulls (0x00), to 16 octets.

Key identifier

Specifies the password identification number for authentication. For communication purposes, the port at the other end requires the same key ID.

The prerequisite for changing the value is that, in the *Authentication* column, you specify the value *MD5*.

Possible values:

- `0..255`

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Route redistribution]

Route distribution describes how RIP propagates routes that RIP transferred from other protocols to other RIP routers.

### Table

Source

Displays the source from which RIP takes over routing information:

Possible values:

- *connected*
  The route points to networks of local router interfaces where RIP is not enabled.
- *static*
  The route is in the static routing table.
- *ospf*
  The route is from OSPF.

Active

Activates/deactivates route-redistribution for a particular source protocol.

Possible values:

- `marked`
  The router redistributes routes received with this protocol.
- `unmarked` (default setting)
  The device blocks redistribution.

Metric

Specifies the metric that RIP assigns to the routes from the source.

Possible values:

- `0` (default setting)
  RIP uses the value specified in the *Default metric* field.
- `1..15`

Match internal

Enables/disables the router to process internal OSPF routes.

Possible values:

- *Active* (default setting)
  RIP adopts OSPF Intra and OSPF Inter routes.
- *Inactive*
  RIP rejects OSPF Intra and OSPF Inter routes.

Match external 1

Enables/disables the router to process external OSPF routes of metric type 1.

Possible values:

- *Active*
  RIP adopts OSPF Ext T1 routes.
- *Inactive* (default setting)
  RIP rejects OSPF Ext T1 routes.

Match external 2

Enables/disables the router to process external OSPF routes of metric type 2.

Possible values:

- *Active*
  RIP adopts OSPF Ext T2 routes.
- *Inactive* (default setting)
  RIP rejects OSPF Ext T2 Inter routes.

Match NSSAExternal 1

Enables/disables the router to process external OSPF routes of metric type 1.

Possible values:

- *Active*
  RIP adopts OSPF Intra and OSPF Inter routes.
- *Inactive* (default setting)
  RIP rejects OSPF Intra and OSPF Inter routes.

Match NSSAExternal 2

Enables/disables the router to process external OSPF routes of metric type 2.

Possible values:

- *Active*
  RIP adopts NSSA (Not so Stubby Area) routes.
- *Inactive* (default setting)
  RIP rejects NSSA (Not so Stubby Area) routes.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Statistics]

The RIP statistics tab displays counters that count events relevant to routing.

### Information

Global route changes

Displays the number of route changes to the IP Route Database by RIP in the routing table

Global queries

Displays the number of responses sent to queries from other systems.

### Table

Port

Displays the port number.

Receive bad packets

Displays the number of received routing data packets that the router rejected for various reasons, such as different protocol version, or unknown command type.

Receive bad routes

Displays the number of routing information messages received, which the router ignored because the input format was invalid.

Sent updates

Displays the number of routing tables sent with changed routing entries.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 6.6 Open Shortest Path First

[ Routing > OSPF ]

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 Mbit/s) / (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

# 6.6.1 OSPF Global

[Routing > OSPF > Global]

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

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:

- `1..4294967` (default setting: `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:

- `1..4` (default setting: `4`)
- `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:

- `0` (default setting)
  OSPF automatically assigns a cost of 20 for routes learned from external sources (static or directly connected).
- `1..16777214`

Send trap

Activates/deactivates the sending of SNMP traps when the device detects a change in an OSPF parameter.

Possible values:

- `marked`
  The sending of SNMP traps is active.
  If the device detects changes in the OSPF parameters, 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.

### 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 a 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 16.

## [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 `0.0.0.0/0` 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 `0.0.0.0/0` 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 16.

## [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.
- *rip*
  The router has learned the route using the RIP protocol.

### 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 16.

## 6.6.2 OSPF Areas

[ Routing > 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 30 OSPF Areas.

### Table

Area ID

Displays the area ID.

Area type

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:

- *area* (default setting)
  The router imports type 5 AS external LSAs into the area.
- *stub area*
  The router ignores type 5 AS external LSAs.
- *nssa*
  The router translates type 7AS external LSAs into type 5 NSSA summary LSAs and imports them into the area.

SPF runs

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.

Area border router

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.

AS boundary router

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.

Area LSAs

Displays the total number of link state advertisements in the link state database of this area, excluding AS External LSAs.

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 16.

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

# 6.6.3 OSPF Stub Areas

[Routing > 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

Area ID

Displays the area ID for the stub area.

Default cost

Specifies the external metric value for the metric type.

Possible values:

- `0..16777215`
  The router sets the default value to equal the lower cost within the area for the metric type.

Metric type

Specifies the type of metric used for the default route advertised into the area.

The border router of a stub area advertises a default route as a network summary LSA.

Possible values:

- *`OSPF metric`* (default setting)
  The ABR advertises the metric as OSPF internal, which is the cost of an intra-area route to the ABR.
- *`External type 1`*
  The ABR advertises the metric as *`External type 1`*, which is the cost of the OSPF internal metric plus external metric to the ASBR.
- *`External type 2`*
  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.

Totally stub

Activates/deactivates the import of summary LSAs into stub areas.

Possible values:

- `marked` (default setting)
  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`
  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 16.

## 6.6.4 OSPF Not So Stubby Areas

[ Routing > OSPF > NSSA ]

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

Area ID

Displays the area ID to which the table entries apply.

Redistribute

Activates/deactivates external route redistribution into the NSSA.

Possible values:

- `marked` (default setting)
  The NSSA ASBRs suppress external route redistribution into the NSSA. Furthermore, the ASBR stops to create type 7 external LSAs for external routes.
- `unmarked`
  The NSSA ASBRs redistribute external routes into the NSSA.

Originate default info

Activates/deactivates the creation of type 7 default LSAs.

The prerequisite for the creation of type 7 default LSAs is that the router is an NSSA ABR or ASBR.

Possible values:

- `marked`
  The router creates type 7 default LSAs and sends then into the NSSA.
- `unmarked` (default setting)
  The router suppresses type 7 default LSAs.

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` (default setting)
  The router suppresses summary route importation making the area a Totally NSSA.
- `unmarked`
  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 16.

# 6.6.5 OSPF Interfaces

[ Routing > OSPF > Interfaces ]

This dialog lets you specify, activate, and display OSPF parameters on the 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

Port

Displays the interface to which the table entry applies.

IP address

Displays the IP address of this OSPF interface.

Active

Activates/deactivates the OSPF administrative status of the interface.

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.

Area ID

Specifies the area ID of the domain to which the interface connects.

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.

- *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 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*.

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.

Fast Hello mode

Activates/deactivates the Fast Hello mode on the port. For a ring that contains 8 devices, the function makes it possible for the recovery time to be less than 1.5 seconds for a detected link or router failure.

The prerequisite is that you specify a value of `1` second for the following parameters:

- *Dead interval [s]* column
- *Delay time [s]* column in the *Routing > OSPF > Global* dialog, *Shortest path first* frame

Possible values:

- `marked`
  The device sends the Hello packets every 250 ms, and ignores the value specified in the *Hello interval [s]* column.
- `unmarked` (default setting)
  The device sends the Hello packets according to the value specified in the *Hello interval [s]* column.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 6.6.6 OSPF Virtual Links

[ Routing > 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:

☐ Click the button.

### Table

Area ID

Displays the area ID for the transit area that the virtual link traverses.

Neighbor ID

Displays the router ID of the virtual neighbor.

The router learns this value from Hello packets received from the virtual neighbor. The value is a static value for virtual adjacencies.

Transmit delay [s]

Specifies the estimated number of seconds it takes to transmit an LS 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 the LS advertisement retransmissions for adjacencies belonging to this interface.

You also use this value when retransmitting Database Description (DD) and LS Request packets.

Possible values:

▶ `0..3600` (default setting: `5`)

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.

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:

- `1..65535` (default setting: `10`)

Status

Displays the OSPF virtual interface state.

Possible values:

- *down* (default setting)
  The interface is in the initial state and is blocking traffic.
- *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.

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 *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 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 16.

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.

# 6.6.7 OSPF Ranges

[ Routing > 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

Area ID

Displays the area ID of the address range.

LSDB type

Displays 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.

Network

Displays the IP address of the subnet of the range.

Netmask

Displays the netmask of the subnet of the range.

Effect

Specifies the external advertisement of the subnet ranges.

Possible values:

- *advertiseMatching* (default setting)
  The router advertises the range in other areas.
- *doNotAdvertiseMatching*
  The router withholds range advertisement to other external areas.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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.

# 6.6.8 OSPF Diagnostics

[Routing > 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 16.

## [Link state database]

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

Area ID

Displays the area ID from which router received the LSA.

Type

Displays the type of the LSAs received.

Each LSA type has a separate advertisement format.

Possible values:
- *routerLink*
  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.
- *networkLink*
  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.
- *summaryLink*
  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.
- *asSummaryLink*
  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.
- *asExternalLink*
  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.
- *nssaExternalLink*
  The router received the information from a router in a NSSA using a type 7 LSA.

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 16.

## [Neighbors]

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]*.

- *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.

Dead time

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.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Virtual neighbors]

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

Area ID

Displays the transit area ID of the virtual link.

Router ID

Displays the router ID of the other virtual endpoint ABR.

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.

IP address

Displays the IP address of the virtual neighbor.

The router uses the IP address to send OSPF packets across the transit network to the virtual neighbor.

Options

Displays the information contained in the options field of the LSA. This value indicates the capabilities of virtual neighbor.

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.

- `4,6,12,14,36,38,44,46`
  The values indicate that the virtual neighbor supports multicast routing.
- `8,10,12,14,40,42,44,46`
  The values indicate that the virtual neighbor supports type 7 LSAs.
- `32,34,36,38,40,42,44,46`
  The values indicate that the virtual neighbor supports demand circuits.

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. 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.

Events

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 16.

## [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 16.

## [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 16.

## 6.7 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.

Protocol

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.
- `rip`
  The *RIP* function created this route. See the *Routing > RIP* 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.

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 16.

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 precendence over the setting in the following dialog:
  – *Basic Settings > Out of Band* dialog, *Gateway address* field
  – *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*.

## 6.8 Tracking

[ Routing > Tracking ]

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

# 6.8.1 Tracking Configuration

[ Routing > 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.
    or
  - The remote router or end device is reachable.
    or
  - The result of the logical link is TRUE.
- *down*
  The monitoring result is negative:
  - The link status is inactive.
    or
  - The remote router or end device is not reachable.
    or
  - 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 16.

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

# 6.8.2 Tracking Applications

[Routing > 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 button top open the *Create* window and select the tracking object in the *Track name* drop-down list.

### Table

Type

Displays the type of the tracking object.

Track ID

Displays the identification number of the tracking object.

Application

Displays the name of the application that is linked with the tracking object.

Possible values:
- Tracking objects of the `logical` type
- Static routes
- Virtual router of a VRRP instance

Track name

Displays the name of the tracking object made up of *Type* and *Track ID*.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 6.9 L3 Relay

[ Routing > 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 severs 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

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 lest 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.

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 16.

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.

- `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.

# 6.10 Loopback Interface

[ Routing > Loopback Interface ]

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

Index

Displays the number that uniquely identifies the loopback interface.

Port

Displays the name of the loopback interface.

IP address

Specifies the IP address for the loopback interface.

Possible values:

- Valid IPv4 address (default setting: `0.0.0.0`)

Subnet mask

Specifies the netmask for the loopback interface.

Possible values:

- Valid IPv4 netmask (default setting: `0.0.0.0`)
  Example: `255.255.255.255`

Active

Displays if the loopback interface is active or inactive.

Possible values:

- `marked` (default setting)
  The loopback interface is active.
  When sending SNMP traps, the device uses the IP address of the first loopback interface as the sender.
- `unmarked`
  The loopback interface is inactive.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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`

# 6.11 Multicast Routing

[ Routing > Multicast Routing ]

The menu contains the following dialogs:

- Multicast Routing Global
- Multicast Routing Boundary Configuration
- Multicast Routing Static
- IGMP

# 6.11.1 Multicast Routing Global

[Routing > Multicast Routing > Global]

IP multicast routing is the distribution of IP data packets to multiple participants simultaneously under one IP address.

The menu lets you specify and display global settings and static counters of the *Multicast Routing* function. Here you also display and specify parameters for the IGMP, IGMP Proxy, DVMRP and PIM-SM/PIM-DM protocols.

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

## [Configuration]

This tab lets you enable IP multicast routing and specify and display global parameters for the function.

### Operation

Operation

Enables/disables the *Multicast Routing* function.

Possible values:
- `On`
  The *Multicast Routing* function is enabled.
- `Off` (default setting)
  The *Multicast Routing* function is disabled.

### Configuration

DSCP

Specifies the DSCP value that the device writes in routed multicast data packets.

The DSCP value (Differentiated Services Code Point) corresponds to bits 0 to 5 of the TOS field of a IP data packet. The TOS field (Type of Service) is used to prioritize data packets.

Possible values:
- `0..64` (default setting: `48`)
  The value `64` means that the device leaves the DSCP value of received data packets unchanged.

### Information

Multicast routing entries

Displays the maximum number of entries in the IP multicast routing table.

IGMP proxy active

Displays if the IGMP proxy function (Internet Group Management Protocol) is active.

Possible values:

- `marked`
  IGMP proxy is active.
- `unmarked`
  IGMP proxy is inactive.

### Table

Port

Displays the number of the router interface to which the table entry relates.

TTL

Specifies the TTL value (Time to Live) for this router interface. The device discards IP multicast data packets whose TTL value is below the specified value.

The TTL value is an 8-bit field in the IP data packet. With each hop (the next router on the path to the destination network) the multicast router reduces the TTL value by 1.

Possible values:

- `0`
  The device forwards every multicast data packet received on this router interface.
- `1..255` (default setting: `1`)

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Statistics]

This tab lets you display the statistic counters of the multicast routing function.

### Table

Multicast group address

Displays the IP address of the multicast group to which the table entry relates.

Possible values:

- Valid IPv4 address

Multicast source address

Displays the IP address of the multicast source to which the table entry relates. The device identifies the multicast source in combination with the related netmask.

Possible values:

- Valid IPv4 address

Upstream neighbor

Displays the IP address of the upstream neighbor from which the device receives IP data packets sent to this multicast address.

The upstream neighbor for the device is the next participating neighbor in the upstream direction (in the direction of the source of the multicast stream).

For example, the device uses the RPF algorithm (Reverse Path Forwarding) to calculate the multicast route and to determine the upstream neighbor.

Possible values:

- Valid IPv4 address
  The value `0.0.0.0` means that the upstream neighbor is unknown.

Port

Displays the port number.

Outgoing interfaces

Displays a list of the outgoing interfaces.

Uptime

Displays the time that has elapsed since the multicast router last modified the table entry for the port.

Timeout

Displays the time remaining until the multicast router deletes the entry for the participant from the group table when the participant is inactive.

The value `0` means that there is no time limit for the entry.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 6.11.2 Multicast Routing Boundary Configuration

[Routing > Multicast Routing > Boundary Configuration]

The multicast boundary function lets you reject selectively IP multicast streams.

This dialog lets you specify and display the parameters for restricting the IP multicast streams on specific ports. This restriction includes incoming as well as outgoing data packets.

### Table

Port

Displays the port number.

On this port the device discards multicast data packets whose address is in the range specified in the *IP address* and *Netmask* fields.

You specify the value in the *Create* dialog.

IP address

Displays the IP address of the multicast group to which this restriction applies.

The *IP address* of the multicast group combined with the associated *Netmask* specify the range for the multicast restriction. The device discards multicast data packets from this range.

You specify the value in the *Create* dialog.

Possible values:

- `239.0.0.0..239.255.255.255`

Netmask

Displays the netmask of the multicast group to which this restriction applies.

The *IP address* of the multicast group combined with the associated *Netmask* specify the range for the multicast restriction. The device discards multicast data packets from this range.

You specify the value in the *Create* dialog.

Status

Specifies the status for processing this table entry.

This value determines the procedure the router uses to create new table entries or delete certain entries from the table.

Possible values:

- *active*
  The table entry for the multicast routing restriction is active on this port.
  The table entry exists and is available for the router to use.
- *notInService* (default setting)
  The table entry for the multicast routing restriction is inactive on this port.
  The table entry exists, but is unavailable for the router to use.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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

- In the *Port* field, you specify the port to which the device applies the multicast restriction.
- In the *IP address* field, you specify the IP address for the multicast source.
- In the *Netmask* field, you specify the netmask for the multicast source.

## 6.11.3 Multicast Routing Static

[ Routing > Multicast Routing > Static ]

The *Multicast static* routing function lets you specify the route of the multicast data traffic in the network. The device uses the Reverse Path Forwarding (RPF) algorithm to define the path of the multicast data traffic through the multicast routers. The RPF algorithm uses the static entries to calculate the path of the multicast data traffic.

This dialog lets you specify and display the parameters for the static multicast routing function.
- IP address and netmask of the multicast data source
- RPF address (upstream neighbor of the device)
- Priority of the static multicast routing entry

### Table

IP address

Displays the IP address of the multicast data source.

You specify the value in the *Create* dialog.

Netmask

Displays the associated netmask for the IP address of the multicast data source.

You specify the value in the *Create* dialog.

RPF address

Specifies the IP address of the neighbor multicast router in the upstream direction (in the direction of the source of the multicast stream) that the RPF algorithm uses. The upstream neighbor for the device is the next participating neighbor in the upstream direction.

Specifying a valid IP address is the prerequisite for having the option of activating the static multicast routing entry.

Preference

Specifies the priority of this static multicast routing entry with which the device considers this route when selecting the best route.

The lower the value, the higher the priority. The value `255` means “not accessible”, the device ignores this route for the transmission of the multicast data traffic.

Specifying a valid priority is the prerequisite for having the option of activating the static multicast routing entry.

Possible values:

- `1..255` (default setting: `1`)

Status

Activates/deactivates the static multicast routing entry.

The prerequisite for activating the static multicast routing entry is that you specified valid values in the *RPF address* and *Preference* fields.

Possible values:

- `active`
  The table entry for the static multicast routing is active on this router interface
  The table entry exists and is available for the router to use.
- `notInService` (default setting)
  The table entry for the static multicast routing is inactive on this port.
  The table entry exists, but is unavailable for the router to use.

If the table entry is unavailable for the router due to missing information or to interruption, then the router displays this value:

- *notReady*
  The device detected unfulfilled conditions on the port or device level.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 16.

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

- In the *IP address* field, you specify the IP address for the multicast data source.
- In the *Netmask* field, you specify the netmask for the multicast data source.

## 6.11.4 IGMP

[Routing > Multicast Routing > IGMP]

The Internet Group Management Protocol (IGMP) enables IPv4 multicasting (group communication), that means the distribution of data packets to multiple participants simultaneously using one IP address. IGMP enables multicast groups to be managed dynamically. The management is carried out by local routers. The participants of a multicast group are connected directly to the local routers.

The menu contains the following dialogs:

- IGMP Configuration
- IGMP Proxy Configuration
- IGMP Proxy Database

# 6.11.4.1 IGMP Configuration

[ Routing > Multicast Routing > IGMP > Configuration ]

The Internet Group Management Protocol (IGMP) lets you manage IP multicast groups dynamically. The participants (hosts) of a multicast use IGMP for logging in and off the multicast router (querier).

The device supports the versions IGMPv1, IGMPv2, and IGMPv3. The IGMPv1 and IGMPv2 versions are backward compatible.

- IGMPv1
  Lets participants join a multicast group. In case of inactivity, the multicast router removes the participant from the multicast group after expiration of the timeout.
- IGMPv2
  In addition to IGMPv1, IGMPv2 provides the participant with the opportunity to log off from the multicast group (Leave message).
- IGMPv3
  In addition to IGMPv1 and IGMPv2, IGMPv3 provides the participant with the opportunity to specify the source from which it wishes to receive the multicast stream:
  - Receive only data packets from certain source addresses
  - Discard data packets from certain source addresses

The multicast routers send queries (periodic requests) to the participants.

- IGMPv1 and IGMPv2
  The participants respond to these queries for one multicast group in each case. The router enters the address of the multicast group into the database.
- IGMPv3
  Participants respond to these queries for one or more multicast groups. The router enters into the database the addresses of the multicast groups as well as the desired source addresses for a multicast stream.

IGMP routing uses the following message types to manage multicast groups:

- Membership Query
  Queries of the router regarding membership in a group (general queries, queries to groups, queries to groups and to specific source addresses)
- Membership Report
  The participant's responses regarding membership in a group
- Leave Group
  Messages from the participant when logging off from a group

### Operation

The dialog contains the following tabs:

- [Port]
- [Cache information]
- [Interface membership]

Operation

Enables/disables the *IGMP* function in the device.

Possible values:

- *On*
  The *IGMP* function is enabled.
- *Off* (default setting)
  The *IGMP* function is disabled.

## [Port]

This tab lets you set and monitor the parameters for IGMP routing.

### Table

Port

Displays the router interface number.

Configure at least one multicast router interface before viewing or configuring parameters for an IGMP-enabled router interface. Otherwise, the device displays a detected error.

Querier

Displays the IP address of the multicast router (IGMP querier) in the IP subnet to which the selected router interface belongs.

Possible values:

- Valid IPv4 address (default setting: 0.0.0.0)

Query interval

Specifies the time interval in seconds that the device uses to send IGMP host queries (queries to the IGMP-enabled participants) from this router interface

The IGMP-capable network devices in the network respond to the queries with report messages.

Possible values:

- 1..3600 (default setting: 125)

Status

Activates/deactivates the IGMP routing function.

Possible values:

- *active*
  The IGMP routing function is active on this router interface.
- *notInService* (default setting)
  The IGMP routing function is inactive on this router interface.

Version

Specifies the IGMP version used for this router interface.

Activate IGMP routing on this router interface before you configure the entry in the *Version* column.

Possible values:

- `1`
  Specifies version IGMPv1 for this router interface.
- `2`
  Specifies version IGMPv2 for this router interface.
- `3` (default setting)
  Specifies version IGMPv3 for this router interface.

Max. response time

Specifies the maximum query response time in tenths of a second for this router interface for IGMPv2 and IGMPv3.

If the router interface responds to the query of the multicast router within this time, then the router interface remains a member of the multicast group.

Possible values:

- `0..255` (default setting: `100`)

Robustness

Specifies the value for the IGMP robustness for this router interface.

The robustness lets you adjust the router interface to the expected packet loss in the subnet.

The IGMP routing function behaves in a robust manner in regard to the following number of packet losses in the subnet: *Robustness* minus 1.

Possible values:

- `1..255` (default setting: `2`)
  Use high values for the robustness if you expect a large number of packet losses in a subnet.

Last member query interval

Specifies the *Last member query interval* in tenths of a second, for IGMPv2 and IGMPv3.

To log off from a multicast group, the participant sends a message to the multicast router (a Leave Group Message). Then the multicast router sends a query to the participant.

The value of the parameter specifies the maximum allowable response time to this query for the participant. In addition, this value specifies the time interval between the group-specific queries of the multicast router.

Possible values:

- `0..255` (default setting: `10`)

Last member queries

Displays the number of queries that the multicast router sends if it receives a report for logging off from a multicast group (Leave Group Report).

Possible values:

- `1..20` (default setting: `2`)

Startup queries

Displays the number of startup queries (queries in the start-up phase) which the multicast router sends.

The intervals between the queries are specified in the *Startup query interval* column.

Possible values:

- `1..20` (default setting: `2`)

Startup query interval

Displays the time in seconds between successive startup queries (queries in the startup phase) of the multicast router.

The number of periodic queries are specified by *Startup queries*.

Possible values:

- `1..300` (default setting: `31`)

Querier uptime

Displays the time that has elapsed since the multicast router last modified the table entry for the port.

Querier expiry time

Displays the remaining time until the multicast router deletes the entry for the port from the multicast group table.

If the device itself is the querier (multicast router), then the *Querier expiry time* parameter has the value of `0`.

Wrong version queries

Displays how many times participants attempted to access the port with an IGMP protocol version detected to be incorrect.

The prerequisite is that the IGMP routing function is active for this port.

You specify the same IGMP version for every router within the network. If the device receives queries with other IGMP versions, then the device reports a detected configuration error.

Joins

Displays how many IGMP membership reports for a multicast group this router interface has received. The value of the parameter is related to the frequency with which a multicast router adds entries for this router interface to the cache table. The parameter indicates IGMP activity on this router interface.

The prerequisite is that the *IGMP* function is enabled for this router interface.

Groups

Displays how many multicast groups the cache table currently contains for the multicast router for this router interface.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Cache information]

This tab lets you monitor the parameters from the cache table of the IGMP multicast router.

### Table

Port

Displays the router interface number.

The prerequisite is that the IGMP routing function is active for this router interface.

Address

Displays the IP address of the multicast group to which the table entry relates.

The prerequisite is that the IGMP routing function is active on this router interface and that the router interface receives IGMP membership reports.

Possible values:

- Valid IPv4 address

Last reporter

Displays the source IP address from which the device last received an IGMP membership report (report for membership of a multicast group) for this router interface.

Possible values:

- Valid IPv4 address

Uptime

Displays the time in `[hh:mm:ss]` that has elapsed since the multicast router created the table entry for this participant.

Expiry time

Displays the value of the cache timer (time limiter) in `[hh:mm:ss]`. After this time has elapsed, the multicast router deletes the entry from the cache table. When the device receives an IGMP membership report for this multicast group on this router interface, the device resets the value of this timer.

V1 host timer

Displays the value of the host present timer (time limiter) in `[hh:mm:ss]` for IGMPv1 participants. This is the time remaining until the local multicast router assumes that none of the participants in the IP subnet connected through this port are active any more. When the multicast router receives IGMP membership reports again (reports on the membership of multicast groups), it resets the value of this timer.

As long as the value is greater than null, the multicast router ignores IGMPv2 and IGMPv3 Leave Group messages that it receives on this router interface.

V2 host timer

Displays the value of the host present timer (time limiter) in `[hh:mm:ss]` for IGMPv2 participants. This is the time remaining until the local multicast router assumes that none of the stations in the IP subnet connected through this port are active any more. When the multicast router receives IGMP membership reports again (reports on the membership of multicast groups), it resets the value of this timer.

As long as the value is greater than null, the multicast router ignores IGMPv3 Leave Group messages that it receives on this router interface.

Source filter mode

Displays the filter mode provided in the IGMPv3 report for source IP addresses for the multicast group.

Possible values:

- *include*
  The participant receives the multicast stream only from specific source IP addresses.

- *exclude*
  The participant receives the multicast stream without specific source IP addresses.
- NA (default setting)
  The filter mode for source IP addresses is inactive. The field remains empty.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Interface membership]

The table in this tab displays detailed information on the source addresses included in an IGMP multicast group. This information is provided in the IGMPv3 membership reports.

### Table

Port

Displays the port number.

The prerequisite is that the *IGMP* function is active for this port.

Address

Displays the IP address of the multicast group for which the router has received an IGMPv3 membership report on this router interface.

The prerequisite is that the *IGMP* function is active on this port and that the port receives IGMP membership reports.

Possible values:

- Valid IPv4 address

Host address

Displays the source IP addresses of this multicast group.

Possible values:

- Valid IPv4 address

Expire

Displays the value of the time limiter in [hh:mm:ss] for this multicast group. This is the time remaining until the multicast router deletes the multicast group entry. When the multicast router receives IGMP membership reports for this source specific multicast again, it resets the value of this timer.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 6.11.4.2 IGMP Proxy Configuration

[ Routing > Multicast Routing > IGMP > Proxy Configuration ]

This dialog lets you configure and monitor the parameters for the IGMP proxy router interface.

The multicast router learns information about membership of multicast groups through the IGMP router interface (downstream interface). In this direction, the device operates as a querier. On the IGMP proxy router interface (upstream interface) the device operates as a host and sends IGMP membership reports for the registered multicast groups from the downstream router interfaces.

### Table

Port

Displays the number of the upstream router interface on which the IGMP proxy function is active.

The prerequisite is that this router interface is not an IGMP downstream router interface.

Querier

Displays the IP address of the multicast router (IGMP querier) in the IP subnet to which the upstream interface belongs.

Possible values:

- Valid IPv4 address (default setting: `0.0.0.0`)

V1 querier timer

Displays the remaining time in seconds until the device assumes that no IGMPv1 querier is active on the upstream router interfaces.

V2 querier timer

Displays the remaining time in seconds until the device assumes that no IGMPv2 querier is active on the upstream router interfaces.

Version

Specifies the IGMP version used for this router interface.

Disable IGMP globally before you configure the entry in the *Version* column.

Possible values:

- `1`
  Specifies version IGMPv1 for this upstream router interface.
- `2`
  Specifies version IGMPv2 for this upstream router interface.
- `3` (default setting)
  Specifies version IGMPv3 for this upstream router interface.

Robustness

Specifies the value for the IGMP robustness for this upstream router interface.

The robustness lets you adjust the port to the expected packet loss in the subnet.

The IGMP routing function behaves in a robust manner in regard to the following number of packet losses in the subnet: *Robustness* minus 1.

The host repeats the transfer of the status report *Robustness* minus 1 times.

Possible values:

- `1..255` (default setting: `2`)
  Use high values if you expect a large number of packet losses in a subnet.

Unsolicited report interval

Specifies the interval in seconds in which the device sends unsolicited reports to the multicast router on the upstream interface.

Possible values:

- `1..260` (default setting: `1`)

Groups

Displays the number of multicast groups for which the upstream router interface sends IGMP membership reports.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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

In the *Port* field, you specify the number of the port on which the IGMP proxy function is active.

# 6.11.4.3 IGMP Proxy Database

[ Routing > Multicast Routing > IGMP > Proxy Database ]

This dialog lets you monitor the parameters for membership of multicast groups and the source list.

When registering or de-registering Multicast members on downstream interfaces, the IGMP Proxy device updates the database entries and sends IGMP Membership reports and Leave Group messages. The proxy interface sends this information in the upstream direction. Upon request, the device sends IGMP Membership reports to the upstream interfaces.

The dialog contains the following tabs:
- [Groups]
- [Source list]

## [Groups]

### Table

Port

Displays the port number to which the table entry relates.

IP multicast group address

Displays the IP address of the registered multicast group.

Possible values:
- Valid IPv4 multicast address

Creation time

Displays the time in seconds that has elapsed since the multicast router created the table entry.

Last reporter

Displays the source IP address of the IGMP proxy router interface from which the device last sent an IGMP membership report in the upstream direction.

Possible values:
- Valid IPv4 multicast address

Filter mode

Displays the filter mode for source IP addresses for the multicast groups.

Possible values:
- *include*
  The participant gets the multicast stream only from specific source IP addresses.

- *exclude*
  The participant discards the multicast stream from specific source IP addresses.
- None (default setting)
  The filter mode for source IP addresses is inactive. The field remains empty.

### Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

## [Source list]

### Table

Port

Displays the router interface number to which the table entry relates.

IP address

Displays the IP address of the multicast group.

Possible values:
- Valid IPv4 multicast address

Host address

Displays the source IP addresses of this multicast group.

Possible values:
- Valid IPv4 address

Expiry time

Displays the value of the time limiter for this multicast group entry. This is the time remaining until the device deletes the entry for this multicast group when the participants of the IGMP router interface are inactive.

When the parameter has the value null, the device deletes the entry.

### Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

# 6.12 L3-Redundancy

[ Routing > L3-Redundancy ]

The menu contains the following dialogs:

- VRRP

## 6.12.1 VRRP

[ Routing > L3-Redundancy > 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.

Hirschmann has further developed VRRP into the Hirschmann Virtual Router Redundancy Protocol (HiVRRP). With the appropriate configuration, this protocol provides switching times of less than 400 ms.

**Note:** You find detailed information on *VRRP* in the “Configuration” user manual.

The menu contains the following dialogs:

- VRRP Configuration
- VRRP Domains
- VRRP Statistics
- VRRP Tracking

# 6.12.1.1 VRRP Configuration

[ Routing > L3-Redundancy > VRRP > Configuration ]

This dialog lets you specify the following settings:
- up to 8 virtual routers per router interface
- up to 32 addresses per virtual router
- up to 16 virtual routers per physical router with HiVRRP

### Operation

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

Port

Displays the port number to which the table entry relates.

VRID

Displays the Virtual Router IDentifier.

Active

Activates/deactivates the VRRP instance specified in this row.

Possible values:

- `marked`
  The *VRRP* instance is active.
- `unmarked` (default setting)
  The *VRRP* instance is inactive.

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.

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.

State

Displays the VRRP state.

Possible values:

- *`initialize`*
  VRRP is in the initialization phase, the function is inactive, or the master router is still unnamed.

- *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

VRRP advert interval [ms]

Specifies the interval for sending out advertisement messages as the master router.

Possible values:

- 100..900 (default setting: 100)
  Interval for HiVRRP
  The device automatically activates HiVRRP if you specify a value within this range.
- 1000..255000 (default setting: 1000)
  Interval for VRRP

VRRP advert address

Specifies the IP address to which the virtual router sends advertisements.

Possible values:

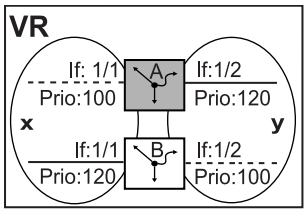
- Valid IPv4 address (default setting: `224.0.0.18`)

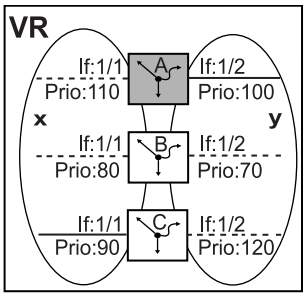
Link-down notify address

Specifies the IP address to which the local router sends notifications when changes on the link occur. Sending the notifications informs the back up router that a link on the master router is down reducing failover times.

If the virtual router consists of only 2 routers, routers A and B for example, then specify the IP address of the interface on the backup router that is linked to the opposite virtual router interface. For example, when specifying the link down notification address for interface `1/2` on router A, specify the IP address of interface `1/1` on router B.

If the virtual router consists of more than 2 routers, then specify the IP address of the interface with the second highest priority that is linked to the other virtual router interface. For example, when specifying the link down notification address for interface `1/2` on router A, specify the IP address of interface `1/1` on router C.




Possible values:

- Valid IP address (default setting: `0.0.0.0`)
  The value 0.0.0.0 suppresses notifications.

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.

Preempt delay [s]

Specifies the pre-empt delay time in seconds.

With the pre-empt mode activated and in collaboration with VRRP tracking, a reassignment of the master router role is possible. However, dynamic routing procedures take a certain amount of time to react to route changes and to refill routing tables. To help avoid the loss of packets during this time, the device lets you specify a pre-empt delay. The delay lets the dynamic routing procedure fill the routing tables before reassignment of the master router role.

Possible values:

- `0..65535` (default setting: `0`)

Domain ID

Specifies the virtual domain in which the router participates.

VRRP domains bundle a set of VRRP instances together. The supervisor router sends advertisement packets. The members follow the supervisor. If the loss of a single instance within a domain is likely, then configure the device to send advertisements to the member.

Possible values:

- `0` (default setting)
  No domain specified.
- `1..8`

Domain role

Specifies the role of this router in the virtual domain.

Possible values:

- *`none`* (default setting: `0`)
  The router is currently not a domain member.
- *`member`*
  The router copies the behavior of the supervisor.
- *`supervisor`*
  The router determines the behavior of the domain.

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`)

Ping answer

Activates/deactivates the ping answer function on the virtual router. 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 function globally. In the *Routing > Global* dialog, *ICMP filter* frame, mark the *Send echo reply* checkbox.

Possible values:

- `marked` (default setting)
  The device answers ICMP ping requests.
- `unmarked`
  The device ignores ICMP ping requests.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

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:

- ☐ In the *Routing > L3-Redundancy > VRRP > Configuration* dialog, open the *Wizard* window.
- ☐ 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.
- ☐ 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.

- Open the *HiVRRP* tab.
  The *HiVRRP* tab helps you to set up the following parameters:
  - failover times of less than 3 s,
  - the routers to use Unicasts to communicate with each other
  - to set up domains or
  - to send link-down notifications
- In the *Configuration* frame, specify the values for the following parameters:
  - *VRRP advert address* (IP address of the partner HiVRRP router)
  - *VRRP advert interval [ms]*
  - *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

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 communication 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) – Edit entry – HiVRRP]

### Information

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`

### Configuration

VRRP advert address

Specifies the IP address to which the virtual router sends advertisements.

Possible values:

- Valid IPv4 address (default setting: `224.0.0.18`)

VRRP advert interval [ms]

Specifies the interval for sending out messages (advertisements) as the master router.

The devices lets you specify up to 16 instances with advertisement intervals between 100 ms and 1000 ms.

Possible values:

- `100..255000` (default setting: `1000`)

Link-down notify address

Specifies the management IP address to which the virtual router sends notifications when changes occur within the virtual router.

Possible values:

- Valid IP address (default setting: `0.0.0.0`)

Domain ID

Specifies the virtual domain in which the router participates.

VRRP domains bundle a set of VRRP instances together. The supervisor router sends advertisement packets. The members follow the supervisor. If the loss of a single instance within a domain is likely, then configure the device to send advertisements to the members.

Possible values:

- `0..8` (default setting: `0`)
  The value `0` means „no domain“.

Domain role

Specifies the role of this router in the virtual domain.

Possible values:

- *`none`* (default setting: `0`)
  The router is currently not a domain member.

- *member*
  The router copies the behavior of the supervisor.
- *supervisor*
  The router determines the behavior of the domain.

## [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.
- *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]

The device lets you specify up to 8 virtual routers per router interface

Each virtual router supports up to 32 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.

# 6.12.1.2 VRRP Domains

[Routing > L3-Redundancy > VRRP > Domains]

HiVRRP provides various mechanisms to decrease the failover time or reduce the number of multicasts. In an HiVRRP domain, you combine multiple HiVRRP instances of a router into one administrative unit. You nominate one HiVRRP instance as the supervisor of the HiVRRP domain. This supervisor regulates the behavior of the HiVRRP instances in its domain.

The router supports up to 8 domains.

If you divide domain instances (members) among different physical router interfaces, then by default, the router monitors supervisor advertisements for interruptions. The checkbox *Redundancy check per member* is `unmarked`.

You also have the option of monitoring the other data links within the domain for interruptions. If the supervisor is unresponsive, then the other members of the domain start sending HiVRRP messages. To enable this function, perform the following step:

- ☐ In the *Redundancy check per member* column, you enable the function for a selected domain. With this function, you allow every member of the domain to send HiVRRP messages when detecting data link interruptions.

**Note:** If there is a low probability of a data link interruption, then select a long HiVRRP message interval to minimize the network load.

### Table

Domain ID

Displays the virtual domain in which the router participates.

VRRP domains bundle a set of VRRP instances together. The supervisor router sends advertisement packets. The members follow the supervisor. If the loss of a single instance within a domain is likely, then configure the device to send advertisements to the members.

Possible values:

- `0..8` (default setting: `0`)
  The value `0` means „no domain“.

Status

Displays the status of the domain supervisor.

Possible values:

- *`noError`*
  The routers supervisor function is active.
- *`supervisorDown`*
  The routers supervisor function is inactive.
- *`noSupervisor`* (default setting)
  The supervisor function is undefined.

Supervisor port

Displays the supervisor router interface for a VRRP instance.

Possible values:

- Available ports

Supervisor VRID

Displays the VRID of the supervisor.

Supervisor status

Displays the status of the supervisor.

Possible values:

- *initialize*
  VRRP is in the initialization phase. No master has been named yet.
- *backup*
  The router sees the possibility of becoming master.
- *master*
  The router is master.
- *unknown*
  no supervisor.

Current priority

Displays the current VRRP priority of the domain supervisor.

Possible values:

- 1..255

Redundancy check per member

Activates the function for the selected domain.

Possible values:

- marked
  The device sends advertisement packets even when a virtual router is in the member role.
- unmarked (default setting)
  The supervisor of the domain only sends advertisement packets.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 6.12.1.3 VRRP Statistics

[ Routing > L3-Redundancy > 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 16.

# 6.12.1.4 VRRP Tracking

[Routing > L3-Redundancy > 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

Port

Displays the router interface number of the virtual router.

VRID

Displays the virtual router ID for this virtual router.

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.

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.
    or
  - The remote router or end device is reachable.
- *down*
  The monitoring result is negative:
  - The link status is inactive.
    or
  - 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 16.

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 Diagnostics

The menu contains the following dialogs:

- Status Configuration
- System
- Email Notification
- Syslog
- Ports
- Loop Protection
- LLDP
- SFlow
- Report

## 7.1 Status Configuration

[ Diagnostics > Status Configuration ]

The menu contains the following dialogs:

- Device Status
- Security Status
- Signal Contact
- MAC Notification
- Alarms (Traps)

# 7.1.1 Device Status

[Diagnostics > Status Configuration > 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

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 a change in a monitored function.

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.

Ring redundancy

Activates/deactivates the monitoring of the ring redundancy.

Possible values:

- `marked`
  Monitoring is active.
  In the *Device status* frame, the value changes to `error` in the following situations:
  - The redundancy function becomes active (loss of redundancy reserve).
  - The device is a normal ring participant and detects an error in its settings.
- `unmarked` (default setting)
  Monitoring is inactive.

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.

Ethernet module removal

Activates/deactivates the monitoring of the modules.

Possible values:

- `marked`
  Monitoring is active.
  If you remove a module from the device, then in the *Device status* frame, the value changes to `error`.
  Further down, you have the option of selecting the modules 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.

You specify the active external memory in the *Basic Settings > Load/Save* dialog, *External memory* frame.

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.

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.

Ethernet module

Activates/deactivates the monitoring of this module.

Possible values:

- `marked`
  Monitoring is active.
  If you remove the module from the device, then in the *Device status* frame, the value changes to `error`.
- `unmarked` (default setting)
  Monitoring is inactive.

This setting is effective when you mark the *Ethernet module removal* checkbox further up.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [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 16.

## [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 16.

## 7.1.2 Security Status

[ Diagnostics > Status Configuration > 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 a change in a monitored function.

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.

Telnet server active

Activates/deactivates the monitoring of the Telnet server.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If you enable the Telnet server, then in the *Security status* frame, the value changes to `error`.
- `unmarked`
  Monitoring is inactive.

You enable/disable the Telnet server in the *Device Security > Management Access > Server* dialog, *Telnet* tab.

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.
    and
  - The *Config priority* column in the *Basic Settings > External Memory* dialog has the value `first` or `second`.
- `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 16.

## [Port]

### Table

Port

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 16.

## [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 16.

## 7.1.3 Signal Contact

[ Diagnostics > Status Configuration > 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

# 7.1.3.1 Signal Contact 1 / Signal Contact 2

[Diagnostics > Status Configuration > Signal Contact > Signal Contact 1]

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

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 a change in a monitored function.

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`
  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` (default setting)
  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.

Ring redundancy

Activates/deactivates the monitoring of the ring redundancy.

Possible values:

- `marked`
  Monitoring is active.
  The signal contact opens in the following situations:
  – The redundancy function becomes active (loss of redundancy reserve).
  – The device is a normal ring participant and detects an error in its settings.
- `unmarked` (default setting)
  Monitoring is inactive.

Ethernet module removal

Activates/deactivates the monitoring of the modules.

Possible values:

- `marked`
  Monitoring is active.
  If you remove a module from the device, then the signal contact opens.
  Further down, you have the option of selecting the modules to be monitored individually.
- `unmarked` (default setting)
  Monitoring is inactive.

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.

You specify the active external memory in the *Basic Settings > Load/Save* dialog, *External memory* frame.

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.

Ethernet loops

Activates/deactivates the monitoring of layer 2 Ethernet loops. You specify the settings for the *Loop Protection* function in the *Diagnostics > Loop Protection* dialog.

Possible values:

- `marked`
  Monitoring is active.
  If the device has detected an Ethernet loop, then the signal contact opens.
- `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.

Ethernet module

Activates/deactivates the monitoring of this module.

Possible values:

- `marked`
  Monitoring is active.
  If you remove this module from the device, then the signal contact opens.
- `unmarked` (default setting)
  Monitoring is inactive.

This setting is effective when you mark the *Ethernet module removal* checkbox further up.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [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 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 16.

**[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 16.

## 7.1.4 MAC Notification

[ Diagnostics > Status Configuration > MAC Notification ]

The device lets you track changes in the network using the MAC address of the devices in the network. The device saves the combination of port and MAC address in its MAC address table. If the device (un)learns the MAC address of a (dis)connected device, then the device sends an SNMP trap.

This function is intended for ports to which you connect end devices and thus the MAC address changes infrequently.

**Operation**

Operation

Enables/disables the *MAC Notification* function in the device.

Possible values:

- *On*
  The *MAC Notification* function is enabled.
- *Off* (default setting)
  The *MAC Notification* function is disabled.

### Configuration

Interval [s]

Specifies the send interval in seconds. If the device (un)learns the MAC address of a (dis)connected device, then the device sends an SNMP trap after this time.

Possible values:

- `0..2147483647` (default setting: `30`)

Before sending an SNMP trap, the device registers up to 20 MAC addresses. If the device detects a high number of changes, then the device sends the SNMP trap before the send interval expires.

### Table

Port

Displays the port number.

Active

Activates/deactivates the *MAC Notification* function on the port.

Possible values:

- `marked`
  The *MAC Notification* function is active on the port.
  The device sends an SNMP trap in case of one of the following events:
  - The device learns the MAC address of a newly connected device.
  - The device unlearns the MAC address of a disconnected device.
- `unmarked` (default setting)
  The *MAC Notification* function is inactive on the port.

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.

Last MAC address

Displays the MAC address of the device last connected on or disconnected from the port.

The device detects the MAC addresses of devices which are connected as follows:

- directly connected to the port
- connected to the port through other devices in the network

Last MAC status

Displays the status of the *Last MAC address* value on this port.

Possible values:

- `added`
  The device detected that another device was connected at the port.

- `removed`
  The device detected that the connected device was removed from the port.
- `other`
  The device did not detect a status.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 7.1.5 Alarms (Traps)

[Diagnostics > Status Configuration > 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
- in the *Diagnostics > Status Configuration > MAC Notification* 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 16.

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`.

# 7.2 System

[ Diagnostics > System ]

The menu contains the following dialogs:

- System Information
- Hardware State
- Configuration Check
- IP Address Conflict Detection
- ARP
- Selftest

## 7.2.1 System Information

[ Diagnostics > System > 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 16.

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 bowser command.

## 7.2.2 Hardware State

[ Diagnostics > System > Hardware State ]

This dialog provides information about the distribution and state of the flash memory of the device.

### Information

Uptime

Displays the total operating time of the device since it was delivered.

Possible values:

- `..d ..h ..m ..s`
  Day(s) Hour(s) Minute(s) Second(s)

### Table

Flash region

Displays the name of the respective memory area.

Description

Displays a description of what the device uses the memory area for.

Flash sectors

Displays how many sectors are assigned to the memory area.

Sector erase operations

Displays how many times the device has overwritten the sectors of the memory area.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 7.2.3 Configuration Check

[ Diagnostics > System > 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:** A neighboring device without LLDP support, which forwards LLDP packets, can be the cause of equivocal messages in the dialog. This occurs if the neighboring device is a hub or a switch without management, which ignores the IEEE 802.1D-2004 standard. In this case, the dialog displays the devices recognized and connected to the neighboring device as connected to the device itself, even though they are connected to the neighboring device.

### 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 `ERROR` level deviations that the device detected during the configuration check.

Warning

Displays the number of `WARNING` level deviations that the device detected during the configuration check.

Information

Displays the number of `INFORMATION` level deviations 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.

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 16.

# 7.2.4 IP Address Conflict Detection

[ Diagnostics > System > IP Address Conflict Detection ]

Using the *IP Address Conflict Detection* function the device verifies that its IP address is unique in the network. For this purpose, the device analyzes received ARP packets.

In this dialog you specify the procedure with which the device detects address conflicts and specify the required settings for this.

The device displays detected address conflicts in the table in the *Management* tab.

When the device detects an address conflicts on its router interfaces, the device displays the most recent address conflict in the *Routing* tab.

When the device detects an address conflict, the status LED of the device flashes red 4 times.

The dialog contains the following tabs:
- [Management]
- [Routing]

## [Management]

### Operation

Operation

Enables/disables the *IP Address Conflict Detection* function.

Possible values:

- `On` (default setting)
  The *IP Address Conflict Detection* function is enabled.
  The device verifies that its IP address is unique in the network.
- `Off`
  The *IP Address Conflict Detection* function is disabled.

### Configuration

Detection mode

Specifies the procedure with which the device detects address conflicts.

Possible values:

- `active and passive` (default setting)
  The device uses active and passive address conflict detection.

- *active*
  Active address conflict detection. The device actively helps avoid communicating with an IP address that already exists in the network. The address conflict detection begins as soon as you connect the device to the network or change its IP parameters.
  - The device sends 4 ARP probe data packets at the interval specified in the *Detection delay [ms]* field. If the device receives a response to these data packets, then there is an address conflict.
  - If the device does not detect an address conflict, then it sends 2 gratuitous ARP data packets as an announcement. The device also sends these data packets when the address conflict detection is disabled.
  - If the IP address already exists in the network, then the device changes back to the previously used IP parameters (if possible).
    If the device receives its IP parameters from a DHCP server, then it sends a DHCPDECLINE message back to the DHCP server.
  - After the period specified in the *Release delay [s]* field, the device checks if the address conflict still exists. When the device detects 10 address conflicts one after the other, the device extends the waiting time to 60 s for the next check.
  - When the device resolves the address conflict, the device management returns to the network again.
- *passive*
  Passive address conflict detection. The device analyzes the data traffic in the network. If another device in the network is using the same IP address, then the device initially “defends” its IP address. The device stops sending if the other device keeps sending with the same IP address.
  - As a “defence” the device sends gratuitous ARP data packets. The device repeats this procedure for the number of times specified in the *Address protections* field.
  - If the other device continues sending with the same IP address, then after the period specified in the *Release delay [s]* field, the device periodically checks if the address conflict still exists.
  - When the device resolves the address conflict, the device management returns to the network again.

### Send periodic ARP probes

Activates/deactivates the periodic address conflict detection.

Possible values:

- `marked` (default setting)
  The periodic address conflict detection is active.
  - The device periodically sends an ARP probe data packet every 90 to 150 seconds and waits for the time specified in the *Detection delay [ms]* field for a response.
  - If the device detects an address conflict, then the device applies the passive detection mode function. If the *Send trap* function is active, then the device sends an SNMP trap.
- `unmarked`
  The periodic address conflict detection is inactive.

Detection delay [ms]

Specifies the period in milliseconds for which the device waits for a response after sending a ARP data packets.

Possible values:

- `20..500` (default setting: `200`)

Release delay [s]

Specifies the period in seconds after which the device checks again if the address conflict still exists.

Possible values:

- `3..3600` (default setting: `15`)

Address protections

Specifies how many times the device sends gratuitous ARP data packets in the passive detection mode to “defend” its IP address.

Possible values:

- `0..100` (default setting: `3`)

Protection interval [ms]

Specifies the period in milliseconds after which the device sends gratuitous ARP data packets again in the passive detection mode to “defend” its IP address.

Possible values:

- `20..5000` (default setting: `200`)

Send trap

Activates/deactivates the sending of SNMP traps when the device detects an address conflict.

Possible values:

- `marked`
  The sending of SNMP traps is active.
  If the device detects an address conflict, 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.

### Information

Conflict detected

Displays if an address conflict currently exists.

Possible values:

- `marked`
  The device detects an address conflict.
- `unmarked`
  The device does not detect an address conflict.

### Table

Timestamp

Displays the time at which the device detected an address conflict.

Port

Displays the number of the port on which the device detected the address conflict.

IP address

Displays the IP address that is causing the address conflict.

MAC address

Displays the MAC address of the device with which the address conflict exists.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Routing]

### Configuration

Send trap

Activates/deactivates the sending of SNMP traps when the device detects an address conflict.

Possible values:

- `marked`
  The sending of SNMP traps is active.
  If the device detects an address conflict, 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.

### Information

The device continues to display the information in this frame, even if the last address conflict that the device has detected is no longer present. To reset the values, click the button and then the *Reset routing statistics* item.

IP address conflict detected

Displays if the device has detected an address conflict.

Possible values:

- `marked`
  The device has detected an address conflict.
- `unmarked`
  The device has not detected an address conflict.

IP address

Displays the IP address that has caused the address conflict.

MAC address

Displays the MAC address of the device that has caused the address conflict.

Time since last conflict

Displays the time that has elapsed since the device has detected the address conflict.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset routing statistics

Resets the values in the *Information* frame.

Run routing conflict detection

Starts the detection on its router interfaces.

The device sends a broadcast on the router interfaces. The device then analyzes the received ARP packets.

## 7.2.5 ARP

[ Diagnostics > System > ARP ]

This dialog displays the MAC and IP addresses of the neighboring devices connected to the device management.

### Table

Port

Displays the port number.

IP address

Displays the IPv4 address of a neighboring device.

MAC address

Displays the MAC address of a neighboring device.

Last updated

Displays the time in seconds since the current settings of the entry were registered in the ARP table.

Type

Displays the type of the entry.

Possible values:

- `static`
  Static entry. When the ARP table is deleted, the device keeps the static entry.
- `dynamic`
  Dynamic entry. When the *Aging time [s]* has been exceeded and the device does not receive any data from this device during this time, the device deletes the dynamic entry.
- `local`
  IP and MAC address of the device management.

Active

Displays that the ARP table contains the IP/MAC address assignment as an active entry.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset ARP table

Removes the dynamically set up addresses from the ARP table.

# 7.2.6 Selftest

[ Diagnostics > System > Selftest ]

This dialog lets you do the following:
- Activate/deactivate the RAM test when the device is being started.
- 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.

RAM test

Activates/deactivates the RAM memory check during the restart.

Possible values:
- `marked` (default setting)
  The RAM memory check is activated. During the restart, the device checks the RAM memory.
- `unmarked`
  The RAM memory check is deactivated. This shortens the start time for the device.

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 16.

## 7.3 Email Notification

[ Diagnostics > Email Notification ]

The device lets you inform multiple recipients by email about events that have occurred.

The device sends the emails immediately or periodically depending on the event severity. Usually you specify events with a high severity to be sent immediately.

You can specify multiple recipients to which the device sends the emails either immediately or periodically.

The menu contains the following dialogs:

- Email Notification Global
- Email Notification Recipients
- Email Notification Mail Server

# 7.3.1 Email Notification Global

[ Diagnostics > Email Notification > Global ]

In this dialog you specify the sender settings. Also, you specify for which event severities the device sends the emails immediately and for which periodically.

### Operation

Operation

Enables/disables the sending of emails:

Possible values:

- *On*
  The sending of emails is enabled.
- *Off* (default setting)
  The sending of emails is disabled.

### Certificate

The device can send messages to a server over unsecured networks. To help deny a “man in the middle” attack, request that the Certificate Authority creates a certificate for the server. Configure the server to use the certificate. Transfer the certificate onto the device.

If you specify the settings for the mail servers, then use the IP address or DNS name provided as `Common Name` or `Subject Alternative Name` in the certificate. Otherwise the certificate validation will fail.

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 reason, 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.
- Import from an FTP server
  When the certificate is on a FTP server, specify the URL for the file in the following form:
  `ftp://<user>:<password>@<IP address>:<port>/<path>/<file name>`

- Import from a TFTP server
  When the certificate is on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Import from an SCP or SFTP server
  When the certificate is on an SCP or SFTP server, you specify the URL for the file in the following form:
  - `scp://` or `sftp://<IP address>/<path>/<file name>`
    When you click the *Start* button, the device displays the *Credentials* window. There you enter *User name* and *Password*, to log in to the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

Start

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

### Sender

Address

Specifies the email address of the device.

The device sends the emails using this email address as the sender.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters
  (default setting: `switch@hirschmann.com`)

### Notification immediate

Here you specify the settings for emails which the device sends immediately.

Severity

Specifies the minimum severity of events for which the device immediately sends an email. If an event of this severity occurs, or of a more urgent severity, then the device sends an email to the recipients.

Possible values:

- *emergency*
- *alert* (default setting)
- *critical*
- *error*
- *warning*
- *notice*
- *informational*
- *debug*

Subject

Specifies the subject of the email.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

### Notification periodic

Here you specify the settings for emails which the device sends periodically.

Severity

Specifies the minimum severity of events for which the device periodically sends an email. If an event of this severity occurs, or of a more urgent severity, then the device registers the event in the buffer. The device sends the buffer content periodically or when the buffer overflows.

If an event of a less urgent severity occurs, then the device does not register the event in the buffer.

Possible values:

- *emergency*
- *alert*
- *critical*
- *error*
- *warning* (default setting)
- *notice*
- *informational*
- *debug*

Subject

Specifies the subject of the email.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

Sending interval [min]

Specifies the send interval in minutes.

If the device has registered at least one event, then the device sends an email with the log file after the time expires.

Possible values:

- `30..1440` (default setting: `30`)

Send

Sends an email immediately with the buffer content and clears the buffer.

### Information

Sent messages

Displays how many times the device has successfully sent an email to the mail server.

Undeliverable messages

Displays how many times the device has unsuccessfully tried to send an email to the mail server.

Time of the last messages sent

Displays the date and time at which the device has last sent an email to the mail server.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Clear email notification statistics

Resets the counters in the *Information* frame to `0`.

### Meaning of the event severities

| Severity | Meaning |
|---|---|
| `emergency` | Device not ready for operation |
| `alert` | Immediate user intervention required |
| `critical` | Critical status |
| `error` | Error status |
| `warning` | Warning |
| `notice` | Significant, normal status |
| `informational` | Informal message |
| `debug` | Debug message |

## 7.3.2 Email Notification Recipients

[ Diagnostics > Email Notification > Recipients ]

In this dialog you specify the recipients to which the device sends the emails. The device lets you specify up to 10 recipients.

### Table

Index

Displays the index number to which the table entry relates.

Notification type

Specifies if the device sends the emails to this recipient immediately or periodically.

Possible values:

- *immediate*
  The device sends the emails to this recipient immediately.
- *periodic*
  The device sends the emails to this recipient periodically.

Address

Specifies the email address of the recipient.

Possible values:

- Valid email address with up to 255 characters

Active

Activates/deactivates the informing of the recipient.

Possible values:

- marked (default setting)
  The informing of the recipient is active.
- unmarked
  The informing of the recipient is inactive.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 7.3.3 Email Notification Mail Server

[Diagnostics > Email Notification > Mail Server]

In this dialog you specify the settings for the mail servers. The device supports encrypted and unencrypted connections to the mail server.

### Table

Index

Displays the index number to which the table entry relates.

Description

Specifies the name of the server.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

IP address

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

Possible values:

- Valid IPv4 address (default setting: `0.0.0.0`)
- DNS name in the format `domain.tld` or `host.domain.tld`
  If you specify a DNS name, then also enable the *Client* function in the *Advanced > DNS > Client > Global* dialog.
  If you establish encrypted connections using the certificate, then verify that the DNS name is equal to the server DNS name mentioned in the certificate.

Destination TCP port

Specifies the TCP port of the server.

Possible values:

- `1..65535` (default setting: `25`)
  Exception: Port `2222` is reserved for internal functions.

Frequently used TCP-Ports:

- SMTP `25`
- Message Submission `587`

Encryption

Specifies the protocol which encrypts the connection between the device and the mail server.

Possible values:

- `none` (default setting)
  The device establishes an an unencrypted connection to the server.
- `tlsv1`
  The device establishes an encrypted connection to the server using the startTLS extension.

User name

Specifies the user name of the account which the device uses to authenticate on the mail server.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

Password

Specifies the password of the account which the device uses to authenticate on the mail server.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

Timeout [s]

Specifies the time in seconds after which the device sends an email again. The prerequisite is that the device has failed to send the complete email due to a connection error.

Possible values:

- `1..15` (default setting: `3`)

Active

Activates/deactivates the use of the mail server.

Possible values:

- `marked`
  The mail server is active.
  The device sends emails to this mail server.
- `unmarked` (default setting)
  The mail server is inactive.
  The device does not send emails to this mail server.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Connection test

Opens the *Connection test* dialog to send a test email.

If the mail server settings are correct, then the selected recipients receive a test email.

- In the *Recipient* field, you specify to which recipients the device sends the test email:
  - *immediate*
    The device sends the test email to the recipients to which the device sends emails immediately.
  - *periodic*
    The device sends the test email to the recipients to which the device sends emails periodically.
- In the *Message text* field, you specify the text of the test email.

# 7.4 Syslog

[ Diagnostics > 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*
  The sending of events is enabled.
  The device sends the events specified in the table to the specified syslog servers.
- *Off* (default setting)
  The sending of events is disabled.

### Certificate

The device can send messages to a server over unsecured networks. To help deny a “man in the middle” attack, request that the Certificate Authority creates a certificate for the server. Configure the server to use the certificate. Transfer the certificate onto the device.

If you specify the parameters on the server, then verify that you specify the IP address and DNS name provided in the certificate as the Common Name or Subject Alternative Name. Otherwise the certificate validation will fail.

**Note:** In order for the changes to take effect after loading a new certificate, restart the *Syslog* function.

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 reason, 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.
- Import from an FTP server
  When the certificate is on a FTP server, specify the URL for the file in the following form:
  `ftp://<user>:<password>@<IP address>:<port>/<path>/<file name>`
- Import from a TFTP server
  When the certificate is on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Import from an SCP or SFTP server
  When the certificate is on an SCP or SFTP server, you specify the URL for the file in the following form:
  - `scp://` or `sftp://<IP address>/<path>/<file name>`
    When you click the *Start* button, the device displays the *Credentials* window. There you enter *User name* and *Password*, to log in to the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

Start

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

### 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 TCP or UDP port on which the syslog server expects the log entries.

Possible values:

- `1..65535` (default setting: `514`)

Transport type

Specifies the transport type the device uses to send the events to the syslog server.

Possible values:

- `udp` (default setting)
  The device sends the events over the UDP port specified in the *Destination UDP port* column.
- `tls`
  The device sends the events over TLS on the TCP port specified in the *Destination UDP port* column.

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 16.

# 7.5 Ports

[ Diagnostics > Ports ]

The menu contains the following dialogs:

- SFP
- TP cable diagnosis
- Port Monitor
- Auto-Disable
- Port Mirroring

## 7.5.1 SFP

[ Diagnostics > Ports > 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.

Port

Displays the port number.

Module type

Type of the SFP transceiver, for example M-SFP-SX/LC.

Serial number

Displays the serial number of the SFP transceiver.

Connector type

Displays the connector type.

Supported

Displays if the device supports the SFP transceiver.

Temperature [°C]

Operating temperature of the SFP transceiver in °Celsius.

Tx power [mW]

Transmission power of the SFP transceiver in mW.

Rx power [mW]

Receiving power of the SFP transceiver in mW.

Tx power [dBm]

Transmission power of the SFP transceiver in dBm.

Rx power [dBm]

Receiving power of the SFP transceiver in dBm.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 7.5.2 TP cable diagnosis

[Diagnostics > Ports > TP cable diagnosis]

This feature tests the cable attached to an interface for short or open circuit. The table displays the cable status and estimated length. The device also displays the individual cable pairs connected to the port. When the device detects a short circuit or an open circuit in the cable, it also displays the estimated distance to the problem.

To receive dependable results, use the *TP cable diagnosis* function for twisted pair cables with a minimum length of 3 meters.

**Note:** This test interrupts traffic on the port.

### Information

Port

Displays the port number.

Status

Status of the Virtual Cable Tester.

Possible values:

- *active*
  Cable testing is in progress.
  To start the test, click the button and then the *Start cable diagnosis...* item. This action opens the *Select port* dialog.
- *success*
  The device displays this entry after performing a successful test.
- *failure*
  The device displays this entry after an interruption in the test.
- *uninitialized*
  The device displays this entry while in standby.

### Table

Cable pair

Displays the cable pair to which this entry relates. The device uses the first PHY index supported to display the values.

Result

Displays the results of the cable test.

Possible values:

- *normal*
  The cable is functioning properly.

- *open*
  There is a break in the cable causing an interruption.
- *short*
  Wires in the cable are touching together causing a short circuit.
- *unknown*
  The device displays this value for untested cable pairs.

The device displays different values than expected in the following cases:

- If no cable is connected to the port, then the device displays the value *unknown* instead of *open*.
- If the port is deactivated, then the device displays the value *short*.

Min. length

Displays the minimum estimated length of the cable in meters.

If the cable length is unknown or in the *Information* frame the *Status* field displays the value *active*, *failure* or *uninitialized*, then the device displays the value 0.

Max. length

Displays the maximum estimated length of the cable in meters.

If the cable length is unknown or in the *Information* frame the *Status* field displays the value *active*, *failure* or *uninitialized*, then the device displays the value 0.

Distance [m]

Displays the estimated distance in meters from the end of the cable to the failure location.

If the cable length is unknown or in the *Information* frame the *Status* field displays the value *active*, *failure* or *uninitialized*, then the device displays the value 0.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Start cable diagnosis...

Opens the *Select port* dialog.

In the *Port* drop-down list you select the port to be tested. Use for copper-based ports only.

To initiate the cable test on the selected port, click the *Ok* button.

# 7.5.3 Port Monitor

[Diagnostics > Ports > Port Monitor]

The *Port Monitor* function monitors the adherence to the specified parameters on the ports. If the *Port Monitor* function detects that the parameters are being exceeded, then the device performs an action.

To apply the *Port Monitor* function, perform the following steps:
- *Global* tab
  - Enable the *Operation* function in the *Port Monitor* frame.
  - Activate for each port those parameters that you want the *Port Monitor* function to monitor.
- *Link flap*, *CRC/Fragments* and *Overload detection* tabs
  - Specify the threshold values for the parameters for each port.
- *Link speed/Duplex mode detection* tab
  - Activate the allowed combinations of speed and duplex mode for each port.
- *Global* tab
  - Specify for each port an action that the device carries out if the *Port Monitor* function detects that the parameters have been exceeded.
- *Auto-disable* tab
  - Mark the *Auto-disable* checkbox for the monitored parameters if you have specified the `auto-disable` action at least once.

The dialog contains the following tabs:
- [Global]
- [Auto-disable]
- [Link flap]
- [CRC/Fragments]
- [Overload detection]
- [Link speed/Duplex mode detection]

## [Global]

In this tab you enable the *Port Monitor* function and specify the parameters that the *Port Monitor* function is monitoring. Also specify the action that the device carries out if the *Port Monitor* function detects that the parameters have been exceeded.

### Operation

Operation

Enables/disables the *Port Monitor* function globally.

Possible values:
- `On`
  The *Port Monitor* function is enabled.
- `Off` (default setting)
  The *Port Monitor* function is disabled.

### Table

Port

Displays the port number.

Link flap on

Activates/deactivates the monitoring of link flaps on the port.

Possible values:

- `marked`
  Monitoring is active.
  - The *Port Monitor* function monitors link flaps on the port.
  - If the device detects too many link flaps, then the device executes the action specified in the *Action* column.
  - On the *Link flap* tab, specify the parameters to be monitored.
- `unmarked` (default setting)
  Monitoring is inactive.

CRC/Fragments on

Activates/deactivates the monitoring of CRC/fragment errors on the port.

Possible values:

- `marked`
  Monitoring is active.
  - The *Port Monitor* function monitors CRC/fragment errors on the port.
  - If the device detects too many CRC/fragment errors, then the device executes the action specified in the *Action* column.
  - On the *CRC/Fragments* tab, specify the parameters to be monitored.
- `unmarked` (default setting)
  Monitoring is inactive.

Duplex mismatch detection active

Activates/deactivates the monitoring of duplex mismatches on the port.

Possible values:

- `marked`
  Monitoring is active.
  - The *Port Monitor* function monitors duplex mismatches on the port.
  - If the device detects a duplex mismatch, then the device executes the action specified in the *Action* column.
- `unmarked` (default setting)
  Monitoring is inactive.

Overload detection on

Activates/deactivates the overload detection on the port.

Possible values:

- `marked`
  Monitoring is active.
  - The *Port Monitor* function monitors the data load on the port.
  - If the device detects a data overload on the port, then the device executes the action specified in the *Action* column.
  - On the *Overload detection* tab, specify the parameters to be monitored.
- `unmarked` (default setting)
  Monitoring is inactive.

Link speed/Duplex mode detection on

Activates/deactivates the monitoring of the link speed and duplex mode on the port.

Possible values:

- `marked`
  Monitoring is active.
  - The *Port Monitor* function monitors the link speed and duplex mode on the port.
  - If the device detects an unpermitted combination of link speed and duplex mode, then the device executes the action specified in the *Action* column.
  - On the *Link speed/Duplex mode detection* tab, specify the parameters to be monitored.
- `unmarked` (default setting)
  Monitoring is inactive.

Active condition

Displays the monitored parameter that led to the action on the port.

Possible values:

- `-`
  No monitored parameter.
  The device does not carry out any action.
- *`Link flap`*
  Too many link changes in the observed period.
- *`CRC/Fragments`*
  Too many CRC/fragment errors in the observed period.
- *`Duplex mismatch`*
  Duplex mismatch detected.
- *`Overload detection`*
  Overload detected in the observed period.
- *`Link speed/Duplex mode detection`*
  Impermissible combination of speed and duplex mode detected.

Action

Specifies the action that the device carries out if the *Port Monitor* function detects that the parameters have been exceeded.

Possible values:

- *disable port*
  The device disables the port and sends an SNMP trap.
  The “Link status” LED for the port flashes 3× per period.
  - To re-enable the port, highlight the port and click the ☰ button and then the *Reset* item.
  - If the parameters are no longer being exceeded, then the *Auto-Disable* function enables the relevant port again after the specified waiting period. The prerequisite is that on the *Auto-disable* tab the checkbox for the monitored parameter is marked.
- *send trap*
  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.
- *auto-disable* (default setting)
  The device disables the port and sends an SNMP trap.
  The “Link status” LED for the port flashes 3× per period.
  The prerequisite is that on the *Auto-disable* tab the checkbox for the monitored parameter is marked.
  - The *Diagnostics > Ports > Auto-Disable* dialog displays which ports are currently disabled due to the parameters being exceeded.
  - The *Auto-Disable* function reactivates the port automatically. For this you go to the *Diagnostics > Ports > Auto-Disable* dialog and specify a waiting period for the relevant port in the *Reset timer [s]* column.

Port status

Displays the operating state of the port.

Possible values:

- up
  The port is enabled.
- down
  The port is disabled.
- notPresent
  Physical port unavailable.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset

Enables the port highlighted in the table again and resets its counter to 0. This affects the counters in the following dialogs:

- *Diagnostics > Ports > Port Monitor* dialog
  - *Link flap* tab
  - *CRC/Fragments* tab
  - *Overload detection* tab
- *Diagnostics > Ports > Auto-Disable* dialog

## [Auto-disable]

In this tab you activate the *Auto-Disable* function for the parameters monitored by the *Port Monitor* function.

### Table

Reason

Displays the parameters monitored by the *Port Monitor* function.

Mark the adjacent checkbox so that the *Port Monitor* function carries out the `auto-disable` action if it detects that the monitored parameters have been exceeded.

Auto-disable

Activates/deactivates the *Auto-Disable* function for the adjacent parameters.

Possible values:

- `marked`
  The *Auto-Disable* function for the adjacent parameters is active.
  If the adjacent parameters are exceeded and the value `auto-disable` is specified in the *Action* column, then the device carries out the *Auto-Disable* function.
- `unmarked` (default setting)
  The *Auto-Disable* function for the adjacent parameters is inactive.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset

Enables the port highlighted in the table again and resets its counter to `0`. This affects the counters in the following dialogs:

- *Diagnostics > Ports > Port Monitor* dialog
  - *Link flap* tab
  - *CRC/Fragments* tab
  - *Overload detection* tab
- *Diagnostics > Ports > Auto-Disable* dialog

## [Link flap]

In this tab you specify individually for every port the following settings:

- The number of link changes.
- The period during which the *Port Monitor* function monitors a parameter to detect discrepancies.

You also see how many link changes the *Port Monitor* function has detected up to now.

The *Port Monitor* function monitors those ports for which the checkbox in the *Link flap on* column is marked on the *Global* tab.

### Table

Port

Displays the port number.

Sampling interval [s]

Specifies in seconds, the period during which the *Port Monitor* function monitors a parameter to detect discrepancies.

Possible values:

- `1..180` (default setting: `10`)

Link flaps

Specifies the number of link changes.

If the *Port Monitor* function detects this number of link changes in the monitored period, then the device performs the specified action.

Possible values:

- `1..100` (default setting: `5`)

Last sampling interval

Displays the number of errors that the device has detected during the period that has elapsed.

Total

Displays the total number of errors that the device has detected since the port was enabled.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset

Enables the port highlighted in the table again and resets its counter to `0`. This affects the counters in the following dialogs:

- *Diagnostics > Ports > Port Monitor* dialog
  - *Link flap* tab
  - *CRC/Fragments* tab
  - *Overload detection* tab
- *Diagnostics > Ports > Auto-Disable* dialog

## [CRC/Fragments]

In this tab you specify individually for every port the following settings:
- The fragment error rate.
- The period during which the *Port Monitor* function monitors a parameter to detect discrepancies.

You also see the fragment error rate that the device has detected up to now.

The *Port Monitor* function monitors those ports for which the checkbox in the *CRC/Fragments on* column is marked on the *Global* tab.

### Table

Port

Displays the port number.

Sampling interval [s]

Specifies in seconds, the period during which the *Port Monitor* function monitors a parameter to detect discrepancies.

Possible values:
- `5..180` (default setting: `10`)

CRC/Fragments count [ppm]

Specifies the fragment error rate (in parts per million).

If the *Port Monitor* function detects this fragment error rate in the monitored period, then the device performs the specified action.

Possible values:
- `1..1000000` (default setting: `1000`)

Last active interval [ppm]

Displays the fragment error rate that the device has detected during the period that has elapsed.

Total [ppm]

Displays the fragment error rate that the device has detected since the port was enabled.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset

Enables the port highlighted in the table again and resets its counter to `0`. This affects the counters in the following dialogs:

- *Diagnostics > Ports > Port Monitor* dialog
  - *Link flap* tab
  - *CRC/Fragments* tab
  - *Overload detection* tab
- *Diagnostics > Ports > Auto-Disable* dialog

## [Overload detection]

In this tab you specify individually for every port the following settings:
- The load threshold values.
- The period during which the *Port Monitor* function monitors a parameter to detect discrepancies.

You also see the number of data packets that the device has detected up to now.

The *Port Monitor* function monitors those ports for which the checkbox in the *Overload detection on* column is marked on the *Global* tab.

The *Port Monitor* function does not monitor any ports that are members of a link aggregation group.

### Table

Port

Displays the port number.

Traffic type

Specifies the type of data packets that the device considers when monitoring the load on the port.

Possible values:

- `all`
  The *Port Monitor* function monitors Broadcast, Multicast and Unicast packets.
- `bc` (default setting)
  The *Port Monitor* function monitors only Broadcast packets.
- `bc-mc`
  The *Port Monitor* function monitors only Broadcast and Multicast packets.

Threshold type

Specifies the unit for the data rate.

Possible values:

- `pps` (default setting)
  packets per second
- `kbps`
  kbit per second
  The prerequisite is that the value in the *Traffic type* column = `all`.

Lower threshold

Specifies the lower threshold value for the data rate.

The *Auto-Disable* function enables the port again only when the load on the port is lower than the value specified here.

Possible values:

- `0..10000000` (default setting: `0`)

Upper threshold

Specifies the upper threshold value for the data rate.

If the *Port Monitor* function detects this load in the monitored period, then the device performs the specified action.

Possible values:

- `0..10000000` (default setting: `0)`)

Interval [s]

Specifies in seconds, the period that the *Port Monitor* function observes a parameter to detect that a parameter is being exceeded.

Possible values:

- `1..20` (default setting: `1`)

Packets

Displays the number of Broadcast, Multicast and Unicast packets that the device has detected during the period that has elapsed.

Broadcast packets

Displays the number of Broadcast packets that the device has detected during the period that has elapsed.

Multicast packets

Displays the number of Multicast packets that the device has detected during the period that has elapsed.

Kbit/s

Displays the data rate in Kbits per second that the device has detected during the period that has elapsed.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset

Enables the port highlighted in the table again and resets its counter to `0`. This affects the counters in the following dialogs:

- *Diagnostics > Ports > Port Monitor* dialog
  - *Link flap* tab
  - *CRC/Fragments* tab
  - *Overload detection* tab
- *Diagnostics > Ports > Auto-Disable* dialog

## [Link speed/Duplex mode detection]

In this tab you activate the allowed combinations of speed and duplex mode for each port.

The *Port Monitor* function monitors those ports for which the checkbox in the *Link speed/Duplex mode detection on* column is marked on the *Global* tab.

The *Port Monitor* function monitors only enabled physical ports.

### Table

Port

Displays the port number.

10 Mbit/s HDX

Activates/deactivates the port monitor to accept a half-duplex and 10 Mbit/s data rate combination on the port.

Possible values:

- `marked`
  The port monitor takes into consideration the speed and duplex combination.
- `unmarked`
  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

10 Mbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 10 Mbit/s data rate combination on the port.

Possible values:

- `marked`
  The port monitor takes into consideration the speed and duplex combination.
- `unmarked`
  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

100 Mbit/s HDX

Activates/deactivates the port monitor to accept a half-duplex and 100 Mbit/s data rate combination on the port.

Possible values:

- `marked`
  The port monitor takes into consideration the speed and duplex combination.
- `unmarked`
  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

100 Mbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 100 Mbit/s data rate combination on the port.

Possible values:

- `marked`
  The port monitor takes into consideration the speed and duplex combination.
- `unmarked`
  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

1,000 Mbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 1 Gbit/s data rate combination on the port.

Possible values:

- `marked`
  The port monitor takes into consideration the speed and duplex combination.
- `unmarked`
  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

2.5 Gbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 2.5 Gbit/s data rate combination on the port.

Possible values:

- `marked`
  The port monitor takes into consideration the speed and duplex combination.
- `unmarked`
  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

10 Gbit/s

Activates/deactivates the port monitor to accept a full-duplex and 10 Gbit/s data rate combination on the port.

Possible values:

- `marked`
  The port monitor takes into consideration the speed and duplex combination.
- `unmarked`
  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset

Enables the port highlighted in the table again and resets its counter to `0`. This affects the counters in the following dialogs:

- *Diagnostics > Ports > Port Monitor* dialog
  - *Link flap* tab
  - *CRC/Fragments* tab
  - *Overload detection* tab
- *Diagnostics > Ports > Auto-Disable* dialog

# 7.5.4 Auto-Disable

[Diagnostics > Ports > Auto-Disable]

The *Auto-Disable* function lets you disable monitored ports automatically and enable them again as you desire.

For example, the *Port Monitor* function and selected functions in the *Network Security* menu use the *Auto-Disable* function to disable ports if monitored parameters are exceeded.

If the parameters are no longer being exceeded, then the *Auto-Disable* function enables the relevant port again after the specified waiting period.

The dialog contains the following tabs:
- [Port]
- [Status]

## [Port]

This tab displays which ports are currently disabled due to the parameters being exceeded. If the parameters are no longer being exceeded and you specify a waiting period in the *Reset timer [s]* column, then the *Auto-Disable* function automatically enables the relevant port again.

### Table

Port

Displays the port number.

Reset timer [s]

Specifies the waiting period in seconds, after which the *Auto-Disable* function enables the port again.

Possible values:
- `0` (default setting)
  The timer is inactive. The port remains disabled.
- `30..4294967295`
  If the parameters are no longer being exceeded, then the *Auto-Disable* function enables the port again after the waiting period specified here.

Error time

Displays when the device disabled the port due to the parameters being exceeded.

Remaining time [s]

Displays the remaining time in seconds, until the *Auto-Disable* function enables the port again.

Component

Displays the software component in the device that disabled the port.

Possible values:

- `PORT_MON`
  *Port Monitor*
  See the *Diagnostics > Ports > Port Monitor* dialog.
- `PORT_ML`
  *Port Security*
  See the *Network Security > Port Security* dialog.
- `DHCP_SNP`
  *DHCP Snooping*
  See the *Network Security > DHCP Snooping* dialog.
- `DOT1S`
  *BPDU guard*
  See the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- `DAI`
  *Dynamic ARP Inspection*
  See the *Network Security > Dynamic ARP Inspection* dialog.

Reason

Displays the monitored parameter that led to the port being disabled.

Possible values:

- `none`
  No monitored parameter.
  The port is enabled.
- `link-flap`
  Too many link changes. See the *Diagnostics > Ports > Port Monitor* dialog, *Link flap* tab.
- `crc-error`
  Too many CRC/fragment errors. See the *Diagnostics > Ports > Port Monitor* dialog, *CRC/Fragments* tab.
- `duplex-mismatch`
  Duplex mismatch detected. See the *Diagnostics > Ports > Port Monitor* dialog, *Global* tab.
- `dhcp-snooping`
  Too many DHCP packages from untrusted sources. See the *Network Security > DHCP Snooping > Configuration* dialog, *Port* tab.
- `arp-rate`
  Too many ARP packages from untrusted sources. See the *Network Security > Dynamic ARP Inspection > Configuration* dialog, *Port* tab.
- `bpdu-rate`
  STP-BPDUs received. See the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- `mac-based-port-security`
  Too many data packets from undesired senders. See the *Network Security > Port Security* dialog.
- `overload-detection`
  Overload. See the *Diagnostics > Ports > Port Monitor* dialog, *Overload detection* tab.
- `speed-duplex`
  Impermissible combination of speed and duplex mode detected. See the *Diagnostics > Ports > Port Monitor* dialog, *Link speed/Duplex mode detection* tab.
- `Loop protection`
  A layer 2 network loop detected on the port. See the *Diagnostics > Loop Protection* dialog, *Loop detected* column.

Active

Displays if the port is currently disabled due to the parameters being exceeded.

Possible values:

- `marked`
  The port is currently disabled.
- `unmarked`
  The port is enabled.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Status]

This tab displays the monitored parameters for which the *Auto-Disable* function is activated.

### Table

Reason

Displays the parameters that the device monitors.

Mark the adjacent checkbox so that the *Auto-Disable* function disables and, when applicable, enables the port again if the monitored parameters are exceeded.

Category

Displays which function the adjacent parameter belongs to.

Possible values:

- `port-monitor`
  The parameter belongs to the functions in the *Diagnostics > Port > Port Monitor* menu.
- `network-security`
  The parameter belongs to the functions in the *Network Security* menu.
- `l2-redundancy`
  The parameter belongs to the functions in the *Switching > L2-Redundancy* menu.

Auto-disable

Displays if the *Auto-Disable* function is activated/deactivated for the adjacent parameter.

Possible values:

- `marked`
  The *Auto-Disable* function for the adjacent parameters is active.
  The *Auto-Disable* function disables and, when applicable, enables the relevant port again if the monitored parameters are exceeded.
- `unmarked` (default setting)
  The *Auto-Disable* function for the adjacent parameters is inactive.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset

Enables the port highlighted in the table again and resets its counter to `0`. This affects the counters in the following dialogs:

- *Diagnostics > Ports > Port Monitor* dialog
  - *Link flap* tab
  - *CRC/Fragments* tab
  - *Overload detection* tab
- *Diagnostics > Ports > Auto-Disable* dialog

# 7.5.5 Port Mirroring

[ Diagnostics > Ports > Port Mirroring ]

The *Port Mirroring* function lets you copy received and sent data packets from selected ports to a destination port. You can watch and process the data stream using an analyzer or an RMON probe, connected to the destination port. The data packets remain unmodified on the source port.

**Note:** To enable the access to the device management using the destination port, mark the checkbox *Allow management* in the *Destination port* frame before you enable the *Port Mirroring* function.

### Operation

Operation

Enables/disables the *Port Mirroring* function.

Possible values:

- *On*
  The *Port Mirroring* function is enabled.
  The device copies the data packets from the selected source ports to the destination port.
- *Off* (default setting)
  The *Port Mirroring* function is disabled.

### Destination port

Primary port

Specifies the destination port.

Suitable ports are those ports that are not used for the following purposes:

- Source port
- L2 redundancy protocols
- Port-based router interface

Possible values:

- `no Port` (default setting)
  No destination port selected.
- `<Port number>`
  Number of the destination port. The device copies the data packets from the source ports to this port.

On the destination port, the device adds a VLAN tag to the data packets that the source port transmits. The destination port transmits unmodified the data packets that the source port receives.

**Note:** The destination port needs sufficient bandwidth to absorb the data stream. If the copied data stream exceeds the bandwidth of the destination port, then the device discards surplus data packets on the destination port.

Secondary port

Specifies a second destination port. The prerequisite is that you have specified a primary port.

Possible values:

- `no Port` (default setting)
  No destination port selected.
- `<Port number>`
  Number of the destination port. The device copies the data packets from the source ports to this port.
  The port transmits the same data as the port specified above. Exception:
  - No *VLAN mirroring* data
  - No *RSPAN* data

Allow management

Activates/deactivates the access to the device management using the destination port.

Possible values:

- `marked`
  The access to the device management using the destination port is active.
  The device lets users have access to the device management using the destination port without interrupting the active *Port Mirroring* session.
  - The device duplicates multicasts, broadcasts and unknown unicasts on the destination port.
  - The VLAN settings on the destination port remain unchanged. The prerequisite for access to the device management using the destination port is that the destination port is not a member of the VLAN of the device management.
- `unmarked` (default setting)
  The access to the device management using the destination port is inactive.
  The device prohibits the access to the device management using the destination port.

## VLAN mirroring

The *VLAN mirroring* function lets you copy ingress data packets in a specific VLAN to the selected destination port. The device forwards the data stream out of the specified destination port.

**Note:** The *VLAN mirroring* function is only available on the primary port.

Source VLAN ID

Specifies the VLAN from which the device mirrors data to the destination port.

Possible values:

- `0` (default setting)
  Disables the *VLAN mirroring* function.
- `2..4042`
  The device lets you specify a VLAN only if no source port is specified.

### RSPAN

The *RSPAN* (Remote Switched Port Analyzer) function extends the mirroring function by allowing the device to forward the monitored data across multiple devices, on a specific VLAN, to a single destination.

**Note:** If you use the device on the path between the source and destination device, then specify in the *VLAN ID* field the VLAN needed to use the *RSPAN* function. For this, the *Port Mirroring* function is not required and remains disabled.

**Note:** The *RSPAN* function is only available on the primary port.

Source VLAN ID

Specifies the source VLAN from which the device mirrors data to the destination VLAN.

Possible values:

- `0` (default setting: `0`)
  The source VLAN is inactive.
- `2..4042`
  Mirrored ports cannot be members of the RSPAN VLAN.

VLAN ID

Specifies the VLAN that the device uses to tag and forward mirrored data.

Possible values:

- `0` (default setting: `0`)
  The RSPAN VLAN is inactive.
- `2..4042`
  The device uses the value to tag and forward mirrored data.

Destination VLAN ID

Specifies the VLAN that the device uses to forward the network traffic to the destination device.

Possible values:

- `0` (default setting: `0`)
  The destination VLAN is inactive.
- `2..4042`
  The device uses this value to tag data and to forward the network traffic to the destination device.

### Table

Source port

Specifies the port number.

Possible values:

- `<Port number>`

Enabled

Activates/deactivates the copying of the data packets from this source port to the destination port.

Possible values:

- `marked`
  The copying of the data packets is active.
  The port is specified as a source port.
- `unmarked` (default setting)
  The copying of the data packets is inactive.
- (Grayed-out display)
  It is not possible to copy the data packets for this port.
  Possible causes:
  - The port is already specified as a destination port.
  - The port is a logical port, not a physical port.

**Note:** The device lets you activate every physical port as source port except for the destination port.

Type

Specifies which data packets the device copies to the destination port.

On the destination port, the device adds a VLAN tag to the data packets that the source port transmits. The destination port transmits unmodified the data packets that the source port receives.

Possible values:

- `none` (default setting)
  No data packets.
- `tx`
  Data packets that the source port transmits.
- `rx`
  Data packets that the source port receives.
- `txrx`
  Data packets that the source port transmits and receives.

**Note:** With the `txrx` setting the device copies transmitted and received data packets. The destination ports needs at least a bandwidth that corresponds to the sum of the send and receive channel of the source ports. For example, for similar ports the destination port is at 100 % capacity when the send and receive channel of a source port are at 50 % capacity respectively.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset config

Resets the settings in the dialog to the default settings and transfers the changes to the volatile memory of the device (*RAM*).

## 7.6 LLDP

[ Diagnostics > 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

# 7.6.1 LLDP Configuration

[ Diagnostics > LLDP > Configuration ]

This dialog lets you configure the topology discovery for every port.

### Operation

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]

Specifies the delay in seconds for the reinitialization of a port.

Possible values:

- `1..10` (default setting: `2`)

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]

Specifies the delay in seconds for transmitting successive LLDP data packets after configuration changes in the device occur.

Possible values:

- `1..8192` (default setting: `2`)

The recommended value is between a minimum of `1` and a maximum of a quarter of the value in the *Transmit interval [s]* field.

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

Port

Displays the port number.

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.
- `both`
  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 16.

## 7.6.2 LLDP Topology Discovery

[ Diagnostics > 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.

The dialog contains the following tabs:
- [LLDP]
- [LLDP-MED]

### [LLDP]

This tab 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

Port

Displays the port number.

Neighbor identifier

Displays the chassis ID of the neighboring device. This can be the basis MAC address of the neighboring device, for example.

FDB

Displays if the connected device has active LLDP support.

Possible values:

- `marked`
  The connected device does not have active LLDP support.
  The device uses information from its address table (FDB, Forwarding Database)
- `unmarked` (default setting)
  The connected device has active LLDP support.

Neighbor IP address

Displays the IP address with which the access to the neighboring device management is possible.

Neighbor port description

Displays a description for the port of the neighboring device.

Neighbor system name

Displays the device name of the neighboring device.

Neighbor system description

Displays a description for the neighboring device.

Port ID

Displays the ID of the port through which the neighboring device is connected to the device.

Autonegotiation supported

Displays if the port of the neighboring device supports autonegotiation.

Autonegotiation

Displays if autonegotiation is enabled on the port of the neighboring device.

PoE supported

Displays if the port of the neighboring device supports Power over Ethernet (PoE).

PoE enabled

Displays if Power over Ethernet (PoE) is enabled on the port of the neighboring device.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [LLDP-MED]

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices and network devices. It specifically provides support for VoIP applications. In this support rule, it provides an additional set of common advertisement, Type Length Value (TLV), messages. The device uses the TLVs for capabilities discovery such as network policy, Power over Ethernet, inventory management and location information.

### Table

Port

Displays the port number.

Device class

Displays the device class of the remotely connected device.

- A value of `notDefined` indicates that the device has capabilities not covered by any of the *LLDP-MED* classes.
- A value of `endpointClass1..3` indicates that the device has "endpoint class 1..3" capabilities.
- A value of `networkConnectivity` indicates that the device has network connectivity device capabilities.

VLAN ID

Displays the extension of the VLAN Identifier for the remote system connected to this port, as defined in IEEE 802.3.

- The device uses a value from `1` through `4042` to specify a valid Port VLAN ID.
- The device displays the value `0` for priority tagged packets. This means that only the 802.1D priority is significant and the device uses the default VLAN ID of the ingress port.

Priority

Displays the value of the 802.1D priority which is associated with the remote system connected to the port.

DSCP

Displays the value of the Differentiated Service Code Point (DSCP) which is associated with the remote system connected to the port.

Unknown bit status

Displays the unknown bit status of incoming traffic.

- A value of `true` indicates that the network policy for the specified application type is currently unknown. In this case, the VLAN ID ignores the Layer 2 priority and value of the *DSCP* field.
- A value of `false` indicates a specified network policy.

Tagged bit status

Displays the tagged bit status.

- A value of `true` indicates that the application uses a tagged VLAN.
- A value of `false` indicates that for the specific application the device uses untagged VLAN operation. In this case, the device ignores both the VLAN ID and the Layer 2 priority fields. The DSCP value, however, is relevant.

Hardware revision

Displays the vendor-specific hardware revision string as advertised by the remote endpoint.

Firmware revision

Displays the vendor-specific firmware revision string as advertised by the remote endpoint.

Software revision

Displays the vendor-specific software revision string as advertised by the remote endpoint.

Serial number

Displays the vendor-specific serial number as advertised by the remote endpoint.

Manufacturer name

Displays the vendor-specific manufacturer name as advertised by the remote endpoint.

Model name

Displays the vendor-specific model name as advertised by the remote endpoint.

Asset ID

Displays the vendor-specific asset tracking identifier as advertised by the remote endpoint.

#### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 7.7 Loop Protection

[ Diagnostics > Loop Protection ]

The *Loop Protection* function helps protect against layer 2 network loops.

A network loop can lead to a standstill of the network due to overload. A possible reason is the continuous duplication of data packets due to a misconfiguration. The cause could be, for example, an incorrectly plugged cable or faulty settings in the device.

For example, a layer 2 network loop can occur in the following cases, if no redundancy protocols are active:

- Two ports of the same device are directly connected to each other.
- More than one active connection is established between two devices.

In redundant network topologies, multiple redundancy protocols are typically active. You usually disable the *Spanning Tree* function on the ports involved in other redundancy protocols. The redundancy protocols already help to avoid loops.

### Operation

Operation

Enables/disables the *Loop Protection* function.

Possible values:

- `On`
  The *Loop Protection* function is enabled.
  - On active and passive ports, the device evaluates received *loop detection* packets.
    On active ports, the device sends *loop detection* packets at regular intervals as specified in the *Transmit interval* field.
    The prerequisite is that the *Loop Protection* function is active on the port.
  - The device lets you monitor Ethernet loops with the signal contact. See the *Diagnostics* > Status Configuration > *Signal Contact* > *Signal Contact 1* dialog, checkbox for the *Ethernet loops* parameter.
- `Off` (default setting)
  The *Loop Protection* function is disabled.
  The device neither sends *loop detection* packets nor evaluates received *loop detection* packets.

### Global

Transmit interval

Specifies the interval in seconds at which the device sends *loop detection* packets if the *Loop Protection* function is active on the port.

Possible values:

- `1..10`

Receive threshold

Specifies the threshold value for the number of *loop detection* packets received in a row. If the number reaches or exceeds this threshold, then the device will perform the action specified in the *Action* column.

Possible values:

- `1..50`

### Configuration

Auto-disable

Activates/deactivates the *Auto-Disable* function for *Loop Protection*.

Possible values:

- `marked`
  The *Auto-Disable* function for *Loop Protection* is active.
  The prerequisite for disabling the port is that the *auto-disable* or the *all* action is specified in the *Action* column.
  The device lets you specify the waiting period in seconds after which the *Auto-Disable* function enables the port again. To do this, in the *Diagnostics > Ports > Auto-Disable* dialog, specify the waiting period in the *Reset timer [s]* column.
- `unmarked` (default setting)
  The *Auto-Disable* function for *Loop Protection* is inactive.

### Table

Port

Displays the port number.

Active

Activates/deactivates the *Loop Protection* function on the port.

Possible values:

- `marked`
  The *Loop Protection* function is active on the port.
  Activate the function only on ports which are not part of a redundant network path. This helps avoid an accidental shutdown of redundant network paths.
  If the device receives a *loop detection* packet on this port, sent from another port on the same device, then the device performs the action specified in the *Action* column.
- `unmarked` (default setting)
  The *Loop Protection* function is inactive on the port. The port neither sends *loop detection* packets nor evaluates received *loop detection* packets.

Mode

Specifies the behavior of the *Loop Protection* function on the port.

Possible values:

- *active*
  The device sends *loop detection* packets and evaluates received *loop detection* packets.
- *passive*
  The device evaluates received *loop detection* packets.

Action

Specifies the action the device performs when it detects a layer 2 network loop on this port.

Possible values:

- *trap*
  The device sends a trap.
- *auto-disable*
  The device disables the port using the *Auto-Disable* function.
  The prerequisite for disabling the port is that the *Auto-disable* checkbox in the *Configuration* frame is marked.
- *all*
  The device sends a trap. Then the device disables the port using the *Auto-Disable* function.
  The prerequisite for disabling the port is that the *Auto-disable* checkbox in the *Configuration* frame is marked.

VLAN ID

Specifies the VLAN in which the device sends the *loop detection* packets.

Possible values:

- `0` (default setting)
  The device sends the *loop detection* packets without a VLAN tag.
- `1..4042`
  The device sends the *loop detection* packets in the specified VLAN. The prerequisite is that the VLAN is already configured and that the port is a member of the VLAN. See the *Switching* > VLAN > *Port* dialog.

Loop detected

Displays if the device has detected a layer 2 network loop on the port.

Possible values:

- *yes*
  The device has detected a layer 2 network loop on the port.
  After the loop has ended and the port is enabled again, the device resets the value to *no*.
- *no*
  The device has not detected a layer 2 network loop on the port.

Loop count

Displays the number of loops the device has detected on the port since the last port statistics reset or since the last restart of the device.

Last loop time

Displays the time at which the device detected the last loop on the port.

The prerequisite for the correct evaluation of the value is that you synchronize the system time of the device with the appropriate reference time. See the *Time > Basic Settings* dialog.

Sent frames

Displays the number of *loop detection* packets sent on the port since the last port statistics reset or since the last restart of the device.

Received frames

Displays the number of sent and received back *loop detection* packets on the port since the last port statistics reset or since the last restart of the device.

Discarded frames

Displays the number of discarded *loop detection* packets on the port.

Examples of reasons for discarded packets:

- The device detects packets with an incorrect format.
- The device detects packets with expired timestamps (packets received more than 5 seconds after sending).
- The device received a data packet with an unexpected VLAN information.
- The device detects received packets on a port that is disabled.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Clear port statistics

Resets the values in the following columns:

- *Loop count*
- *Sent frames*
- *Received frames*

## 7.8 SFlow

[ Diagnostics > SFlow ]

sFlow is a standard protocol for monitoring networks. The device contains the sFlow feature which gives you visibility into network activity, allowing for effective management and control of network resources.

The sFlow monitoring system consists of an sFlow agent and a central sFlow collector. The agent uses the following forms of sampling:

- statistical packet-based sampling of packet flows
- time-based sampling of counters

The device combines both types of samples into datagrams. sFlow uses the datagrams to forward the sampled traffic statistics to an sFlow collector for analysis.

In order to perform packet flow sampling, you configure an instance with a sampling rate. You then configure the instance with a polling interval for counter sampling.

The menu contains the following dialogs:

- SFlow Configuration
- SFlow Receiver

# 7.8.1 SFlow Configuration

[Diagnostics > SFlow > Configuration]

This dialog displays device parameters and lets you set up sFlow instances.

The dialog contains the following tabs:
- [Global]
- [Sampler]
- [Poller]

## [Global]

### Information

Version

Displays the MIB version, the organization responsible for agent implementation, and the device software revision.

IP address

Displays the IP address associated with the agent providing SNMP connectivity.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Sampler]

### Table

Port

Displays the physical source of data for the sampler.

Receiver

Displays the receiver index associated with the sampler.

Sampling rate

Specifies the static sampling rate for the sampling of the packets from this source.

Possible values:

- `0` (default setting)
  Deactivates the sampling.
- `256..65535`
  When the ports receive data, the device increments to the set value and then samples the data.

Max. header size [byte]

Specifies the maximum header size in bytes copied from a sampled packet.

Possible values:

- `20..256` (default setting: `128`)

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [Poller]

### Table

Port

Displays the physical source of data for the poller counter.

Receiver

Displays the receiver index associated with the query counter.

Possible values:

- `0..8` (default setting: `0`)

Interval [s]

Specifies the maximum number of seconds between successive samples of the counters which are associated with this data source.

Possible values:

- `0..86400` (default setting: `0`)

A sampling interval with the value `0` deactivates the sampling of the counters.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 7.8.2 SFlow Receiver

[ Diagnostics > SFlow > Receiver ]

In order to help avoid a condition where 2 persons or organizations attempt to assume control of the same sampler, the person or organization sets both the *Name* and *Timeout [s]* parameters in the same SNMP set request.

When releasing a sampler, the controlling person or organization deletes the value in the *Name* column. The controlling person or organization also restores the other parameters in this row to their default settings.

### Table

Index

Displays the index number to which the table entry relates.

Name

Specifies the name of the person or company which uses the entry. An empty field indicates that the entry is currently unused. Edit this field before making changes to other sampler parameters.

Possible values:

- Alphanumeric ASCII character string with 0..127 characters

Timeout [s]

Displays the time, in seconds, remaining before the sampler is released and stops sampling.

Datagram size [byte]

Specifies the maximum number of data bytes that are sent in one sample datagram.

Possible values:

- `200..3996` (default setting: `1400`)

IP address

Specifies the IP address of the sFlow collector.

Possible values:

- Valid IPv4 address (default setting: `0.0.0.0`)

Destination UDP port

Specifies the number of the UDP port for sFlow datagrams.

Possible values:

- `1..65535` (default setting: `6343`)
  Exception: Port `2222` is reserved for internal functions.

Datagram version

Displays the version of sFlow datagrams requested.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 7.9 Report

[ Diagnostics > Report ]

The menu contains the following dialogs:

- Report Global
- Persistent Logging
- System Log
- Audit Trail

# 7.9.1 Report Global

[ Diagnostics > 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
- on a connection to the Command Line Interface set up using Telnet

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 16.

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

| File name | Format | Comments |
|---|---|---|
| `audittrail.html` | HTML | Contains the chronological recording of the system events and saved user changes in the Audit Trail. |
| `defaultconfig.xml` | XML | Contains the configuration profile with the default settings. |
| `script` | TEXT | Contains the output of the command `show running-config script`. |
| `runningconfig.xml` | XML | Contains the configuration profile with the current operating settings. |
| `supportinfo.html` | TEXT | Contains device internal service information. |
| `systeminfo.html` | HTML | Contains information about the current settings and operating parameters. |
| `systemlog.html` | HTML | Contains the logged events in the Log file. See the *Diagnostics* > Report > *System Log* dialog. |

### Meaning of the event severities

| Severity | Meaning |
|---|---|
| `emergency` | Device not ready for operation |
| `alert` | Immediate user intervention required |
| `critical` | Critical status |

| Severity | Meaning |
|---|---|
| error | Error status |
| warning | Warning |
| notice | Significant, normal status |
| informational | Informal message |
| debug | Debug message |

# 7.9.2 Persistent Logging

[ Diagnostics > Report > 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

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:

- `sd`
  External SD memory (ACA31)
- `usb`
  External USB memory (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 16.

Delete persistent log file

Removes the log files from the external memory.

## 7.9.3 System Log

[ Diagnostics > Report > 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 16.

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 bowser command.

Delete log file

Removes the logged events from the log file.

## 7.9.4 Audit Trail

[Diagnostics > Report > 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 16.

Save audit trail 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 bowser command.

# 8 Advanced

The menu contains the following dialogs:
- DHCP L2 Relay
- DHCP Server
- DNS
- Command Line Interface

## 8.1 DHCP L2 Relay

[ Advanced > DHCP L2 Relay ]

A network administrator uses the DHCP L2 *Relay Agent* to add DHCP client information. L3 *Relay Agents* and DHCP servers need the DHCP client information to assign an IP address and a configuration to the clients.

When active, the relay adds *Option 82* information configured in this dialog to the packets before it relays DHCP requests from the clients to the server. The *Option 82* fields provide unique information about the client and relay. This unique identifier consists of a *Circuit ID* for the client and a *Remote ID* for the relay.

In addition to the type, length, and multicast fields, the *Circuit ID* includes the VLAN ID, unit number, slot number, and port number for the connected client.

The *Remote ID* consists of a type and length field and either a MAC address, IP address, client identifier, or a user-defined device description. A client identifier is the user-defined system name for the device.

The menu contains the following dialogs:
- DHCP L2 Relay Configuration
- DHCP L2 Relay Statistics

# 8.1.1 DHCP L2 Relay Configuration

[ Advanced > DHCP L2 Relay > Configuration ]

This dialog lets you activate the relay function on an interface and VLAN. When you activate this function on a port, the device either relays the *Option 82* information or drops the information on untrusted ports. Furthermore, the device lets you specify the remote identifier.

The dialog contains the following tabs:
- [Interface]
- [VLAN ID]

### Operation

Operation

Enables/disables the DHCP L2 Relay function of the device globally.

Possible values:

- `On`
  Enables the *DHCP L2 Relay* function in the device.
- `Off` (default setting)
  Disables the *DHCP L2 Relay* function in the device.

## [Interface]

### Table

Port

Displays the port number.

Active

Activates/deactivates the *DHCP L2 Relay* function on the port.

The prerequisite is that you enable the function globally.

Possible values:

- `marked`
  The *DHCP L2 Relay* function is active.
- `unmarked` (default setting)
  The *DHCP L2 Relay* function is inactive.

Trusted port

Activates/deactivates the secure *DHCP L2 Relay* mode for the corresponding port.

Possible values:

- `marked`
  The device accepts DHCPv4 packets with *Option 82* information.
- `unmarked` (default setting)
  The device discards DHCPv4 packets received on non-secure ports that contain *Option 82* information.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## [VLAN ID]

### Table

VLAN ID

VLAN to which the table entry relates.

Active

Activates/deactivates the *DHCP L2 Relay* function on the VLAN.

The prerequisite is that you enable the function globally.

Possible values:

- `marked`
  The *DHCP L2 Relay* function is active.
- `unmarked` (default setting)
  The *DHCP L2 Relay* function is inactive.

Circuit ID

Activates or deactivates the addition of the *Circuit ID* to the *Option 82* information.

Possible values:

- `marked` (default setting)
  Enables *Circuit ID* and *Remote ID* to be sent together.
- `unmarked`
  The device sends only the *Remote ID*.

Remote ID type

Specifies the components of the *Remote ID* for this VLAN.

Possible values:

- `ip`
  Specifies the IP address of the device as *Remote ID*.
- `mac` (default setting)
  Specifies the MAC address of the device as *Remote ID*.
- `client-id`
  Specifies the system name of the device as *Remote ID*.
- `other`
  When you use this value, enter in the *Remote ID* column user-defined information.

Remote ID

Displays the *Remote ID* for the VLAN.

When you specify the value `other` in the *Remote ID type* column, specify the identifier.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 8.1.2 DHCP L2 Relay Statistics

[ Advanced > DHCP L2 Relay > Statistics ]

The device monitors the traffic on the ports and displays the results in tabular form.

This table is divided into various categories to aid you in traffic analysis.

### Table

Port

Displays the port number.

Untrusted server messages with Option 82

Displays the number of DHCP server messages received with *Option 82* information on the untrusted interface.

Untrusted client messages with Option 82

Displays the number of DHCP client messages received with *Option 82* information on the untrusted interface.

Trusted server messages without Option 82

Displays the number of DHCP server messages received without *Option 82* information on the trusted interface.

Trusted client messages without Option 82

Displays the number of DHCP client messages received without *Option 82* information on the trusted interface.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Reset

Resets the entire table.

# 8.2 DHCP Server

[Advanced > DHCP Server]

With the DHCP server, you manage a database of available IP addresses and configuration information. When the device receives a request from a client, the DHCP server validates the DHCP client network, and then leases an IP address. When activated, the DHCP server also allocates configuration information appropriate for that client. The configuration information specifies, for example, which IP address, DNS server and the default route a client uses.

The DHCP server assigns an IP address to a client for a user-defined interval. The DHCP client is responsible for renewing the IP address before the interval expires. When the DHCP client is unable to renew the address, the address returns to the pool for reassignment.

The menu contains the following dialogs:

- DHCP Server Global
- DHCP Server Pool
- DHCP Server Lease Table

# 8.2.1 DHCP Server Global

[ Advanced > DHCP Server > Global ]

Activate the function either globally or per port according to your requirements.

### Operation

Operation

Enables/disables the DHCP server function of the device globally.

Possible values:

- `On`
- `Off` (default setting)

### Configuration

IP Probe

Activates/deactivates the probing for unique IP addresses. Before assigning an IP address, the server uses an *ICMP Echo* request to check whether this IP address is already in use on the network.

Possible values:

- `marked` (default setting)
  The *IP Probe* function is active.
- `unmarked`
  The *IP Probe* function is inactive.

### Table

Port

Displays the port number.

DHCP server active

Activates/deactivates the DHCP server function on this port.

The prerequisite is that you enable the function globally.

Possible values:

- `marked` (default setting)
  The DHCP server function is active.
- `unmarked`
  The DHCP server function is inactive.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 8.2.2 DHCP Server Pool

[ Advanced > DHCP Server > Pool ]

Assign an IP address to an end device or switch connected to a port or included in a VLAN.

The DHCP server provides IP address pools from which it allocates IP addresses to clients. A pool consists of a list of entries. Specify an entry as static to a specific IP address, or as dynamic to an IP address range. The device holds a maximum of 128 pools. The pools together hold a maximum of 1000 entries.

With static allocation, the DHCP server assigns an IP address to a specific client. The DHCP server identifies the client using a unique hardware ID. A static address entry contains one IP address. You apply this IP address to every port or to a specific port of the device. For static allocation, enter an IP address for allocation in the *IP address* field, and leave the *Last IP address* column empty. Enter a hardware ID with which the DHCP server uniquely identifies the client. This ID is either a MAC address, a Client ID, a Remote ID, or a Circuit ID. When a client contacts the device with a known hardware ID, the DHCP server allocates the static IP address.

In dynamic allocation, when a DHCP client makes contact on a port, the DHCP server assigns an available IP address from a pool for this port. For dynamic allocation, create a pool for the ports by assigning an IP address range. Specify the first and last IP addresses for the IP address range. Leave the *MAC address*, *Client ID*, *Remote ID* and *Circuit ID* fields empty. You have the option of creating multiple pool entries. This lets you create an IP address range that contains gaps.

When routing is enabled, the *DHCP Server* function for a specific DHCP pool only takes effect if one of the following prerequisites is met:

- The device has a router interface in the subnet of the respective DHCP pool.
- The device management is located in the subnet of the respective DHCP pool.

This dialog displays the different information that is required for the assignment of an IP address for a port or a VLAN. Use the button to add an entry. The device adds a writable and readable entry.

### Table

Index

Displays the index number to which the table entry relates.

Active

Activates/deactivates the DHCP server function on this port.

Possible values:

- `marked`
  The DHCP server function is active.
- `unmarked` (default setting)
  The DHCP server function is inactive.

IP address

Specifies the IP address for static IP address assignment. When using dynamic IP address assignment, this value specifies the start of the IP address range.

Possible values:

- Valid IPv4 address

Last IP address

When using dynamic IP address assignment, this value specifies the end of the IP address range.

Possible values:

- Valid IPv4 address

Port

Displays the port number.

VLAN ID

Displays the VLAN to which the table entry relates.

A value of `1` corresponds to the default device management VLAN.

Possible values:

- `1..4042`

MAC address

Specifies the MAC address of the device leasing the IP address.

Possible values:

- Valid Unicast MAC address
  Specify the value with a colon separator, for example `00:11:22:33:44:55`.
- `–`
  For the IP address assignment, the server ignores this variable.

DHCP relay

Specifies the IP address of the DHCP relay through which the clients transmit their requests to the DHCP server. When the DHCP server receives the client's request through another DHCP relay, it ignores this request.

Possible values:

- Valid IPv4 address
  IP address of the DHCP relay.
- `–`
  Between the client and the DHCP server there is no DHCP relay.

Client ID

Specifies the identification of the client device leasing the IP address.

Possible values:

- 1..80 bytes (format `XX XX .. XX`)
- `-`
  For the IP address assignment, the server ignores this variable.

Remote ID

Specifies the identification of the remote device leasing the IP address.

Possible values:

- 1..80 bytes (format `XX XX .. XX`)
- `-`
  For the IP address assignment, the server ignores this variable.

Circuit ID

Specifies the Circuit ID of the device leasing the IP address.

Possible values:

- 1..80 bytes (format `XX XX .. XX`)
- `-`
  For the IP address assignment, the server ignores this variable.

Hirschmann device

Activates/deactivates Hirschmann multicasts.

If the device in this IP address range serves only Hirschmann devices, then activate this function.

Possible values:

- `marked`
  In this IP address range, the device serves only Hirschmann devices. Hirschmann multicasts are activated.
- `unmarked` (default setting)
  In this IP address range, the device serves the devices of different manufacturers. Hirschmann multicasts are deactivated.

Configuration URL

Specifies the protocol to be used as well as the name and path of the configuration file.

Possible values:

- Alphanumeric ASCII character string with 0..70 characters
  Example: `tftp://192.9.200.1/cfg/config.xml`

When you leave this field blank, the device leaves this option field blank in the DHCP message.

Lease time [s]

Specifies the lease time in seconds.

Possible values:

- `60..220752000` (default setting: `86400`)
- `4294967295`
  Use this value for assignments unlimited in time and for assignments via BOOTP.

Default gateway

Specifies the IP address of the default gateway.

A value of `0.0.0.0` disables the attachment of the option field in the DHCP message.

Possible values:

- Valid IPv4 address

Netmask

Specifies the mask of the network to which the client belongs.

A value of `0.0.0.0` disables the attachment of the option field in the DHCP message.

Possible values:

- Valid IPv4 netmask

WINS server

Specifies the IP address of the Windows Internet Name Server which converts NetBIOS names.

A value of `0.0.0.0` disables the attachment of the option field in the DHCP message.

Possible values:

- Valid IPv4 address

DNS server

Specifies the IP address of the DNS server.

A value of `0.0.0.0` disables the attachment of the option field in the DHCP message.

Possible values:

- Valid IPv4 address

Hostname

Specifies the hostname.

When you leave this field blank, the device leaves this option field blank in the DHCP message.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

## 8.2.3 DHCP Server Lease Table

[ Advanced > DHCP Server > Lease Table ]

This dialog displays the status of IP address leasing on a per port basis.

### Table

Port

Displays the port number to which the address is currently being leased.

IP address

Displays the leased IP address to which the entry refers.

Status

Displays the lease phase.

According to the standard for DHCP operations, there are 4 phases to leasing an IP address: Discovery, Offer, Request, and Acknowledgement.

Possible values:

- `bootp`
  A DHCP client is attempting to discover a DHCP server for IP address allocation.
- `offering`
  The DHCP server is validating that the IP address is suitable for the client.
- `requesting`
  A DHCP client is acquiring the offered IP address.
- `bound`
  The DHCP server is leasing the IP address to a client.
- `renewing`
  The DHCP client is requesting an extension to the lease.
- `rebinding`
  The DHCP server is assigning the IP address to the client after a successful renewal.
- `declined`
  The DHCP server denied the request for the IP address.
- `released`
  The IP address is available for other clients.

Remaining lifetime

Displays the time remaining on the leased IP address.

Leased MAC address

Displays the MAC address of the device leasing the IP address.

Gateway

Displays the Gateway IP address of the device leasing the IP address.

Client ID

Displays the client identifier of the device leasing the IP address.

Remote ID

Displays the remote identifier of the device leasing the IP address.

Circuit ID

Displays the Circuit ID of the device leasing the IP address.

**Buttons**

You find the description of the standard buttons in section “Buttons” on page 16.

## 8.3 DNS

[ Advanced > DNS ]

The menu contains the following dialogs:
- DNS Client

### 8.3.1 DNS Client

[ Advanced > 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
- DNS Client Static Hosts

# 8.3.1.1 DNS Client Global

[ Advanced > DNS > Client > Global ]

In this dialog you enable the *Client* function and the *Cache* function.

### Operation

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.

### Cache

Cache

Enables/disables the *Cache* function.

Possible values:

- *On* (default setting)
  The *Cache* function is enabled.
  The device temporarily saves up to 128 DNS server responses (hostname and corresponding IP address) in the cache. When the cache contains a matching entry, the host name of a new request the device resolves itself. This makes sending a new query to the DNS server unnecessary.
- *Off*
  The *Cache* function is disabled.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Flush cache

Removes every entry from the DNS cache.

# 8.3.1.2 DNS Client Current

[ Advanced > DNS > Client > Current ]

This dialog displays to which DNS servers the device sends requests for resolving hostnames in IP addresses.

### Table

Index

Displays the sequential number of the DNS server.

Address

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.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 8.3.1.3 DNS Client Static

[Advanced > 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 yourself or to transfer the IP addresses from a DHCP server.

### 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.
- `mgmt-dhcp` (default setting)
  The device uses the IP addresses which the DHCP server delivers to the device.

Domain name

Specifies the domain name according to RFC 1034 which the device adds to hostnames without a domain suffix.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

Request timeout [s]

Specifies the time interval in seconds for sending again a request to the server.

Possible values:

- `0`
  Deactivates the function. The device does not send a request to the server again.
- `1..3600` (default setting: `3`)

Request retransmits

Specifies, how many times the device retransmits a request.

The prerequisite is that, in the *Request timeout [s]* field, you specify a value >`0`.

Possible values:

- `0..100` (default setting: `2`)

### 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.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 8.3.1.4 DNS Client Static Hosts

[Advanced > DNS > Client > Static Hosts]

This dialog lets you specify up to 64 hostnames which you link with one IP address each. Upon a request for resolving hostnames in IP addresses, the device searches this table for a corresponding entry. When the device does not find a corresponding entry, it forwards the request.

### Table

Index

Displays the index number to which the table entry relates.

Possible values:

- `1..64`

Name

Specifies the hostname.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

IP address

Specifies the IP address under which the host is reachable.

Possible values:

- Valid IPv4 address

Active

Activates/deactivates the table entry.

Possible values:

- `marked`
  The device resolves a request for the host name for this entry.
- `unmarked`
  After receiving a request for this host name, the device sends a request to one of the configured name servers for resolution.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

# 8.3.2 OPC UA Server

[ Advanced > Industrial Protocols > OPC UA Server ]

The protocol *OPC UA* is a standardized protocol for industrial communication defined in the standard IEC 62541. The *OPC UA Server* function monitors the *OPC UA* information model data for the industrial automation equipments such as Programmable Logic Controllers (PLC), sensors and meters.

To monitor the *OPC UA* information model data of the connected end devices, use an *OPC UA* client application.

In this dialog you enable the *OPC UA Server* function and specify the required settings. You can also specify the number of sessions allowed to be open at the same time. The dialog lets you manage the *OPC UA* user accounts required to access the device using a *OPC UA* client application. Every *OPC UA* user requires an active *OPC UA* user account to gain access to the *OPC UA* server of the device.

## Operation

Operation

Enables/disables the *OPC UA Server* function in the device.

Possible values:

- `On`
  The *OPC UA Server* function is enabled.
- `Off` (default setting)
  The *OPC UA Server* function is disabled.

## Configuration

Listening port

Specifies the TCP port number that the *OPC UA Server* server uses for communication.

Possible values:

- `1..65535` (default setting: `4840`)
  Exception: Port `2222` is reserved for internal functions.

Sessions (max.)

Specifies the maximum number of *OPC UA* connections to the device that can be set up simultaneously. Each accessing *OPC UA* client application establishes a separate *OPC UA* connection to the device.

Possible values:

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

Security policy

Specifies the authentication and encryption protocol that the device applies for the *OPC UA* user.

Possible values:

- *none* (default setting)
  The *OPC UA* user does not need to authenticate oneself.
- *basic128Rsa15*
  The *OPC UA* user authenticates using the *Basic128Rsa15* protocol.
- *basic256*
  The *OPC UA* user authenticates using the *Basic256* protocol.
- *basic256Sha256*
  The *OPC UA* user authenticates using the *Basic256Sha256* protocol.

### Table

User name

Displays the name of the *OPC UA* user having access to the device using an *OPC UA* client application.

Password

Specifies the password that the user applies to access the device using an *OPC UA* client application.

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`
  - `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`

Access role

Specifies the role that regulates the access of the *OPC UA* user using an *OPC UA* client application.

Possible values:

- `readOnly` (default setting)
  The *OPC UA* user account has read-only access to the device. The *OPC UA* user can view the *OPC UA* information model data of the connected end devices.

Active

Activates/deactivates the *OPC UA* user account in the device.

Possible values:

- `marked`
  The *OPC UA* user account is active. The device accepts the login of an *OPC UA* user with this user name.
- `unmarked` (default setting)
  The *OPC UA* user account is inactive. The device rejects the login of an *OPC UA* user with this user name.

### Buttons

You find the description of the standard buttons in section “Buttons” on page 16.

Opens the *Create* window to add a new entry to the table. The device lets you specify up to 4 *OPC UA* user accounts.

- In the *User name* field, you specify the name of the *OPC UA* user account.
  Possible values:
  Alphanumeric ASCII character string with 1..32 characters
  The following characters are allowed:
  - `a..z`
  - `A..Z`
  - `0..9`
  - `<space>`
  - `-_`

# 8.4 Command Line Interface

[ Advanced > CLI ]

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 16.

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


**0-9**

802.1D/p mapping . . . 267
802.1X . . . 109, 152

**A**

Access control . . . 152
Access control lists . . . 205
Access restriction . . . 135
ACL . . . 205
Address conflict detection . . . 29, 517
Aging time . . . 227, 523
Alarms . . . 510
ARP . . . 367, 374, 517
ARP inspection . . . 196
ARP table . . . 374, 523
Audit trail . . . 590
Authentication history . . . 166
Authentication list . . . 109
Auto disable . . . 148, 185, 199, 201, 316, 545, 546, 554, 572
Auto summary . . . 383

**B**

Boundary clock . . . 85
Bridge . . . 313

**C**

Cable diagnosis . . . 540
Certificate . . . 21, 51, 114, 132, 133, 499, 527, 534
CLI . . . 139
Command line interface . . . 139
Community names . . . 142
Configuration check . . . 515
Configuration profile . . . 15, 41
Context menu . . . 15
Counter reset . . . 68
Count-to-infinity . . . 383

**D**

Daylight saving time . . . 72
Device software . . . 38
Device software backup . . . 38
Device status . . . 19, 490
DHCP L2 relay . . . 591
DHCP server . . . 596
DHCP snooping . . . 184
Distance vector . . . 382
DNS . . . 605
DNS cache . . . 606
DNS client . . . 606
Domain name system . . . 605
DoS . . . 179
DSCP . . . 269
Dynamic ARP inspection . . . 196

**E**
EAPOL . . . . . 164
Egress rate limiter . . . . . 230
Email notification . . . . . 526
Encryption . . . . . 41
ENVM . . . . . 39, 46, 53, 492, 498, 505, 587
Event severity . . . . . 530, 584
External memory . . . . . 39, 46, 53, 587

**F**
FAQ . . . . . 621
FDB . . . . . 233
Filter MAC addresses . . . . . 233
Fingerprint . . . . . 127, 131
Flash memory . . . . . 39, 514
Flow control . . . . . 227
Forwarding database . . . . . 233

**G**
GARP . . . . . 259
GMRP . . . . . 260
Guards . . . . . 330
GVRP . . . . . 262

**H**
Hardware clock . . . . . 71
Hardware state . . . . . 514
HiDiscovery . . . . . 29, 499, 590
HIPER ring . . . . . 311
HiVRRP . . . . . 467, 468, 482
Host key . . . . . 129
Host routes accept . . . . . 383
HTML . . . . . 513, 589
HTTP . . . . . 129
HTTP server . . . . . 497
HTTPS . . . . . 130

**I**
IAS . . . . . 109, 168
ICMP redirect . . . . . 361, 368
IEEE 802.1X . . . . . 109
IGMP . . . . . 454
IGMP snooping . . . . . 235
Industrial HiVision . . . . . 11, 123
Ingress filtering . . . . . 298
Ingress rate limiter . . . . . 230
Integrated authentication server . . . . . 109, 168
IP access restriction . . . . . 135
IP address conflict detection . . . . . 517
IP DSCP mapping . . . . . 269
IP source guard . . . . . 192
IPv4 rule . . . . . 206

**L**
L2 relay . . . 591
L3 relay . . . 439
LDAP . . . 109
Link aggregation . . . 334
Link backup . . . 342
LLDP . . . 562
Load/save . . . 41
Log file . . . 68, 589
Login banner . . . 140, 143
Loop protection . . . 505
Loopback interface . . . 444
Loops . . . 312

**M**
MAC Address Conflict Detection . . . 29
MAC address table . . . 233
MAC flood . . . 147
MAC rule . . . 214
MAC spoof . . . 147
Mail notification . . . 526
Management access . . . 29, 135
Management VLAN . . . 29
Media redundancy protocol . . . 307
Menu . . . 15
MMRP . . . 251
Modules . . . 491, 504
MRP . . . 307
MRP-IEEE . . . 249
MSTP . . . 313
Multicast . . . 454
Multicast routing . . . 447
MVRP . . . 256

**N**
Network load . . . 61
NVM . . . 14, 15, 23, 39, 46

**O**
OSPF . . . 389
Out-of-band management port . . . 35

**P**

Password . . . . . 104, 496
Password length . . . . . 104, 496
Persistent logging . . . . . 586
PoE . . . . . 63
Port clients . . . . . 162
Port configuration . . . . . 156, 265
Port mirroring . . . . . 558
Port monitor . . . . . 554
Port priority . . . . . 265
Port security . . . . . 147
Port statistics . . . . . 164
Port VLAN . . . . . 297
Port-based access control . . . . . 152
Power over Ethernet . . . . . 63
Power supply . . . . . 21, 492, 505
Pre-Login banner . . . . . 143
Priority queue . . . . . 264
Proxy ARP . . . . . 367

**Q**

Queue management . . . . . 271
Queues . . . . . 264

**R**

RADIUS . . . . . 109, 169
RAM . . . . . 45
RAM test . . . . . 524
Rate limiter . . . . . 230
RCP . . . . . 358
Reboot . . . . . 68
Redundant coupling protocol . . . . . 358
Relay . . . . . 439, 591
Request interval . . . . . 77
Ring structure . . . . . 307
Ring/Network coupling . . . . . 352
RIP . . . . . 382
RIP statistics . . . . . 388
RNC . . . . . 352
Root bridge . . . . . 313
Route distribution . . . . . 386
Router discovery . . . . . 379
Router interface . . . . . 295, 366
Routing information protocol . . . . . 382
Routing profiles . . . . . 362
Routing table . . . . . 427
RSTP . . . . . 312, 313

**S**

Secure shell . . . . . 126
Security status . . . . . 20, 495
Self-test . . . . . 524
Serial interface . . . . . 498
Service port . . . . . 35
Settings . . . . . 41
Severity . . . . . 530, 584
sFlow . . . . . 575
SFP module . . . . . 538
Signal contact . . . . . 20, 501
SNMP server . . . . . 123, 498
SNMP traps . . . . . 59, 65, 149, 313, 338, 391, 433, 468, 490, 495, 503, 510, 519, 521, 545
SNMPv1/v2 . . . . . 142
SNTP . . . . . 75
SNTP client . . . . . 76
SNTP server . . . . . 80
Software backup . . . . . 38
Software update . . . . . 38
Source guard . . . . . 192
Spanning tree protocol . . . . . 312
SSH server . . . . . 126
Subring . . . . . 347
Switch dump . . . . . 584
Syslog . . . . . 534
System information . . . . . 513
System log . . . . . 589
System monitor . . . . . 524
System time . . . . . 71

**T**

Technical questions . . . . . 621
Telnet server . . . . . 124, 497
Temperature . . . . . 22, 491, 504
Threshold values network load . . . . . 230
Time profile . . . . . 222
Time to live . . . . . 364
Topology discovery . . . . . 567
Tracking . . . . . 431, 486
Training courses . . . . . 621
Transparent clock . . . . . 95
Trap destination . . . . . 510
Traps . . . . . 59, 65, 149, 313, 338, 391, 433, 468, 490, 495, 503, 510, 519, 521, 545
Trust mode . . . . . 265
TTL . . . . . 364
Twisted pair . . . . . 540

**U**

Unaware mode . . . . . 227
User administration . . . . . 103
Utilization . . . . . 61

**V**
Virtual local area network . . . . . 292
Virtual router redundancy protocol . . . . . 467
VLAN . . . . . 29, 292, 573
VLAN configuration . . . . . 295
VLAN ports . . . . . 297
VLAN unaware mode . . . . . 227
VRRP . . . . . 467
VRRP statistics . . . . . 484
VRRP tracking . . . . . 486

**W**
Watchdog . . . . . 41, 45
Web server . . . . . 129, 130

**Z**
ZIP archive . . . . . 584

# 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.

### Customer Innovation Center

The Customer Innovation 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.belden.com/solutions/customer-innovation-center.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Customer Innovation 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:

| | Very Good | Good | Satisfactory | Mediocre | Poor |
|---|---|---|---|---|---|
| Precise description | O | O | O | O | O |
| Readability | O | O | O | O | O |
| Understandability | O | O | O | O | O |
| Examples | O | O | O | O | O |
| Structure | O | O | O | O | O |
| Comprehensive | O | O | O | O | O |
| Graphics | O | O | O | O | O |
| Drawings | O | O | O | O | O |
| Tables | O | O | O | O | O |

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

HIRSCHMANN

A BELDEN BRAND

HIRSCHMANN
A BELDEN BRAND

# User Manual

## Configuration
## DRAGON Switch
## HiOS-3A-UR



Technical support
https://hirschmann-support.belden.com

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.

© 2021 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** | 11 |
| | **About this Manual** | 13 |
| | **Key** | 14 |
| | **Replacing a faulty device** | 15 |
| **1** | **User interfaces** | 17 |
| 1.1 | Graphical User Interface | 17 |
| 1.2 | Command Line Interface | 18 |
| 1.2.1 | Preparing the data connection | 18 |
| 1.2.2 | Access to the Command Line Interface using Telnet | 18 |
| 1.2.3 | Access to the Command Line Interface using SSH (Secure Shell) | 21 |
| 1.2.4 | Access to the Command Line Interface using the serial interface | 23 |
| 1.2.5 | Mode-based command hierarchy | 25 |
| 1.2.6 | Executing the commands | 29 |
| 1.2.7 | Structure of a command | 29 |
| 1.2.8 | Examples of commands | 32 |
| 1.2.9 | Input prompt | 33 |
| 1.2.10 | Key combinations | 34 |
| 1.2.11 | Data entry elements | 36 |
| 1.2.12 | Use cases | 37 |
| 1.2.13 | Service Shell | 38 |
| 1.3 | System monitor | 41 |
| 1.3.1 | Functional scope | 41 |
| 1.3.2 | Starting the System Monitor | 41 |
| **2** | **Specifying the IP parameters** | 43 |
| 2.1 | IP parameter basics | 43 |
| 2.1.1 | IPv4 | 43 |
| 2.2 | Specifying the IP parameters using the Command Line Interface | 47 |
| 2.2.1 | IPv4 | 47 |
| 2.3 | Specifying the IP parameters using HiDiscovery | 49 |
| 2.3.1 | Relay | 50 |
| 2.3.2 | Example configuration | 50 |
| 2.4 | Specifying the IP parameters using the Graphical User Interface | 52 |
| 2.4.1 | IPv4 | 52 |
| 2.5 | Specifying the IP parameters using BOOTP | 53 |
| 2.6 | Specifying the IP parameters using DHCP | 54 |
| 2.6.1 | IPv4 | 54 |
| 2.7 | Management address conflict detection | 56 |
| 2.7.1 | Active and passive detection | 56 |
| **3** | **Access to the device** | 57 |
| 3.1 | Access roles | 57 |
| 3.2 | First login (Password change) | 58 |

3.3 Authentication lists . . . 59
3.3.1 Applications . . . 59
3.3.2 Policies . . . 59
3.3.3 Managing authentication lists . . . 59
3.3.4 Adjust the settings . . . 60
3.4 User management . . . 62
3.4.1 Access roles . . . 62
3.4.2 Managing user accounts . . . 64
3.4.3 Default setting . . . 64
3.4.4 Changing default passwords . . . 64
3.4.5 Setting up a new user account . . . 65
3.4.6 Deactivating the user account . . . 66
3.4.7 Adjusting policies for passwords . . . 67
3.5 LDAP . . . 69
3.5.1 Coordination with the server administrator . . . 69
3.5.2 Example configuration . . . 70
3.6 SNMP access . . . 73
3.6.1 SNMPv1/v2 access . . . 73
3.6.2 SNMPv3 access . . . 73
3.7 Out of Band access . . . 75
3.7.1 Specifying the IP parameters . . . 75
3.7.2 Disable the Service Port network interface . . . 77

**4 Synchronizing the system time in the network** . . . 79
4.1 Basic settings . . . 79
4.1.1 Setting the time . . . 79
4.1.2 Automatic daylight saving time changeover . . . 81
4.2 SNTP . . . 82
4.2.1 Preparation . . . 83
4.2.2 Defining settings of the SNTP client . . . 84
4.2.3 Specifying SNTP server settings . . . 85
4.3 PTP . . . 86
4.3.1 Types of clocks . . . 86
4.3.2 Best Master Clock algorithm . . . 87
4.3.3 Delay measurement . . . 87
4.3.4 PTP domains . . . 88
4.3.5 Using PTP . . . 88

**5 Managing configuration profiles** . . . 89
5.1 Detecting changed settings . . . 89
5.1.1 Volatile memory (RAM) and non-volatile memory (NVM) . . . 89
5.1.2 External memory (ACA) and non-volatile memory (NVM) . . . 90
5.2 Saving the settings . . . 91
5.2.1 Saving the configuration profile in the device . . . 91
5.2.2 Saving the configuration profile in the external memory . . . 93
5.2.3 Backup the configuration profile on a remote server . . . 93
5.2.4 Exporting a configuration profile . . . 94
5.3 Loading settings . . . 96
5.3.1 Activating a configuration profile . . . 96
5.3.2 Loading the configuration profile from the external memory . . . 96
5.3.3 Importing a configuration profile . . . 98

5.4 Reset the device to the factory defaults . . . 101
5.4.1 Using the Graphical User Interface or Command Line Interface . . . 101
5.4.2 Using the System Monitor . . . 101

**6 Loading software updates** . . . 103
6.1 Software update from the PC . . . 103
6.2 Software update from a server . . . 104
6.3 Software update from the external memory . . . 105
6.3.1 Manually—initiated by the administrator . . . 105
6.3.2 Automatically—initiated by the device . . . 105
6.4 Loading a previous software version . . . 107

**7 Configuring the ports** . . . 109
7.1 Enabling/disabling the port . . . 109
7.2 Selecting the operating mode . . . 110
7.3 Gigabit Ethernet mode for ports . . . 111
7.3.1 Example . . . 111

**8 Assistance in the protection from unauthorized access** . . . 113
8.1 Changing the SNMPv1/v2 community . . . 113
8.2 Disabling SNMPv1/v2 . . . 114
8.3 Disabling HTTP . . . 115
8.4 Disabling Telnet . . . 116
8.5 Disabling the HiDiscovery access . . . 117
8.6 Activating the IP access restriction . . . 118
8.7 Adjusting the session timeouts . . . 120
8.8 Deactivating the unused modules . . . 122

**9 Controlling the data traffic** . . . 123
9.1 Helping protect against unauthorized access . . . 123
9.2 ACL . . . 125
9.2.1 Creating and editing IPv4 rules . . . 126
9.2.2 Creating and configuring an IP ACL using the Command Line Interface . . . 127
9.2.3 Creating and editing MAC rules . . . 127
9.2.4 Creating and configuring a MAC ACL using the Command Line Interface . . . 128
9.2.5 Assigning ACLs to a port or VLAN . . . 129
9.3 MAC authentication bypass . . . 130

**10 Network load control** . . . 131
10.1 Direct packet distribution . . . 131
10.1.1 Learning MAC addresses . . . 131
10.1.2 Aging of learned MAC addresses . . . 131
10.1.3 Static address entries . . . 131
10.2 Multicasts . . . 134
10.2.1 Example of a Multicast application . . . 134
10.2.2 IGMP snooping . . . 134
10.3 Rate limiter . . . 139

10.4 QoS/Priority . . . 140
10.4.1 Description of prioritization . . . 140
10.4.2 Handling of received priority information . . . 141
10.4.3 VLAN tagging . . . 141
10.4.4 IP ToS (Type of Service) . . . 142
10.4.5 Handling of traffic classes . . . 143
10.4.6 Queue management . . . 144
10.4.7 Management prioritization . . . 146
10.4.8 Setting prioritization . . . 146
10.5 Differentiated services . . . 151
10.5.1 DiffServ example . . . 152
10.6 Flow control . . . 154
10.6.1 Halfduplex or fullduplex link . . . 154
10.6.2 Setting up the Flow Control . . . 155

**11 VLANs** . . . 157
11.1 Examples of VLANs . . . 157
11.1.1 Example 1 . . . 158
11.1.2 Example 2 . . . 161
11.2 Guest VLAN / Unauthenticated VLAN . . . 166
11.3 RADIUS VLAN assignment . . . 168
11.4 Creating a Voice VLAN . . . 169
11.5 MAC based VLANs . . . 170
11.6 IP subnet based VLANs . . . 171
11.7 Protocol-based VLAN . . . 172
11.8 VLAN unaware mode . . . 173

**12 Redundancy** . . . 175
12.1 Network Topology vs. Redundancy Protocols . . . 175
12.1.1 Network topologies . . . 175
12.1.2 Redundancy Protocols . . . 176
12.1.3 Combinations of Redundancies . . . 177
12.2 Media Redundancy Protocol (MRP) . . . 178
12.2.1 Network Structure . . . 178
12.2.2 Reconfiguration time . . . 179
12.2.3 Advanced mode . . . 179
12.2.4 Prerequisites for MRP . . . 179
12.2.5 Example Configuration . . . 180
12.2.6 MRP over LAG . . . 184
12.3 HIPER Ring Client . . . 188
12.3.1 VLANS on the HIPER Ring . . . 188
12.3.2 HIPER Ring over LAG . . . 189
12.4 Spanning Tree . . . 190
12.4.1 Basics . . . 190
12.4.2 Rules for Creating the Tree Structure . . . 193
12.4.3 Examples . . . 196

12.5 The Rapid Spanning Tree Protocol . . . 199
12.5.1 Port roles . . . 199
12.5.2 Port states . . . 200
12.5.3 Spanning Tree Priority Vector . . . 201
12.5.4 Fast reconfiguration . . . 201
12.5.5 Configuring the device . . . 202
12.5.6 Guards . . . 204
12.5.7 Ring only mode . . . 207
12.6 Link Aggregation . . . 209
12.6.1 Methods of Operation . . . 209
12.6.2 Link Aggregation Example . . . 210
12.7 Link Backup . . . 211
12.7.1 Fail Back Description . . . 211
12.7.2 Example Configuration . . . 211
12.8 FuseNet . . . 213
12.9 Subring . . . 214
12.9.1 Subring description . . . 214
12.9.2 Subring example . . . 216
12.9.3 Subring example configuration . . . 217
12.10 Subring with LAG . . . 219
12.10.1 Example . . . 219
12.11 Ring/Network Coupling . . . 223
12.11.1 Methods of Ring/Network Coupling . . . 223
12.11.2 Prepare the Ring/Network Coupling . . . 224
12.12 RCP . . . 237
12.12.1 Application example for RCP coupling . . . 239

**13 Routing** . . . 243
13.1 Configuration . . . 243
13.2 Routing - Basics . . . 244
13.2.1 ARP . . . 245
13.2.2 CIDR . . . 247
13.2.3 Net-directed Broadcasts . . . 248
13.2.4 Multinetting . . . 248
13.3 Static Routing . . . 249
13.3.1 Port-based Router Interface . . . 249
13.3.2 VLAN-based Router-Interface . . . 251
13.3.3 Configuration of a Static Route . . . 253
13.3.4 Static route tracking . . . 256
13.4 Tracking . . . 260
13.4.1 Interface tracking . . . 260
13.4.2 Ping tracking . . . 261
13.4.3 Logical tracking . . . 262
13.4.4 Configuring the tracking . . . 262
13.5 VRRP/HiVRRP . . . 269
13.5.1 VRRP . . . 269
13.5.2 HiVRRP . . . 272
13.5.3 HiVRRP Domains . . . 275
13.5.4 VRRP with load sharing . . . 279
13.5.5 VRRP with Multinetting . . . 279

13.6 RIP . . . 281
13.6.1 Convergence . . . 282
13.6.2 Maximum Network Size . . . 284
13.6.3 General Properties of RIP . . . 284
13.6.4 Configuring the RIP . . . 285
13.7 OSPF . . . 287
13.7.1 OSPF-Topology . . . 288
13.7.2 General Operation of OSPF . . . 292
13.7.3 Setting up the Adjacency . . . 293
13.7.4 Synchronization of the LSDB . . . 294
13.7.5 Route Calculation . . . 295
13.7.6 Configuring OSPF . . . 296
13.7.7 Limiting the distribution of the routes using an ACL . . . 299
13.8 Protocol-based VLANs . . . 310
13.8.1 General Configuration . . . 310
13.8.2 Configuration of the Example . . . 311
13.9 Multicast Routing . . . 314
13.9.1 Multicast Addresses . . . 315
13.9.2 Multicast Group Registration . . . 316
13.9.3 Scoping . . . 318
13.10 Entering the IP Parameters . . . 319

**14 Operation diagnosis** . . . 323
14.1 Sending SNMP traps . . . 323
14.1.1 List of SNMP traps . . . 324
14.1.2 SNMP traps for configuration activity . . . 325
14.1.3 SNMP trap setting . . . 325
14.1.4 ICMP messaging . . . 326
14.2 Monitoring the Device Status . . . 327
14.2.1 Events which can be monitored . . . 327
14.2.2 Configuring the Device Status . . . 328
14.2.3 Displaying the Device Status . . . 329
14.3 Security Status . . . 331
14.3.1 Events which can be monitored . . . 331
14.3.2 Configuring the Security Status . . . 332
14.3.3 Displaying the Security Status . . . 334
14.4 Out-of-Band signaling . . . 335
14.4.1 Controlling the Signal contact . . . 335
14.4.2 Monitoring the Device and Security Statuses . . . 336
14.5 Port status indication . . . 339
14.6 Port event counter . . . 340
14.6.1 Detecting non-matching duplex modes . . . 340
14.7 Auto-Disable . . . 342
14.8 Displaying the SFP status . . . 344
14.9 Topology discovery . . . 345
14.9.1 Displaying the Topology discovery results . . . 345
14.9.2 LLDP-Med . . . 346
14.10 Detecting loops . . . 347
14.11 Help protect against layer 2 network loops . . . 348
14.11.1 Application example . . . 348
14.11.2 Recommendations for redundant ports . . . 350

14.12 Using the Email Notification function . . . 351
14.12.1 Specify the sender address . . . 351
14.12.2 Specify the triggering events . . . 351
14.12.3 Change the send interval . . . 352
14.12.4 Specify the recipients . . . 353
14.12.5 Specify the mail server . . . 353
14.12.6 Enable/disable the Email Notification function . . . 354
14.12.7 Send a test email . . . 354
14.13 Reports . . . 356
14.13.1 Global settings . . . 356
14.13.2 Syslog . . . 358
14.13.3 System Log . . . 359
14.13.4 Syslog over TLS . . . 359
14.13.5 Audit Trail . . . 360
14.14 Network analysis with TCPdump . . . 362
14.15 Monitoring the data traffic . . . 363
14.15.1 Port Mirroring . . . 363
14.15.2 VLAN mirroring . . . 364
14.15.3 Remote SPAN . . . 366
14.16 Self-test . . . 377
14.17 Copper cable test . . . 379
14.18 Network monitoring with sFlow . . . 380

**15 Advanced functions of the device** . . . 383
15.1 Using the device as a DHCP server . . . 383
15.1.1 IP Addresses assigned per port or per VLAN . . . 383
15.1.2 DHCP server static IP address example . . . 384
15.1.3 DHCP server dynamic IP address range example . . . 385
15.2 DHCP L2 Relay . . . 386
15.2.1 Circuit and Remote IDs . . . 386
15.2.2 DHCP L2 Relay configuration . . . 387
15.3 Using the device as a DNS client . . . 389
15.3.1 Configuring a DNS server example . . . 389
15.4 GARP . . . 391
15.4.1 Configuring GMRP . . . 391
15.4.2 Configuring GVRP . . . 392
15.5 MRP-IEEE . . . 393
15.5.1 MRP operation . . . 393
15.5.2 MRP timers . . . 393
15.5.3 MMRP . . . 394
15.5.4 MVRP . . . 395

**16 Industry Protocols** . . . 399
16.1 *OPC UA* Server . . . 400
16.1.1 Enabling the *OPC UA* server . . . 403
16.1.2 Setting up an *OPC UA* user account . . . 404
16.1.3 Deactivating an *OPC UA* user account . . . 405
16.1.4 Delete an *OPC UA* user account . . . 405

**A Setting up the configuration environment** . . . 407
A.1 Setting up a DHCP/BOOTP server . . . 407
A.2 Setting up a DHCP server with Option 82 . . . 411

A.3 Preparing access via SSH . . . 414
A.3.1 Generating a key in the device . . . 414
A.3.2 Loading your own key onto the device . . . 414
A.3.3 Preparing the SSH client program . . . 415
A.4 HTTPS certificate . . . 417
A.4.1 HTTPS certificate management . . . 417
A.4.2 Access through HTTPS . . . 418

**B** **Appendix** . . . 419
B.1 Literature references . . . 419
B.2 Maintenance . . . 420
B.3 Management Information Base (MIB) . . . 421
B.4 List of RFCs . . . 423
B.5 Underlying IEEE Standards . . . 426
B.6 Underlying IEC Norms . . . 427
B.7 Underlying ANSI Norms . . . 428
B.8 Technical Data . . . 429
16.1.5 Switching . . . 429
16.1.6 VLAN . . . 429
16.1.7 Access Control Lists (ACL) . . . 429
16.1.8 Routing/Switching . . . 430
B.9 Copyright of integrated Software . . . 431
B.10 Abbreviations used . . . 432

**C** **Index** . . . 433

**D** **Further support** . . . 441

**E** **Readers' Comments** . . . 442

# 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

# Key

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 96.
- The new device gets its IP address using DHCP *Option 82*.
  See “DHCP L2 Relay” on page 386.
  See “Setting up a DHCP server with Option 82” on page 411.

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 417.
- 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 414.

# 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*

| User interface | Can be reached through … | Prerequisite |
|---|---|---|
| Graphical User Interface | Ethernet (In-Band) | Web browser |
| Command Line Interface | Ethernet (In-Band)<br>Serial interface (Out-of-Band) | Terminal emulation software |
| System monitor | Serial interface (Out-of-Band) | Terminal emulation software |

## 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 43.

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 Telnet

### Telnet connection using Windows

Telnet is only installed as standard in Windows versions before Windows Vista.

Perform the following steps:

- ☐ Start the *Command Prompt* program on your computer.
- ☐ Enter the command `telnet <IP_address>`.

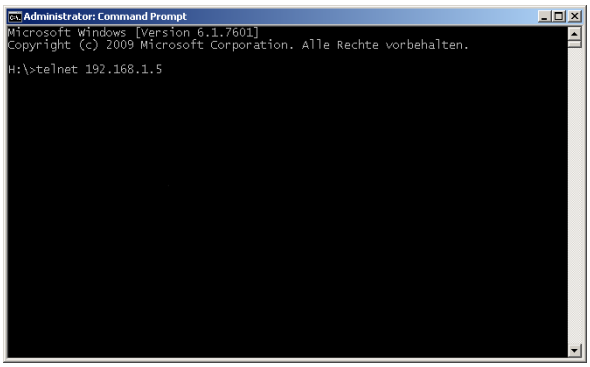



*Figure 1: Command Prompt: Setting up the Telnet connection to the device*

### Telnet connection using PuTTY

Perform the following steps:

- ☐ Start the *PuTTY* program on your computer.

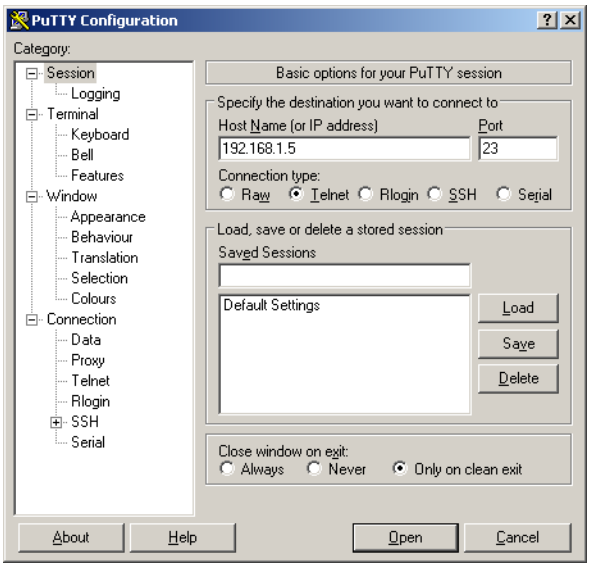



*Figure 2: PuTTY input screen*

- ☐ 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 select the connection type, select the *Telnet* radio button in the *Connection type* option list.
- ☐ Click the *Open* button to set up the data connection to your device.
  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.

**Note:** This device is a security-relevant product. Change the password during the first startup procedure.

Perform the following steps:

- ☐ 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.

```
                Copyright (c) 2011-2021 Hirschmann Automation and Control GmbH

                                All rights reserved

                        DRAGON-00484 Release HiOS-3A-UR-08.7.03

                                (Build date 2021-09-25 13:09)


                    System Name   :  DRAGON-ECE555d5e100
                    Management IP :  192.168.1.5
                    Subnet Mask   :  255.255.255.0
                    1. Router IP  :  0.0.0.0
                    Base MAC      :  EC:E5:55:01:02:03
                    OOB IP        :  192.168.1.1
                    OOB Mask      :  255.255.255.0
                    System Time   :  2021-09-27 16:21:07


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

DRAGON>
```

*Figure 3: Start screen of the Command Line Interface*

### 1.2.3 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.

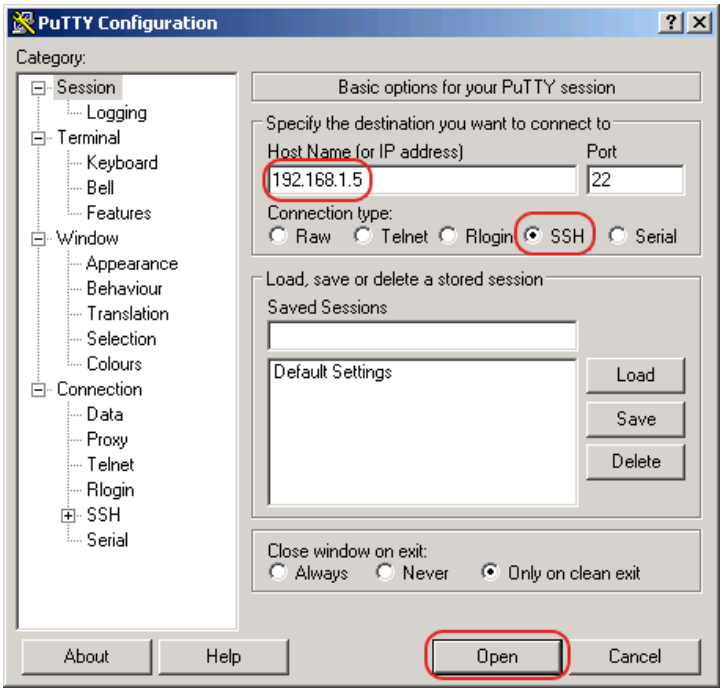



*Figure 4: PuTTY input screen*

- ☐ 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.

- ☐ 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.

*Figure 5: 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.

```
login as: admin
admin@192.168.1.5's password:


                Copyright (c) 2011-2021 Hirschmann Automation and Control GmbH

                                All rights reserved

                        DRAGON-00484 Release HiOS-3A-UR-08.7.03

                                (Build date 2021-09-25 13:09)


                    System Name   :  DRAGON-ECE555d5e100
                    Management IP :  192.168.1.5
                    Subnet Mask   :  255.255.255.0
                    1. Router IP  :  0.0.0.0
                    Base MAC      :  EC:E5:55:01:02:03
                    OOB IP        :  192.168.1.1
                    OOB Mask      :  255.255.255.0
                    System Time   :  2021-09-27 16:21:07


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

DRAGON>
```

*Figure 6: Start screen of the Command Line Interface*

### 1.2.4 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 | |
|---|---|
| Speed | 9600 bit/s |
| Data | 8 bit |
| Stopbit | 1 bit |
| Handshake | off |
| Parity | none |

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.

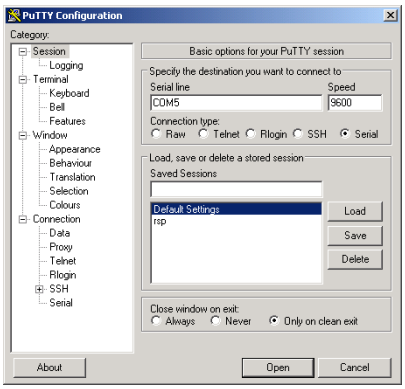



*Figure 7: Serial data connection with the serial interface using the PuTTY program*

- ☐ 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.

```
                Copyright (c) 2011-2021 Hirschmann Automation and Control GmbH

                                All rights reserved

                        DRAGON-00484 Release HiOS-3A-UR-08.7.03

                             (Build date 2021-09-25 13:09)


                    System Name   :  DRAGON-ECE555d5e100
                    Management IP :  192.168.1.5
                    Subnet Mask   :  255.255.255.0
                    1. Router IP  :  0.0.0.0
                    Base MAC      :  EC:E5:55:01:02:03
                    OOB IP        :  192.168.1.1
                    OOB Mask      :  255.255.255.0
                    System Time   :  2021-09-27 16:21:07


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

DRAGON>
```

*Figure 8: Start screen of the Command Line Interface*

### 1.2.5 Mode-based command hierarchy

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 following figure displays the modes of the Command Line Interface.

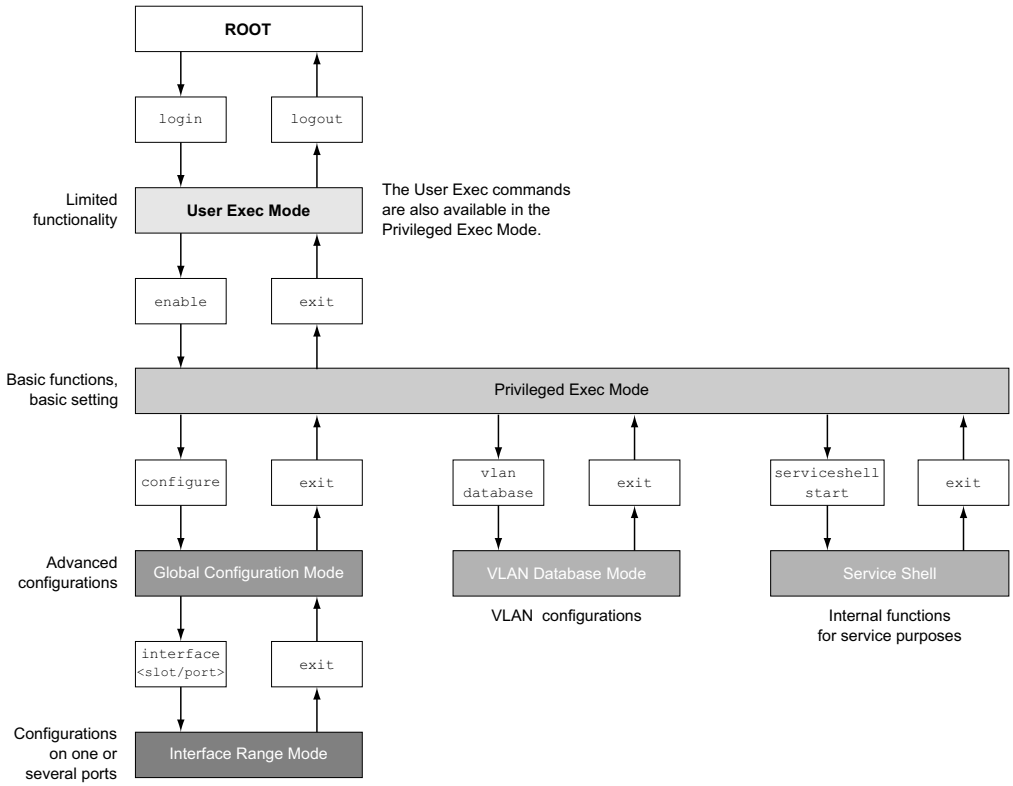



*Figure 9: Structure of the Command Line Interface*

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: `(DRAGON) >`
- 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: `(DRAGON) #`
- VLAN mode
  The VLAN mode contains VLAN-related commands.
  Command prompt: `(DRAGON) (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: `(DRAGON) (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.
  - All physical ports in the device
    Command prompt: `(DRAGON) ((interface) all)#`
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    ```
    (DRAGON) (config)#interface all
    (DRAGON) ((Interface)all)#
    ```
  - A single port on one interface
    Command prompt: `(DRAGON) (interface <slot/port>)#`
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    ```
    (DRAGON) (config)#interface 2/1
    (DRAGON) (interface 2/1)#
    ```
  - A range of ports on one interface
    Command prompt: `(DRAGON) (interface <interface range> )#`
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    ```
    (DRAGON) (config)#interface 1/2-1/4
    (DRAGON) ((Interface)1/2-1/4)#
    ```
  - A list of single ports
    Command prompt: `(DRAGON) (interface <interface list>)#`
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    ```
    (DRAGON) (config)#interface 1/2,1/4,1/5
    (DRAGON) ((Interface)1/2,1/4,1/5)#
    ```
  - A list of port ranges and single ports
    Command prompt: `(DRAGON) (interface <complex range>)#`
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    ```
    (DRAGON) (config)#interface 1/2-1/4,1/6-1/9
    (DRAGON) ((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 2: Command modes*

| Command mode | Access method | Quit or start next mode |
|---|---|---|
| User Exec mode | First access level. Perform basic tasks and list system information. | To quit you enter `logout`:<br>`(DRAGON) >logout`<br>`Are you sure (Y/N) ?y` |
| Privileged Exec mode | From the User Exec mode, you enter the command `enable`:<br>`(DRAGON) >enable`<br>`(DRAGON) #` | To quit the Privileged Exec mode and return to the User Exec mode, you enter `exit`:<br>`(DRAGON) #exit`<br>`(DRAGON) >` |

*Table 2: Command modes*

| Command mode | Access method | Quit or start next mode |
|---|---|---|
| VLAN mode | From the Privileged Exec mode, you enter the command `vlan database`:<br>`(DRAGON) #vlan database`<br>`(DRAGON) (Vlan)#` | To end the VLAN mode and return to the Privileged Exec mode, you enter `exit` or press Ctrl Z.<br>`(DRAGON) (Vlan)#exit`<br>`(DRAGON) #` |
| Global Config mode | From the Privileged Exec mode, you enter the command `configure`:<br>`(DRAGON) #configure`<br>`(DRAGON) (config)#`<br>From the User Exec mode, you enter the command `enable`, and then in Privileged Exec mode, enter the command `Configure`:<br>`(DRAGON) >enable`<br>`(DRAGON) #configure`<br>`(DRAGON) (config)#` | To quit the Global Config mode and return to the Privileged Exec mode, you enter `exit`:<br>`(DRAGON) (config)#exit`<br>`(DRAGON) #`<br>To then quit the Privileged Exec mode and return to the User Exec mode, you enter `exit` again:<br>`(DRAGON) #exit`<br>`(DRAGON) >` |
| Interface Range mode | From the Global Config mode you enter the command `interface {all\|<slot/port>\|<interface range>\|<interface list>\|<complex range>}`.<br>`(DRAGON) (config)#interface <slot/port>`<br>`(DRAGON) (interface slot/port)#` | To quit the Interface Range mode and return to the Global Config mode, you enter `exit`. To return to the Privileged Exec mode, you press Ctrl Z.<br>`(DRAGON) (interface slot/port)#exit`<br>`(DRAGON) #` |

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.

```
(DRAGON)>
  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.
  telnet            Establish a telnet connection to a remote host.

(DRAGON)>
```

*Figure 10: Commands in the User Exec mode*

## 1.2.6 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 `(DRAGON)>` 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:

```
(DRAGON)>show system ino

Error: Invalid command 'ino'
```

### 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.

## 1.2.7 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*

| | |
|---|---|
| `<command>` | Commands in pointed brackets (<>) are obligatory. |
| `[command]` | Commands in square brackets ([]) are optional. |
| `<parameter>` | Parameters in pointed brackets (<>) are obligatory. |
| `[parameter]` | Parameters in square brackets ([]) are optional. |
| `...` | An ellipsis (3 points in sequence without spaces) after an element indicates that you can repeat the element. |
| `[Choice1 \| Choice2]` | A vertical line enclosed in brackets indicates a selection option. Select one value.<br>Elements separated by a vertical line and enclosed in square brackets indicate an optional selection (Option1 or Option2 or no selection). |
| `{list}` | Curved brackets ({}) indicate that a parameter is to be selected from a list of options. |
| `{Choice1 \| Choice2}` | Elements separated by a vertical line and enclosed in curved brackets ({}) indicate an obligatory selection option (option1 or option2). |
| `[param1 {Choice1 \| Choice2}]` | Displays an optional parameter that contains an obligatory selection. |
| `<a.b.c.d>` | Small letters are wild cards. You enter parameters with the notation a.b.c.d with decimal points (for example IP addresses) |
| `<cr>` | You press the <Enter> key to create a line break (carriage return). |

The following list displays the possible parameter values within the Command Line Interface:

*Table 4: Parameter values in the Command Line Interface*

| Value | Description |
|---|---|
| IP address | This parameter represents a valid IPv4 address. The address consists of 4 decimal numbers with values from 0 to 255. The 4 decimal numbers are separated by a decimal point. The IP address `0.0.0.0` is a valid entry. |
| MAC address | This parameter represents a valid MAC address. The address consists of 6 hexadecimal numbers with values from 00 to FF. The numbers are separated by a colon, for example, `00:F6:29:B2:81:40`. |
| string | User-defined text with a length in the specified range, for example a maximum of 32 characters. |
| character string | Use double quotation marks to indicate a character string, for example `"System name with space character"`. |
| number | Whole integer in the specified range, for example `0..999999`. |
| date | Date in format `YYYY-MM-DD`. |
| time | Time in format `HH:MM:SS`. |

### Network addresses

Network addresses are a requirement for establishing a data connection to a remote work station, 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*

| Address Type | Format | Range | Example |
|---|---|---|---|
| IP Address | nnn.nnn.nnn.nnn | nnn: 0 to 255 (decimal) | 192.168.11.110 |
| MAC Address | mm:mm:mm:mm:mm:mm | mm: 00 to ff (hexadecimal number pairs) | A7:C9:89:DD:A9:B3 |

### 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:

```
*(DRAGON)#cli prompt Device name
Error: Invalid command 'name'

*(DRAGON)#cli prompt 'Device name'
```

```
*(Device name)#
```

### 1.2.8 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.

```
(DRAGON) (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.

```
(DRAGON) (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.

## 1.2.9 Input prompt

### Command mode

With the input prompt, the Command Line Interface displays which of the three modes you are in:

- `(DRAGON) >`
  User Exec mode
- `(DRAGON) #`
  Privileged Exec mode
- `(DRAGON) (config)#`
  Global Config mode
- `(DRAGON) (Vlan)#`
  VLAN Database mode
- `(DRAGON) ((Interface)all)#`
  Interface Range mode / All ports of the device
- `(DRAGON) ((Interface)2/1)#`
  Interface Range mode / A single port on one interface
- `(DRAGON) ((Interface)1/2-1/4)#`
  Interface Range mode / A range of ports on one interface
- `(DRAGON) ((Interface)1/2,1/4,1/5)#`
  Interface Range mode / A list of single ports
- `(DRAGON) ((Interface)1/1-1/2,1/4-1/6)#`
  Interface Range mode / A list of port ranges and single ports

### 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.
  `*(DRAGON)>`
- 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.
  *#`(DRAGON)>`
- 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.
  `!(DRAGON)>`

### Wildcards

The device lets you change the command line prompt.

The Command Line Interface supports the following wildcards:

*Table 6: Using wildcards within the Command Line Interface input prompt*

| Wildcard | Description |
|---|---|
| `%d` | System date |
| `%t` | System time |

*Table 6: Using wildcards within the Command Line Interface input prompt*

| Wildcard | Description |
|---|---|
| %i | IP address of the device |
| %m | MAC address of the device |
| %p | Product name of the device |

```
!(DRAGON)>enable

!(DRAGON)#cli prompt %i

!192.168.1.5#cli prompt (DRAGON)%d

!*(DRAGON)2021-09-27#cli prompt (DRAGON)%d%t

!*(DRAGON)2021-09-27 16:21:07#cli prompt %m

!*AA:BB:CC:DD:EE:FF#
```

### 1.2.10 Key combinations

The following key combinations make it easier for you to work with the Command Line Interface:

*Table 7: Key combinations in the Command Line Interface*

| Key combination | Description |
|---|---|
| <CTRL> + <H>, <Backspace> | 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> | Rewrite or paste 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 |

The Help command displays the possible key combinations in Command Line Interface on the screen:

```
(DRAGON) #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

(DRAGON) #
```

*Figure 11: Listing the key combinations with the Help command*

## 1.2.11 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:
  ```
  (DRAGON) (Config)#lo
  (DRAGON) (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 `(DRAGON) >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:

```
!*#(DRAGON)(Config)#show?

   show          Display device options and settings.
```

## 1.2.12 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`).

| Parameter | Meaning | Possible values |
|---|---|---|
| `<1..8>` | RADIUS server index. | `1..8` |
| `<a.b.c.d>` | RADIUS accounting server IP address. | IP address |
| `<string>` | Enter a user-defined text, max. 32 characters. | |
| `<1..65535>` | Enter port number between 1 and 65535. | `1..65535` |

Mode and Privilege Level:

- The prerequisite for executing the command: You are in the Global Config mode. See “Mode-based command hierarchy” on page 25.
- The prerequisite for executing the command: You have the Administrator access role.

Syntax of commands and parameters: See “Structure of a command” on page 29.

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`

### 1.2.13 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: `(DRAGON) >`

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.

```
!DRAGON >enable

!*DRAGON #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 (2021-09-27 16:21:07 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: `(DRAGON) >`

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 deactivate` and press the <Enter> key.
  To reduce the effort when typing:
  - Enter `ser` and press the <Tab> key.
  - Enter `dea` and press the <Tab> key.
- ☐ **This step is irreversible!**
  Press the <Y> key.

```
!DRAGON >enable

!*DRAGON #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

Prerequisites:
- 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:

| VT 100 terminal settings | |
|---|---|
| Speed | 9600 bit/s |
| Data | 8 bit |
| Stopbit | 1 bit |
| Handshake | off |
| Parity | none |

- ☐ 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: ...-8.7.03 (2021-09-25 13:09))

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 12: 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.
- Using BOOTP.
  To configure the installed device using BOOTP, you choose this “In-Band” method. You need a BOOTP server for this method. The BOOTP server assigns the configuration data to the device using its MAC address. The DHCP mode is the default mode for the configuration data reference.
- Configuration using DHCP.
  To configure the installed device using DHCP, you choose this “In-Band” method. You need a DHCP server for this method. The DHCP server assigns the configuration data to the device using its MAC address or its system name.
- 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 8: IP address classes*

| Class | Network address | Host address | Address range |
|---|---|---|---|
| A | 1 Byte | 3 Bytes | 0.0.0.0 to 127.255.255.255 |
| B | 2 Bytes | 2 Bytes | 128.0.0.0 to 191.255.255.255 |
| C | 3 Bytes | 1 Byte | 192.0.0.0 to 223.255.255.255 |
| D | | | 224.0.0.0 to 239.255.255.255 |
| E | | | 240.0.0.0 to 255.255.255.255 |

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

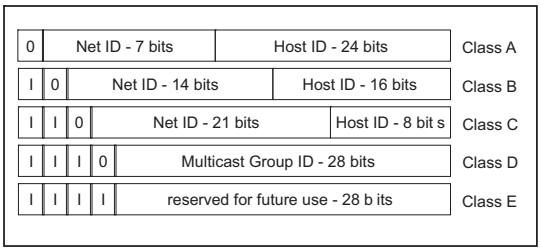



*Figure 13: Bit representation of the IP address*

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 asssigns 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
└──── 128 < 129  191 › Class B

Binary notation
10000001.11011010.01000001.00010001
Subnetwork 1
Network address

Decimal notation
129.218.129.17
└──── 128 < 129  191 › Class B

Binary notation
10000001.11011010.10000001.00010001
Subnetwork 2
Network address

### 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?

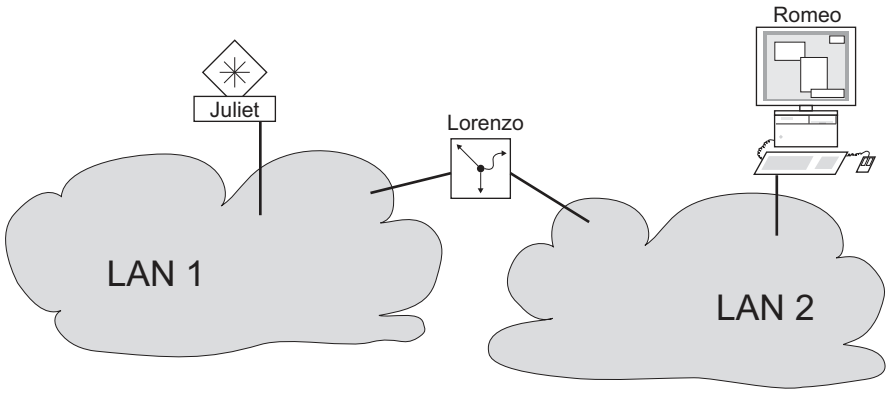



*Figure 14: The management agent is separated from its network management station by a router*

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:

| IP address, decimal | Network mask, decimal | IP address, binary |
|---|---|---|
| 192.168.112.1 | 255.255.255.128 | 11000000 10101000 01110000 00000001 |
| 192.168.112.127 | | 11000000 10101000 01110000 01111111 |

25 mask bits

CIDR notation: 192.168.112.0/25

Mask bits

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:

- BOOTP/DHCP
- 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.

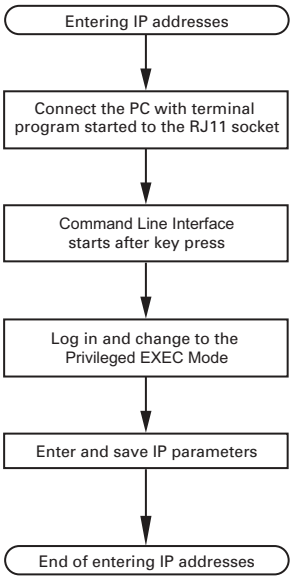



*Figure 15: Flow chart for entering IP addresses*

**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.

Perform the following steps:

- ☐ Set up a connection to the device.
  The start screen appears.

- ☐ Deactivate DHCP.
- ☐ 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 or TFTP server are located in different subnetworks (see on page 45 “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`.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `network protocol none` | Deactivating DHCP. |
| `network parms 10.0.1.23 255.255.255.0` | 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. |
| `copy config running-config nvm` | 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.

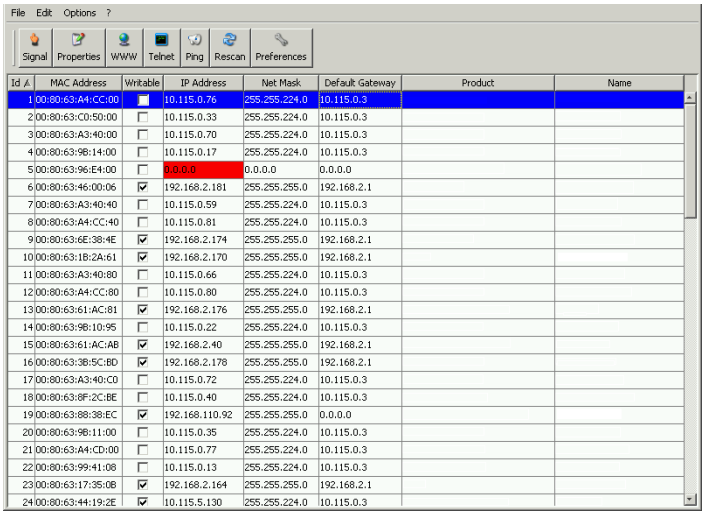



*Figure 16: HiDiscovery*

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.

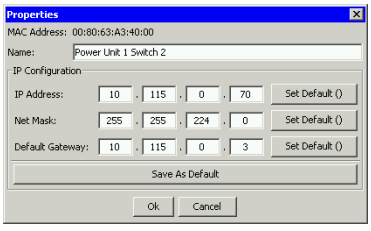



*Figure 17: HiDiscovery – assigning IP parameters*

**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.

### 2.3.1 Relay

When you connect the management station to a switching subnetwork, the HiDiscovery requests collect information from the devices located in that subnetwork. The HiDiscovery Relay lets you discover and set IP parameters on devices in other subnetworks.

The HiDiscovery function and the HiDiscovery Relay are independent from each other. You can enable the HiDiscovery Relay without enabling the HiDiscovery function. When you activate the relay with the function disabled, the device forwards the requests to other subnetworks, but does not respond to requests.

The HiDiscovery Relay is active in the default setting.

**Note:** When you activate the HiDiscovery Relay, the device forwards requests received on the router interfaces only to other router interfaces. A loopback interface is an internal virtual router interface. If you connect the management station to a loopback interface, then the device does not forward the request to the other connected subnetworks. The device does not forward responses received on a router interface to the subnetwork of the management station.

### 2.3.2 Example configuration

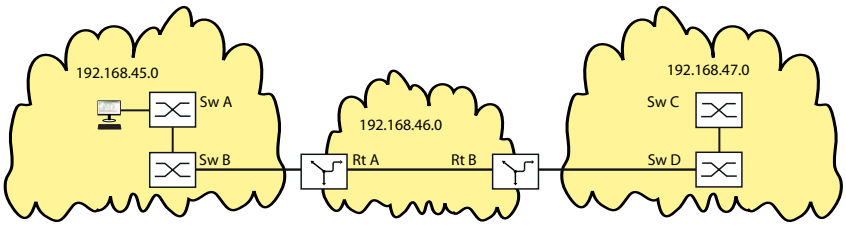



*Figure 18: Management station connected to a switch.*

To poll devices in the `192.168.47.0` subnetwork use the following steps on both `Rt A` and `Rt B`. With the relay activated on router `Rt A`, the device forwards the requests packets into the `192.168.47.0` subnetwork. With the relay activated on router `Rt B`, the device returns the responses from the `192.168.47.0` subnetwork back to the management station.

When the HiDiscovery Relay is inactive on either router, the management station only displays the devices located in the `192.168.45.0` subnetwork.

The prerequisite for these steps is that you already configured the device as a router and installed it in a network.

Perform the following steps:

- ☐ Open the *Basic Settings > Network > Global* dialog.
- ☐ In the *HiDiscovery protocol v1/v2* frame, mark the *Relay status* checkbox.

```
enable
```

Change to the Privileged EXEC mode.

```
network hidiscovery relay
```

Activating the HiDiscovery relay.

# 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 `BOOTP` mode, the configuration is using a BOOTP or DHCP server on the basis of the MAC address of the device.
- ▶ In the `DHCP` mode, the configuration is using a DHCP server on the basis of the MAC address or the name of the device.
- ▶ 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.

## 2.5 Specifying the IP parameters using BOOTP

With the *BOOTP* function activated the device sends a boot request message to the BOOTP server. The boot request message contains the Client ID configured in the *Basic Settings > Network > IPv4* dialog. The BOOTP server enters the Client ID into a database and assigns an IP address. The server answers with a boot reply message. The boot reply message contains the assigned IP address.

# 2.6 Specifying the IP parameters using DHCP

## 2.6.1 IPv4

The DHCP (Dynamic Host Configuration Protocol) is a further development of BOOTP, which it has replaced. The DHCP additionally lets the configuration of a DHCP client using a name instead of using the MAC address.

For the DHCP, this name is known as the “Client Identifier” in accordance with RFC 2131.

The device uses the name entered under sysName in the system group of the MIB II as the Client Identifier. You can change the system name using the Graphical User Interface (see dialog *Basic Settings > System*), the Command Line Interface or SNMP.

The device sends its system name to the DHCP server. The DHCP server then uses the system name to allocate an IP address as an alternative to the MAC address.

In addition to the IP address, the DHCP server sends
- the netmask
- the default Gateway (if available)
- the TFTP URL of the configuration file (if available).

The device applies the configuration data to the appropriate parameters. When the DHCP Sever assigns the IP address, the device permanently saves the configuration data in non-volatile memory.

*Table 9: DHCP options which the device requests*

| Options | Meaning |
|---|---|
| 1 | Subnet Mask |
| 2 | Time Offset |
| 3 | Router |
| 4 | Time server |
| 12 | Host Name |
| 42 | NTP server |
| 61 | Client Identifier |
| 66 | TFTP Server Name |
| 67 | Bootfile Name |

The advantage of using DHCP instead of BOOTP is that the DHCP server can restrict the validity of the configuration parameters (“Lease”) to a specific time period (known as dynamic address allocation). Before this period (“Lease Duration”) elapses, the DHCP client can attempt to renew this lease. Alternatively, the client can negotiate a new lease. The DHCP server then allocates a random free address.

To help avoid this, DHCP servers provide the explicit configuration option of assigning a specific client the same IP address based on a unique hardware ID (known as static address allocation).

In the default setting, DHCP is activated. As long as DHCP is activated, the device attempts to obtain an IP address. When the device cannot find a DHCP server after restarting, it will not have an IP address. The *Basic Settings > Network > IPv4* dialog lets you activate or deactivate DHCP.

**Note:** When using Industrial HiVision network management, verify that DHCP allocates the original IP address to every device.

The appendix contains an example configuration of the BOOTP/DHCP-server.

Example of a DHCP-configuration file:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

Lines beginning with the # character, contain comments.

The lines preceding the individually listed devices refer to settings that apply to the following device.

The fixed-address line assigns a permanent IP address to the device.

For further information, please refer to the DHCP server manual.

# 2.7 Management address conflict detection

You assign an IP address to the device using several different methods. This function helps the device detect IP address conflicts on a network after boot up and the device also checks periodically during operation. This function is described in RFC 5227.

When enabled, the device sends an SNMP trap informing you that it detected an IP address conflict.

The following list contains the default settings for this function:
- *Operation*: `On`
- *Detection mode*: `active and passive`
- *Send periodic ARP probes*: `marked`
- *Detection delay [ms]*: `200`
- *Release delay [s]*: `15`
- *Address protections*: `3`
- *Protection interval [ms]*: `200`
- *Send trap*: `marked`

## 2.7.1 Active and passive detection

Actively checking the network helps prevent the device from connecting to the network with a duplicate IP address. After connecting the device to a network or after configuring the IP address, the device immediately checks if its IP address exists within the network. To check the network for address conflicts, the device sends 4 ARP probes with the detection delay of 200 ms into the network. When the IP address exists, the device attempts to return to the previous configuration, and make another check after the configured release delay time.

When you disable active detection, the device sends 2 gratuitous APR announcements in 2 s intervals. Using the ARP announcements with passive detection enabled, the device polls the network to determine if there is an address conflict. After resolving an address conflict or after expired release delay time, the device reconnects to the network. Following 10 detected conflicts, when the configured release delay interval is less than 60 s, the device sets the release delay interval to 60 s.

After the device performs active detection or you disable the active detection function, with passive detection enabled the device listens on the network for other devices using the same IP address. When the device detects a duplicate IP address, it initially defends its address by employing the ACD mechanism in the passive detection mode and sends out gratuitous ARPs. The number of protections that the device sends and the protection interval are configurable. To resolve conflicts, if the remote device remains connected to the network, then the network interface of the local device disconnects from the network.

When a DHCP server assigns an IP address to the device and an address conflict occurs, the device returns a DHCP decline message.

The device uses the ARP probe method. This has the following advantages:
- ARP caches on other devices remain unchanged
- the method is robust through multiple ARP probe transmissions

# 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 25.

The device offers the following access roles:

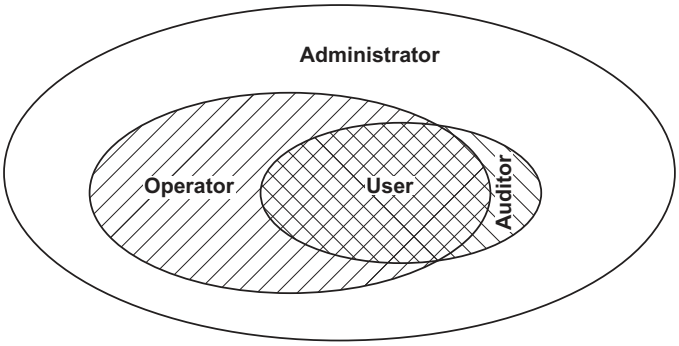



*Table 10: Access roles and scope of user authorizations*

| Access role | User authorizations |
|---|---|
| `User` | Users logged in with the access role `User` are authorized to monitor the device. |
| `Auditor` | Users logged in with the access role `Auditor` are authorized to monitor the device and to save the log file in the *Diagnostics > Report > Audit Trail* dialog. |
| `Operator` | 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. |
| `Administrator` | Users logged in with the access role `Administrator` are authorized to monitor the device and to change the settings. |
| `Unauthorized` | 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. |

## 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.
  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.
- ☐ 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 contact your local support team.

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 Command Line Interface using Telnet: `Telnet`
- Access to the Graphical User Interface: `WebInterface`

The device also provides an application to control the access to the network from connected end devices using port-based access control: `8021x`

## 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

When the end device logs in with valid login data, the device lets the connected end devices have access to the network with the port-based access control according to IEEE 802.1X. The device authenticates the end devices using the following policies:

- RADIUS
- IAS (Integrated Authentication Server)

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:

☐ Open the *Device Security > Authentication List* dialog.

The dialog displays the authentication lists that are set up.

| | |
|---|---|
| `show authlists` | Displays the authentication lists that are set up. |

☐ Deactivate the authentication list for those applications by means of which no access to the device is performed, for example `8021x`.

☐ In the *Active* column of the authentication list `defaultDot1x8021AuthList`, unmark the checkbox.

☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `authlists disable defaultDot1x8021AuthList` | Deactivates the authentication list `defaultDot1x8021AuthList`. |

### 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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `authlists add loginGUI` | 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.

| | |
|---|---|
| `authlists set-policy loginGUI radius local reject reject reject` | Assigns the policies `radius`, `local` and `reject` to the authentication list `loginGUI`. |
| `show authlists` | Displays the authentication lists that are set up. |
| `authlists enable loginGUI` | Activates the authentication list `loginGUI`. |

☐ 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` | Displays the applications and the allocated lists. |
| `applists set-authlist WebInterface loginGUI` | Assigns the `loginGUI` application to the authentication list `WebInterface`. |

# 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 11: Access roles for user accounts*

| Role | Description | Authorized for the following activities |
|---|---|---|
| Administrator | The user is authorized to monitor and administer the device. | All activities with read/write access, including the following activities reserved for an administrator:<br>▶ Add, modify or delete user accounts<br>▶ Activate, deactivate or unlock user accounts<br>▶ Change every password<br>▶ Configure password management<br>▶ Set or change system time<br>▶ Load files to the device, for example device configurations, certificates or software images<br>▶ Reset settings and security-related settings to the state on delivery<br>▶ Configure RADIUS server and authentication lists<br>▶ Apply scripts using the Command Line Interface<br>▶ Enable/disable CLI logging and SNMP logging<br>▶ External memory activation and deactivation<br>▶ System monitor activation and deactivation<br>▶ Enable/disable the services for the access to the device management (for example SNMP).<br>▶ Configure access restrictions to the Graphical User Interface or the Command Line Interface based on the IP addresses |
| Operator | The user is authorized to monitor and configure the device - with the exception of security-related settings. | All activities with read/write access, with the exception of the above-named activities, which are reserved for an administrator: |
| Auditor | The user is authorized to monitor the device and to save the log file in the *Diagnostics > Report > Audit Trail* dialog. | Monitoring activities with read access. |
| Guest | The user is authorized to monitor the device - with the exception of security-related settings. | Monitoring activities with read access. |
| Unauthorized | No access to the device possible.<br>▶ As an administrator you assign this access role to temporarily lock a user account.<br>▶ 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. | No activities allowed. |

### 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 12: Default settings for the factory setting user accounts*

| Parameter | Default setting | |
|---|---|---|
| *User name* | `admin` | `user` |
| *Password* | `private` | `public` |
| *Role* | `administrator` | `guest` |
| *User locked* | `unmarked` | `unmarked` |
| *Policy check* | `unmarked` | `unmarked` |
| *SNMP auth type* | `hmacmd5` | `hmacmd5` |
| *SNMP encryption type* | `des` | `des` |

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.

**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 ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `users password-policy-check <user> enable` | 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` | Specifies the password `SECRET` for the`<user>` user account. Enter at least 6 characters. |
| `save` | Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile. |

### 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:

☐ Create a new user account.

- ☐ Open the *Device Security > User Management* dialog.
- ☐ Click the 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.

- ☐ 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.
- ☐ In the *Role* column, select the user role.
  In this example, we select the value `operator`.
- ☐ To activate the user account, mark the checkbox in the *Active* column.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
  The dialog displays the user accounts that are set up.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `users add USER` | Creates the `USER` user account. |
| `users password-policy-check USER enable` | 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. |
| `users password USER SECRET` | Specifies the password `SECRET` for the user account `USER`. Enter at least 6 characters. |
| `users access-role USER operator` | Assign the user role `operator` to the user account `USER`. |
| `users enable USER` | Activates the user account `USER`. |
| `show users` | Displays the user accounts that are set up. |
| `save` | Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile. |

**Note:** When you are setting up a new user account in the Command Line Interface, remember to allocate the password.

### 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 ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `users disable <user>` | To disable user account. |
| `show users` | Displays the user accounts that are set up. |
| `save` | 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.

☐ Highlight the row for the relevant user account.

☐ Click the button.

| | |
|---|---|
| `users delete <user>` | Deletes the user account `<user>`. |
| `show users` | Displays the user accounts that are set up. |
| `save` | 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
- the Telnet 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `passwords min-length 6` | Specifies the policy for the minimum length of the password. |
| `passwords min-lowercase-chars 1` | Specifies the policy for the minimum number of lower-case letters in the password. |
| `passwords min-numeric-chars 1` | Specifies the policy for the minimum number of digits in the password. |
| `passwords min-special-chars 1` | Specifies the policy for the minimum number of special characters in the password. |
| `passwords min-uppercase-chars 1` | Specifies the policy for the minimum number of upper-case letters in the password. |
| `show passwords` | Displays the policies that are set up. |
| `save` | Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile. |

# 3.5 LDAP

Server administrators manage Active Directorys 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 the `memberOf` 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.

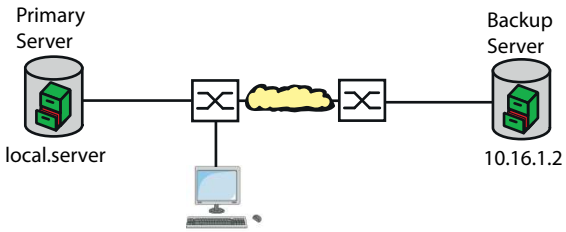



*Figure 19: LDAP Example Configuration*

For this example, the server administrator sent the following information:

| Information | Primary Server | Backup Server |
|---|---|---|
| The server name or IP address | `local.server` | `10.16.1.2` |
| The location of the Active Directory on the server | `Country/City/User` | `Country/Company/User` |
| The type of connection used | `TLS` (with certificate) | `SSL` |
| The server administrator sent the CA certificate in an email. | CA certificate for primary server saved locally | CA certificate for backup server saved locally |
| The TCP listening port | `389 (tls)` | `636 (ssl)` |
| Name of the attribute containing the user name | `userPrincipalName` | `userPrincipalName` |
| The names of the attribute containing the user permission levels | `OPERATOR`<br>`ADMINISTRATOR` | `OPERATOR`<br>`ADMINISTRATOR` |

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 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 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 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 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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `ldap cache-timeout 1440` | Specify the device to flush the non-volatile memory after a day. |

| | |
|---|---|
| `ldap client server add 1 local.server port 389` | Add a connection to the remote authentication client server with the host name `local.server` and the UDP port `389`. |
| `ldap client server modify 1 security startTLS` | Specify the type of security used for the connection. |
| `ldap client server modify 1 description Primary_AD_Server` | Specify the configuration name of the entry. |
| `ldap basedn ou=Users,ou=City,ou=Country,dc=server, dc=local` | Specify the Base Domain Name used to find the Active Directory on the server. |
| `ldap search-attr userPrincipalName` | Specify the attribute to search for in the Active Directory which contains the login credential of the users. |
| `ldap bind-user user@company.com` | Specify the name and domain of the service user. |
| `ldap bind-passwd Ur-123456` | Specify the password of the service user. |
| `ldap client server enable 1` | Enable the remote authentication client server connection. |
| `ldap mapping add 1 access-role operator mapping-type attribute mapping-parameter OPERATOR` | Add a remote authentication role mapping entry for the `Operator` role. Map the `operator` role to the attribute containing the word `OPERATOR`. |
| `ldap mapping enable 1` | Enable the remote authentication role mapping entry. |
| `ldap operation` | 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.

- ☐ 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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `users snmpv3 authentication <user> md5 \| sha1` | Assigning the HMAC-MD5 or HMACSHA protocol for authentication requests to the user account `<user>`. |
| `users snmpv3 encryption <user> des \| aescfb128 \| none` | 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. |
| `show users` | Display the user accounts that have been configured. |
| `save` | Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile. |

# 3.7 Out of Band access

The device comes with a separate port that lets you access the device management out-of-band. When there is a high in-band load on the switching ports, you can still use this separate port to access the device management.

In the default setting, you can access the device management through this port using the following IP parameters:

- *IP address* 192.168.1.1
- *Netmask* 255.255.255.0

To access the device management, assign an IP address in the same subnet to the management station.

The device lets you access the device management using the following protocols:

- SNMP
- Telnet
- SSH
- HTTP
- HTTPS
- FTP
- SCP
- TFTP
- SFTP
- Industry protocols

## 3.7.1 Specifying the IP parameters

In the default setting, the Service Port has static IP parameters. The device lets you change the IP parameters to adapt the device to the requirements of your environment. You can also use an external DHCP server to specify the IP parameters for the Service Port network interface.

Verify that the IP subnet of this network interface is not overlapping with any subnet connected to another interface of the device:

- Management interface
- Router interface
- Loopback interface

If the management station accesses the device management through the Service Port, then the device disconnects the Graphical User Interface and Command Line Interface immediately after you have performed the changes.

### Specifying static IP parameters

Perform the following steps:

- ☐ Open the *Basic Settings > Out of Band* dialog.
- ☐ Overwrite the IP address in the *IP parameter* frame, *IP address* field.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

```
enable
```
Change to the Privileged EXEC mode.

```
network out-of-band parms 192.168.1.1
255.255.255.0 192.168.1.254
```
Specify the IP address `192.168.1.1` and the netmask `255.255.255.0` for the Service Port network interface. Specify the default gateway `192.168.1.254`.

```
show network out-of-band
```
Display the Service Port network interface settings.

```
Out-of-band management settings
------------------------------
Management operation.....................enabled
Interface status.........................up
IP address...............................192.168.1.1
Subnet mask..............................255.255.255.0
Default gateway address..................192.168.1.254
MAC address..............................ec:e5:55:f6:f7:a9
Configuration protocol...................none
```

```
save
```
Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile.

### Specifying the IP parameters using a DCHP server

Perform the following steps:

- ☐ Open the *Basic Settings > Out of Band* dialog.
- ☐ In the *Management interface* frame, select the *DHCP* radio button in the *IP address assignment* option list.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

```
enable
```
Change to the Privileged EXEC mode.

```
network out-of-band protocol dhcp
```
Select `dhcp` as the Service Port configuration protocol.

```
show network out-of-band
```
Display the Service Port network interface settings.

```
Out-of-band management settings
------------------------------
Management operation.....................enabled
Interface status.........................up
IP address...............................0.0.0.0
Subnet mask..............................0.0.0.0
Default gateway address..................0.0.0.0
MAC address..............................ec:e5:55:f6:f7:a9
Configuration protocol...................dhcp
```

```
save
```
Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile.

### 3.7.2 Disable the Service Port network interface

In the default setting, the Service Port network interface is enabled. If you don't want someone to access device management through the Service Port port, then the device lets you disable the Service Port network interface.

If the management station accesses the device management through the Service Port, then the device disconnects the Graphical User Interface and Command Line Interface immediately after you perform the changes.

Perform the following steps:

- ☐ Open the *Basic Settings > Out of Band* dialog.
- ☐ To disable the Service Port network interface, select the *Off* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

```
enable                                  Change to the Privileged EXEC mode.
no network out-of-band operation        Disable the Service Port network interface.
Out-of-band management settings
------------------------------
Management operation.....................disabled
Interface status.........................down
IP address...............................0.0.0.0
Subnet mask..............................0.0.0.0
Default gateway address..................0.0.0.0
MAC address..............................ec:e5:55:f6:f7:a9
Configuration protocol...................dhcp

save                                    Save the settings in the non-volatile memory (nvm)
                                        in the "selected" configuration profile.
```

# 4 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 Simple Network Time Protocol (SNTP) is a simple solution for low accuracy requirements. Under ideal conditions, SNTP achieves an accuracy in the millisecond range. The accuracy depends on the signal delay.
- IEEE 1588 with the Precision Time Protocol (PTP) achieves accuracies on the order of fractions of microseconds. This method is suitable even for demanding applications up to and including process control.

When the involved devices support the PTP protocol, it is the better choice. PTP is more accurate, has advanced methods of error correction, and causes a low network load. The implementation of PTP is comparatively easy.

**Note:** According to the PTP and SNTP standards, both protocols function in parallel in the same network. However, since both protocols influence the system time of the device, situations can occur in which the two protocols conflict with each other.

## 4.1 Basic settings

In the *Time > Basic Settings* dialog, you specify general settings for the time.

### 4.1.1 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 a PTP clock or from an SNTP server.

Alternatively, you configure the settings in the device so that it automatically obtains the current time from an SNTP 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.

**Note:** PTP sends the International Atomic Time (TAI). As of July 1, 2020, the TAI time is 37 s ahead of the UTC time. When the PTP reference time source of the UTC offset is set correctly, the device automatically corrects this difference on the display in the *System time (UTC)* field.

- ☐ 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 SNTP is active and the device receives a valid SNTP packet, the device sets its time source to `sntp`.
  When PTP is active and the device receives a valid PTP message, the device sets its time source to `ptp`. The device prioritizes PTP ahead of SNTP.
- ▶ The *Local offset [min]* value specifies the time difference between the local time and the *System time (UTC)*.
- ☐ In order to cause the device to determine the time zone on your PC, click the *Set time from PC* button. The device calculates the local time difference from UTC and enters the difference into the *Local offset [min]* field.

**Note:** The device provides the option to obtain the local offset from a DHCP server.

- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `clock set <YYYY-MM-DD> <HH:MM:SS>` | Set the system time of the device. |
| `clock timezone offset <-780..840>` | Enter the time difference between the local time and the received UTC time in minutes. |
| `save` | Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile. |

### 4.1.2 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `clock summer-time mode <disable\|recurring\|eu\|usa>` | Configure the automatic daylight saving time changeover: enable/disable or activate with a profile. |
| `clock summer-time recurring start` | Enter the start time for the changeover. |
| `clock summer-time recurring end` | Enter the end time for the changeover. |
| `save` | Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile. |

# 4.2 SNTP

The Simple Network Time Protocol (SNTP) lets you synchronize the system time in your network. The device supports the SNTP client and the SNTP server function.

The SNTP server makes the UTC (Universal Time Coordinated) available. UTC is the time relating to the coordinated world time measurement. The UTC is the same worldwide and ignores local time shifts.

SNTP is a simplified version of NTP (Network Time Protocol). The data packets are identical with SNTP and NTP. Accordingly, both NTP and SNTP servers serve as a time source for SNTP clients.

**Note:** Statements in this chapter relating to external SNTP servers also apply to NTP servers.

SNTP knows the following operation modes for the transmission of time:

- *Unicast*
  In *Unicast* operation mode, an SNTP client sends requests to an SNTP server and expects a response from this server.
- *Broadcast*
  In *Broadcast* operation mode, an SNTP server sends SNTP messages to the network in specified intervals. SNTP clients receive these SNTP messages and evaluate them.

*Table 13: Target IPv4 address classes for Broadcast operation mode*

| IPv4 destination address | Send SNTP packets to |
|---|---|
| `0.0.0.0` | Nobody |
| `224.0.1.1` | *Multicast* address for SNTP messages |
| `255.255.255.255` | *Broadcast* address |

**Note:** An SNTP server in *Broadcast* operation mode also responds to direct requests using *Unicast* from SNTP clients. In contrast, SNTP clients work in either *Unicast* or *Broadcast* operation mode.

### 4.2.1 Preparation

Perform the following steps:

- ☐ To get an overview of how the time is passed on, draw a network plan with the devices participating in SNTP.
  When planning, bear in mind that the accuracy of the time depends on the delays of the SNTP messages. To minimize delays and their variance, place an SNTP server in each network segment. Each of these SNTP servers synchronizes its own system time as an SNTP client with its parent SNTP server (SNTP cascade). The highest SNTP server in the SNTP cascade has the most direct access to a reference time source.

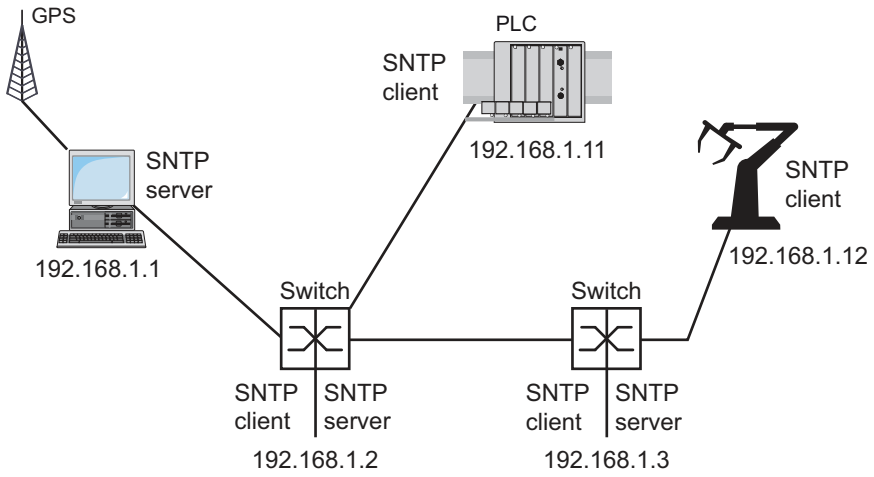



*Figure 20: Example of SNTP cascade*

**Note:** For precise time distribution, between SNTP servers and SNTP clients you preferably use network components (routers and switches) that forward the SNTP packets with a low and uniform transmission time (latency).

- An SNTP client sends its requests to up to 4 configured SNTP servers. When there is no response from the 1st SNTP server, the SNTP client sends its requests to the 2nd SNTP server. When this request is also unsuccessful, it sends the request to the 3rd and finally the 4th SNTP server. If none of these SNTP servers respond, the SNTP client loses its synchronization. The SNTP client periodically sends requests to each SNTP server until a server delivers a valid time.

**Note:** The device provides the option of obtaining a list of SNTP server IP addresses from a DHCP server.

- ☐ If no reference time source is available to you, then determine a device with an SNTP server as a reference time source. Adjust its system time at regular intervals.

### 4.2.2 Defining settings of the SNTP client

As an SNTP client, the device obtains the time information from SNTP or NTP servers and synchronizes its system clock accordingly. To do this, perform the following steps:

- ☐ Open the *Time > SNTP > Client* dialog.
- ☐ Set the SNTP operation mode.
  In the *Configuration* frame, select one of the following values in the *Mode* field:
  - `unicast`
    The device sends requests to an SNTP server and expects a response from this server.
  - `broadcast`
    The device waits for *Broadcast* or *Multicast* messages from SNTP servers on the network.
- ☐ To synchronize the time only once, mark the *Disable client after successful sync* checkbox. After synchronization, the device disables the *SNTP Client* function.
- The table displays the SNTP server to which the SNTP client sends a request in *Unicast* operation mode. The table contains up to 4 SNTP server definitions.
- ☐ To add a table entry, click the button.
- ☐ Specify the connection data of the SNTP server.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the button.
- The *State* field displays the current status of the *SNTP Client* function.

*Table 14: SNTP client settings for the example*

| Device | 192.168.1.1 | 192.168.1.2 | 192.168.1.3 | 192.168.1.11 | 192.168.1.12 |
|---|---|---|---|---|---|
| *SNTP Client* function | `Off` | `On` | `On` | `On` | `On` |
| *Configuration*: *Mode* | `unicast` | `unicast` | `unicast` | `unicast` | `unicast` |
| *Request interval [s]* | `30` | `30` | `30` | `30` | `30` |
| *SNTP Server* address(es) | – | `192.168.1.1` | `192.168.1.2`<br>`192.168.1.1` | `192.168.1.2`<br>`192.168.1.1` | `192.168.1.3`<br>`192.168.1.2`<br>`192.168.1.1` |

### 4.2.3 Specifying SNTP server settings

When the device operates as an SNTP server, it provides its system time in coordinated world time (UTC) in the network. To do this, perform the following steps:

- ☐ Open the *Time > SNTP > Server* dialog.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ To enable the *Broadcast* operation mode, select the *Broadcast admin mode* radio button in the *Configuration* frame.
  In *Broadcast* operation mode, the SNTP server sends SNTP messages to the network in specified intervals. The SNTP server also responds to the requests from SNTP clients in *Unicast* operation mode.
  - ☐ In the *Broadcast destination address* field, you set the IPv4 address to which the SNTP server sends the SNTP packets. Set a *Broadcast* address or a *Multicast* address.
  - ☐ In the *Broadcast UDP port* field, you specify the number of the UDP port to which the SNTP server sends the SNTP packets in *Broadcast* operation mode.
  - ☐ In the *Broadcast VLAN ID* field, you specify the ID of the VLAN to which the SNTP server sends the SNTP packets in *Broadcast* operation mode.
  - ☐ In the *Broadcast send interval [s]* field, you enter the time interval at which the SNTP server of the device sends SNTP *Broadcast* packets.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
- ▶ The *State* field displays the current status of the *SNTP Server* function.

*Table 15: Settings for the example*

| Device | 192.168.1.1 | 192.168.1.2 | 192.168.1.3 | 192.168.1.11 | 192.168.1.12 |
|---|---|---|---|---|---|
| *SNTP Server* function | `On` | `On` | `On` | `Off` | `Off` |
| *UDP port* | `123` | `123` | `123` | `123` | `123` |
| *Broadcast admin mode* | `unmarked` | `unmarked` | `unmarked` | `unmarked` | `unmarked` |
| *Broadcast destination address* | `0.0.0.0` | `0.0.0.0` | `0.0.0.0` | `0.0.0.0` | `0.0.0.0` |
| *Broadcast UDP port* | `123` | `123` | `123` | `123` | `123` |
| *Broadcast VLAN ID* | `1` | `1` | `1` | `1` | `1` |
| *Broadcast send interval [s]* | `128` | `128` | `128` | `128` | `128` |
| *Disable server at local time source* | `unmarked` | `unmarked` | `unmarked` | `unmarked` | `unmarked` |

# 4.3 PTP

In order for LAN-controlled applications to work without latency, precise time management is required. With PTP (Precision Time Protocol), IEEE 1588 describes a method that enables precise synchronization of clocks in the network.

PTP enables synchronization with an accuracy of a few 100 ns. PTP uses Multicasts for the synchronization messages, which keeps the network load low.

## 4.3.1 Types of clocks

PTP defines the roles of “master” and “slave” for the clocks in the network:
- A master clock (reference time source) distributes its time.
- A slave clock synchronizes itself with the timing signal received from the master clock.

### Boundary clock

The transmission time (latency) in routers and switches has a measurable effect on the precision of the time transmission. To correct such inaccuracies, PTP defines what are known as boundary clocks.

In a network segment, a boundary clock is the reference time source (master clock) to which the subordinate slave clocks synchronize. Typically routers and switches take on the role of boundary clock.

The boundary clock in turn obtains the time from a higher-level reference time source (Grandmaster).

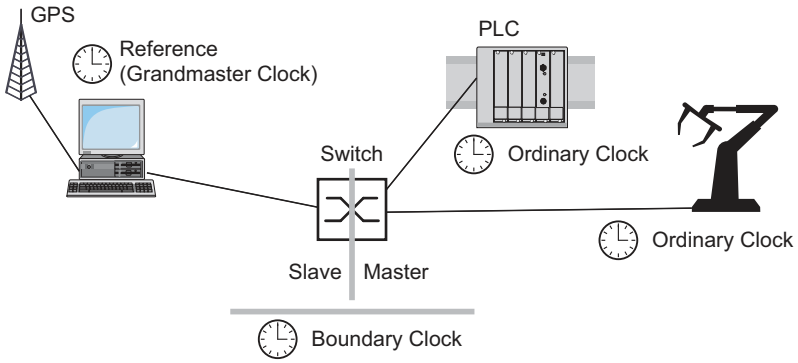



*Figure 21: Position of the boundary clock in a network*

### Transparent Clock

Switches typically take on the Transparent Clock role to enable high accuracy across the cascades. The Transparent Clock is a Slave clock that corrects its own transmission time when it forwards received synchronization messages.

#### Ordinary Clock

PTP designates the clock in a end device as an “Ordinary Clock”. An Ordinary Clock functions either as a master clock or slave clock.

### 4.3.2 Best Master Clock algorithm

The devices participating in PTP designate a device in the network as a reference time source (Grandmaster). Here the “Best Master Clock” algorithm is used, which determines the accuracy of the clocks available in the network.

The “Best Master Clock” algorithm evaluates the following criteria:

- *Priority 1*
- *Clock class*
- *Clock accuracy*
- *Clock variance*
- *Priority 2*

The algorithm first evaluates the value in the *Priority 1* field of the participating devices. The device with the smallest value in the *Priority 1* field becomes the reference time source (Grandmaster). When the value is the same for multiple devices, the algorithm takes the next criterion. When this is also the same, it takes the next criterion after this one. If these values are the same for multiple devices, then the smallest value in the *Clock identity* field decides which device becomes the reference time source (Grandmaster).

In the settings of the boundary clock, the device lets you individually specify the values for *Priority 1* and *Priority 2*. This lets you influence which device will be the reference time source (Grandmaster) in the network.

### 4.3.3 Delay measurement

The delay of the synchronization messages between the devices affects the accuracy. The delay measurement lets the devices take into account the average delay.

PTP version 2 offers the following methods for delay measurement:

- `e2e` (End to End)
  The slave clock measures the delay of synchronization messages to the master clock.
- `e2e-optimized`
  The slave clock measures the delay of synchronization messages to the master clock.
  This method is available only for transparent clocks. The device forwards the synchronization messages sent using Multicast only to the master clock, keeping the network load low. When the device receives a synchronization message from another master clock, it forwards the synchronization messages only to this new port.
  When the device knows no master clock, it forwards synchronization messages to every port.
- `p2p` (Peer to Peer)
  The slave clock measures the delay of synchronization messages to the master clock.
  In addition, the master clock measures the delay to each slave clock, even across blocked ports. This requires that the master and slave clock support Peer-to-Peer (`p2p`).
  In case of interruption of a redundant ring, for example, the slave clock becomes the master clock and the master clock becomes the slave clock. This switch occurs without loss of precision, because the clocks already know the delay in the other direction.

### 4.3.4 PTP domains

The device transmits synchronization messages only from and to devices in the same PTP domain. The device lets you set the domain for the boundary clock and for the transparent clock individually.

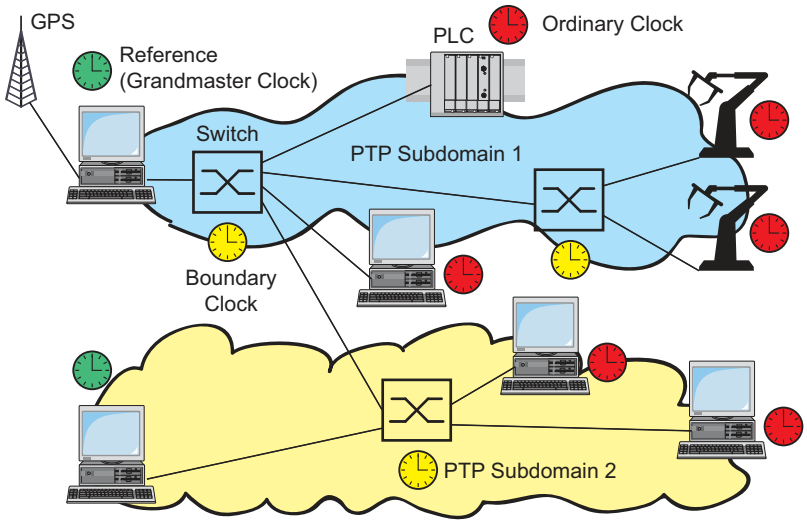



*Figure 22: Example of PTP domains*

### 4.3.5 Using PTP

In order to synchronize the clocks precisely with PTP, only use switches with a boundary clock or transparent clock as nodes.

Perform the following steps:

- ☐ To gain an overview of the distribution of clocks, draw a network plan with the devices involved in PTP.
- ☐ Specify the role for each participating switch (boundary clock or transparent clock). In the device, this setting is called *PTP mode*.

*Table 16: Possible settings for PTP mode*

| PTP mode | Application |
|---|---|
| `v2-boundary-clock` | As a boundary clock, the device distributes synchronization messages to the slave clocks in the subordinate network segment.<br>The boundary clock in turn obtains the time from a higher-level reference time source (Grandmaster). |
| `v2-transparent-clock` | As a transparent clock, the device forwards received synchronization messages after they have been corrected by the delay of the transparent clock. |

- ☐ Enable PTP on each participating switch.
  PTP is then configured on a largely automatic basis.
- ☐ Enable PTP on the end devices.
- ☐ The device lets you influence which device in the network becomes the reference clock (Grandmaster). Therefore, change the default value in the *Priority 1* and *Priority 2* fields for the *Boundary Clock*.

# 5 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.

## 5.1 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.

### 5.1.1 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.

```
show config status

Configuration Storage sync State
--------------------------------
running-config to NV.....................out of sync
...
```

### 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 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”.

| | |
|---|---|
| `show config profiles nvm` | Displays the configuration profiles contained in the non-volatile memory (`nvm`). |
| `enable` | Change to the Privileged EXEC mode. |
| `copy config running-config nvm profile <string>` | Save 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”. |

### 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`.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `show config profiles nvm` | Displays the configuration profiles contained in the non-volatile memory (`nvm`). |
| `configure` | Change to the Configuration mode. |
| `config profile select nvm 1` | Identifier of the configuration profile. Take note of the adjacent name of the configuration profile. |
| `save` | Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile. |

### 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `config envm config-save sd`<br>`config envm config-save usb` | Enable the function.<br>When you save a configuration profile, the device saves a copy in the external memory.<br>`sd` = External SD memory<br>`usb` = External USB memory |
| `no config envm config-save sd`<br>`no config envm config-save usb` | Disable the function.<br>The device does not save a copy in the external memory.<br>`sd` = External SD memory<br>`usb` = External USB memory |
| `save` | Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile. |

### 5.2.3 Backup the configuration profile on a remote server

The device lets you automatically backup the configuration profile to a remote server.
The prerequisite is that you activate the function before you save the configuration profile.

After you save the configuration profile in the non-volatile memory (*NVM*), the device sends a copy to the specified URL.

Perform the following steps:

- ☐ Open the *Basic Settings > Load/Save* dialog.
  In the *Backup config on a remote server when saving* frame, perform the following steps:
- ☐ In the *URL* field, specify the server as well as the path and file name of the backed up configuration profile.
- ☐ Click the *Set credentials* button.
  The dialog displays the *Credentials* window.
- ☐ Enter the login credentials needed to authenticate on the remote server.
- ☐ In the *Operation* option list, enable the function.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `show config remote-backup` | Check status of the function. |
| `configure` | Change to the Configuration mode. |
| `config remote-backup destination` | Enter the destination URL for the configuration profile backup. |
| `config remote-backup username` | Enter the user name to authenticate on the remote server. |
| `config remote-backup password` | Enter the password to authenticate on the remote server. |
| `config remote-backup operation` | Enable the function. |

If the transfer to the remote server is unsuccessful, then the device logs this event in the log file (System Log).

### 5.2.4 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 *Export...* item.
  The dialog displays the *Export...* window.
- ☐ In the *URL* field, specify the file URL on the remote server:
  - ☐ To save the file on an FTP server, specify the URL for the file in the following form:
    `ftp://<user>:<password>@<IP address>:<port>/<file name>`
  - ☐ To save the file on a TFTP server, specify the URL for the file in the following form:
    `tftp://<IP address>/<path>/<file name>`
  - ☐ To save the file on an SCP or SFTP server, specify the URL for the file in one of the following forms:
    `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`
    `scp://` or `sftp://<IP address>/<path>/<file name>`
    When you click the *Ok* button, the device displays the *Credentials* window. There you enter *User name* and *Password* to log in to the server.
- ☐ Click the *Ok* button.
  The configuration profile is now saved as an XML file in the specified location.

| | |
|---|---|
| `show config profiles nvm` | Displays the configuration profiles contained in the non-volatile memory (`nvm`). |
| `enable` | Change to the Privileged EXEC mode. |
| `copy config running-config remote tftp://<IP_address>/ <path>/<file_name>` | Save the current settings on a TFTP server. |
| `copy config nvm remote sftp://<user_name>:<password>@<IP_address>/<path>/<file_name>` | Save the selected configuration profile in the non-volatile memory (`nvm`) on a SFTP server. |
| `copy config nvm profile config3 remote tftp://<IP_address>/ <path>/<file_name>` | Save the configuration profile `config3` in the non-volatile memory (`nvm`) on a TFTP server. |
| `copy config nvm profile config3 remote ftp://<IP_address>:<port>/<path>/<file_name>` | Save the configuration profile `config3` in the non-volatile memory (`nvm`) on an FTP 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `config envm load-priority sd first` | Enable the function.<br>Upon reboot, the device loads a configuration profile from the external memory.<br>`sd` = External SD memory |
| `config envm load-priority usb first` | Enable the function.<br>Upon reboot, the device loads a configuration profile from the external memory.<br>`usb` = External USB memory |
| `show config envm settings` | Displays the settings of the external memory (`envm`). |

```
Type   Status      Auto Update Save Config Config Load Prio
------ ----------- ----------- ----------- ----------------
sd     ok          [x]         [x]           second
usb    ok          [x]         [x]           first
```

| | |
|---|---|
| `save` | Save the settings in a configuration profile in the non-volatile memory (*NVM*) of the device. |

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 profiles nvm` | Displays the configuration profiles contained in the non-volatile memory (`nvm`). |
| `enable` | Change to the Privileged EXEC mode. |
| `copy config envm profile config3 nvm` | Copy the configuration profile `config3` from the external memory (`envm`) to the non-volatile memory (`nvm`). |

The device can also automatically load a configuration profile from a script file during the boot process.

Prerequisites:

- ▶ Verify that the external memory is connected before you start the device.
- ▶ The root directory of the external memory contains a text file `startup.txt` with the content `script=<file_name>`. The placeholder `<file_name>` represents the script file that the device executes during the boot process.
- ▶ The root directory of the external memory contains the script file. You have the option to save the script with a user-specified name. Save the file with the file extension `.cli`.

**Note:** Verify that the script saved in the external memory is not empty. If the script is empty, then the device loads the next configuration profile as per the configuration priority settings.

After applying the script, the device automatically saves the configuration profile from the script file as an XML file in the external memory. When you type the appropriate command into the script file, you have the option to disable this function:

- `no config envm config-save sd`
  The device does not create a copy in the external SD memory.
- `no config envm config-save usb`
  The device does not create a copy in the external USB memory.

When the script file contains an incorrect command, the device does not apply this command during the boot process. The device logs the event in the log file (System Log).

### 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 selected 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 an FTP server, specify the URL for the file in the following form:
    `ftp://<user>:<password>@<IP address>:<port>/<file name>`
  - ☐ When the file is located on a TFTP server, specify the URL for the file in the following form:
    `tftp://<IP address>/<path>/<file name>`
  - ☐ When the file is located on an SCP or SFTP server, specify the URL for the file in one of the following forms:
    `scp://` or `sftp://<IP address>/<path>/<file name>`
    When you click the *Start* button, the device displays the *Credentials* window. There you enter *User name* and *Password* to log in to the server.
    `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`
- ☐ 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` | Change to the Privileged EXEC mode. |
| `copy config remote ftp://<IP_address>:<port>/<path>/<file_name> running-config` | Import and activate the settings of a configuration profile saved on an FTP server.<br>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. |
| `copy config remote tftp://<IP_address>/ <path>/<file_name> running-config` | Import and activate the settings of a configuration profile saved on a TFTP server.<br>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. |
| `copy config remote sftp://<user name>:<password>@<IP_address>/<path>/<file_name> running-config` | Import and activate the settings of a configuration profile saved on a SFTP server.<br>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. |
| `copy config remote ftp://<IP_address>:<port>/<path>/<file_name> nvm profile config3` | Import the settings of a configuration profile saved on an FTP server and save the settings in the configuration profile `config3` in the non-volatile memory (`nvm`). |
| `copy config remote tftp://<IP_address>/<path>/<file_name> nvm profile config3` | Import the settings of a configuration profile saved on a TFTP server and save the settings in the configuration profile `config3` in the non-volatile memory (`nvm`). |

**Note:** Upgrading from Classic to HiOS? Convert your device configuration files using our online tool: https://convert.hirschmann.com

# 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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `clear factory` | 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.

| | |
|---|---|
| `enable` | 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.

## 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.

To update the software using TFTP, 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.
- ☐ In the *Software update* frame, *URL* field, enter the URL for the image file in the following form:
  - ▶ When the image file is saved on an FTP server:
    `ftp://<IP_address>:<port>/<path>/<image_file_name>.bin`
  - ▶ When the image file is saved on a TFTP server:
    `tftp://<IP_address>/<path>/<image_file_name>.bin`
  - ▶ When the image file is saved on a SCP or SFTP server:
    `scp://` or `sftp://<IP_address>/<path>/<image_file_name>.bin`
    `scp://` or `sftp://<username>:<password>@<IP_address>/<path>/<image_file_name>.bin`
    When you enter the URL without the user name and password, the device displays the *Credentials* window. There you enter the login credentials needed to log in to the server.
- ☐ 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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `copy firmware remote tftp://10.0.1.159/product.bin system` | Transfer the `product.bin` file from the TFTP server with the IP address `10.0.1.159` to the device. |

# 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_SWUPDATE_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
- Gigabit Ethernet mode for ports

## 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `no shutdown` | 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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `no auto-negotiate` | Disable the automatic configuration mode. |
| `speed 100 full` | Port speed 100 MBit/s, full duplex |

# 7.3 Gigabit Ethernet mode for ports

The device supports 2.5 Gbit/s on several interfaces with one of the following SFP transceivers:
- M-SFP-2.5-MM/LC EEC
- M-SFP-2.5-SM-/LC EEC
- M-SFP-2.5-SM/LC EEC
- M-SFP-2.5-SM+/LC EEC

The device supports 10 Gbit/s on several interfaces with one of the following SFP+ transceivers:
- M-SFP-10-SR/LC EEC
- M-SFP-10-LR/LC EEC
- M-SFP-10-ER/LC EEC
- M-SFP-10-ZR/LC

The type of the transceiver plugged into the slot determines the port speed. The device has no option to set the speed manually. Ports with 2.5 Gbit/s or 10 Gbit/s port speed are unable to support data rates of 100 Mbit/s.

**Note:** You find more information about the transceiver order numbers in the “Accessories” chapter of the “Installation” user manual.

## 7.3.1 Example

You use the Gigabit Ethernet mode to get a higher bandwidth for uplinks. To use this function, insert an applicable transceiver type in the appropriate slot.

Perform the following steps:

☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.

The column *Manual configuration* displays the value `2.5 Gbit/s FDX` for the ports that have a 2.5 Gbit/s SFP transceiver inserted.

The column *Manual configuration* displays the value `10 Gbit/s FDX` for the ports that have a 10 Gbit/s SFP+ transceiver inserted.

You cannot change the speed.

| | |
|---|---|
| `show port 1/1` | Displays the parameters for slot `1` port `1`. The `Physical Mode` list entry displays the value `2500 full` for the ports that have a 2.5 Gbit/s SFP transceiver inserted. |

```
Interface.....................1/1
Name..........................My interface
--
Cable-crossing Setting........-
Physical Mode.................2500 full
Physical Status...............-
```

```
show port 1/2
```

Displays the parameters for slot 1 port 2. The `Physical Mode` list entry displays the value `10G full` for the ports that have a 10 Gbit/s SFP+ transceiver inserted.

```
Interface.....................1/2
Name..........................My interface
--
Cable-crossing Setting........-
Physical Mode.................10G full
Physical Status...............-
```

# 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 Telnet
- Disabling HiDiscovery
- Enable IP access restriction
- Adjusting the session timeouts
- Deactivating the unused modules

## 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:

- ☐ Open the *Device Security > Management Access > SNMPv1/v2 Community* dialog.

The dialog displays the communities that are set up.

- ☐ 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.
- ☐ Save the changes temporarily. To do this, click the ☑ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `snmp community rw <community name>` | Specify the community for read/write access. |
| `show snmp community` | Display the communities that have been configured. |
| `save` | 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:

- ☐ Open the *Device Security > Management Access > Server* dialog, *SNMP* tab.

The dialog displays the settings of the SNMP server.

- ☐ To deactivate the SNMPv1 protocol, you unmark the *SNMPv1* checkbox.
- ☐ To deactivate the SNMPv2 protocol, you unmark the *SNMPv2* checkbox.
- ☐ Save the changes temporarily. To do this, click the button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `no snmp access version v1` | Deactivate the SNMPv1 protocol. |
| `no snmp access version v2` | Deactivate the SNMPv2 protocol. |
| `show snmp access` | Display the SNMP server settings. |
| `save` | 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:

- ☐ Open the *Device Security > Management Access > Server* dialog, *HTTP* tab.
- ☐ To disable the HTTP protocol, select the `Off` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `no http server` | Disable the HTTP protocol. |

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:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `https server` | Enable the HTTPS protocol. |

## 8.4 Disabling Telnet

The device lets you remotely access the device management using Telnet or SSH. Telnet connections are unencrypted, while SSH connections are encrypted.

The Telnet server is enabled in the device by default. If you disable Telnet, then unencrypted remote access to the Command Line Interface is no longer possible. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *Telnet* tab.
- ☐ To disable the Telnet server, select the `Off` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `no telnet server` | Disable the Telnet server. |

If the SSH server is disabled and you also disable Telnet, then access to the Command Line Interface is only possible through the serial interface of the device. To work remotely with the Command Line Interface, enable SSH. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *SSH* tab.
- ☐ To enable the *SSH* server, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `ssh server` | Enable the SSH server. |

# 8.5 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` | Change to the Privileged EXEC mode. |
| `network hidiscovery mode read-only` | Disable write permission of the HiDiscovery software. |
| `no network hidiscovery operation` | Disable HiDiscovery access. |

# 8.6 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 17: Parameters for the IP access restriction*

| Parameter | Company network | Mobile phone network |
|---|---|---|
| Network address | `192.168.1.0` | `109.237.176.0` |
| Netmask | `24` | `24` |
| Desired protocols | https, snmp | ssh |

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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `show network management access global` | Displays if IP access restriction is enabled or disabled. |
| `show network management access rules` | Display the entries that have been configured. |
| `no network management access operation` | Disable the IP access restriction. |
| `network management access add 2` | Create the entry for the address range of the company network.<br>Number of the next available index in this example: 2. |
| `network management access modify 2 ip 192.168.1.0` | Specify the IP address of the company network. |
| `network management access modify 2 mask 24` | Specify the netmask of the company network. |
| `network management access modify 2 ssh disable` | Deactivate SSH for the address range of the company network.<br>Repeat the operation for every unwanted protocol. |
| `network management access add 3` | Create an entry for the address range of the mobile phone network.<br>Number of the next available index in this example: 3. |
| `network management access modify 3 ip 109.237.176.0` | Specify the IP address of the mobile phone network. |
| `network management access modify 3 mask 24` | Specify the netmask of the mobile phone network. |
| `network management access modify 3 snmp disable` | Deactivate SNMP for the address range of the mobile phone network.<br>Repeat the operation for every unwanted protocol. |
| `no network management access status 1` | Deactivate the default entry.<br>This entry lets users have access to the device from any IP address and the supported protocols. |
| `network management access status 2` | Activate an entry for the address range of the company network. |
| `network management access status 3` | Activate an entry for the address range of the mobile phone network. |
| `show network management access rules` | Display the entries that have been configured. |
| `network management access operation` | Enable the IP access restriction. |

# 8.7 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 Telnet 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `ssh timeout <0..160>` | Specify the timeout period in minutes for Command Line Interface sessions using an SSH connection. |

### Timeout for Command Line Interface sessions using a Telnet connection

Perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *Telnet* 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `telnet timeout <0..160>` | Specify the timeout period in minutes for Command Line Interface sessions using a Telnet 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` | Change to the Privileged EXEC mode. |
| `cli serial-timeout <0..160>` | 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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `network management access web timeout <0..160>` | Specify the timeout period in minutes for Graphical User Interface sessions |

# 8.8 Deactivating the unused modules

The default settings of a media module slot allow access to the network. If a media module is inserted into an empty slot, the media module's ports will establish network connections by default.

To help prevent unauthorized network access, deactivate the unused slots. To do this, perform the following steps:

- ☐ Open the *Basic Settings > Modules* dialog.
- ☐ To deactivate the slot and deny network access, unmark the *Active* checkbox.
- ☐ Save the changes temporarily. To do this, click the button.

# 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:
- Service request control (Denial of Service, DoS)
- Denying access to devices based on their IP or MAC address (Access Control List)

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 data packets go through the filter functions of the device in the following sequence:
- DoS … if `permit` or `accept`, then progress to the next rule
- ACL … if `permit` or `accept`, then progress to the next rule

## 9.1 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 18: DoS filters for TCP packets*

| Filter | Action |
|---|---|
| Activate Null Scan Filter | The device detects and discards incoming TCP packets with the following properties:<br>- No TCP flags are set.<br>- The TCP sequence number is 0. |

*Table 18: DoS filters for TCP packets*

| Filter | Action |
|---|---|
| Activate Xmas Filter | The device detects and discards incoming TCP packets with the following properties:<br>▶ The TCP flags *FIN*, *URG* and *PSH* are simultaneously set.<br>▶ The TCP sequence number is 0. |
| Activate SYN/FIN Filter | The device detects and discards incoming TCP packets in which the TCP flags *SYN* and *FIN* are simultaneously set. |
| Activate Minimal Header Filter | The device detects and discards incoming TCP packets in which the TCP header is too short. |

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, then 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.

# 9.2 ACL

In this menu you can enter the parameters for the Access Control Lists (ACLs).

The device uses ACLs to filter data packets received on VLANs or on individual or multiple ports. In a ACL, you specify rules that the device uses to filter data packets. When such a rule applies to a packet, the device applies the actions specified in the rule to the packet. The available actions are as follows:

- allow (`permit`)
- discard (`deny`)
- redirect to a certain port (see *Redirection port* field)
- mirror (see *Mirror port* field)

The list below contains criteria that you can apply to filter the data packets:

- Source or destination address of a packet (MAC)
- Source or destination address of a data packet (IPv4)
- Type of the transmitting protocol (MAC/IPv4)
- Source or destination port of a data packet (IPv4)
- Service class of a packet (MAC)
- Membership of a specific VLAN (MAC)
- DSCP classification (IPv4)
- ToS classification (IPv4)
- Packet Fragmentation (IPv4)

You can specify the following ACL types:

- IP ACLs for VLANs
- IP ACLs for ports
- MAC ACLs for VLANs
- MAC ACLs for ports

When you assign both an IP ACL and MAC ACL to the same interface, the device first uses the IP ACL to filter the data stream. The device applies the MAC ACL rules only after the packets are filtered through the IP ACL. The priority of an ACL is independent of the index of a rule.

Within an ACL, the device processes the rules in order. The index of the respective rule determines the order in which the device filters the data stream. When you assign an ACL to a port or VLAN, you can specify its priority with the index. The lower the number, the higher the priority. The device processes the rule with the higher priority first.

If none of the rules specified in an ACL applies to a data packet, then the implicit `deny` rule applies. As a result, the device drops the received data packets.

Keep in mind that the device directly implements the implicit `deny` rule.

**Note:** The number of available ACLs depends on the device. You find more information about the ACL values in the chapter “Technical Data” on page 429.

**Note:** You can assign a single ACL to any number of ports or VLANs.

**Note:** If you activate the *Packet fragmented* function for a rule, then the rule processes IPv4 fragments with the offset other than zero. The rule processes every IPv4 fragment except for the initial IPv4 fragment.

The *ACL* menu contains the following dialogs:
- *ACL IPv4 Rule*
- *ACL MAC Rule*
- *ACL Assignment*

These dialogs provide the following options:
- To specify the rules for the various ACL types.
- To provide the rules with the required priorities.
- To assign the ACLs to ports or VLANs.

### 9.2.1 Creating and editing IPv4 rules

When filtering IPv4 data packets, the device lets you:
- create new groups and rules
- add new rules to existing groups
- edit an existing rule
- activate and deactivate groups and rules
- delete existing groups and rules
- change the order of existing rules

**Note:** You cannot apply IP ACL rules and DiffServ rules together in the same direction on a port.

Perform the following steps:

- ☐ Open the *Network Security > ACL > IPv4 Rule* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ To create a group, specify a meaningful name in the *Group name* field. You can combine several rules in one group.
- ☐ To add a rule to an existing group, select the name of the group in the *Group name* field.
- ☐ In the *Index* field you specify the number for the rule within the ACL.
  This number defines the priority of the rule.
- ☐ Click the *Ok* button.
  The device adds the rule to the table.
  Group and role are active immediately.
  To deactivate group or rules, unmark the checkbox in the *Active* column.
  To remove a rule, highlight the affected table entry and click the button.
- ☐ Edit the rule parameters in the table.
  To change a value, double-click the relevant field.
- ☐ Save the changes temporarily. To do this, click the button.

**Note:** The device lets you use wildcards with the *Source IP address* and *Destination IP address* parameters. If you enter for example, `192.168.?.?`, then the device allows addresses that start with `192.168`.

**Note:** The prerequisite for changing the values in the *Source TCP/UDP port* and *Destination TCP/UDP port* column is that you specify the value `tcp` or `udp` in the *Protocol* column.

**Note:** The prerequisite for changing the value in the *Redirection port* and *Mirror port* column is that you specify the value `permit` in the *Action* column.

### 9.2.2 Creating and configuring an IP ACL using the Command Line Interface

In the following example, you configure ACLs to block communications from computers B and C, to computer A via IP (TCP, UDP, etc.).

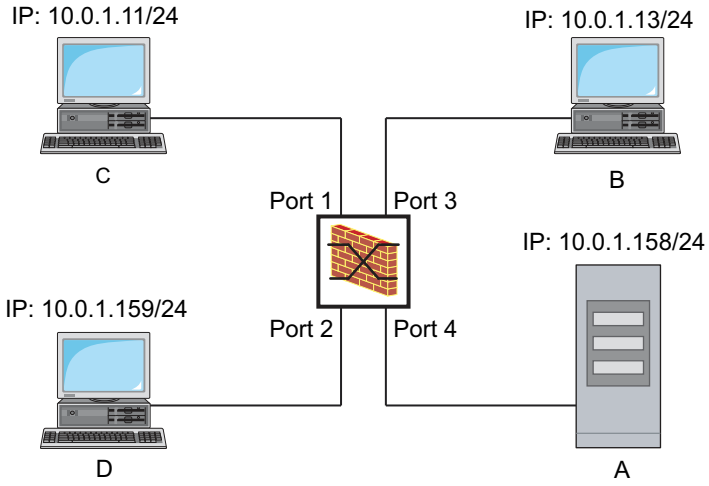



*Figure 23: Example of an IP ACL*

Perform the following steps:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `ip access-list extended name filter1 deny src 10.0.1.11-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1` | Add IP ACL with name `filter1`. Add rule denying IP data packets from `10.0.1.11` to `10.0.1.158`. Priority `1` (highest priority). |
| `ip access-list extended name filter1 permit src any dst any` | Add rule to the IP ACL admitting IP data packets. |
| `show access-list ip filter1` | Display rules of the IP ACL `filter1`. |
| `ip access-list extended name filter2 deny src 10.0.1.13-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1` | Add IP ACL with name `filter2`. Add rule denying IP data packets from `10.0.1.13` to `10.0.1.158`. Priority `1` (highest priority). |
| `show access-list ip filter2` | Display rules of the IP ACL `filter2`. |

### 9.2.3 Creating and editing MAC rules

When filtering MAC data packets, the device lets you:

- create new groups and rules
- add new rules to existing groups
- edit an existing rule
- activate and deactivate groups and rules
- delete existing groups and rules
- change the order of existing rules

Perform the following steps:

- ☐ Open the *Network Security > ACL > MAC Rule* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ To create a group, specify a meaningful name in the *Group name* field. You can combine several rules in one group.
- ☐ To add a rule to an existing group, select the name of the group in the *Group name* field.
- ☐ In the *Index* field you specify the number for the rule within the ACL.
  This number defines the priority of the rule.
- ☐ Click the *Ok* button.
  The device adds the rule to the table.
  Group and role are active immediately.
  To deactivate group or rules, unmark the checkbox in the *Active* column.
  To remove a rule, highlight the affected table entry and click the button.
- ☐ Edit the rule parameters in the table.
  To change a value, double-click the relevant field.
- ☐ Save the changes temporarily. To do this, click the button.

**Note:** In the *Source MAC address* and *Destination MAC address* fields you can use wildcards in the `FF:??:??:??:??:??` or `??:??:??:??:00:01` form. Use capital letters here.

### 9.2.4 Creating and configuring a MAC ACL using the Command Line Interface

In the following example, AppleTalk and IPX are to be filtered out from the entire network. To do this, perform the following steps:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `mac acl add 1 macfilter` | Adds an MAC ACL with the ID `1` and the name `macfilter`. |
| `mac acl rule add 1 1 deny src any any dst any any etype appletalk` | Adds a rule to position `1` of the MAC ACL with the ID `1` rejecting packets with EtherType `0x809B (AppleTalk)`. |
| `mac acl rule add 1 2 deny src any any dst any any etype ipx-old` | Adds a rule to position `2` of the MAC ACL with the ID `1` rejecting packets with EtherType `0x8137 (IPX alt)`. |
| `mac acl rule add 1 3 deny src any any dst any any etype ipx-new` | Adds a rule to position `3` of the MAC ACL with the ID `1` rejecting packets with EtherType `0x8138 (IPX)`. |
| `mac acl rule add 1 4 permit src any any dst any any` | Adds a rule to position `4` of the MAC ACL with the ID `1` forwarding packets. |
| `show acl mac rules 1` | Displays the rules of the MAC ACL with the ID `1`. |
| `interface 1/1,1/2,1/3,1/4,1/5,1/6` | Change to the interface configuration mode of the interfaces `1/1` to `1/6`. |

| | |
|---|---|
| `acl mac assign 1 in 1` | Assigns the MAC ACL with the ID `1` to incoming data packets (`1/1`) on interfaces `1/6` to `in`. |
| `exit` | Leaves the interface mode. |
| `show acl mac assignment 1` | Displays the assignment of the MAC ACL with the ID `1` to interfaces or VLANs. |

### 9.2.5 Assigning ACLs to a port or VLAN

When you assign ACLs to a port or VLAN, the device gives you the following options:

- To select the port or VLAN.
- To specify the ACL priority.
- To select the direction.
- To select the ACL using the group name.

Perform the following steps:

- ☐ Open the *Network Security > ACL > Assignment* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
  - ☐ In the *Port/VLAN* field, specify the desired port or the desired VLAN.
  - ☐ In the *Priority* field, specify the priority.
  - ☐ In the *Direction* field, specify the data packets to which the device applies the rule.
  - ☐ In the *Group name* field, specify the rule the device assigns to the port or the VLAN.
- ☐ Click the *Ok* button.
- ☐ Save the changes temporarily. To do this, click the button.

# 9.3 MAC authentication bypass

The *MAC authorized bypass* function lets clients that do not support 802.1X, such as printers and fax machines, authenticate to the network using their MAC address. The device lets you specify the format of the MAC address used to authenticate the clients on the RADIUS server.

Example:

Split the MAC address into 6 groups of 2 characters. Use uppercase letters and a colon character as separator: `AA:BB:CC:DD:EE:FF`

Use the passwort `xY-45uM_e`. To do this, perform the following steps:

- ☐ Open the *Network Security > 802.1X Port Authentication > Global* dialog.
  In the *MAC authentication bypass format options* frame, perform the following steps:
- ☐ In the *Group size* drop-down list, select the value `2`.
  The device splits the MAC address into 6 groups of 2 characters.
- ☐ In the *Group separator* drop-down list, select the `:` character.
- ☐ In the *Upper or lower case* drop-down list, select the `upper-case` item.
- ☐ In the *Password* field, enter the password `xY-45uM_e`.
  The device uses this password for every client that authenticates to the RADIUS server. If you leave the field empty, then the device uses the formatted MAC address also as the password.
- ☐ To temporarily save the settings, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `dot1x mac-authentication-bypass format group-size 2` | Specify the group size `2`. |
| `dot1x mac-authentication-bypass format group-separator :` | Specify the group separator `:`. |
| `dot1x mac-authentication-bypass format letter-case upper-case` | Specify that the device formats the authentication data in uppercase letters. |
| `dot1x mac-authentication-bypass password xY-45uM_e` | Specify the password `xY-45uM_e`. The device uses this password to authenticate every client on the RADIUS server. |

# 10 Network load control

The device features a number of functions that can help you reduce the network load:
- Direct packet distribution
- Multicasts
- Rate limiter
- Prioritization - QoS
- Differentiated services
- Flow control

## 10.1 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.

### 10.1.1 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.

### 10.1.2 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).

### 10.1.3 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:

☐ 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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `mac-filter <MAC address> <VLAN ID>` | Create the MAC address filter, consisting of a MAC address and VLAN ID. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `mac-filter <MAC address> <VLAN ID>` | Assign the port to a previously created MAC address filter. |
| `save` | Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile. |

☐ 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `no mac-filter <MAC address> <VLAN ID>` | Cancel the assignment of the MAC address filter on the port. |
| `exit` | Change to the Configuration mode. |
| `no mac-filter <MAC address> <VLAN ID>` | Deleting the MAC address filter, consisting of a MAC address and VLAN ID. |
| `exit` | Change to the Privileged EXEC mode. |
| `save` | Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile. |

☐ 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). |

# 10.2 Multicasts

By default, the device floods data packets with a Multicast address, that is, the device forwards the data packets to every port. This leads to an increased network load.

The use of IGMP snooping can reduce the network load caused by Multicast data traffic. IGMP snooping lets the device send Multicast data packets only on those ports to which devices “interested” in Multicast are connected.

## 10.2.1 Example of a Multicast application

Surveillance cameras transmit images to monitors in the machine room and in the monitoring room. With an IP Multicast transmission, the cameras transmit their graphic data over the network in Multicast packets.

The Internet Group Management Protocol (IGMP) organizes the Multicast data traffic between the Multicast routers and the monitors. The switches in the network between the Multicast routers and the monitors monitor the IGMP data traffic continuously (“IGMP Snooping”).

Switches register logins for receiving a Multicast stream (IGMP report). The device then creates an entry in the MAC address table (FDB) and forwards Multicast packets only to the ports on which it has previously received IGMP reports.

## 10.2.2 IGMP snooping

The Internet Group Management Protocol (IGMP) describes the distribution of Multicast information between routers and connected receivers on Layer 3. IGMP Snooping describes the function of a switch of continuously monitoring IGMP traffic and optimizing its own transmission settings for this data traffic.

The *IGMP Snooping* function in the device operates according to RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches).

Multicast routers with an active *IGMP* function periodically request (query) registration of Multicast streams in order to determine the associated IP Multicast group members. IP Multicast group members reply with a Report message. This Report message contains the parameters required by the *IGMP* function. The Multicast router enters the IP Multicast group address from the Report message in its routing table. This causes it to forward data packets with this IP Multicast group in the destination address field according to its routing table.

When leaving a Multicast group (IGMP version 2 and higher), receivers log out with a “Leave” message and do not send any more Report messages. If it does not receive any more Report messages from this receiver within a certain time (aging time), then the Multicast router removes the routing table entry of a receiver.

When several IGMP Multicast routers are in the same network, the device with the smaller IP address takes over the query function. When there are no Multicast routers on the network, you have the option to enable the query function in an appropriately equipped switch.

A switch that connects one Multicast receiver with a Multicast router analyzes the IGMP information with the IGMP snooping method.

The IGMP snooping method also makes it possible for switches to use the *IGMP* function. A switch stores the MAC addresses derived from IP addresses of the Multicast receivers as recognized Multicast addresses in its MAC address table (FDB). In addition, the switch identifies the ports on which it has received reports for a specific Multicast address. In this way, the switch forwards Multicast packets only to ports to which Multicast receivers are connected. The other ports do not receive these packets.

A special feature of the device is the possibility of determining the processing of data packets with unknown Multicast addresses. Depending on the setting, the device discards these data packets or forwards them to every port. By default, the device transmits the data packets only to ports with connected devices, which in turn receive query packets. You also have the option of additionally sending known Multicast packets to query ports.

### Setting IGMP snooping

Perform the following steps:

- ☐ Open the *Switching > IGMP Snooping > Global* dialog.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.

When the *IGMP Snooping* function is disabled, the device behaves as follows:

- The device ignores the received query and report messages.
- The device forwards (floods) received data packets with a Multicast address as the destination address to every port.

- ☐ Save the changes temporarily. To do this, click the ☑ button.

☐ Specifying the settings for a port:

- ☐ Open the *Switching > IGMP Snooping > Configuration* dialog, *Port* tab.
- ☐ To activate the *IGMP Snooping* function on a port, mark the checkbox in the *Active* column for the relevant port.
- ☐ Save the changes temporarily. To do this, click the ☑ button.

☐ Specifying the settings for a VLAN:

- ☐ Open the *Switching > IGMP Snooping > Configuration* dialog, *VLAN ID* tab.
- ☐ To activate the *IGMP Snooping* function for a specific VLAN, mark the checkbox in the *Active* column for the relevant VLAN.
- ☐ Save the changes temporarily. To do this, click the ☑ button.

### Setting the IGMP querier function

The device itself optionally sends active query messages; alternatively, it responds to query messages or detects other Multicast queriers in the network (*IGMP Snooping Querier* function).

Prerequisite:

The *IGMP Snooping* function is enabled globally.

Perform the following steps:

- ☐ Open the *Switching > IGMP Snooping > Querier* dialog.
- ☐ In the *Operation* frame, enable/disable the *IGMP Snooping Querier* function of the device globally.
- ☐ To activate the *IGMP Snooping Querier* function for a specific VLAN, mark the checkbox in the *Active* column for the relevant VLAN.
- ▶ The device carries out a simple selection process: When the IP source address of the other Multicast querier is lower than its own, the device switches to the passive state, in which it does not send out any more query requests.
- ▶ In the *Address* column, you specify the IP Multicast address that the device inserts as the sender address in generated query requests. You use the address of the Multicast router.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

### IGMP snooping enhancements (table)

The *Switching > IGMP Snooping > Snooping Enhancements* dialog provides you access to enhanced settings for the *IGMP Snooping* function. You activate or deactivate the settings on a per port basis in a VLAN.

The following settings are possible:

- ▶ `Static`
  Use this setting to set the port as a static query port. The device forwards every IGMP message on a static query port, even if it has previously received no IGMP query messages on this port. When the static option is disabled and the device has previously received IGMP query messages, it forwards IGMP messages on this port. When this is the case, the entry displays `L` (“learned”).
- ▶ `Learn by LLDP`
  A port with this setting automatically discovers other Hirschmann devices using LLDP (Link Layer Discovery Protocol). The device then learns the IGMP query status of this port from these Hirschmann devices and configures the *IGMP Snooping Querier* function accordingly. The `ALA` entry indicates that the `Learn by LLDP` function is activated. When the device has found another Hirschmann device on this port in this VLAN, the entry also displays an `A` (“automatic”).
- ▶ `Forward All`
  With this setting, the device forwards the data packets addressed to a Multicast address to this port. The setting is suitable in the following situations, for example:
  - For diagnostic purposes.
  - For devices in an MRP ring: After the ring is switched, the `Forward All` function makes it possible to reconfigure the network rapidly for data packets with registered Multicast destination addresses. Activate the `Forward All` function on every ring port.

Prerequisite:

The *IGMP Snooping* function is enabled globally.

Perform the following steps:

- ☐ Open the *Switching > IGMP Snooping > Snooping Enhancements* dialog.
- ☐ Double-click the desired port in the desired VLAN.

- ☐ To activate one or more functions, select the corresponding options.
- ☐ Click the *Ok* button.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `igmp-snooping vlan-id 1 forward-all 1/1` | Activate the `Forward All` function for port `1/1` in VLAN `1`. |

### Configure Multicasts

The device lets you configure the exchange of Multicast data packets. The device provides different options depending on whether the data packets are to be sent to unknown or known Multicast receivers.

The settings for unknown Multicast addresses are global for the entire device. The following options can be selected:

- The device discards unknown Multicasts.
- The device forwards unknown Multicasts to every port.
- The device forwards unknown Multicasts only to ports that have previously received query messages (query ports).

**Note:** The exchange settings for unknown Multicast addresses also apply to the reserved IP addresses from the “Local Network Control Block” (`224.0.0.0..224.0.0.255`). This behavior can affect higher-level routing protocols.

For each VLAN, you specify the sending of Multicast packets to known Multicast addresses individually. The following options can be selected:

- The device forwards known Multicasts to the ports that have previously received query messages (query ports) and to the registered ports. Registered ports are ports with Multicast receivers registered with the corresponding Multicast group. This option helps ensure that the transfer works with basic applications without further configuration.
- The device forwards known Multicasts only to the registered ports. The advantage of this setting is that it uses the available bandwidth optimally through direct distribution.

Prerequisite:

The *IGMP Snooping* function is enabled globally.

Perform the following steps:

- ☐ Open the *Switching > IGMP Snooping > Multicasts* dialog.

- ☐ In the *Configuration* frame, you specify how the device sends data packets to unknown Multicast addresses.
  - ▶ *send to registered ports*
    The device forwards packets with unknown Multicast address to every query port.
  - ▶ *send to query and registered ports*
    The device forwards packets with unknown Multicast address to every port.
- ☐ In the *Known multicasts* column, you specify how the device sends data packets to known Multicast addresses in the corresponding VLAN. Click the relevant field and select the desired value.
- ☐ Save the changes temporarily. To do this, click the ✔ button.

# 10.3 Rate limiter

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:

- ☐ Open the *Switching > Rate Limiter* dialog.
- 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 interpretes the threshold values as percent of the port bandwidth or as packets per second. The threshold value `0` deactivates the rate limiter.
- ☐ Save the changes temporarily. To do this, click the ☑ button.

# 10.4 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.

## 10.4.1 Description of prioritization

For data traffic prioritization, traffic classes are defined in the device. The device prioritizes higher traffic classes over lower traffic classes. The number of traffic classes depends on the device type.

To provide for optimal data flow for delay-sensitive data, you assign higher traffic classes to this data. You assign lower traffic classes to data that is less sensitive to delay.

### Assigning traffic classes to the data

The device automatically assigns traffic classes to inbound data (traffic classification). The device takes the following classification criteria into account:

- Methods according to which the device carries out assignment of received data packets to traffic classes:
  - `trustDot1p`
    The device uses the priority of the data packet contained in the VLAN tag.
  - `trustIpDscp`
    The device uses the QoS information contained in the IP header (ToS/DiffServ).
  - `untrusted`
    The device ignores possible priority information within the data packets and uses the priority of the receiving port directly.
- The priority assigned to the receiving port.

Both classification criteria are configurable.

During traffic classification, the device uses the following rules:

- When the receiving port is set to `trustDot1p` (default setting), the device uses the data packet priority contained in the VLAN tag. When the data packets do not contain a VLAN tag, the device is guided by the priority of the receiving port.
- When the receiving port is set to `trustIpDscp`, the device uses the QoS information (ToS/DiffServ) in the IP header. When the data packets do not contain IP packets, the device is guided by the priority of the receiving port.
- When the receiving port is set to `untrusted`, the device is guided by the priority of the receiving port.

### Prioritizing traffic classes

For prioritization of traffic classes, the device uses the following methods:

- `Strict`
  When transmission of data of a higher traffic class is no longer taking place or the relevant data is still in the queue, the device sends data of the corresponding traffic class. If every traffic class is prioritized according to the `Strict` method, then under high network load the device can permanently block the data of lower traffic classes.
- `Weighted Fair Queuing`
  The traffic class is assigned a specific bandwidth. This helps ensure that the device sends the data traffic of this traffic class, although there is a great deal of data traffic in higher traffic classes.

## 10.4.2 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)
- Type-of-Service (ToS) or DiffServ (DSCP) for VLAN Management IP packets (Layer 3)

The device lets you evaluate this priority information using the following options:

- `trustDot1p`
  The device assigns VLAN-tagged data packets to the different traffic classes according to their VLAN priorities. The corresponding allocation is configurable. The device assigns the priority of the receiving port to data packets it receives without a VLAN tag.
- `trustIpDscp`
  The device assigns the IP packets to the different traffic classes according to the DSCP value in the IP header, although the packet was also VLAN-tagged. The corresponding allocation is configurable. The device prioritizes non-IP packets according to the priority of the receiving port.
- `untrusted`
  The device ignores the priority information in the data packets and assigns the priority of the receiving port to them.

## 10.4.3 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”).

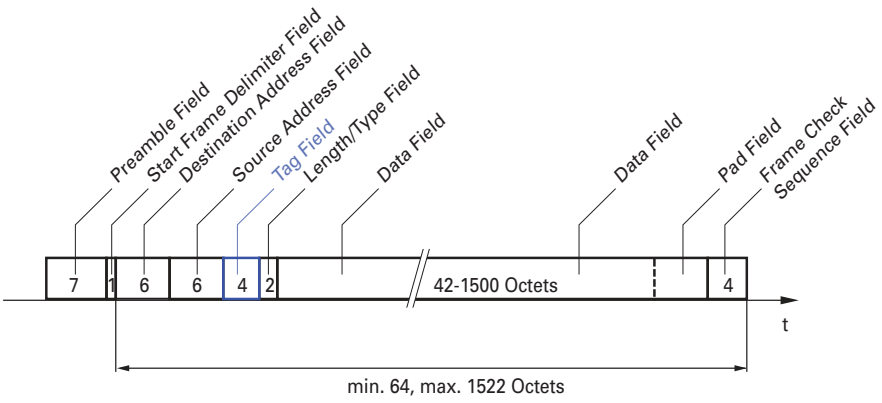



*Figure 24: Ethernet data packet with tag*

For data packets with VLAN tags, the device evaluates the following information:
- Priority information
- When VLANs are configured, VLAN tagging

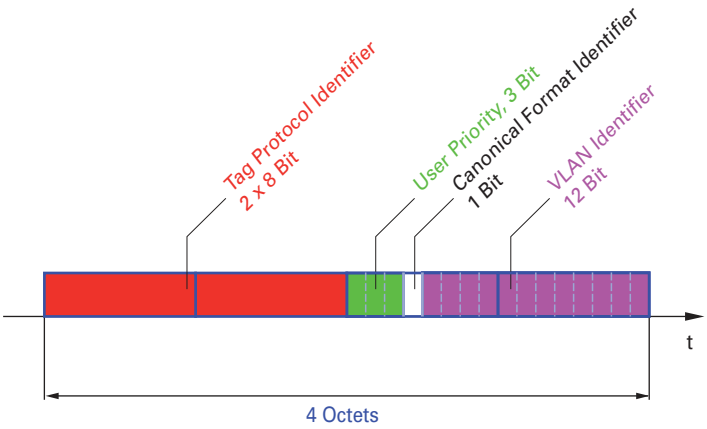



*Figure 25: Structure of the VLAN tagging*

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.

### 10.4.4 IP ToS (Type of Service)

The Type-of-Service field (ToS) in the IP header was already part of the IP protocol from the start, and is used to differentiate different services in IP networks. Even back then, there were ideas about differentiated treatment of IP packets, due to the limited bandwidth available and the unreliable connection paths. Because of the continuous increase in the available bandwidth, there was no need to use the ToS field.

Only with the real-time requirements of today's networks has the ToS field become significant again. Selecting the ToS byte of the IP header enables you to differentiate between different services. However, this field is not widely used in practice.

*Table 19: ToS field in the IP header*

| Bits (0-2): IP Precedence Defined | Bits (3-6): Type of Service Defined | Bit (7) |
|---|---|---|
| 111 - Network Control | 0000 - [all normal] | 0 - Zero |
| 110 - Internetwork Control | 1000 - [minimize delay] | |
| 101 - CRITIC / ECP | 0100 - [maximize throughput | |

*Table 19: ToS field in the IP header (cont.)*

| Bits (0-2): IP Precedence Defined | Bits (3-6): Type of Service Defined | Bit (7) |
|---|---|---|
| 100 - Flash Override | 0010 - [maximize reliability] | |
| 011 - Flash | 0001 - [minimize monetary cost] | |
| 010 - Immediate | | |
| 001 - Priority | | |
| 000 - Routine | | |

## 10.4.5 Handling of traffic classes

The device provides the following options for handling traffic classes:
- Strict Priority
- Weighted Fair Queuing
- Strict Priority combined with Weighted Fair Queuing
- Queue management

### Strict Priority description

With the Strict Priority setting, the device first transmits data packets that have a higher traffic class (higher priority) before transmitting a data packet with the next highest traffic class. When there are no other data packets remaining in the queue, the device transmits a data packet with the lowest traffic class (lowest priority). In unfortunate cases, if there is a high volume of high-priority traffic waiting to be sent on this port, then the device does not send packets with a low priority.

In delay-sensitive applications, such as VoIP or video, Strict Priority lets data to be sent immediately.

### Weighted Fair Queuing description

With Weighted Fair Queuing, also called Weighted Round Robin (WRR), you assign a minimum or reserved bandwidth to each traffic class. This helps ensure that data packets with a lower priority are also sent although the network is very busy.

The reserved values range from 0% through 100% of the available bandwidth, in steps of 1%.
- A reservation of 0 is equivalent to a "no bandwidth" setting.
- The sum of the individual bandwidths can be up to 100%.

When you assign Weighted Fair Queuing to every traffic class, the entire bandwidth of the corresponding port is available to you.

### Combining Strict Priority and Weighted Fair Queuing

When combining Weighted Fair Queuing with Strict Priority, verify that the highest traffic class of Weighted Fair Queuing is lower than the lowest traffic class of Strict Priority.

If you combine Weighted Fair Queuing with Strict Priority, then a high Strict Priority network load can significantly reduce the bandwidth available for Weighted Fair Queuing.

## 10.4.6 Queue management

### Queue Shaping

Queue Shaping throttles the rate at which queues transmit packets. For example, using Queue Shaping, you rate-limit a higher strict-priority queue so that it lets a lower strict-priority queue to send packets even though higher priority packets are still available for transmission. The device lets you setup Queue Shaping for any queue. You specify Queue Shaping as the maximum rate at which traffic passes through a queue by assigning a percentage of the available bandwidth.

### Defining settings for queue management

Perform the following steps:

- ☐ Open the *Switching > QoS/Priority > Queue Management* dialog.

The total assigned bandwidth in the *Min. bandwidth [%]* column is 100%.

- ☐ To activate Weighted Fair Queuing for *Traffic class* = `0`, proceed as follows:
  - Unmark the checkbox in the *Strict priority* column.
  - In the *Min. bandwidth [%]* column, specify the value `5`.
- ☐ To activate Weighted Fair Queuing for *Traffic class* = `1`, proceed as follows:
  - Unmark the checkbox in the *Strict priority* column.
  - In the *Min. bandwidth [%]* column, specify the value `20`.
- ☐ To activate Weighted Fair Queuing for *Traffic class* = `2`, proceed as follows:
  - Unmark the checkbox in the *Strict priority* column.
  - In the *Min. bandwidth [%]* column, specify the value `30`.
- ☐ To activate Weighted Fair Queuing for *Traffic class* = `3`, proceed as follows:
  - Unmark the checkbox in the *Strict priority* column.
  - In the *Min. bandwidth [%]* column, specify the value `20`.
- ☐ To activate Weighted Fair Queuing and Queue Shaping for *Traffic class* = `4`, proceed as follows:
  - Unmark the checkbox in the *Strict priority* column.
  - In the *Min. bandwidth [%]* column, specify the value `10`.
  - In the *Max. bandwidth [%]* column, specify the value `10`.

  When using a Weighted Fair Queuing and Queue Shaping combination for a specific traffic class, specify a higher value in the *Max. bandwidth [%]* column than the value specified in the *Min. bandwidth [%]* column.
- ☐ To activate Weighted Fair Queuing for *Traffic class* = `5`, proceed as follows:
  - Unmark the checkbox in the *Strict priority* column.
  - In the *Min. bandwidth [%]* column, specify the value `5`.
- ☐ To activate Weighted Fair Queuing for *Traffic class* = `6`, proceed as follows:
  - Unmark the checkbox in the *Strict priority* column.
  - In the *Min. bandwidth [%]* column, specify the value `10`.
- ☐ To activate Strict Priority and Queue Shaping for *Traffic class* = `7`, proceed as follows:
  - Mark the checkbox in the *Strict priority* column.
  - In the *Max. bandwidth [%]* column, specify the value `10`.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

```
enable                                  Change to the Privileged EXEC mode.
configure                               Change to the Configuration mode.
cos-queue weighted 0                    Enabling Weighted Fair Queuing for traffic class 0.
cos-queue min-bandwidth: 0 5            Assigning a weight of 5 % to traffic class 0.
cos-queue weighted 1                    Enabling Weighted Fair Queuing for traffic class 1.
cos-queue min-bandwidth: 1 20           Assigning a weight of 20 % to traffic class 1.
cos-queue weighted 2                    Enabling Weighted Fair Queuing for traffic class 2.
cos-queue min-bandwidth: 2 30           Assigning a weight of 30 % to traffic class 2.
cos-queue weighted 3                    Enabling Weighted Fair Queuing for traffic class 3.
cos-queue min-bandwidth: 3 20           Assigning a weight of 20 % to traffic class 3.
show cos-queue
Queue Id  Min. bandwidth  Max. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         0               0               strict
5         0               0               strict
6         0               0               strict
7         0               0               strict
```

### Combining Weighted Fair Queuing and Queue Shaping

Perform the following steps:

```
enable                                  Change to the Privileged EXEC mode.
configure                               Change to the Configuration mode.
cos-queue weighted 4                    Enabling Weighted Fair Queuing for traffic class 4.
cos-queue min-bandwidth: 4 10           Assigning a weight of 10 % to traffic class 4.
cos-queue max-bandwidth: 4 10           Assigning a weight of 10 % to traffic class 4.
cos-queue weighted 5                    Enabling Weighted Fair Queuing for traffic class 5.
cos-queue min-bandwidth: 5 5            Assigning a weight of 5 % to traffic class 5.
cos-queue weighted 6                    Enabling Weighted Fair Queuing for traffic class 6.
cos-queue min-bandwidth: 6 10           Assigning a weight of 10 % to traffic class 6.
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               0               strict
```

### Setting up Queue Shaping

Perform the following steps:

```
enable                                  Change to the Privileged EXEC mode.
configure                               Change to the Configuration mode.
cos-queue max-bandwidth: 7 10           Assigning a weight of 10 % to traffic class 7.
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               10              strict
```

## 10.4.7 Management prioritization

In order for you to constantly have access to the device management, although there is a high network load, the device lets you prioritize management packets.

When prioritizing management packets, the device sends the management packets with priority information.

- On Layer 2, the device modifies the VLAN priority in the VLAN tag.
  The prerequisite for this function is that the corresponding ports are set to allow sending packets with a VLAN tag.
- On Layer 3, the device modifies the IP-DSCP value.

## 10.4.8 Setting prioritization

### Assigning the port priority

Perform the following steps:

- ☐ Open the *Switching > QoS/Priority > Port Configuration* dialog.
- ☐ 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.
- ☐ In the *Trust mode* column, you specify the criteria the device uses to assign a traffic class to data packets received.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `vlan priority 3` | Assign interface `1/1` the port priority `3`. |
| `exit` | 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `classofservice dot1p-mapping 0 2` | Assigning a VLAN priority of `0` to traffic class `2`. |
| `classofservice dot1p-mapping 1 2` | Assigning a VLAN priority of `1` to traffic class `2`. |
| `exit` | Change to the Privileged EXEC mode. |
| `show classofservice dot1p-mapping` | Display the assignment. |

### Assign port priority to received data packets

Perform the following steps:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `classofservice trust untrusted` | Assigning the `untrusted` mode to the interface. |
| `classofservice dot1p-mapping 0 2` | Assigning a VLAN priority of `0` to traffic class `2`. |
| `classofservice dot1p-mapping 1 2` | Assigning a VLAN priority of `1` to traffic class `2`. |
| `vlan priority 1` | Specifying the value `1` for the port priority. |
| `exit` | Change to the Configuration mode. |

```
exit
```
Change to the Privileged EXEC mode.

```
show classofservice trust
```
Displaying the Trust mode of the ports/interfaces.

```
 Interface Trust Mode
 --------- -------------
 1/1       untrusted
 1/2       dot1p
 1/3       dot1p
 1/4       dot1p
 1/5       dot1p
 1/6       dot1p
 1/7       dot1p
```

### Assigning DSCP to a traffic class

Perform the following steps:

- ☐ Open the *Switching > QoS/Priority > IP DSCP Mapping* dialog.
- ☐ Specify the desired value in the *Traffic class* column.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

```
enable
```
Change to the Privileged EXEC mode.

```
configure
```
Change to the Configuration mode.

```
classofservice  ip-dscp-mapping cs1 1
```
Assigning the DSCP value `CS1` to traffic class `1`.

```
show classofservice  ip-dscp-mapping
```
Displaying the IP DSCP assignments

```
    IP DSCP       Traffic Class
-------------     -------------
  be                   2
  1                    2
  .                    .
  .                    .
  (cs1)                1
  .                    .
```

### Assign the DSCP priority to received IP data packets

Perform the following steps:

```
enable
```
Change to the Privileged EXEC mode.

```
configure
```
Change to the Configuration mode.

```
interface 1/1
```
Change to the interface configuration mode of interface `1/1`.

```
classofservice trust ip-dscp
```
Assigning the `trust ip-dscp` mode globally.

```
exit
```
Change to the Configuration mode.

```
show classofservice trust
```
Displaying the Trust mode of the ports/interfaces.

```
 Interface     Trust Mode
 ----------    -------------
 1/1           ip-dscp
 1/2           dot1p
 1/3           dot1p
 .             .
 .             .
 1/5           dot1p
 .             .
```

### Configuring traffic shaping on a port

Perform the following steps:

```
enable
```
Change to the Privileged EXEC mode.

```
configure
```
Change to the Configuration mode.

```
interface 1/2
```
Change to the interface configuration mode of interface `1/2`.

```
traffic-shape bw 50
```
Limiting the maximum bandwidth of the port `1/2` to 50%.

```
exit
```
Change to the Configuration mode.

```
exit
```
Change to the Privileged EXEC mode.

```
show traffic-shape
```
Display the Traffic Shaping configuration.

```
Interface  Shaping rate
---------  ------------
1/1        0  %
1/2        50 %
1/3        0  %
1/4        0  %
```

### Configuring Layer 2 management priority

Perform the following steps:

- ☐ Open the *Switching > QoS/Priority > Global* dialog.
- ☐ In the *VLAN priority for management packets* field, specify the VLAN priority with which the device sends management data packets.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

```
enable
```
Change to the Privileged EXEC mode.

```
network management priority dot1p 7
```
Assigning the VLAN priority of 7 to management packets. The device sends management packets with the highest priority.

```
show network parms
```
Displaying the priority of the VLAN in which the device management is located.

```
IPv4 Network
------------
...
Management VLAN priority.....................7
...
```

### Configuring Layer 3 management priority

Perform the following steps:

- ☐ Open the *Switching > QoS/Priority > Global* dialog.
- ☐ In the *IP DSCP value for management packets* field, specify the DSCP value with which the device sends management data packets.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

```
enable
```
Change to the Privileged EXEC mode.

```
network management priority ip-dscp 56
```
Assigning the DSCP value of 56 to management packets. The device sends management packets with the highest priority.

```
show network parms
```
Displaying the priority of the VLAN in which the device management is located.

```
IPv4 Network
------------
...
Management IP-DSCP value....................56
```

# 10.5 Differentiated services

RFC 2474 defines the “Differentiated Services” field in the IP header. This field is also called “DiffServ Codepoint” or DSCP. The DSCP field is used for classification of packets into different quality classes.

The DSCP field replaces the ToS field. The first 3 bits of the DSCP field are used to divide the packets into classes. The next 3 bits are used to further subdivide the classes on the basis of different criteria. This results in up to 64 different service classes.

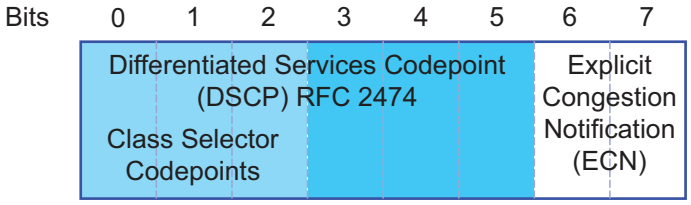



*Figure 26: Differentiated Services field in the IP header*

The different DSCP values get the device to employ a different forwarding behavior, what is known as Per Hop Behavior (PHB). The following PHB classes are defined:

- Class Selector (CS0–CS7)
  For backward compatibility, the Class Selector PHB assigns the 7 possible IP precedence values from the previous ToS field to specific DSCP values.
- Expedited Forwarding (EF)
  For applications with high priority. The Expedited Forwarding PHB reduces delays (latency), jitter, and packet loss (RFC 2598).
- Assured Forwarding (AF)
  The Assured Forwarding PHB provides a differentiated schema for handling different data traffic (RFC 2597).
- Default Forwarding/Best Effort
  This PHB stands for the dispensation with a specific prioritization.

*Table 20: Assigning the IP precedence values to the DSCP value*

| ToS Meaning | Precedence Value | Assigned DSCP |
|---|---|---|
| Network Control | 111 | CS7 (111000) |
| Internetwork Control | 110 | CS6 (110000) |
| Critical | 101 | CS5 (101000) |
| Flash Override | 100 | CS4 (100000) |
| Flash | 011 | CS3 (011000) |
| Immediate | 010 | CS2 (010000) |
| Priority | 001 | CS1 (001000) |
| Routine | 000 | CS0 (000000) |

### 10.5.1 DiffServ example

Configure the device to drop packets received on port `1/1` with the source IP address `10.20.10.11`, the TCP protocol and the source port `80` using the following steps.

Perform the following steps:

☐ Step 1: Create a class.

- ☐ Open the *Switching* > *QoS/Priority* > *DiffServ* > *Class* dialog.
- ☐ Create a class:
  - ▶ Click the button.
    The dialog displays the *Create* window.
  - ▶ In the *Class name* field, enter the `class1` item.
    After the `class1` item is created, you can select it in the *Class name* drop-down list.
  - ▶ In the *Type* drop-down list, select the *protocol* item.
  - ▶ In the *Protocol number* field, enter the value `6`.
    Specify a value according to the „Assigned Internet Protocol Numbers“ defined by the IANA.
    Use this link to find a list of the protocol numbers:
    http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml
  - ▶ Click the *Ok* button.
- ☐ Add the source IP address and mask to the class:
  - ▶ Click the button.
    The dialog displays the *Create* window.
  - ▶ In the *Class name* drop-down list, select the `class1` item.
  - ▶ In the *Type* drop-down list, select the *srcip* item.
  - ▶ In the *Source IP address* field, enter the value `10.20.10.11`.
  - ▶ Click the *Ok* button.
- ☐ Add the source port to the class.
  - ▶ Click the button.
    The dialog displays the *Create* window.
  - ▶ In the *Class name* drop-down list, select the `class1` item.
  - ▶ In the *Type* drop-down list, select the *srcl4port* item.
  - ▶ In the *Source IP address* field, enter the value `80`.
  - ▶ Click the *Ok* button.
- ☐ Save the changes temporarily. To do this, click the button.

☐ Step 2: Create a policy.

- ☐ Open the *Switching* > *QoS/Priority* > *DiffServ* > *Policy* dialog.
- ☐ Create a policy:
  - ▶ Click the button.
    The dialog displays the *Create* window.
  - ▶ In the *Policy name* field, enter the `policy1` item.
  - ▶ In the *Direction* drop-down list, select the *in* item.
  - ▶ In the *Class name* field, select the `class1` item.
  - ▶ In the *Type* field, select the *drop* item.
  - ▶ Click the *Ok* button.
- ☐ Save the changes temporarily. To do this, click the button.

☐ Step 3: Assign the policy to a port.

- ☐ Open the *Switching* > *QoS/Priority* > *DiffServ* > *Assignment* dialog.
- ☐ Assign the policy to a port:
  - ▶ Click the button.
    The dialog displays the *Create* window.
  - ▶ In the *Port* drop-down list, select port `1/1`.
  - ▶ In the *Direction* drop-down list, select the *In* item.
  - ▶ In the *Policy* drop-down list, select the `policy1` item.
  - ▶ Click the *Ok* button.

**Note:** You cannot apply IP ACL rules and DiffServ rules together in the same direction on a port.

- ☐ Save the changes temporarily. To do this, click the button.

☐ Step 4: Enable the function globally.

- ☐ Open the *Switching* > *QoS/Priority* > *DiffServ* > *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.

When the link on the port is up, the value is `up`, in the *Status* column.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `class-map match-all class1` | Creating a class named `class1`. |
| `class-map name class1 match protocol tcp` | Adding the `tcp` protocol as a match condition to the class. |
| `class-map name class1 match srcip 10.20.10.11 255.255.255.0` | Adding the source IP address `10.20.10.11` as a match condition to the class. |
| `class-map name class1 match srcl4port http` | Adding the value `http` (TCP Port 80) as a match condition to the class. |
| `policy-map create policy1 in` | Creating a policy named `policy1` for incoming data packets (`in`). |
| `policy-map name policy1 class add class1` | Assigning the class with the name `class1` to the policy with the name `policy1`. |
| `policy-map name policy1 class name class1 drop` | Drop data packets. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `service-policy in policy1` | Assigning the policy with the name `policy1` to the interface `1/1`. |
| `exit` | Change to the Configuration mode. |
| `diffserv enable` | Enable the *DiffServ* function globally. |

# 10.6 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 transmition speed. This results in the receiving port no longer being overwhelmed and is able to process the incoming traffic.

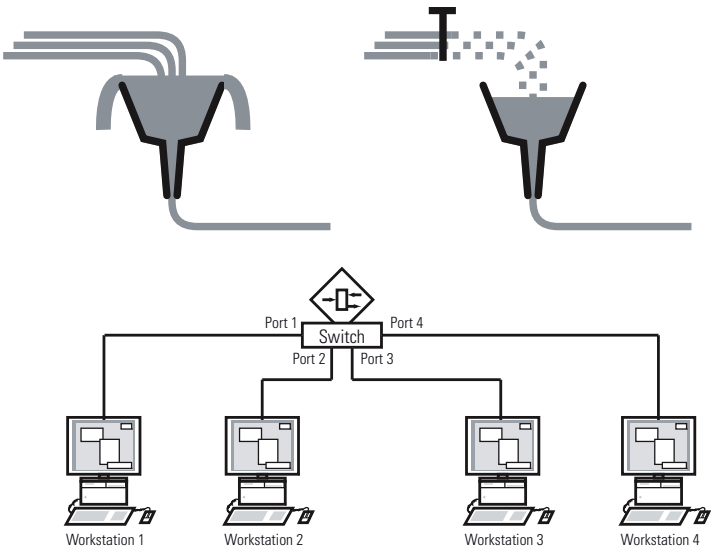



*Figure 27: Example of flow control*

## 10.6.1 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.

### 10.6.2 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.

**Note:** When you are using a redundancy function, 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.

# 11 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.

## 11.1 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.

### 11.1.1 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.

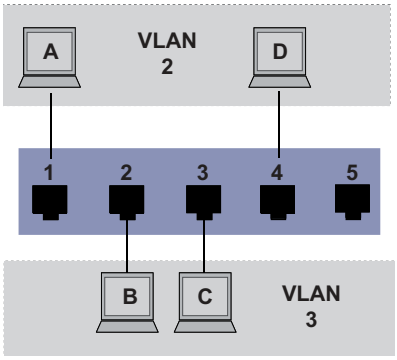



*Figure 28: Example of a simple port-based VLAN*

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 21: Ingress table*

| Terminal | Port | Port VLAN identifier (PVID) |
|---|---|---|
| A | 1 | 2 |
| B | 2 | 3 |
| C | 3 | 3 |
| D | 4 | 2 |
| | 5 | 1 |

*Table 22: Egress table*

| VLAN ID | Port | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| 1 | | | | | U |
| 2 | U | | | U | |
| 3 | | U | U | | |

Perform the following steps:

☐ Setting up the VLAN

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Click the 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` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 2` | Creates a new VLAN with the VLAN ID `2`. |
| `name 2 VLAN2` | Assign the name `2` to the VLAN `VLAN2`. |
| `vlan add 3` | Creates a new VLAN with the VLAN ID `3`. |
| `name 3 VLAN3` | Assign the name `3` to the VLAN `VLAN3`. |
| `name 1 VLAN1` | Assign the name `1` to the VLAN `VLAN1`. |
| `exit` | Change to the Privileged EXEC mode. |
| `show vlan brief` | Display the current VLAN configuration. |

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 512
Number of currently configured VLANs............ 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                           default    0 days, 00:00:05
2       VLAN2                           static     0 days, 02:44:29
3       VLAN3                           static     0 days, 02:52:26
```

☐ 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.
    Changes using the *GVRP* function are disabled.
  - `-` = The port is not a member of this VLAN.
    Changes using the *GVRP* function are allowed.

  Because end devices usually interpret untagged data packets, you specify the value `U`.
- ☐ 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:
  `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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `vlan participation include 2` | The port `1/1` becomes a member of the VLAN `2` and transmits the data packets without a VLAN tag. |
| `vlan pvid 2` | Assign the port VLAN ID `1/1` to port `2`. |
| `exit` | Change to the Configuration mode. |
| `interface 1/2` | Change to the interface configuration mode of interface `1/2`. |
| `vlan participation include 3` | The port `1/2` becomes a member of the VLAN `3` and transmits the data packets without a VLAN tag. |
| `vlan pvid 3` | Assign the port VLAN ID `1/2` to port `3`. |
| `exit` | Change to the Configuration mode. |
| `interface 1/3` | Change to the interface configuration mode of interface `1/3`. |
| `vlan participation include 3` | The port `1/3` becomes a member of the VLAN `3` and transmits the data packets without a VLAN tag. |
| `vlan pvid 3` | Assign the port VLAN ID `1/3` to port `3`. |
| `exit` | Change to the Configuration mode. |
| `interface 1/4` | Change to the interface configuration mode of interface `1/4`. |
| `vlan participation include 2` | The port `1/4` becomes a member of the VLAN `2` and transmits the data packets without a VLAN tag. |
| `vlan pvid 2` | Assign the port VLAN ID `1/4` to port `2`. |
| `exit` | Change to the Configuration mode. |
| `exit` | Change to the Privileged EXEC mode. |
| `show vlan id 3` | Displays details for VLAN `3`. |

```
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1            -      Autodetect   Tagged
1/2         Include   Include      Untagged
1/3         Include   Include      Untagged
1/4            -      Autodetect   Tagged
1/5            -      Autodetect   Tagged
```

### 11.1.2 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).

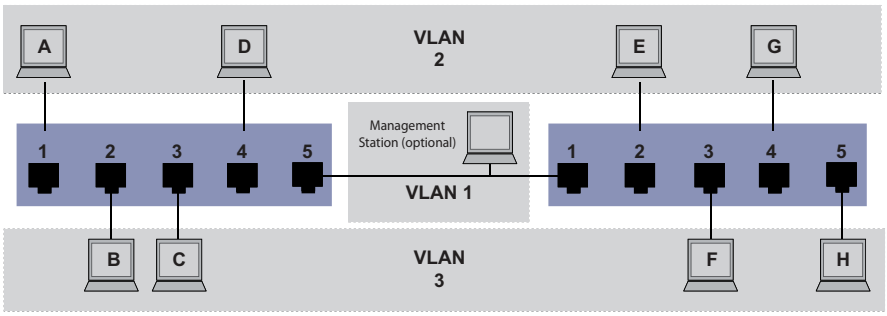



*Figure 29: Example of a more complex VLAN configuration*

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 23: Ingress table for device on left*

| Terminal | Port | Port VLAN identifier (PVID) |
|---|---|---|
| A | 1 | 2 |
| B | 2 | 3 |
| C | 3 | 3 |
| D | 4 | 2 |
| Uplink | 5 | 1 |

*Table 24: Ingress table for device on right*

| Terminal | Port | Port VLAN identifier (PVID) |
|---|---|---|
| Uplink | 1 | 1 |
| E | 2 | 2 |
| F | 3 | 3 |
| G | 4 | 2 |
| H | 5 | 3 |

*Table 25: Egress table for device on left*

| VLAN ID | Port | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| 1 | | | | | U |
| 2 | U | | | U | T |
| 3 | | U | U | | T |

*Table 26: Egress table for device on right*

| VLAN ID | Port | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| 1 | U | | | | |
| 2 | T | U | | U | |
| 3 | T | | U | | U |

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 button.
The dialog displays the *Create* window.

☐ In the *VLAN ID* field, specify the VLAN ID, for example `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` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 2` | Creates a new VLAN with the VLAN ID `2`. |
| `name 2 VLAN2` | Assign the name `2` to the VLAN `VLAN2`. |
| `vlan add 3` | Creates a new VLAN with the VLAN ID `3`. |
| `name 3 VLAN3` | Assign the name `3` to the VLAN `VLAN3`. |
| `name 1 VLAN1` | Assign the name `1` to the VLAN `VLAN1`. |
| `exit` | Change to the Privileged EXEC mode. |
| `show vlan brief` | Display the current VLAN configuration. |

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 512
Number of currently configured VLANs........... 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                           default    0 days, 00:00:05
2       VLAN2                           static     0 days, 02:44:29
3       VLAN3                           static     0 days, 02:52:26
```

☐ 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.
    Changes using the *GVRP* function are disabled.
  - `-` = The port is not a member of this VLAN.
    Changes using the *GVRP* function are disabled.

  Because end devicees 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `vlan participation include 1` | The port `1/1` becomes a member of the VLAN `1` and transmits the data packets without a VLAN tag. |
| `vlan participation include 2` | The port `1/1` becomes a member of the VLAN `2` and transmits the data packets without a VLAN tag. |
| `vlan tagging 2 enable` | The port `1/1` becomes a member of the VLAN `2` and transmits the data packets with a VLAN tag. |
| `vlan participation include 3` | The port `1/1` becomes a member of the VLAN `3` and transmits the data packets without a VLAN tag. |
| `vlan tagging 3 enable` | The port `1/1` becomes a member of the VLAN `3` and transmits the data packets with a VLAN tag. |
| `vlan pvid 1` | Assigning the Port VLAN ID `1` to port `1/1`. |
| `vlan ingressfilter` | Activate ingress filtering on port `1/1`. |
| `vlan acceptframe vlanonly` | Port `1/1` only forwards packets with a VLAN tag. |
| `exit` | Change to the Configuration mode. |
| `interface 1/2` | Change to the interface configuration mode of interface `1/2`. |
| `vlan participation include 2` | The port `1/2` becomes a member of the VLAN `2` and transmits the data packets without a VLAN tag. |
| `vlan pvid 2` | Assigning the Port VLAN ID `2` to port `1/2`. |
| `exit` | Change to the Configuration mode. |
| `interface 1/3` | Change to the interface configuration mode of interface `1/3`. |
| `vlan participation include 3` | The port `1/3` becomes a member of the VLAN `3` and transmits the data packets without a VLAN tag. |
| `vlan pvid 3` | Assigning the Port VLAN ID `3` to port `1/3`. |
| `exit` | Change to the Configuration mode. |
| `interface 1/4` | Change to the interface configuration mode of interface `1/4`. |
| `vlan participation include 2` | The port `1/4` becomes a member of the VLAN `2` and transmits the data packets without a VLAN tag. |
| `vlan pvid 2` | Assigning the Port VLAN ID `2` to port `1/4`. |
| `exit` | Change to the Configuration mode. |
| `interface 1/5` | Change to the interface configuration mode of interface `1/5`. |
| `vlan participation include 3` | The port `1/5` becomes a member of the VLAN `3` and transmits the data packets without a VLAN tag. |
| `vlan pvid 3` | Assigning the Port VLAN ID `3` to port `1/5`. |
| `exit` | Change to the Configuration mode. |

```
exit
```

Change to the Privileged EXEC mode.

```
show vlan id 3
```

Displays details for VLAN 3.

```
VLAN ID.....................3
VLAN Name...................VLAN3
VLAN Type...................Static
VLAN Creation Time...........0 days, 00:07:47 (System Uptime)
VLAN Routing................disabled

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Include   Include      Tagged
1/2         -         Autodetect   Untagged
1/3         Include   Include      Untagged
1/4         -         Autodetect   Untagged
1/5         Include   Include      Untagged
```

# 11.2 Guest VLAN / Unauthenticated VLAN

A Guest VLAN lets a device provide port-based Network Access Control (IEEE 802.1x) to non-802.1x capable supplicants. This feature provides a mechanism to allow guests to access external networks only. If you connect non-802.1x capable supplicants to an active unauthorized 802.1x port, then the supplicants send no responds to 802.1x requests. Since the supplicants send no responses, the port remains in the unauthorized state. The supplicants have no access to external networks.

The Guest VLAN supplicant is a per-port basis configuration. When you configure a port as a Guest VLAN and connect non-802.1x capable supplicants to this port, the device assigns the supplicants to the Guest VLAN. Adding supplicants to a Guest VLAN causes the port to change to the authorized state allowing the supplicants to access to external networks.

An Unauthenticated VLAN lets the device provide service to 802.1x capable supplicants which authenticate incorrectly. This function lets the unauthorized supplicants have access to limited services. If you configure an Unauthenticated VLAN on a port with 802.1x port authentication and the global operation enabled, then the device places the port in an Unauthenticated VLAN. When a 802.1x capable supplicant incorrectly authenticates on the port, the device adds the supplicant to the Unauthenticated VLAN. If you also configure a Guest VLAN on the port, then non-802.1x capable supplicants use the Guest VLAN.

If the port has an Unauthenticated VLAN assigned, then the reauthentication timer counts down. When the time specified in the *Reauthentication period [s]* column expires and supplicants are present on the port, the Unauthenticated VLAN reauthenticates. When no supplicants are present, the device places the port in the configured Guest VLAN.

The following example explains how to create a Guest VLAN. Create an Unauthorized VLAN in the same manner.

Perform the following steps:

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *VLAN ID* field, specify the value `10`.
- ☐ Click the *Ok* button.
- ☐ For the VLAN, specify the name `Guest`:
  Double-click in the *Name* column and specify the name.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *VLAN ID* field, specify the value `20`.
- ☐ Click the *Ok* button.
- ☐ For the VLAN, specify the name `Not authorized`:
  Double-click in the *Name* column and specify the name.
- ☐ Open the *Network Security > 802.1X Port Authentication > 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.

- ☐ Open the *Network Security > 802.1X Port Authentication > Port Configuration* dialog.
- ☐ Specify the following settings for port `1/4`:
  - The value `auto` in the *Port control* column
  - The value `10` in the *Guest VLAN ID* column
  - The value `20` in the *Unauthenticated VLAN ID* column
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 10` | Creates VLAN `10`. |
| `vlan add 20` | Creates VLAN `20`. |
| `name 10 Guest` | Renames VLAN `10` to `Guest`. |
| `name 20 Unauth` | Renames VLAN `20` to `Unauth`. |
| `exit` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `dot1x system-auth-control enable` | Enable the *802.1X Port Authentication* function globally. |
| `dot1x port-control auto` | Enables port control on port `1/4`. |
| `interface 1/4` | Change to the interface configuration mode of interface `1/4`. |
| `dot1x guest-vlan 10` | Assign the guest vlan to port `1/4`. |
| `dot1x unauthenticated-vlan 20` | Assign the unauthorized vlan to port `1/4`. |
| `exit` | Change to the Configuration mode. |

## 11.3 RADIUS VLAN assignment

The RADIUS VLAN assignment feature makes it possible for a RADIUS VLAN ID attribute to be associated with an authenticated client. When a client authenticates successfully, and the RADIUS server sends a VLAN attribute, the device associates the client with the RADIUS assigned VLAN. As a result, the device adds the physical port as an member to the appropriate VLAN and sets the port VLAN ID (PVID) with the given value. The port transmits the data packets without a VLAN tag.

# 11.4 Creating a Voice VLAN

Use the Voice VLAN feature to separate voice and data traffic on a port, by VLAN and/or priority. A primary benefit of using Voice VLAN is to safeguard the sound quality of an IP phone in cases where there is high data traffic on the port.

The device uses the source MAC address to identify and prioritize the voice data flow. Using a MAC address to identify devices helps prevent a rogue client from connecting to the same port causing the voice traffic to deteriorate.

Another benefit of the Voice VLAN feature is that a VoIP phone obtains a VLAN ID or priority information using LLDP-MED. As a result, the VoIP phone sends voice data as tagged, priority tagged or untagged. This depends on the Voice VLAN Interface configuration.

The following Voice VLAN interface modes are possible. The first 3 methods segregate and prioritize voice and data traffic. Traffic segregation results in an increased voice traffic quality during high traffic periods.

- Configuring the port to using the `vlan` mode lets the device tag the voice data coming from a VoIP phone with the user-defined voice VLAN ID. The device assigns regular data to the default port VLAN ID.
- Configuring the port to use the `dot1p-priority` mode lets the device tag the data coming from a VoIP phone with VLAN 0 and the user-defined priority. The device assigns the default priority of the port to regular data.
- Configure both the voice VLAN ID and the priority using the `vlan/dot1p-priority` mode. In this mode the VoIP phone sends voice data with the user-defined voice VLAN ID and priority information. The device assigns the default PVID and priority of the port to regular data.
- When configured as `untagged`, the phone sends untagged packets.
- When configured as `none`, the phone uses its own configuration to send voice traffic.

# 11.5 MAC based VLANs

Use the MAC-based VLAN to forward traffic based on the source MAC address associated with the VLAN. A MAC-based VLAN defines the filtering criteria for untagged or priority tagged packets.

You specify a MAC-based VLAN filter by assigning a specific source address to a MAC-based VLAN. The device forwards untagged packets received with the source MAC address on the MAC-based VLAN ID. The other untagged packets are subject to normal VLAN classification rules.

# 11.6 IP subnet based VLANs

In an IP subnet-based VLAN, the device forwards traffic based on the source IP address and subnet mask associated with the VLAN. User-defined filters determine if a packet belongs to a particular VLAN.

Use the IP subnet-based VLAN to specify the filtering criteria for untagged or priority tagged packets. For example, assign a specific subnet address to an IP subnet-based VLAN. When the device receives untagged packets from the subnet address, it forwards them to the IP subnet-based VLAN. Other untagged packets are subject to normal VLAN classification rules.

To configure an IP subnet-based VLAN, specify an IP address, a subnet mask and the associated VLAN ID. In case of multiple matching entries, the device associates the VLAN ID to the entry with the longer prefix first.

# 11.7 Protocol-based VLAN

In a protocol-based VLAN, the device bridges traffic through specified ports based on the protocol associated with the VLAN. User-defined packet filters determine if a packet belongs to a particular VLAN.

Configure protocol-based VLANs using the value in the *Ethertype* column as the filtering criteria for untagged packets. For example, assign a specific protocol to a protocol-based VLAN. When the device receives untagged packets with the protocol, it forwards them to the protocol-based VLAN. The device assigns the other untagged packets to the port VLAN ID.

# 11.8 VLAN unaware mode

The *VLAN unaware mode* defines the operation of the device in a LAN segmented by VLANs. The device accepts packets and processes them according to its inbound rules. Based on the IEEE 802.1Q specifications, the function governs how the device processes VLAN tagged packets.

Use the VLAN aware mode to apply the user-defined VLAN topology configured by the network administrator. When the device forwards packets, it uses VLAN tagging in combination with the IP or Ethernet address. The device processes inbound and outbound packets according to the defined rules. VLAN configuration is a manual process.

Use the VLAN unaware mode to forward traffic as received, without any modification. When the device receives packets as tagged, it transmits tagged packets. When the device receives packets as untagged, it transmits untagged packets. Regardless of VLAN assignment mechanisms, the device assigns packets to VLAN ID 1 and to a Multicast group, indicating that the packet flood domain is according to the VLAN.

# 12 Redundancy

## 12.1 Network Topology vs. Redundancy Protocols

When using Ethernet, a significant prerequisite is that data packets follow a single (unique) path from the sender to the receiver. The following network topologies support this prerequisite:

- Line topology
- Star topology
- Tree topology

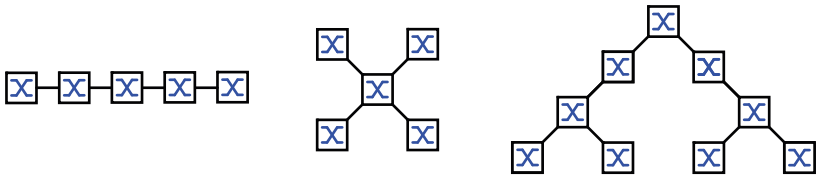


*Figure 30: Network with line, star and tree topologies*

To maintain communication in case a connection fails, install additional physical connections between the network nodes. Redundancy protocols help ensure that the additional connections remain switched off while the original connection is still working. When the connection fails, the redundancy protocol generates a new path from the sender to the receiver via the alternative connection.

To introduce redundancy onto Layer 2 of a network, you first define which network topology you require. Depending on the network topology selected, you then choose from the redundancy protocols that can be used with this network topology.

### 12.1.1 Network topologies

#### Meshed topology

For networks with star or tree topologies, redundancy procedures are only possible in connection with physical loop creation. The result is a meshed topology.

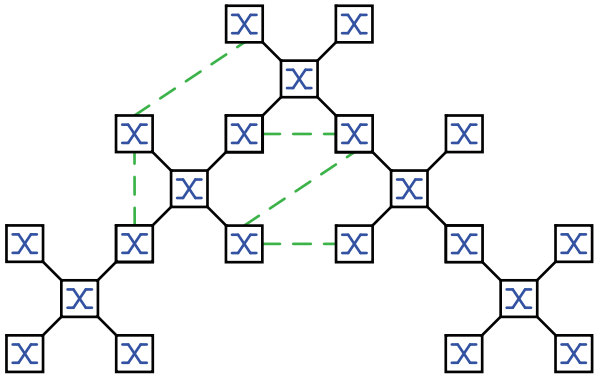


*Figure 31: Meshed topology: Tree topology with physical loops*

For operating in this network topology, the device provides you with the following redundancy protocols:

- Rapid Spanning Tree (RSTP)

#### Ring topology

In networks with a line topology, you can use redundancy procedures by connecting the ends of the line. This creates a ring topology.

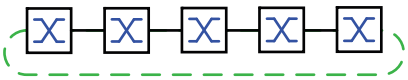


*Figure 32: Ring topology: Line topology with connected ends*

For operating in this network topology, the device provides you with the following redundancy protocols:

- Media Redundancy Protocol (MRP)
- Rapid Spanning Tree (RSTP)

### 12.1.2 Redundancy Protocols

For operating in different network topologies, the device provides you with the following redundancy protocols:

*Table 27: Overview of redundancy protocols*

| Redundancy protocol | Network topology | Comments |
|---|---|---|
| MRP | Ring | The switching time can be selected and is practically independent of the number of devices.<br>An MRP-Ring consists of up to 50 devices that support the MRP protocol according to IEC 62439.<br>When you only use Hirschmann devices, up to 100 devices are possible in the MRP-Ring. |
| Subring | Ring | The *Sub Ring* function enables you to easily couple network segments to existing redundancy rings. |
| Ring/Network coupling | Ring | |
| RCP | Ring | |
| RSTP | Random structure | The switching time depends on the network topology and the number of devices.<br>- typ. < 1 s with RSTP<br>- typ. < 30 s with STP |
| Link Aggregation | Random structure | A Link Aggregation Group is the combining of 2 or more, full-duplex point-to-point links operating at the same rate, on a single switch to increase bandwidth. |

*Table 27: Overview of redundancy protocols (cont.)*

| Redundancy protocol | Network topology | Comments |
|---|---|---|
| Link Backup | Random structure | When the device detects an error on the primary link, the device transfers traffic to the backup link. You typically use Link Backup in service-provider or enterprise networks. |
| HIPER Ring Client | Ring | Extend an existing HIPER ring or replace a device already participating as a client in a HIPER ring. |
| HIPER Ring over LAG | Ring | Link devices together over a Link Aggregation Group (LAG). The ring clients and Ring Manager behave in the same manner as a ring without a LAG instance. |

**Note:** If you are using a redundancy function, then you deactivate the flow control on the participating device 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.

### 12.1.3 Combinations of Redundancies

*Table 28: Overview of redundancy protocols*

| | MRP | RSTP/MSTP | Link Aggreg. | Link Backup | Subring | HIPER Ring |
|---|---|---|---|---|---|---|
| MRP | ▲ | – – – | – – – | – – – | – – – | – – – |
| RSTP/ MSTP 3) | ▲ 1) | ▲ | – – – | – – – | – – – | – – – |
| Link Aggreg. | ▲ 2) | ▲ 2) | ▲ | – – – | – – – | – – – |
| Link Backup | ▲ | ▲ | ▲ | ▲ | – – – | – – – |
| Subring | ▲ | ▲ | ▲ 2) | ▲ | ▲ | – – – |
| HIPER Ring | ▲ | ▲ 1) | ▲ 2) | ▲ | ▲ | ▲ |

▲ Combination applicable

1) A redundant coupling between these network topologies will possibly lead to loops. To redundantly couple these topologies, refer to chapter “FuseNet” on page 213.

2) Combination applicable on the same port

3) In combination with MSTP, the failover times of other redundancy protocols can slightly increase.

# 12.2 Media Redundancy Protocol (MRP)

Since May 2008, the Media Redundancy Protocol (MRP) has been a standardized solution for ring redundancy in the industrial environment.

MRP is compatible with redundant ring coupling, supports VLANs, and is distinguished by very short reconfiguration times.

An MRP-Ring consists of up to 50 devices that support the MRP protocol according to IEC 62439. When you only use Hirschmann devices, up to 100 devices are possible in the MRP-Ring.

When you use the fixed MRP redundant port (Fixed Backup) and the primary ring link fails, the Ring Manager forwards data to the secondary ring link. When the primary link is restored, the secondary link continues to be in use.

## 12.2.1 Network Structure

The concept of ring redundancy lets you construct high-availability ring-shaped network structures.

With the help of the RM (**R**ing**M**anager) function, the two ends of a backbone in a line structure can be closed to a redundant ring. The Ring Manager keeps the redundant line open as long as the line structure is intact. When a segment becomes inoperable, the Ring Manager immediately closes the redundant line, and line structure is intact again.

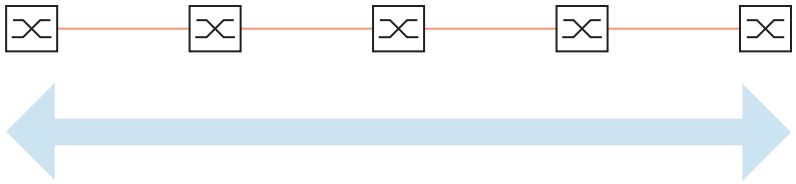


*Figure 33: Line structure*

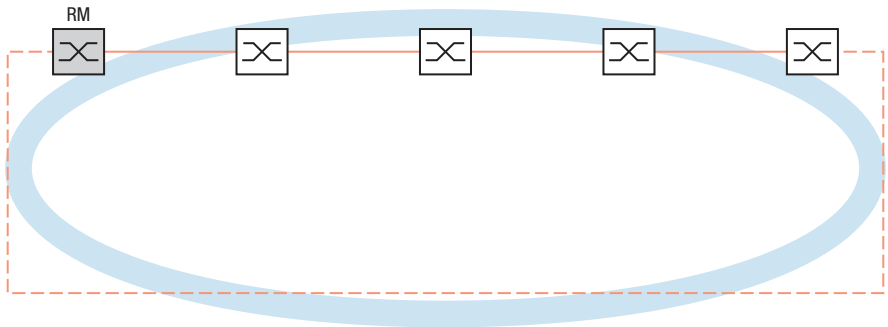



*Figure 34: Redundant ring structure*
*RM = Ring Manager*
*—— main line*
*- - - redundant line*

### 12.2.2 Reconfiguration time

When a line section fails, the Ring Manager changes the MRP-Ring back into a line structure. You define the maximum time for the reconfiguration of the line in the Ring Manager.

Possible values for the maximum delay time:
- `500ms`
- `30ms`

**Note:** If every device in the ring supports the shorter delay time, then you can configure the reconfiguration time with a value less than `500ms`.

Otherwise the devices that only support longer delay times might not be reachable due to overloading. Loops can occur as a result.

### 12.2.3 Advanced mode

For times even shorter than the specified reconfiguration times, the device provides the advanced mode. When the ring participants inform the Ring Manager of interruptions in the ring via link-down notifications, the advanced mode speeds up the link failure recognition.

Hirschmann devices support link-down notifications. Therefore, you generally activate the advanced mode in the Ring Manager.

When you are using devices that do not support link-down notifications, the Ring Manager reconfigures the line in the selected maximum reconfiguration time.

### 12.2.4 Prerequisites for MRP

Before setting up an MRP-Ring, verify that the following conditions are fulfilled:
- All ring participants support MRP.
- The ring participants are connected to each other via the ring ports. Apart from the device's neighbors, no other ring participants are connected to the respective device.
- All ring participants support the configuration time specified in the Ring Manager.
- There is only one Ring Manager in the ring.

If you are using VLANs, then configure every ring port with the following settings:
- ☐ Deactivate ingress filtering - see the *Switching > VLAN > Port* dialog.
- ☐ Define the port VLAN ID (PVID) - see the *Switching > VLAN > Port* dialog.
  - PVID = `1` in cases where the device transmits the MRP data packets untagged (VLAN ID = `0` in *Switching > L2-Redundancy > MRP* dialog)
    By setting the PVID = `1`, the device automatically assigns the received untagged packets to VLAN 1.
  - PVID = `any` in cases where the device transmits the MRP data packets in a VLAN (VLAN ID ≥ `1` in the *Switching > L2-Redundancy > MRP* dialog)
- ☐ Define egress rules - see *Switching > VLAN > Configuration* dialog.
  - `U` (untagged) for the ring ports of VLAN 1 in cases where the device transmits the MRP data packets untagged (VLAN ID = `0` in the *Switching > L2-Redundancy > MRP* dialog, the MRP ring is not assigned to a VLAN).
  - `T` (tagged) for the ring ports of the VLAN which you assign to the MRP ring. Select `T`, in cases where the device transmits the MRP data packets in a VLAN (VLAN ID ≥ `1` in the *Switching > L2-Redundancy > MRP* dialog).

### 12.2.5 Example Configuration

A backbone network contains 3 devices in a line structure. To increase the availability of the network, you convert the line structure to a redundant ring structure. Devices from different manufacturers are used. All devices support MRP. On every device you define ports 1.1 and 1.2 as ring ports.

When the primary ring link fails, the Ring Manager sends data on the secondary ring link. When the primary link is restored, the secondary link reverts back to the backup mode.

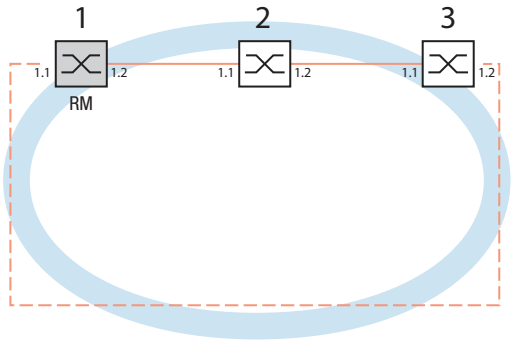



*Figure 35: Example of MRP-Ring*
*RM = Ring Manager*
*—— main line*
*- - - redundant line*

The following example configuration describes the configuration of the Ring Manager device (1). You configure the 2 other devices (2 to 3) in the same way, but without activating the *Ring manager* function. This example does not use a VLAN. You specify the value `30ms` as the ring recovery time. Every device supports the advanced mode of the Ring Manager.

- ☐ Set up the network to meet your demands.
- ☐ Configure every port so that the transmission speed and the duplex settings of the lines correspond to the following table:

*Table 29: Port settings for ring ports*

| Port type | Bit rate | Port on | Automatic configuration | Manual configuration |
|---|---|---|---|---|
| TX | 100 Mbit/s | `marked` | `unmarked` | *`100 Mbit/s FDX`* |
| TX | 1 Gbit/s | `marked` | `marked` | – |
| Optical | 100 Mbit/s | `marked` | `unmarked` | *`100 Mbit/s FDX`* |
| Optical | 1 Gbit/s | `marked` | `marked` | – |
| Optical | 2.5 Gbit/s | `marked` | – | *`2.5 Gbit/s FDX`* |
| Optical | 10 Gbit/s | `marked` | – | *`10 Gbit/s`* |

**Note:** You configure optical ports without support for autonegotiation (automatic configuration) with 100 Mbit/s full duplex (FDX) or 1000 Mbit/s full duplex (FDX).

**Note:** You configure optical ports without support for autonegotiation (automatic configuration) with 100 Mbit/s full duplex (FDX).

**Note:** Configure every device of the MRP-Ring individually. Before you connect the redundant line, verify that you have completed the configuration of every device of the MRP-Ring. You thus help avoid loops during the configuration phase.

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. (Default setting: flow control deactivated globally and activated on every port.)

Disable the *Spanning Tree* function in every device in the network. To do this, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- ☐ Disable the function.
  In the state on delivery, Spanning Tree is enabled in the device.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `no spanning-tree operation` | Switches Spanning Tree off. |
| `show spanning-tree global` | Displays the parameters for checking. |

Enable MRP on every device in the network. To do this, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > MRP* dialog.
- ☐ Specify the desired ring ports.

In the Command Line Interface you first define an additional parameter, the MRP domain ID. Configure every ring participant with the same MRP domain ID. The MRP domain ID is a sequence of 16 number blocks (8-bit values).

When configuring with the Graphical User Interface, the device uses the default value `255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255`.

| | |
|---|---|
| `mrp domain add default-domain` | Creates a new MRP domain with the ID `default-domain`. |
| `mrp domain modify port 1/1 primary` | Specifies port *1/1* as ring port `1`. |
| `mrp domain modify port 1/2 secondary` | Specifies port *1/2* as ring port `2`. |

Enable the *Fixed backup* port. To do this, perform the following steps:

- ☐ Enable the Ring Manager.
  For the other devices in the ring, leave the setting as *Off*.
- ☐ To allow the device to continue sending data on the secondary port after the ring is restored, mark the *Fixed backup* checkbox.

**Note:** When the device reverts back to the primary port, the maximum ring recovery time can be exceeded.

When you unmark the *Fixed backup* checkbox, and the ring is restored, the Ring Manager blocks the secondary port and unblocks the primary port.

```
mrp domain modify port secondary 1/2
fixed-backup enable
```

Activates the *Fixed backup* function on the secondary port. The secondary port continues forwarding data after the ring is restored.

☐ Enable the Ring Manager.
For the other devices in the ring, leave the setting as *Off*.

```
mrp domain modify mode   manager
```

Specifies that the device operates as the *Ring manager*. For the other devices in the ring, leave the default setting.

☐ Select the checkbox in the *Advanced mode* field.

```
mrp domain modify   advanced-mode
enabled
```

Activates the advanced mode.

☐ In the *Ring recovery* field, select the value `30ms`.

```
mrp domain modify   recovery-delay
200ms
```

Specifies the value `30ms` as the max. delay time for the reconfiguration of the ring.

**Note:** If selecting the value `30ms` for the ring recovery does not provide the ring stability necessary to meet the requirements of your network, then select the value `500ms`.

☐ Switch the operation of the MRP-Ring on.
☐ Save the changes temporarily. To do this, click the ☑ button.

```
mrp domain modify operation   enable
```

Activates the MRP-Ring.

When every ring participant is configured, close the line to the ring. To do this, you connect the devices at the ends of the line via their ring ports.

Check the messages from the device. To do this, perform the following steps:

```
show mrp
```

Displays the parameters for checking.

The *Operation* field displays the operating state of the ring port.

Possible values:

- `forwarding`
  The port is enabled, connection exists.
- `blocked`
  The port is blocked, connection exists.
- `disabled`
  The port is disabled.
- `not-connected`
  No connection exists.

The *Information* field displays messages for the redundancy configuration and the possible causes of errors.

When the device is operating as a ring client or a Ring Manager, the following messages are possible:

- *Redundancy available*
  The redundancy is set up. When a component of the ring is down, the redundant line takes over its function.
- *Configuration error: Error on ringport link.*
  Error in the cabling of the ring ports.

When the device is operating as a Ring Manager, the following messages are possible:

- *Configuration error: Packets from another ring manager received.*
  Another device exists in the ring that is operating as the Ring Manager.
  Activate the *Ring manager* function on exactly one device in the ring.
- *Configuration error: Ring link is connected to wrong port.*
  A line in the ring is connected with a different port instead of with a ring port. The device only receives test data packets on one ring port.

When applicable, integrate the MRP ring into a VLAN. To do this, perform the following steps:

- ☐ In the *VLAN ID* field, define the MRP VLAN ID. The MRP VLAN ID determines in which of the configured VLANs the device transmits the MRP packets.
  To set the MRP VLAN ID, first configure the VLANs and the corresponding egress rules in the *Switching > VLAN > Configuration* dialog.
  - If the MRP-Ring is not assigned to a VLAN (like in this example), then leave the VLAN ID as `0`.
    In the *Switching > VLAN > Configuration* dialog, specify the VLAN membership as `U` (untagged) for the ring ports in VLAN `1`.
  - If the MRP-Ring is assigned to a VLAN, then enter a VLAN ID >`0`.
    In the *Switching > VLAN > Configuration* dialog, specify the VLAN membership as `T` (tagged) for the ring ports in the selected VLAN.

`mrp domain modify vlan <0..4042>` Assigns the VLAN ID.

## 12.2.6 MRP over LAG

Hirschmann devices allow you to combine Link Aggregation Groups (LAG) to increase bandwidth with the Media Redundancy Protocol (MRP) providing redundancy. The function lets you increase the bandwidth on individual segments or on the entire network.

The *Link Aggregation* function helps you overcome bandwidth limitations of individual ports. LAG lets you combine 2 or more links in parallel, creating one logical link between 2 devices. The parallel links increase the bandwidth for the data stream between the 2 devices.

An MRP ring consists of up to 50 devices that support the MRP protocol according to IEC 62439. When you use only Hirschmann devices, the protocol lets you configure MRP rings with up to 100 devices.

You use MRP over LAG in the following cases:
- to increase bandwidth only on specific segments of an MRP ring
- to increase bandwidth on the entire MRP ring

### Network Structure

When configuring an MRP ring with LAGs, the Ring Manager (RM) monitors both ends of the backbone for continuity. The RM blocks data on the secondary (redundant) port as long as the backbone is intact. When the RM detects an interruption of the data stream on the ring, it begins forwarding data on the secondary port, which restores backbone continuity.

You use LAG instances in MRP rings to increase bandwidth only, in this case MRP provides the redundancy.

In order for the RM to detect an interruption on the ring, MRP requires a device to block every port in the LAG instance in cases where a port in the instance is down.

### LAG on a single segment of an MRP ring

The device lets you configure a LAG instance on specific segments of an MRP ring.

You use the LAG Single Switch method for devices in the MRP ring. The Single Switch method provides you an inexpensive way to grow your network by using only one device on each side of a segment to provide the physical ports. You group the ports of the device into a LAG instance to provide increased bandwidth on specific segments where needed.

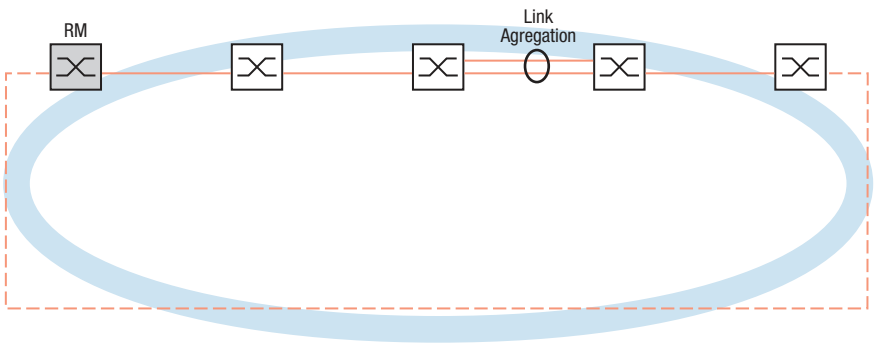



*Figure 36: Link Aggregation over a single link of an MRP ring.*

### LAG on an entire MRP ring

Besides being able to configure a LAG instance on specific segments of an MRP ring, Hirschmann devices also allow you to configure LAG instances on every segment, which increases bandwidth on the entire MRP ring.

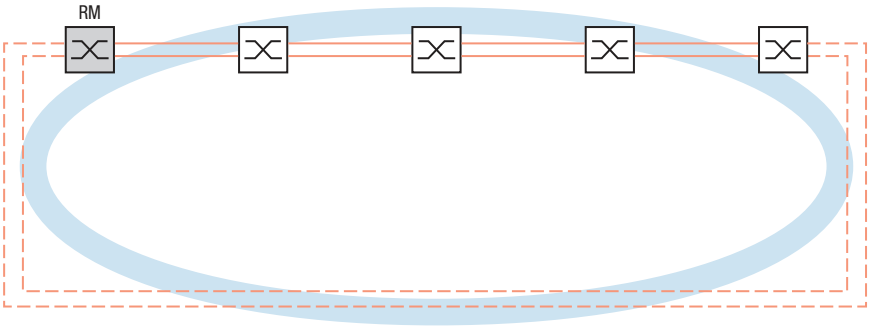



*Figure 37: Link Aggregation over the entire MRP ring.*

### Detecting interruptions on the ring

When configuring the LAG instance, specify the *Active ports (min.)* value to equal the total number of ports used in the LAG instance. When a device detects an interruption on a port in the LAG instance, it blocks data on the other ports of the instance. With every port of an instance blocked, the RM senses that the ring is open and begins forwarding data on the secondary port. This way the RM is able to restore continuity to the devices on the other side of the interrupted segment.

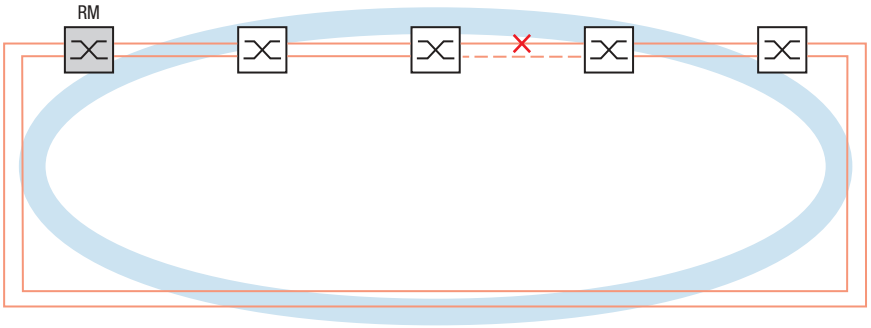



*Figure 38: Interruption of a link in an MRP ring.*

### Example Configuration

In the following example, switch A and switch B link two departments together. The departments produce traffic too high for the individual port bandwidth to handle. You configure a LAG instance for the single segment of the MRP ring, increasing the bandwidth of the segment.

The prerequisite for the example configuration is that you begin with an operational MRP ring.

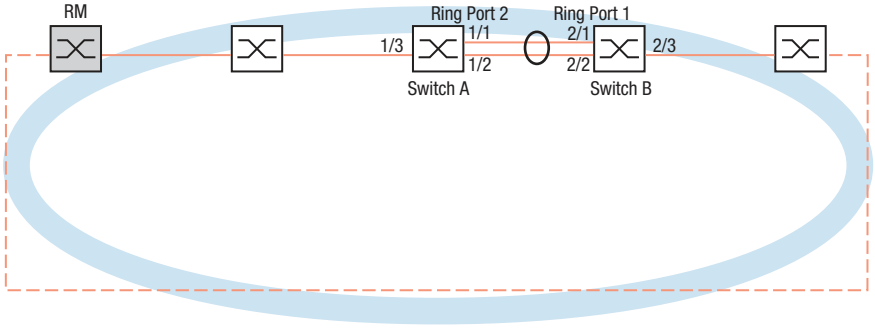



*Figure 39: MRP over LAG Configuration Example*

Configure switch A first. To do this, perform the following steps. Then configure switch B using the same steps, substituting the appropriate port and ring port numbers.

- ☐ Open the *Switching > L2-Redundancy > Link Aggregation* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *Trunk port* drop-down list, select the instance number of the link aggregation group.
- ☐ In the *Port* drop-down list, select port *1/1*.
- ☐ Click the *Ok* button.
- ☐ Repeat the preceding steps and select the port *1/2*.
- ☐ Click the *Ok* button.
- ☐ In the *Active ports (min.)* column enter `2`, which in this case is the total number of ports in the instance. When combining MRP and LAG you specify the total number of ports as the *Active ports (min.)*. When the device detects an interruption on a port, it blocks the other ports in the instance causing the ring to open. The Ring Manager senses that the ring is open, then begins forwarding data on its secondary ring port which restores the connectivity to the other devices in the network.
- ☐ Save the changes temporarily. To do this, click the button.
- ☐ Open the *Switching > L2-Redundancy > MRP* dialog.
- ☐ In the *Ring port 2* frame, select port `lag/1` in the *Port* drop-down list.
- ☐ Save the changes temporarily. To do this, click the button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `link-aggregation add lag/1` | Creates a Link Aggregation Group `lag/1`. |
| `link-aggregation modify lag/1 addport 1/1` | Adds port *1/1* to the Link Aggregation Group. |

| | |
|---|---|
| `link-aggregation modify lag/1 addport 1/2` | Adds port *1/2* to the Link Aggregation Group. |
| `mrp domain modify port secondary lag/1` | Specifies port `lag/1` as ring port `2`. |
| `copy config running-config nvm` | Save the current settings in the non-volatile memory (`nvm`) in the “selected” configuration profile. |

# 12.3 HIPER Ring Client

The concept of HIPER Ring Redundancy enables the construction of high-availability, ring-shaped network structures. The *HIPER Ring* Client function lets the network administrator extend an existing HIPER Ring or replace a client device already participating in a HIPER Ring.

When the device senses that the link on a ring port goes down, the device sends a LinkDown packet to the Ring Manager (RM) and flushes the FDB table. Once the RM receives the LinkDown packet, it immediately forwards the data stream over both the primary and secondary ring ports. Thus, the RM is able to maintain the integrity of the HIPER Ring.

The device only supports Fast Ethernet and Gigabit Ethernet ports as ring ports. Furthermore, you can include the ring ports in a LAG instance.

In the default state, the HIPER Ring client is inactive, and the primary and secondary ports are set to `no Port`.

**Note:** Deactivate the Spanning Tree Protocol (STP) for the ring ports in the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, because STP and HIPER Ring have different reaction times.

*Table 30: Port settings for ring ports*

| Port type | Bit rate | Port on | Automatic configuration | Manual configuration |
|---|---|---|---|---|
| TX | 100 Mbit/s | `marked` | `unmarked` | *`100 Mbit/s FDX`* |
| TX | 1 Gbit/s | `marked` | `marked` | – |
| Optical | 100 Mbit/s | `marked` | `unmarked` | *`100 Mbit/s FDX`* |
| Optical | 1 Gbit/s | `marked` | `marked` | – |
| Optical | 2.5 Gbit/s | `marked` | – | *`2.5 Gbit/s FDX`* |
| Optical | 10 Gbit/s | `marked` | – | *`10 Gbit/s`* |

## 12.3.1 VLANS on the HIPER Ring

The device lets you forward VLAN data over the HIPER Ring. Thus the device provides redundancy for your VLAN data. The ring device forwards management data around the ring for example, on VLAN 1. In order for the data to reach the management station, the ring devices forward the untagged management data on the ring ports. Also, specify the ring ports as members in VLAN 1.

When you have other VLANs traversing your ring devices, the ring devices forward the other VLAN data as tagged.

Specify the VLAN settings. To do this, perform the following steps:

- Open the *Switching > VLAN > Configuration* dialog.
- Forward untagged VLAN management data on the ring ports.
  In the VLAN 1 row, select the `U` item in the drop-down list in the columns related to the ring port.
- Block management packets from being forwarded to the non-ring ports.
  In the VLAN 1 row, select the `-` item in the drop-down list in the columns **not** related to the ring port.
- Allow a ring device to forward VLAN data to and from ports with VLAN membership.
  In the VLAN row, select the `T` item in the drop-down list in the columns related to the ring port.
- Open the *Switching > VLAN > Port* dialog.
- Assign VLAN 1 membership to the ring ports.
  Enter the value `1` in the *Port-VLAN ID* column of the ring port rows.
- Assign VLAN membership to the non-ring ports.
  Enter the appropriate VLAN ID in the *Port-VLAN ID* column of the non-ring port rows.

### 12.3.2 HIPER Ring over LAG

The *HIPER Ring* function lets you link the devices together over a Link Aggregation Group (LAG). The ring clients and Ring Manager behave in the same manner as a ring without a LAG instance.

If a LAG link goes down, then the other link in the instance also goes down making a break in the ring. After detecting a break in the ring, the affected ports send a Link Down packet to the Ring Manager. The Ring Manager unblocks the secondary port, sending data in both directions around the ring, and replies with a Delete packet. Upon receiving a Delete packet the ring participates flush their FDB.

# 12.4 Spanning Tree

**Note:** The Spanning Tree Protocol is a protocol for MAC bridges. For this reason, the following description uses the term bridge for the device.

Local networks are getting bigger and bigger. This applies to both the geographical expansion and the number of network participants. Therefore, it is advantageous to use multiple bridges, for example:

- to reduce the network load in sub-areas,
- to set up redundant connections and
- to overcome distance limitations.

However, using multiple bridges with multiple redundant connections between the subnetworks can lead to loops and thus interruption of communication across the network. In order to help avoid this, you can use Spanning Tree. Spanning Tree enables loop-free switching through the systematic deactivation of redundant connections. Redundancy enables the systematic reactivation of individual connections as needed.

RSTP is a further development of the Spanning Tree Protocol (STP) and is compatible with it. When a connection or a bridge becomes inoperable, the STP requires a maximum of 30 seconds to reconfigure. This is no longer acceptable in time-sensitive applications. RSTP achieves average reconfiguration times of less than a second. When you use RSTP in a ring topology with 10 to 20 devices, you can even achieve reconfiguration times in the order of milliseconds.

**Note:** RSTP reduces a layer 2 network topology with redundant paths into a tree structure (Spanning Tree) that does not contain any more redundant paths. One of the devices takes over the role of the root bridge here. The maximum number of devices permitted in an active branch (from the root bridge to the tip of the branch) is specified by the variable *Max age* for the current root bridge. The preset value for *Max age* is `20`, which can be increased up to `40`.

If the device working as the root is inoperable and another device takes over its function, then the *Max age* setting of the new root bridge determines the maximum number of devices allowed in a branch.

**Note:** The RSTP standard requires that every device within a network operates with the (Rapid) Spanning Tree Algorithm. When STP and RSTP are used at the same time, the advantages of faster reconfiguration with RSTP are lost in the network segments that are operated in combination.

A device that only supports RSTP works together with MSTP devices by not assigning an MST region to itself, but rather the CST (Common Spanning Tree).

## 12.4.1 Basics

Because RSTP is a further development of the STP, every of the following descriptions of the STP also apply to RSTP.

### The tasks of the STP

The Spanning Tree Algorithm reduces network topologies built with bridges and containing ring structures due to redundant links to a tree structure. In doing so, STP opens ring structures according to preset rules by deactivating redundant paths. When a path is interrupted because a network component becomes inoperable, STP reactivates the previously deactivated path again. This lets redundant links increase the availability of communication.

STP determines a bridge that represents the STP tree structure‘s base. This bridge is called root bridge.

Features of the STP algorithm:
- automatic reconfiguration of the tree structure in the case of a bridge becoming inoperable or the interruption of a data path
- the tree structure is stabilized up to the maximum network size,
- stabilization of the topology within a short time period
- topology can be specified and reproduced by the administrator
- transparency for the end devices
- low network load relative to the available transmission capacity due to the tree structure created

### Bridge parameters

In the context of Spanning Tree, each bridge and its connections are uniquely described by the following parameters:
- Bridge Identifier
- Root Path Cost for the bridge ports,
- Port Identifier

### Bridge Identifier

The Bridge Identifier consists of 8 bytes. The 2 highest-value bytes are the priority. When configuring the network, the Management Administrator can change the default setting for the priority number which is 32768 (8000H). The 6 lowest-value bytes of the bridge identifier are the bridge’s MAC address. The MAC address lets each bridge have unique bridge identifiers.

The bridge with the smallest number for the bridge identifier has the highest priority.

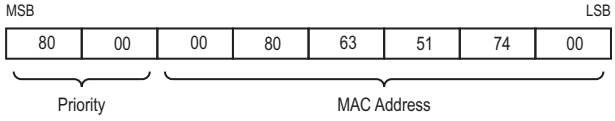



*Figure 40: Bridge Identifier, Example (values in hexadecimal notation)*

### Root Path Cost

Each path that connects 2 bridges is assigned a cost for the transmission (path cost). The device determines this value based on the transmission speed (see table 31). The device assigns a higher path cost to paths with lower transmission speeds.

Alternatively, the Administrator can set the path cost. Like the device, the Administrator assigns a higher path cost to paths with lower transmission speeds. However, since the Administrator can choose this value freely, he has a tool with which he can give a certain path an advantage among redundant paths.

The root path cost is the sum of the individual costs of those paths that a data packet has to traverse from a connected bridge‘s port to the root bridge.

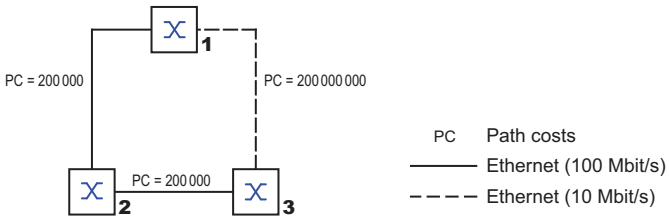



*Figure 41: Path costs*

*Table 31: Recommended path costs for RSTP based on the data rate.*

| Data rate | Recommended value | Recommended range | Possible range |
|---|---|---|---|
| ≤100 kbit/s | 200 000000[1] | 20000000-200000000 | 1-200000000 |
| 1 Mbit/s | 20000000[a] | 2000000-200000000 | 1-200000000 |
| 10 Mbit/s | 2000000[a] | 200000-20000000 | 1-200000000 |
| 100 Mbit/s | 200000[a] | 20000-2000000 | 1-200000000 |
| 1 Gbit/s | 20000 | 2000-200000 | 1-200000000 |
| 10 Gbit/s | 2000 | 200-20000 | 1-200 000000 |
| 100 Gbit/s | 200 | 20-2000 | 1-200000000 |
| 1 TBit/s | 20 | 2-200 | 1-200000000 |
| 10 TBit/s | 2 | 1-20 | 1-200000000 |

1. Bridges that conform with IEEE 802.1D 1998 and only support 16-bit values for the path costs should use the value 65,535 (FFFFH) for path costs in cases where they are used in conjunction with bridges that support 32-bit values for the path costs.

### Port Identifier

The port identifier consists of 2 bytes. One part, the lower-value byte, contains the physical port number. This provides a unique identifier for the port of this bridge. The second, higher-value part is the port priority, which is specified by the Administrator (default value: 128). It also applies here that the port with the smallest number for the port identifier has the highest priority.

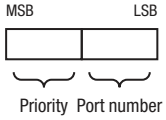



*Figure 42: Port Identifier*

### Max Age and Diameter

The “Max Age” and “Diameter” values largely determine the maximum expansion of a Spanning Tree network.

### Diameter

The number of connections between the devices in the network that are furthest removed from each other is known as the network diameter.

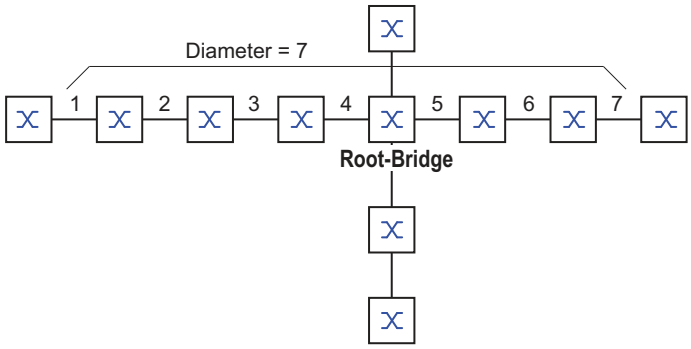



*Figure 43: Definition of diameter*

The network diameter that can be achieved in the network is MaxAge-1.

In the state on delivery, MaxAge = 20 and the maximum diameter that can be achieved = 19. When you set the maximum value of 40 for MaxAge, the maximum diameter that can be achieved = 39.

### MaxAge

Every STP-BPDU contains a “MessageAge” counter. When a bridge is passed through, the counter increases by 1.

Before forwarding a STP-BPDU, the bridge compares the “MessageAge” counter with the “MaxAge” value specified in the device:

- When MessageAge < MaxAge, the bridge forwards the STP-BPDU to the next bridge.
- When MessageAge = MaxAge, the bridge discards the STP-BPDU.

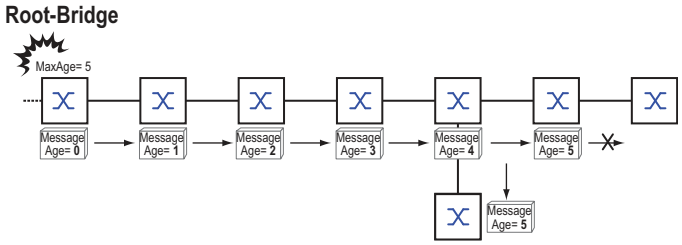



*Figure 44: Transmission of an STP-BPDU depending on MaxAge*

## 12.4.2 Rules for Creating the Tree Structure

### Bridge information

To determine the tree structure, the bridges need more detailed information about the other bridges located in the network.

To obtain this information, each bridge sends a BPDU (Bridge Protocol Data Unit) to the other bridges.

The contents of a BPDU include:
- Bridge identifier
- Root path costs
- Port identifier

(see IEEE 802.1D)

### Setting up the tree structure

The bridge with the smallest number for the bridge identifier is called the root bridge. It is (or will become) the root of the tree structure.

The structure of the tree depends on the root path costs. Spanning Tree selects the structure so that the path costs between each individual bridge and the root bridge become as small as possible.

- When there are multiple paths with the same root path costs, the bridge further away from the root decides which port it blocks. For this purpose, it uses the bridge identifiers of the bridge closer to the root. The bridge blocks the port that leads to the bridge with the numerically higher ID (a numerically higher ID is the logically worse one). When 2 bridges have the same priority, the bridge with the numerically larger MAC address has the numerically higher ID, which is logically the worse one.
- When multiple paths with the same root path costs lead from one bridge to the same bridge, the bridge further away from the root uses the port identifier of the other bridge as the last criterion (see figure 42). In the process, the bridge blocks the port that leads to the port with the numerically higher ID (a numerically higher ID is the logically worse one). When 2 ports have the same priority, the port with the higher port number has the numerically higher ID, which is logically the worse one.

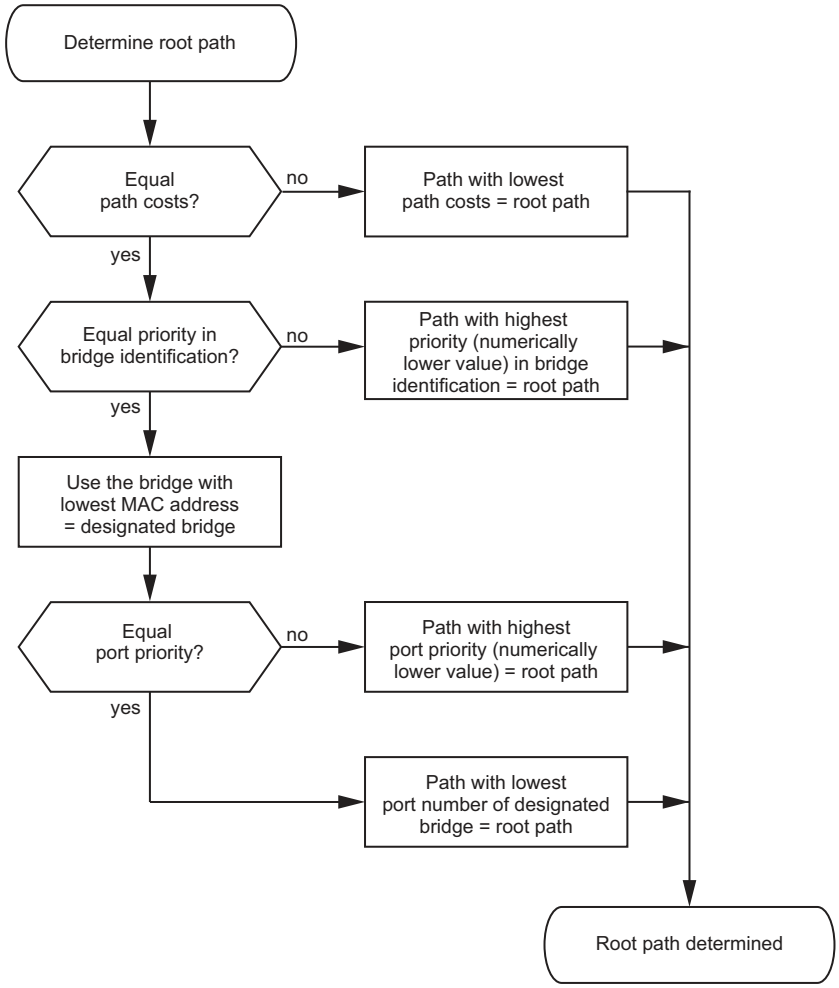



*Figure 45: Flow diagram for specifying the root path*

## 12.4.3 Examples

### Example of determining the root path

You can use the network plan (see figure 46) to follow the flow chart (see figure 45) for determining the root path. The administrator has specified a priority in the bridge identification for each bridge. The bridge with the smallest numerical value for the bridge identification takes on the role of the root bridge, in this case, bridge 1. In the example every sub-path has the same path costs. The protocol blocks the path between bridge 2 and bridge 3 as a connection from bridge 3 via bridge 2 to the root bridge would result in higher path costs.

The path from bridge 6 to the root bridge is interesting:

- The path via bridge 5 and bridge 3 creates the same root path costs as the path via bridge 4 and bridge 2.
- STP selects the path using the bridge that has the lowest MAC address in the bridge identification (bridge 4 in the illustration).
- There are also 2 paths between bridge 6 and bridge 4.
  The port identifier is decisive here (Port 1 < Port 3).

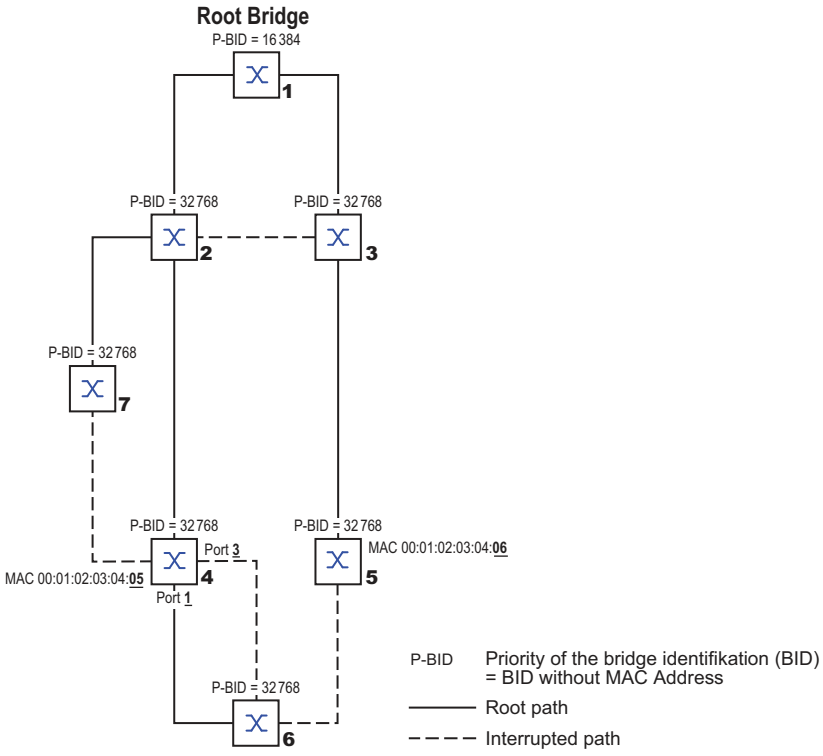



*Figure 46: Example of determining the root path*

**Note:** When the current root bridge goes down, the MAC address in the bridge identifier alone determines which bridge becomes the new root bridge, because the Administrator does not change the default values for the priorities of the bridges in the bridge identifier, apart from the value for the root bridge.

### Example of manipulating the root path

You can use the network plan (see figure 47) to follow the flow chart (see figure 45) for determining the root path. The Administrator has performed the following:

- Left the default value of 32768 (8000H) for every bridge apart from bridge 1 and bridge 5, and
- assigned to bridge 1 the value 16384 (4000H), thus making it the root bridge.
- To bridge 5 he assigned the value 28672 (7000H).

The protocol blocks the path between bridge 2 and bridge 3 as a connection from bridge 3 via bridge 2 to the root bridge would mean higher path costs.

The path from bridge 6 to the root bridge is interesting:

▶ The bridges select the path via bridge 5 because the value 28672 for the priority in the bridge identifier is smaller than value 32768.

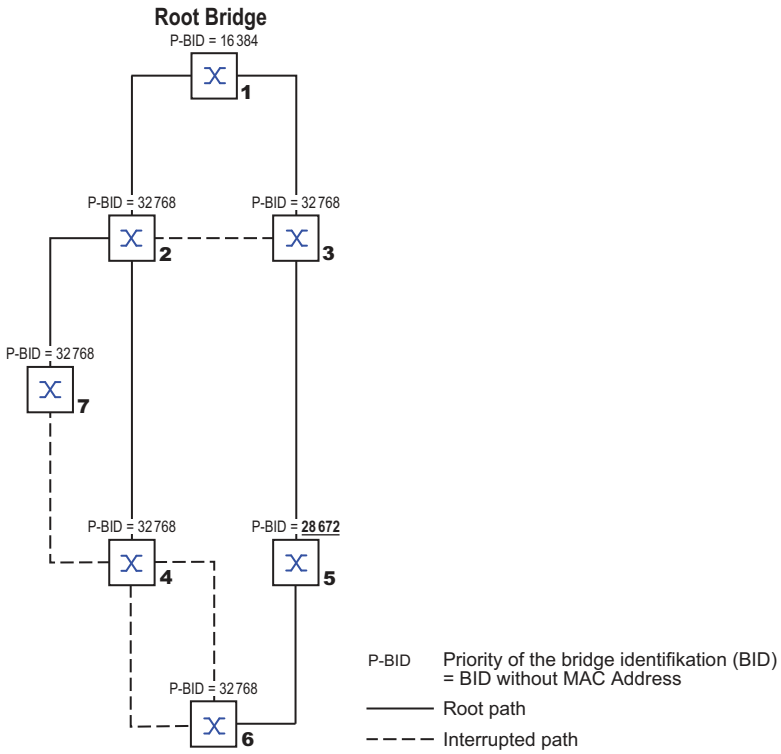



*Figure 47: Example of manipulating the root path*

### Example of manipulating the tree structure

The Management Administrator soon discovers that this configuration with bridge 1 as the root bridge is invalid. On the paths from bridge 1 to bridge 2 and bridge 1 to bridge 3, the control packets which the root bridge sends to every other bridge add up.

When the Management Administrator configures bridge 2 as the root bridge, the burden of the control packets on the subnetworks is distributed much more evenly. The result is the configuration shown here (see figure 48). The path costs for most of the bridges to the root bridge have decreased.

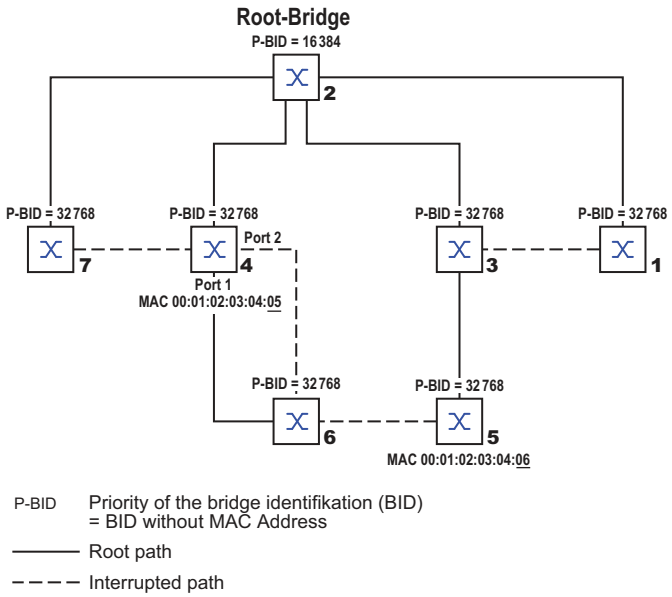



*Figure 48: Example of manipulating the tree structure*

# 12.5 The Rapid Spanning Tree Protocol

The RSTP uses the same algorithm for determining the tree structure as STP. When a link or bridge becomes inoperable, RSTP merely changes parameters, and adds new parameters and mechanisms that speed up the reconfiguration.

The ports play a significant role in this context.

## 12.5.1 Port roles

RSTP assigns each bridge port one of the following roles (see figure 49):

- Root Port:
  This is the port at which a bridge receives data packets with the lowest path costs from the root bridge.
  When there are multiple ports with equally low path costs, the bridge ID of the bridge that leads to the root (designated bridge) decides which of its ports is given the role of the root port by the bridge further away from the root.
  When a bridge has multiple ports with equally low path costs to the same bridge, the bridge uses the port ID of the bridge leading to the root (designated bridge) to decide which port it selects locally as the root port (see figure 45).
  The root bridge itself does not have a root port.
- Designated port:
  The bridge in a network segment that has the lowest root path costs is the designated bridge. When more than one bridge has the same root path costs, the bridge with the smallest value bridge identifier becomes the designated bridge. The designated port on this bridge is the port that connects a network segment leading away from the root bridge. When a bridge is connected to a network segment with more than one port (via a hub, for example), the bridge gives the role of the designated port to the port with the better port ID.
- Edge port
  Every network segment with no additional RSTP bridges is connected with exactly one designated port. In this case, this designated port is also an edge port. The distinction of an edge port is the fact that it does not receive any RST BPDUs (Rapid Spanning Tree Bridge Protocol Data Units).
- Alternate port
  When the connection to the root bridge is lost, this blocked port takes over the task of the root port. The alternate port provides a backup for the connection to the root bridge.

- Backup port
  This is a blocked port that serves as a backup in case the connection to the designated port of this network segment (without any RSTP bridges) is lost
- Disabled port
  This is a port that does not participate in the Spanning Tree Operation, that means, the port is switched off or does not have any connection.

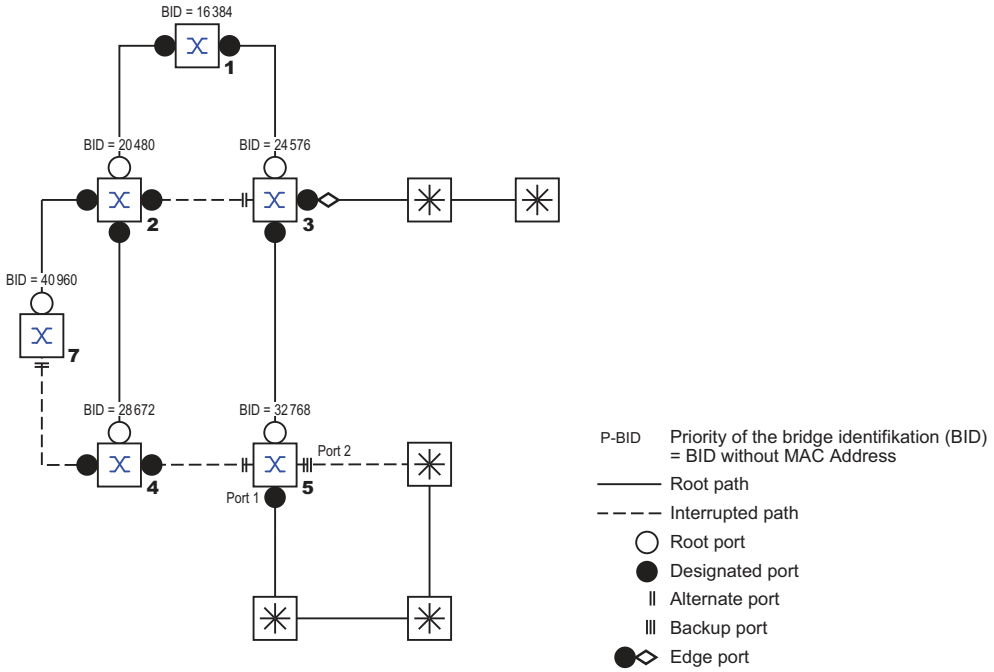



*Figure 49: Port role assignment*

## 12.5.2 Port states

Depending on the tree structure and the state of the selected connection paths, the RSTP assigns the ports their states.

*Table 32: Relationship between port state values for STP and RSTP*

| STP port state | Administrative bridge port state | MAC Operational | RSTP Port state | Active topology (port role) |
|---|---|---|---|---|
| DISABLED | Disabled | FALSE | Discarding[1] | Excluded (disabled) |
| DISABLED | Enabled | FALSE | Discarding[a] | Excluded (disabled) |
| BLOCKING | Enabled | TRUE | Discarding[2] | Excluded (alternate, backup) |
| LISTENING | Enabled | TRUE | Discarding[b] | Included (root, designated) |
| LEARNING | Enabled | TRUE | Learning | Included (root, designated) |
| FORWARDING | Enabled | TRUE | Forwarding | Included (root, designated) |

1. The dot1d-MIB displays “Disabled”.
2. The dot1d-MIB displays “Blocked”.

Meaning of the RSTP port states:
- Disabled: Port does not belong to the active topology
- Discarding: No address learning in FDB, no data traffic except for STP-BPDUs

- Learning: Address learning active (FDB), no data traffic apart from STP-BPDUs
- Forwarding: Address learning active (FDB), sending and receiving of every packet type (not only STP-BPDUs)

### 12.5.3 Spanning Tree Priority Vector

To assign roles to the ports, the RSTP bridges exchange configuration information with each other. This information is known as the Spanning Tree Priority Vector. It is part of the RSTP BPDUs and contains the following information:

- Bridge identification of the root bridge
- Root path costs of the sending bridge
- Bridge identification of the sending bridge
- Port identifiers of the ports through which the message was sent
- Port identifiers of the ports through which the message was received

Based on this information, the bridges participating in RSTP are able to determine port roles themselves and define the port states of their own ports.

### 12.5.4 Fast reconfiguration

Why can RSTP react faster than STP to an interruption of the root path?

- Introduction of edge-ports:
  During a reconfiguration, RSTP sets an edge port into the transmission mode after 3 seconds (default setting). To ascertain that no bridge sending BPDUs is connected, RSTP waits for the “Hello Time” to elapse.
  When you verify that an end device is and remains connected to this port, there are no waiting times at this port in the case of a reconfiguration.
- Introduction of alternate ports:
  As the port roles are already distributed in normal operation, a bridge can immediately switch from the root port to the alternate port after the connection to the root bridge is lost.
- Communication with neighboring bridges (point-to-point connections):
  Decentralized, direct communication between neighboring bridges enables reaction without wait periods to status changes in the spanning tree topology.
- Address table:
  With STP, the age of the entries in the FDB determines the updating of communication. RSTP immediately deletes the entries in those ports affected by a reconfiguration.
- Reaction to events:
  Without having to adhere to any time specifications, RSTP immediately reacts to events such as connection interruptions, connection reinstatements, etc.

**Note:** Data packages could be duplicated and/or arrive at the recipient in the wrong order during the reconfiguration phase of the RSTP topology. You may also use the Spanning Tree Protocol or select another redundancy procedure described in this manual.

### 12.5.5 Configuring the device

RSTP configures the network topology completely autonomously. The device with the lowest bridge priority automatically becomes the root bridge. However, to define a specific network structure regardless, you specify a device as the root bridge. In general, a device in the backbone takes on this role.

Perform the following steps:

- ☐ Set up the network to meet your requirements, initially without redundant lines.
- ☐ 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. (Default setting: flow control deactivated globally and activated on every port.)
- ☐ Disable MRP on every device.
- ☐ Enable Spanning Tree on every device in the network.
  In the state on delivery, Spanning Tree is switched on in the device.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- ☐ Enable the function.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `spanning-tree operation` | Enables Spanning Tree. |
| `show spanning-tree global` | Displays the parameters for checking. |

Now connect the redundant lines.

Define the settings for the device that takes over the role of the root bridge.

Perform the following steps:

- ☐ In the *Priority*field you enter a numerically lower value.
  The bridge with the numerically lowest bridge ID has the highest priority and becomes the root bridge of the network.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `spanning-tree mst priority 0 <0..61440>` | Specifies the bridge priority of the device.<br><br>**Note:** Specify the bridge priority in the range `0..61440` in steps of 4096. |

After saving, the dialog shows the following information:

- The *Bridge is root* checkbox is marked.
- The *Root port* field shows the value `0.0`.
- The *Root path cost* field shows the value `0`.

| | |
|---|---|
| `show spanning-tree global` | Displays the parameters for checking. |

- ☐ If applicable, then change the values in the *Forward delay [s]* and *Max age* fields.
  - The root bridge transmits the changed values to the other devices.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `spanning-tree forward-time <4..30>` | Specifies the delay time for the status change in seconds. |
| `spanning-tree max-age <6..40>` | Specifies the maximum permissible branch length, for example the number of devices to the root bridge. |
| `show spanning-tree global` | Displays the parameters for checking. |

**Note:** The parameters *Forward delay [s]* and *Max age* have the following relationship:

*Forward delay [s]* ≥ (*Max age*/2) + 1

If you enter values in the fields that contradict this relationship, then the device replaces these values with the last valid values or with the default value.

**Note:** When possible, do not change the value in the “Hello Time” field.

Check the following values in the other devices:
- Bridge ID (bridge priority and MAC address) of the corresponding device and the root bridge.
- Number of the device port that leads to the root bridge.
- Path cost from the root port of the device to the root bridge.

Perform the following steps:

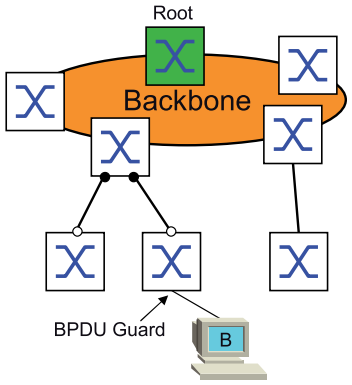
| | |
|---|---|
| `show spanning-tree global` | Displays the parameters for checking. |

### 12.5.6 Guards

The device lets you activate various protection functions (guards) in the device ports.

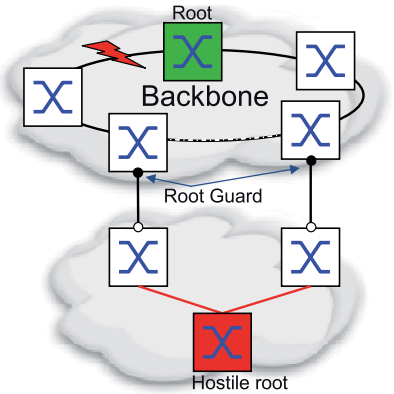
The following protection functions help protect your network from incorrect configurations, loops and attacks with STP-BPDUs:

- BPDU Guard – for manually specified edge ports (end device ports)
  You activate this protection function globally in the device.



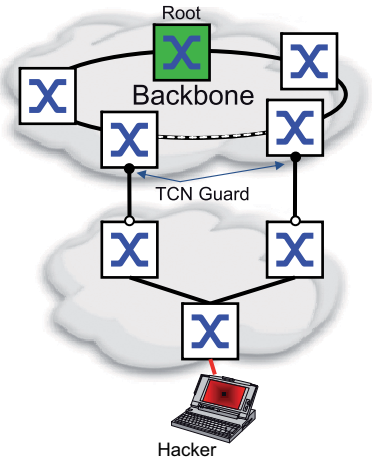

Terminal device ports do not normally receive any STP-BPDUs. If an attacker still attempts to feed in STP-BPDUs on this port, then the device deactivates the device port.

- Root Guard – for designated ports
  You activate this protection function separately for every device port.



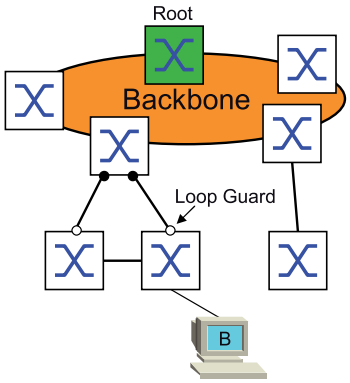

When a designated port receives an STP-BPDU with better path information to the root bridge, the device discards the STP-BPDU and sets the transmission state of the port to `discarding` instead of `root`.
When there are no STP-BPDUs with better path information to the root bridge, after 2 × *Hello time [s]* the device resets the state of the port to a value according to the port role.

- TCN Guard – for ports that receive STP-BPDUs with a Topology Change flag
  You activate this protection function separately for every device port.




If the protection function is activated, then the device ignores Topology Change flags in received STP-BPDUs. This does not change the content of the address table (FDB) of the device port. However, additional information in the BPDU that changes the topology is processed by the device.

- Loop Guard – for root, alternate and backup ports
  You activate this protection function separately for every device port.




If the port does not receive any more STP-BPDUs, then this protection function helps prevent the transmission status of a port from unintentionally being changed to `forwarding`. If this situation occurs, then the device designates the loop status of the port as inconsistent, but does not forward any data packets.

### Activating the BPDU Guard

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- ☐ Mark the *BPDU guard* checkbox.
- ☐ Save the changes temporarily. To do this, click the ☑ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |

| | |
|---|---|
| `configure` | Change to the Configuration mode. |
| `spanning-tree bpdu-guard` | Activates the BPDU Guard. |
| `show spanning-tree global` | Displays the parameters for checking. |

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.
- ☐ Switch to the *CIST* tab.
- ☐ For end device ports, mark the checkbox in the *Admin edge port*column.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `interface <x/y>` | Change to the interface configuration mode of interface `<x/y>`. |
| `spanning-tree edge-port` | Designates the port as a terminal device port (edge port). |
| `show spanning-tree port x/y` | Displays the parameters for checking. |
| `exit` | Leaves the interface mode. |

When an edge port receives an STP-BPDU, the device behaves as follows:

- ▶ The device deactivates this port.
  In the *Basic Settings > Port* dialog, *Configuration* tab, the checkbox for this port in the *Port on* column is `unmarked`.
- ▶ The device designates the port.

You can determine if a port has disabled itself because of a received a BPDU. To do this, perform the following steps:

In the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *Guards* tab, the checkbox in the *BPDU guard effect* column is `marked`.

| | |
|---|---|
| `show spanning-tree port x/y` | Displays the parameters of the port for checking. The value of the *BPDU guard effect* parameter is `enabled`. |

Reset the status of the device port to the value `forwarding`. To do this, perform the following steps:

- ☐ When the port still receives BPDUs:
  - – Remove the manual definition as an edge port (end device port).
    or
  - – Deactivate the BPDU Guard.
- ☐ Activate the device port again.

### Activating Root Guard / TCN Guard / Loop Guard

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.
- ☐ Switch to the *Guards* tab.
- ☐ For designated ports, select the checkbox in the *Root guard* column.
- ☐ For ports that receive STP-BPDUs with a Topology Change flag, select the checkbox in the *TCN guard* column.
- ☐ For root, alternate or backup ports, mark the checkbox in the *Loop guard* column.

**Note:** The *Root guard* and *Loop guard* functions are mutually exclusive. If you try to activate the *Root guard* function while the *Loop guard* function is active, then the device deactivates the *Loop guard* function.

- ☐ Save the changes temporarily. To do this, click the ✔ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface <x/y>` | Change to the interface configuration mode of interface `<x/y>`. |
| `spanning-tree guard-root` | Switches the Root Guard on at the designated port. |
| `spanning-tree guard-tcn` | Switches the TCN Guard on at the port that receives STP-BPDUs with a Topology Change flag. |
| `spanning-tree guard-loop` | Switches the Loop Guard on at a root, alternate or backup port. |
| `exit` | Leaves the interface mode. |
| `show spanning-tree port x/y` | Displays the parameters of the port for checking. |

## 12.5.7 Ring only mode

You use the *Ring only mode* function to recognize full-duplex connectivity and to configure the ports that are connected to the end stations. The *Ring only mode* function lets the device transition to the ‘forwarding’ state, and suppress the Topology Change Notification PDUs.

### Configuring the Ring only mode

When you activate the *Ring only mode* function on the ports, and the device ignores the message age of normal BDPUs, the device sends Topology Change messages with the message age of `1`.

### Example

The given example describes the configuration of the *Ring only mode* function.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- ☐ In the *Ring only mode* frame, select the port *1/1* in the *First port* field.
- ☐ In the *Ring only mode* frame, select the port *1/2* in the *Second port* field.
- ☐ To activate the function, in the *Ring only mode* frame, mark the *Active* checkbox.
- ☐ Save the changes temporarily. To do this, click the ✔ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `spanning-tree ring-only-mode operation` | Enable the *Ring only mode* function. |
| `spanning-tree ring-only-mode first-port 1/1` | Specify port *1/1* as the first interface. |
| `spanning-tree ring-only-mode second-port 1/2` | Specify port *1/2* as the second interface. |

# 12.6 Link Aggregation

The *Link Aggregation* function using the single switch method helps you overcome 2 limitations with Ethernet links, namely bandwidth, and redundancy.

The *Link Aggregation* function helps you overcome bandwidth limitations of individual ports. The *Link Aggregation* function lets you combine 2 or more links in parallel, creating 1 logical link between 2 devices. The parallel links increase the bandwidth for traffic between the 2 devices.

You typically use the *Link Aggregation* function on the network backbone. The function provides you an inexpensive way to incrementally increase bandwidth.

Furthermore, the *Link Aggregation* function provides for redundancy with a seamless failover. When a link goes down, with 2 or more links configured in parallel, the other links in the group continue to forward traffic.

The device uses a hash option to determine load balancing across the port group. Tagging the egress traffic lets the device transmit associated packets across the same link.

The default settings for a new *Link Aggregation* instance are as follows:
- In the *Configuration* frame, the value in the *Hashing option* field is `sourceDestMacVlan`.
- In the *Active* column, the checkbox is marked.
- In the *Send trap (Link up/down)* column, the checkbox is marked.
- In the *Static link aggregation* column, the checkbox is unmarked.
- In the *Hashing option* column, the value is `sourceDestMacVlan`.
- In the *Active ports (min.)* column, the value is `1`.

## 12.6.1 Methods of Operation

The device operates on the Single Switch method. The Single Switch method provides you an inexpensive way to grow your network. The single switch method states that you need one device on each side of a link to provide the physical ports. The device balances the traffic load across the group member ports.

The device also uses the Same Link Speed method in which the group member ports are full-duplex, point-to-point links having the same transmission rate. The first port that you add to the group is the master port and determines the bandwidth for the other member ports of the Link Aggregation Group.

The device lets you set up up to 16 Link Aggregation groups. The number of useable ports per Link Aggregation group depends on the device.

### Hash Algorithm

The frame distributor is responsible for receiving frames from the end devices and transmitting them over the Link Aggregation Group. The frame distributor implements a distribution algorithm responsible for choosing the link used for transmitting any given packet. The hash option helps you achieve load balancing across the group.

The following list contains options which you set for link selection.
- Source MAC address, VLAN ID, EtherType, and receiving port
- Destination MAC address, VLAN ID, EtherType, and receiving port

- Source/Destination MAC address, VLAN ID, EtherType, and receiving port
- Source IP address and Source TCP/UDP port
- Destination IP address and destination TCP/UDP port
- Source/destination IP address and source/destination TCP/UDP port

### Static and Dynamic Links

The device lets you set up static and dynamic links.

- Static Links - The administrator sets up and maintains the links manually. For example, when a link fails and there is a media converter between the devices, the media converter continues forwarding traffic on the link causing the link to fail. Another possibility is that cabling or an undetected configuration mistake causes undesirable network behavior. In this case, the network administrator manually changes the link setup to restore traffic.
- Dynamic Links - The device confirms that the setup on the remote device is able to handle link aggregation and failover occurs automatically.

## 12.6.2 Link Aggregation Example

Connect multiple workstations using one aggregated link group between Switch 1 and 2. By aggregating multiple links, higher speeds are achievable without a hardware upgrade.

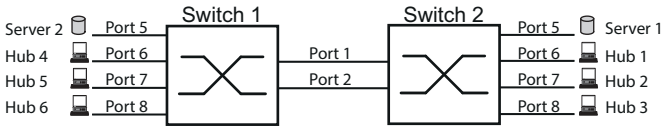



*Figure 50: Link Aggregation Switch to Switch Network*

Configure Switch 1 and 2 in the Graphical User Interface. To do this, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Link Aggregation* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *Trunk port* drop-down list, select the instance number of the link aggregation group.
- ☐ In the *Port* drop-down list, select port *1/1*.
- ☐ Click the *Ok* button.
- ☐ Repeat the preceding steps and select the port *1/2*.
- ☐ Click the *Ok* button.
- ☐ Save the changes temporarily. To do this, click the button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `link-aggregation add lag/1` | Creates a Link Aggregation Group `lag/1`. |
| `link-aggregation modify lag/1 addport 1/1` | Adds port *1/1* to the Link Aggregation Group. |
| `link-aggregation modify lag/1 addport 1/2` | Adds port *1/2* to the Link Aggregation Group. |

# 12.7 Link Backup

Link Backup provides a redundant link for traffic on Layer 2 devices. When the device detects an error on the primary link, the device transfers traffic to the backup link. You typically use Link Backup in service-provider or enterprise networks.

You set up the backup links in pairs, one as a primary and one as a backup. When providing redundancy for enterprise networks for example, the device lets you set up more than one pair. The maximum number of link backup pairs is: total number of physical ports / 2. Furthermore, when the state of a port participating in a link backup pair changes, the device sends an SNMP trap.

When configuring link backup pairs, remember the following rules:

- A link pair consists of any combination of physical ports. For example, one port is a 100 Mbit port and the other is a 1000 Mbit SFP port.
- A specific port is a member of one link backup pair at any given time.
- Verify that the ports of a link backup pair are members of the same VLAN with the same VLAN ID. When the primary port or backup port is a member of a VLAN, assign the second port of the pair to the same VLAN.

The default setting for this function is inactive without any link backup pairs.

**Note:** Verify that the Spanning Tree Protocol is disabled on the Link Backup ports.

## 12.7.1 Fail Back Description

Link Backup also lets you set up a Fail Back option. When you activate the fail back function and the primary link returns to normal operation, the device first blocks traffic on the backup port and then forwards traffic on the primary port. This process helps protect the device from causing loops in the network.

When the primary port returns to the link up and active state, the device supports 2 modes of operation:

- When you inactivate *Fail back*, the primary port remains in the blocking state until the backup link fails.
- When you activate *Fail back*, and after the *Fail back delay [s]* timer expires, the primary port returns to the forwarding state and the backup port changes to down.

In the cases listed above, the port forcing its link to forward traffic, first sends a "flush FDB" packet to the remote device. The flush packet helps the remote device quickly relearn the MAC addresses.

## 12.7.2 Example Configuration

In the example network below, you connect ports *2/3* and *2/4* on Switch A to the uplink Switches B and C. When you set up the ports as a Link Backup pair, one of the ports forwards traffic and the other port is in the blocking mode.

The primary, port *2/3* on Switch A, is the active port and is forwarding traffic to port 1 on Switch B. Port *2/4* on Switch A is the backup port and blocks traffic.

When Switch A disables port *2/3* because of a detected error, port *2/4* on Switch A starts forwarding traffic to port 2 on Switch C.

When port *2/3* returns to the active state, “no shutdown“, with *Fail back* activated, and *Fail back delay [s]* set to 30 seconds. After the timer expires, port *2/4* first blocks the traffic and then port *2/3* starts forwarding the traffic.

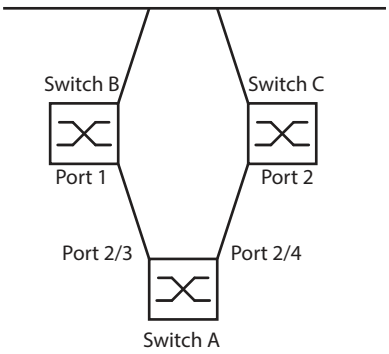



*Figure 51: Link Backup example network*

The following tables contain examples of parameters to configure Switch A.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Link Backup* dialog.
- ☐ Enter a new Link Backup pair in the table:
  - ☐ Click the button.
    The dialog displays the *Create* window.
  - ☐ In the *Primary port* drop-down list, select port *2/3*.
    In the *Backup port* drop-down list, select port *2/4*.
  - ☐ Click the *Ok* button.
- ☐ In the *Description* textbox, enter `Link_Backup_1` as the name for the backup pair.
- ☐ To activate the *Fail back* function for the link backup pair, mark the *Fail back* checkbox.
- ☐ Set the fail back timer for the link backup pair, enter `30` s in *Fail back delay [s]*.
- ☐ To activate the link backup pair, mark the *Active* checkbox.
- ☐ To enable the function, select the *On* radio button in the *Operation* frame.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 2/3` | Change to the interface configuration mode of interface *2/3*. |
| `link-backup add 2/4` | Creates a Link Backup instance where port *2/3* is the primary port and port *2/4* is the backup port. |
| `link-backup modify 2/4 description Link_Backup_1` | Specifies the string `Link_Backup_1` as the name of the backup pair. |
| `link-backup modify 2/4 failback-status enable` | Enable the fail back timer. |
| `link-backup modify 2/4 failback-time 30` | Specify the fail back delay time as `30` s. |
| `link-backup modify 2/4 status enable` | Enable the Link Backup instance. |
| `exit` | Change to the Configuration mode. |
| `link-backup operation` | Enable the *Link Backup* function globally in the device. |

# 12.8 FuseNet

The *FuseNet* protocols let you couple rings that are operating with one of the following redundancy protocols:

- MRP
- HIPER ring
- RSTP

**Note:** The prerequisite for coupling a network to the main ring using the *Ring/Network Coupling* protocol is that the connected network contains only network devices that support the *Ring/Network Coupling* protocol.

Use the following table to select the *FuseNet* coupling protocol to be used in your network:

| Main Ring | Connected Network | | |
|---|---|---|---|
| | **MRP** | **HIPER ring** | **RSTP** |
| **MRP** | *Sub Ring*[1)] | – *Redundant Coupling Protocol*<br>– *Ring/Network Coupling* | – *Redundant Coupling Protocol*<br>– *Ring/Network Coupling* |
| **HIPER ring** | *Sub Ring* | *Ring/Network Coupling* | – *Redundant Coupling Protocol*<br>– *Ring/Network Coupling* |
| **RSTP** | *Redundant Coupling Protocol* | *Redundant Coupling Protocol* | – |

– no suitable coupling protocol

1) with *MRP* configured on different VLANs

# 12.9 Subring

The *Sub Ring* function is an extension of the Media Redundancy Protocol (MRP). This function lets you couple a subring to a main ring using various network structures.

The Subring protocol provides redundancy for devices by coupling both ends of an otherwise flat network to a main ring.

Setting up subrings has the following advantages:

- Through the coupling process, you include the new network segment in the redundancy concept.
- Subrings allow easy integration of new areas into existing networks.
- Subrings allow you easy mapping of the organizational structure of an area in a network topology.
- In an MRP ring, the failover times of the subring in redundancy cases are typically < 100 ms.

## 12.9.1 Subring description

The subring concept lets you couple new network segments to suitable devices in an existing ring (main ring). The devices with which you couple the subring to the main ring are Subring Managers (SRM).

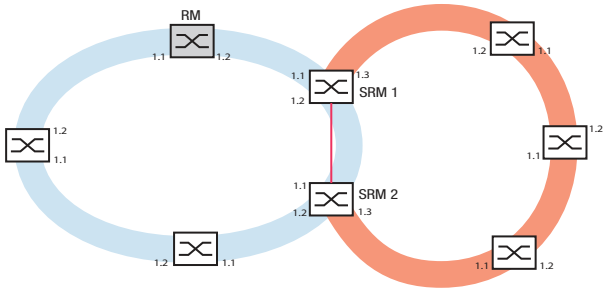



*Figure 52: Example of a subring structure*
*blue ring = Main ring*
*orange ring = Subring*
*red line = Redundant link of Subring*
*SRM = Subring Manager*
*RM = Ring Manager*

The Subring Manager capable devices support up to 20 instances and thus manage up to 20 subrings at the same time.

The *Sub Ring* function lets you integrate devices that support MRP as participants. The devices with which you couple the subring to the main ring require the *Sub Ring* Manager function.

Each subring can consist of up to 200 participants, excluding the Subring Managers themselves and the devices between the Subring Managers in the main ring.

The following figures display examples of possible subring topologies:

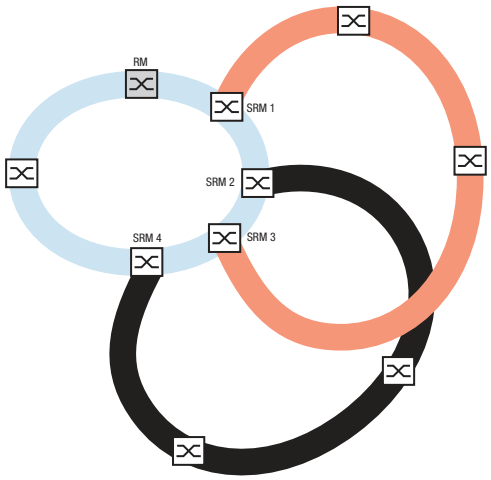



*Figure 53: Example of an overlapping subring structure*

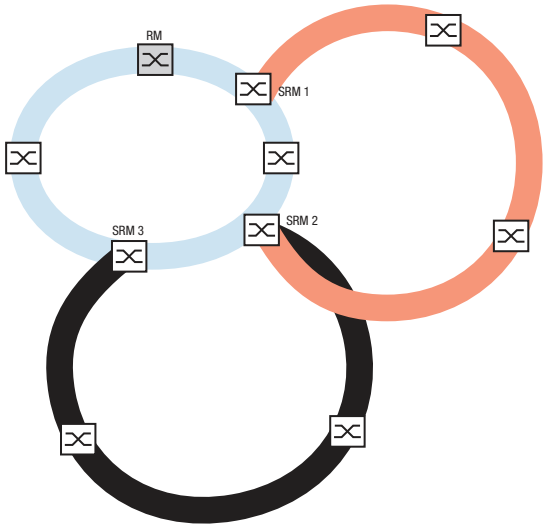



*Figure 54: Special case: A Subring Manager manages 2 subrings (2 instances). The Subring Manager is capable of managing up to 20 instances.*

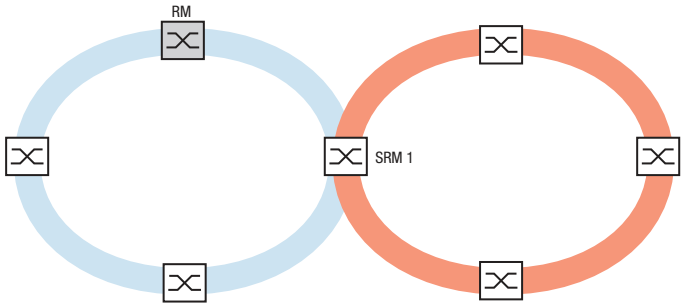



*Figure 55: Special case: a Subring Manager manages both ends of a subring on different ports (Single Subring Manger).*

**Note:** In the previous examples, the Subring Managers only couple subrings to existing main rings. The *Sub Ring* function prohibits cascaded subrings, for example coupling a new subring to another existing subring.

If you use MRP for the main ring and the subring, then specify the VLAN settings as follows:

- VLAN `X` for the main ring
  - on the ring ports of the main ring participants
  - on the main ring ports of the Subring Manager
- VLAN `Y` for the Subring
  - on the ring ports of the Subring participants
  - on the subring ports of the Subring Manager

  You can use the same VLAN for multiple subrings.

### 12.9.2 Subring example

In the following example, you couple a new network segment with 3 devices to an existing main ring which uses the MRP protocol. When you couple the network at both ends instead of one end, the subring provides increased availability with the corresponding configuration.

You couple the new network segment as a subring. You couple the subring to the existing devices of the main ring using the following configuration types.

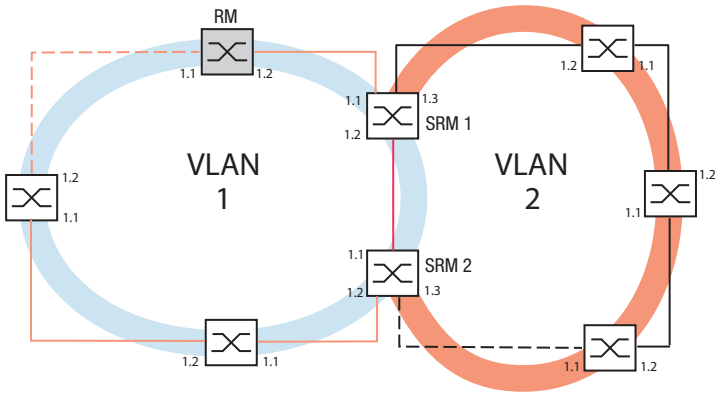



*Figure 56: Example of a subring structure*
*orange line= Main ring members in VLAN 1*
*black line= Subring members in VLAN 2*
*orange dash line= Main ring loop open*
*black dash line= Subring loop open*
*red line = Redundant link member in VLAN 1*
*SRM = Subring Manager*
*RM = Ring Manager*

To configure the subring, perform the following steps:

☐ Configure the three devices of the new network segment as participants in an MRP ring:
  - Configure the transmission rate and the duplex mode for the ring ports in accordance with the following table:

*Table 33: Port settings for subring ports*

| Port type | Bit rate | Port on | Automatic configuration | Manual configuration |
|---|---|---|---|---|
| TX | 100 Mbit/s | `marked` | `unmarked` | *`100 Mbit/s FDX`* |
| TX | 1 Gbit/s | `marked` | `marked` | – |
| Optical | 100 Mbit/s | `marked` | `unmarked` | *`100 Mbit/s FDX`* |
| Optical | 1 Gbit/s | `marked` | `marked` | – |
| Optical | 2.5 Gbit/s | `marked` | – | *`2.5 Gbit/s FDX`* |
| Optical | 10 Gbit/s | `marked` | – | *`10 Gbit/s`* |

The following steps contain additional settings for subring configuration:

- ☐ To help prevent loops during configuration, deactivate the Subring Manager function on the main ring and subring devices. After you completely configure every device participating in the main ring and subrings activate the global *Sub Ring* function and Subring Managers.
- ☐ Disable the RSTP function on the MRP ring ports used in the subring.
- ☐ Verify that the *Link Aggregation* function is inactive on ports participating in the main ring and subring.
- ☐ Specify a different VLAN membership for the main ring ports and subring ports although the main ring is using the MRP protocol. For example, use VLAN ID `1` for the main ring and the redundant link, then use VLAN ID `2` for the subring.
  - For the devices participating in the main ring for example, open the *Switching > VLAN > Configuration* dialog. Create VLAN `1` in the static VLAN table. To tag the main ring ports for membership in VLAN `1`, select the `T` item in the drop-down list of the appropriate port columns.
  - For the devices participating in the subring use the step above and add the ports to VLAN `2` in the static VLAN table.
- ☐ Activate the *MRP* function for the main ring and subring devices.
  - In the *Switching > L2-Redundancy > MRP* dialog, configure the 2 ring ports participating in the main ring on the main ring devices.
  - For the devices participating in the subring use the step above and configure the 2 ring ports participating in the subring on the subring devices.
  - Assign the same MRP domain ID to the main ring and subring devices. When you only use Hirschmann devices, the default values suffice for the MRP domain ID.

**Note:** The *MRP domain* is a sequence of 16 numbers in the range from `0` to `255`. The default value is `255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255`. A *MRP domain* consisting entirely of zeroes is invalid.

The *Sub Ring* dialog lets you change the MRP domain ID. Alternatively, use the Command Line Interface. To do this, perform the following steps:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `mrp domain delete` | Deletes the current MRP domain. |
| `mrp domain add domain-id 0.0.1.1.2.2.3.4.4.111.222.123.0.0.66.99` | Creates a new MRP domain with the specified MRP domain ID. Any subsequent MRP domain changes apply to this domain ID. |

## 12.9.3 Subring example configuration

**Note:** Help avoid loops during configuration. Configure every device of the subring individually. Before you activate the redundant link, completely configure every subring device.

Configure the 2 Subring Managers in the example. To do this, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Sub Ring* dialog.
- ☐ To add a table entry, click the button.
- ☐ In the *Port* column, select the port that couples the device to the subring.
  Use port *1/3* for this example.
  For coupling, use one of the available ports with the exception of the ports which are already connected to the main ring.

- ☐ In the *Name* column, assign a name to the subring.
  For this example enter `Test`.
- ☐ In the *SRM mode* column, select Subring Manager mode.
  You thus specify which port for coupling the subring to the main ring becomes the redundant manager.
  The options for the coupling are:
  - `manager`
    When you specify both Subring Managers with the same value, the device with the higher MAC address manages the redundant link.
  - `redundant manager`
    This device manages the redundant link, as long as you have specified the other Subring Manager as a `manager`. Otherwise the device with the higher MAC address manages the redundant link.

  Specify Subring Manager 1 as `manager`, in accordance with the figure depicting this example.
- ☐ Leave the values in the *VLAN* column and *MRP domain* column unchanged.
  The default values are correct for the example configuration.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `sub-ring add 1` | Creates a new subring with the subring ID `1`. |
| `sub-ring modify 1 port 1/3` | Specify port *1/3* as subring port. |
| `sub-ring modify 1 name Test` | Assign the name `Test` to the subring `1`. |
| `sub-ring modify 1 mode manager` | Assign the `manager` mode to the subring `1`. |
| `show sub-ring ring` | Display the subrings state on this device. |
| `show sub-ring global` | Display the subring global state on this device. |

- ☐ Configure the 2nd Subring Manager in the same way.
  Specify Subring Manager 2 as `redundant manager`, in accordance with the figure depicting this example.

- ☐ To activate the Subring Manager function, mark the *Active* checkbox in the appropriate row.
- ☐ After you have configured both Subring Managers and the devices participating in the subring, enable the function and close the redundant link.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `sub-ring enable 1` | Activate subring `1`. |
| `sub-ring enable 2` | Activate subring `2`. |
| `exit` | Change to the Privileged EXEC mode. |
| `show sub-ring ring <Domain ID>` | Display the settings of the selected subrings. |
| `show sub-ring global` | Display global subring settings. |
| `copy config running-config nvm profile Test` | Save the current settings in the configuration profile named `Test` in non-volatile memory (`nvm`). |

# 12.10 Subring with LAG

When at least two parallel redundant connecting lines exist (known as a trunk) between two devices, and these lines are combined into one logical connection, this is a Link Aggregation (LAG) connection.

The device lets you use the LAG ports as ring ports with the *Sub Ring* protocol.

## 12.10.1 Example

The following example is a simple setup between an MRP ring and a Subring.

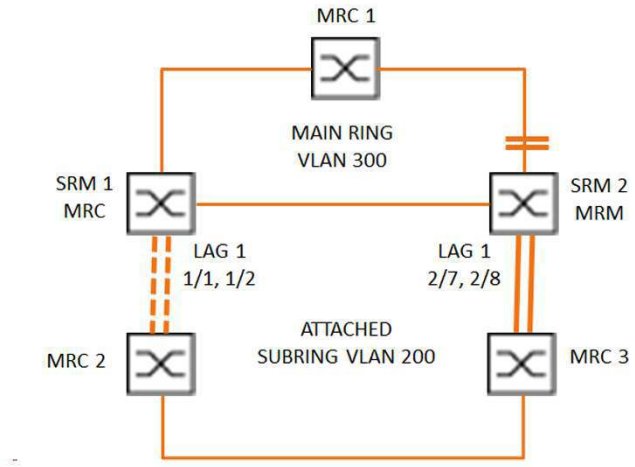



*Figure 57: Subring with Link Aggregation*

The following table describes the device roles as seen in the figure above. The table provides information of how you use the ring ports and Subring ports as LAG ports.

*Table 34: Devices, Ports and Roles*

| Device Name | Ring Port | Main Ring Role | Sub Ring Role | Subring Port |
|---|---|---|---|---|
| MRC1 | 1/3, 1/4 | MRP client | - | - |
| SRM1 | 1/3, 1/4 | MRP client | Redundant Manager | lag/1 |
| SRM2 | 2/4, 2/5 | MRP manager | Manager | lag/1 |
| MRC2 | lag/1, 1/3 | - | MRP client | - |
| MRC3 | lag/1, 1/3 | - | MRP client | - |

### MRP ring configuration

The devices participating in the Main ring are members of VLAN 300.

Perform the following steps:

SRM2

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `mrp domain add default-domain` | Creates a new MRP domain with the ID `default-domain`. |
| `mrp domain modify port primary 2/4` | Specifies port *2/4* as ring port `1`. |
| `mrp domain modify port secondary 2/5` | Specifies port *2/5* as ring port `2`. |
| `mrp domain modify mode manager` | Specifies that the device operates as the *Ring manager*. Do not activate the *Ring manager* function on any other device. |
| `mrp domain modify operation enable` | Activates the MRP-Ring. |
| `mrp domain modify vlan 300` | Specifies the VLAN ID as `300`. |
| `mrp operation` | Enable the *MRP* function in the device. |

MRC1, SRM1

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `mrp domain add default-domain` | Creates a new MRP domain with the ID `default-domain`. |
| `mrp domain modify port primary 1/3` | Specifies port *1/3* as ring port `1`. |
| `mrp domain modify port secondary 1/4` | Specifies port *1/4* as ring port `2`. |
| `mrp domain modify mode client` | Specifies the device role as ring client. |
| `mrp domain modify operation enable` | Activates the MRP-Ring. |
| `mrp domain modify vlan 300` | Specifies the VLAN ID as `300`. |
| `mrp operation` | Enable the *MRP* function in the device. |

### Subring configuration

The devices participating in the attached Sub-ring are members of VLAN 200.

Perform the following steps:

SRM1

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `link-aggregation add lag/1` | Creates a Link Aggregation Group `lag/1`. |

| | |
|---|---|
| `link-aggregation modify lag/1 addport 1/1` | Adds port *1/1* to the Link Aggregation Group. |
| `link-aggregation modify lag/1 addport 1/2` | Adds port *1/2* to the Link Aggregation Group. |
| `link-aggregation modify lag/1 adminmode` | Activate the Link Aggregation Group. |

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `sub-ring add 1` | Creates a new subring with the subring ID `1`. |
| `sub-ring modify 1 name SRM1` | Assign the name `SRM1` to the subring `1`. |
| `sub-ring modify 1 mode redundant-manager vlan 200 port lag/1` | Assign the device the role of `Sub-ring redundant manager`in subring `1`. If the subring is closed, then the device blocks the ring port. VLAN `200` is the set for the VLAN ID of the domain. The `lag/1` port is set as a member in VLAN `200`. |
| `sub-ring enable 1` | Activate subring `1`. |
| `sub-ring operation` | Enable the global Subring Manager functionality on this device. |

`SRM2`

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `link-aggregation add lag/1` | Creates a Link Aggregation Group `lag/1`. |
| `link-aggregation modify lag/1 addport 2/7` | Adds port *2/7* to the Link Aggregation Group. |
| `link-aggregation modify lag/1 addport 2/8` | Adds port *2/8* to the Link Aggregation Group. |
| `link-aggregation modify lag/1 adminmode` | Activate the Link Aggregation Group. |

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `sub-ring add 1` | Creates a new subring with the subring ID `1`. |
| `sub-ring modify 1 mode manager vlan 200 port lag/1` | Assign the device the role of `Subring manager` in subring `1`. VLAN `200` is the set for the VLAN ID of the domain. The `lag/1` port is set as a member in VLAN `200`. |
| `sub-ring modify 1 name SRM2` | Assign the name `SRM2` to the subring `1`. |
| `sub-ring enable 1` | Activate subring `1`. |
| `sub-ring operation` | Enable the global Subring Manager functionality on this device. |

MRC 2, 3

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `mrp domain add default-domain` | Creates a new MRP domain with the ID `default-domain`. |
| `mrp domain modify port primary lag/1` | Specifies port `lag/1` as ring port `1`. |
| `mrp domain modify port secondary 1/3` | Specifies port *1/3* as ring port `2`. |
| `mrp domain modify mode client` | Specifies the device role as ring client. |
| `mrp domain modify operation enable` | Activates the MRP-Ring. |
| `mrp domain modify vlan 200` | Specifies the VLAN ID as `200`. |
| `mrp operation` | Enable the *MRP* function in the device. |

### Disable STP

Disable the *Spanning Tree* function on every port that you specified as an MRP or Sub-ring port. The following example uses port *1/3*.

Perform the following steps:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/3` | Change to the interface configuration mode of interface *1/3*. |
| `no spanning-tree operation` | Disable the *Spanning Tree* function on the port. |

# 12.11 Ring/Network Coupling

Based on a ring, the *Ring/Network Coupling* function couples rings or network segments redundantly. *Ring/Network Coupling* connects 2 rings/network segments through 2 separate paths.

When the devices in the coupled network are Hirschmann devices, the *Ring/Network Coupling* function supports the coupling following ring protocols in the primary and secondary rings:

- HIPER Ring
- Fast HIPER Ring
- MRP

The *Ring/Network Coupling* function can also couple network segments of a bus and mesh structures.

## 12.11.1 Methods of Ring/Network Coupling

### The One-Switch coupling

Two ports of **one** device in the first ring/network connect to one port each of two devices in the second ring/network (see figure 58). In the One-Switch coupling method, the main line forwards data and the device blocks the redundant line.

When the main line no longer functions, the device immediately unblocks the redundant line. When the main line is restored, the device blocks data on the redundant line. The main line forwards data again.

The ring coupling detects and handles an error within 500 ms (typically 150 ms).

### The Two-Switch coupling

One port each from **two** devices in the first ring/network connect to one port each of two devices in the second ring/network segment (see figure 60).

The device in the redundant line and the device in the main line use control packets to inform each other about their operating states, using the Ethernet or a control line.

When the main line no longer functions, the redundant device (Stand-by) immediately unblocks the redundant line. As soon as the main line is restored, the device on the main line informs the redundant device of this. The Stand-by device blocks data on the redundant line. The main line forwards data again.

The ring coupling detects and handles an error within 500 ms (typically 150 ms).

The type of coupling configuration is primarily determined by the network topological and the desired level of availability (see table 35).

*Table 35: Selection criteria for the configuration types for redundant coupling*

| | One-Switch coupling | Two-Switch coupling | Two-Switch coupling with Control line |
|---|---|---|---|
| Application | The 2 devices are in impractical topological positions.<br>Therefore, putting a link between them would involve a lot of effort for two-Switch coupling. | The 2 devices are in practical topological positions.<br>Installing a control line would involve a lot of effort. | The 2 devices are in practical topological positions.<br>Installing a control line would not involve much effort. |
| Disadvantage | If the Switch configured for the redundant coupling becomes inoperable, then no connection remains between the networks. | More effort for connecting the 2 devices to the network (compared with one-Switch coupling). | More effort for connecting the two devices to the network (compared with one-Switch and two-Switch coupling). |
| Advantage | Less effort involved in connecting the 2 devices to the network (compared with two-Switch coupling). | When one of the devices configured for the redundant coupling becomes inoperable, the coupled networks are still connected. | When one of the devices configured for the redundant coupling becomes inoperable, the coupled networks are still connected.<br>The partner determination between the coupling devices occurs more secure and faster than without the control line. |

### 12.11.2 Prepare the Ring/Network Coupling

Using the images in the dialog you define the role of the devices within the *Ring/Network Coupling*.

In the following screen shots and diagrams, the following conventions are used:
- Blue boxes and lines indicate devices or connections of the items currently being described.
- Solid lines indicate a main connection.
- Dash lines indicate a stand-by connection.
- Dotted lines indicate the control line.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Ring/Network Coupling* dialog.
- ☐ In the *Mode* frame, *Type* option list, select the required radio button.
  - *one-switch coupling*
  - *two-switch coupling, master*
  - *two-switch coupling, slave*
  - *two-switch coupling with control line, master*
  - *two-switch coupling with control line, slave*

**Note:** Refrain from combining the Rapid Spanning Tree Protocol and *Ring/Network Coupling*.

### One-Switch coupling

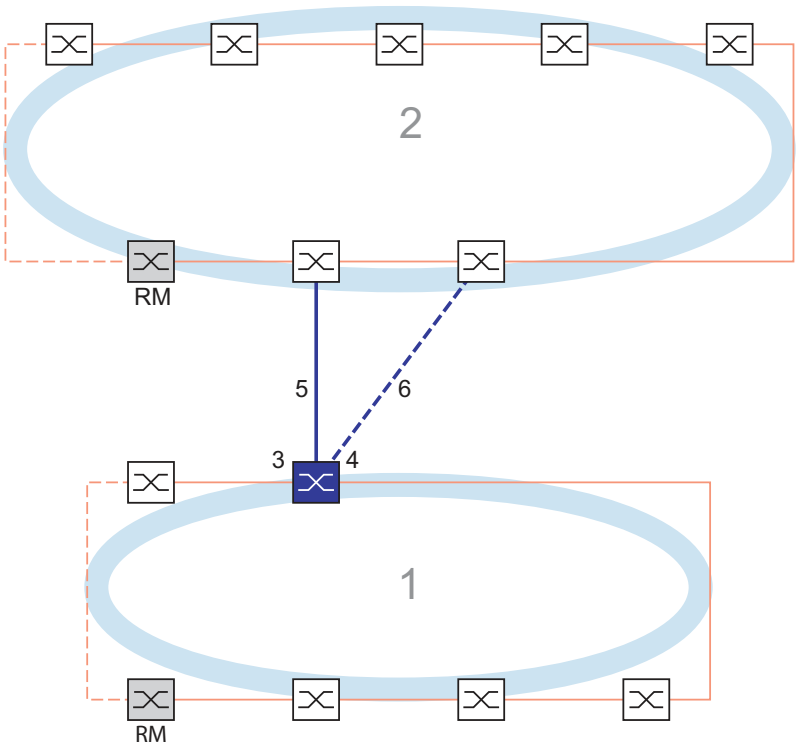



*Figure 58: Example of One-Switch coupling*
*1: Ring*
*2: Backbone*
*3: Partner coupling port*
*4: Coupling port*
*5: Main line*
*6: Redundant line*

The main line, indicated by the solid blue line, which is connected to the partner coupling port provides coupling between the two networks in the normal mode of operation. If the main line is inoperable, then the redundant line, indicated by the dashed blue line, which is connected to the coupling port takes over the ring/network coupling. **One** switch performs the coupling switch-over.

The following settings apply to the device displayed in blue in the selected graphic.

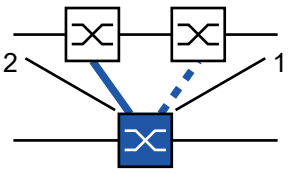



*Figure 59: One-switch-coupling*
*1: Coupling port*
*2: Partner coupling port*

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Ring/Network Coupling* dialog.
- ☐ In the *Mode* frame, *Type* option list, select the `one-switch coupling` radio button.

**Note:** Configure the *Partner coupling port* and the ring ports on different ports.

- In the *Coupling port* frame, select the port on which you connect the redundant line in the *Port* drop-down list.
- In the *Partner coupling port* frame, select the port on which you connect the main line in the *Port* drop-down list.
- To enable the function, select the *On* radio button in the *Operation* frame.
- Save the changes temporarily. To do this, click the ✓ button.
- Connect the redundant line to the Partner coupling port.
  In the *Partner coupling port* frame, the *State* field displays the status of the Partner coupling port.
- Connect the main line to the Coupling port.
  In the *Coupling port* frame, the *State* field displays the status of the Coupling port.

In the *Information* frame, the *Redundancy available* field displays if the redundancy is available. The *Configuration failure* field displays if the settings are complete and correct.

For the coupling ports, perform the following steps:

**Note:** The following settings are required for the coupling ports.

- Open the *Basic Settings > Port* dialog, *Configuration* tab.
- For the ports selected as the coupling ports, specify the settings according to the parameters in the following table.
- Save the changes temporarily. To do this, click the ✓ button.

*Table 36: Port settings for ring ports*

| Port type | Bit rate | Port on | Automatic configuration | Manual configuration |
|---|---|---|---|---|
| TX | 100 Mbit/s | marked | unmarked | *100 Mbit/s FDX* |
| TX | 1 Gbit/s | marked | marked | – |
| Optical | 100 Mbit/s | marked | unmarked | *100 Mbit/s FDX* |
| Optical | 1 Gbit/s | marked | marked | – |
| Optical | 2.5 Gbit/s | marked | – | *2.5 Gbit/s FDX* |
| Optical | 10 Gbit/s | marked | – | *10 Gbit/s* |

If you have configured VLANs on the coupling ports, then you specify the VLAN settings on the coupling and partner coupling ports. To do this, perform the following steps:

- Open the *Switching > VLAN > Port* dialog.
- Change the *Port-VLAN ID* setting to the value of the VLAN ID configured on the ports.
- Unmark the *Ingress filtering* checkbox for both coupling ports.
- Open the *Switching > VLAN > Configuration* dialog.
- To tag the redundant connections for `VLAN 1` and VLAN Membership, enter the value `T` in the cells corresponding to both coupling ports on the `VLAN 1` row.
- Save the changes temporarily. To do this, click the ✓ button.

The coupling devices send the redundancy packets with the highest priority on `VLAN 1`.

- In the *Configuration*frame, *Redundancy mode* option list, specify the type of redundancy:
  - With the *redundant ring/network coupling* setting, either the main line or the redundant line is active. The setting lets the devices toggle between both lines.
  - When you activate the *extended redundancy* setting, the main line and the redundant line are active simultaneously. The setting lets you add redundancy to the coupling network. When the connection between the coupling devices in the second network becomes inoperable the coupling devices continue to transmit and receive data.

**Note:** During the reconfiguration period, packet duplications can occur. Therefore, if your devices detect package duplications, then select this setting.

The *Coupling mode* describes the type of the backbone network to which you connect the ring network (see figure 58).

- In the *Configuration* frame, *Coupling mode* option list, specify the type of the second network:
  - If you connect to a ring network, then select the *ring coupling* radio button.
  - If you connect to a bus or mesh structure, then select the *network coupling* radio button.
- Save the changes temporarily. To do this, click the button.

Reset the coupling settings to the default state. To do this, perform the following steps:

- Click the button and then the *Reset* item.

### Two-Switch coupling

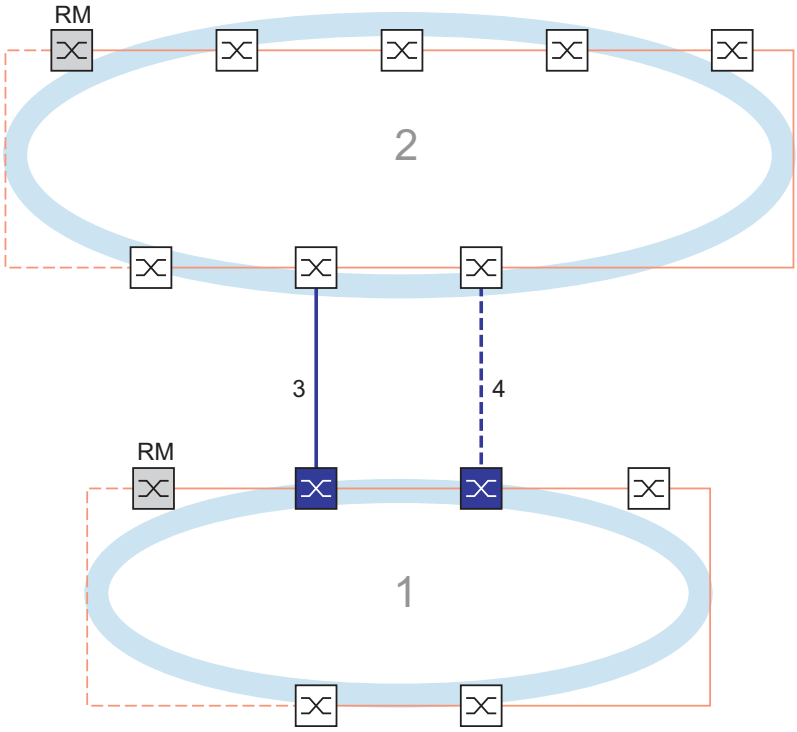



*Figure 60: Example of Two-Switch coupling*
*1: Ring*
*2: Backbone*
*3: Main line*
*4: Redundant line*

The coupling between 2 networks is performed by the main line, indicated by the solid blue line. If the main line or one of the adjacent devices becomes inoperable, then the redundant line, indicated by the dashed black line, takes over the network coupling. The coupling is performed by 2 devices.

The devices send control packages to each other over the Ethernet.

The primary device connected to the main line, and the stand-by device connected to the redundant line are partners with regard to the coupling.

☐ Connect the 2 partners using the ring ports.

### Two-Switch coupling, Primary device

The following settings apply to the device displayed in blue in the selected graphic.

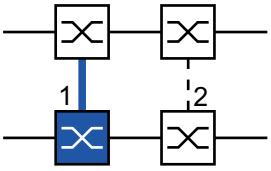



*Figure 61: Two-Switch coupling, Primary device*
*1: Coupling port*
*2: Partner coupling port*

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Ring/Network Coupling* dialog.
- ☐ In the *Mode* frame, *Type* option list, select the `two-switch coupling, master` radio button.
- ☐ In the *Coupling port* frame, select the port on which you connect the network segments in the *Port* drop-down list.
  Configure the *Coupling port* and the ring ports on different ports.
- ☐ To enable the function, select the *On* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ☑ button.
- ☐ Connect the main line to the *Coupling port*.
  In the *Coupling port* frame, the *State* field displays the status of the Coupling port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.

In the *Information* frame, the *Redundancy available* field displays if the redundancy is available. The *Configuration failure* field displays if the settings are complete and correct.

**Note:** If you operate the *Ring manager* function and a two-switch coupling function on the same device, then there is the possibility of creating a loop.

To help prevent continuous loops while the connections are in operation on the ring coupling ports, perform one of the following actions. The device sets the port state of the coupling port to “off”:

- disable the operation
- change the configuration

For the coupling ports, perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- ☐ For the ports selected as the coupling ports, specify the settings according to the parameters in the following table.
- ☐ Save the changes temporarily. To do this, click the ☑ button.

*Table 37: Port settings for ring ports*

| Port type | Bit rate | Port on | Automatic configuration | Manual configuration |
|---|---|---|---|---|
| TX | 100 Mbit/s | `marked` | `unmarked` | *`100 Mbit/s FDX`* |
| TX | 1 Gbit/s | `marked` | `marked` | – |
| Optical | 100 Mbit/s | `marked` | `unmarked` | *`100 Mbit/s FDX`* |
| Optical | 1 Gbit/s | `marked` | `marked` | – |
| Optical | 2.5 Gbit/s | `marked` | – | *`2.5 Gbit/s FDX`* |
| Optical | 10 Gbit/s | `marked` | – | *`10 Gbit/s`* |

If you have configured VLANs on the coupling ports, then you specify the VLAN settings on the coupling and partner coupling ports. To do this, perform the following steps:

- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ Change the *Port-VLAN ID* setting to the value of the VLAN ID configured on the ports.
- ☐ Unmark the *Ingress filtering* checkbox for both coupling ports.
- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ To tag the redundant connections for `VLAN 1` and VLAN Membership, enter the value `T` in the cells corresponding to both coupling ports on the `VLAN 1` row.
- ☐ Save the changes temporarily. To do this, click the ☑ button.

The coupling devices send the redundancy packets with the highest priority on `VLAN 1`.

### Two-Switch coupling, Stand-by device

The following settings apply to the device displayed in blue in the selected graphic.

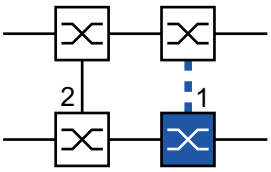



*Figure 62: Two-Switch coupling, Stand-by device*
*1: Coupling port*
*2: Partner coupling port*

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Ring/Network Coupling* dialog.
- ☐ In the *Mode* frame, *Type* option list, select the `two-switch coupling, slave` radio button.
- ☐ In the *Coupling port* frame, select the port on which you connect the network segments in the *Port* drop-down list.
  Configure the *Coupling port* and the ring ports on different ports.
- ☐ To enable the function, select the *On* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ☑ button.
- ☐ Connect the redundant line to the *Coupling port*.
  In the *Coupling port* frame, the *State* field displays the status of the Coupling port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.

In the *Information* frame, the *Redundancy available* field displays if the redundancy is available. The *Configuration failure* field displays if the settings are complete and correct.

**Note:** If you operate the *Ring manager* function and a two-switch coupling function on the same device, then there is the possibility of creating a loop.

To help prevent continuous loops while the connections are in operation on the ring coupling ports, perform one of the following actions. The device sets the port state of the coupling port to “off”:

- disable the operation
- change the configuration

For the coupling ports, perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- ☐ For the ports selected as the coupling ports, specify the settings according to the parameters in the following table.
- ☐ Save the changes temporarily. To do this, click the ☑ button.

*Table 38: Port settings for ring ports*

| Port type | Bit rate | Port on | Automatic configuration | Manual configuration |
|---|---|---|---|---|
| TX | 100 Mbit/s | `marked` | `unmarked` | *`100 Mbit/s FDX`* |
| TX | 1 Gbit/s | `marked` | `marked` | – |
| Optical | 100 Mbit/s | `marked` | `unmarked` | *`100 Mbit/s FDX`* |
| Optical | 1 Gbit/s | `marked` | `marked` | – |
| Optical | 2.5 Gbit/s | `marked` | – | *`2.5 Gbit/s FDX`* |
| Optical | 10 Gbit/s | `marked` | – | *`10 Gbit/s`* |

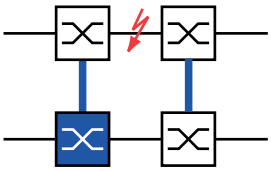
If you have configured VLANs on the coupling ports, then you specify the VLAN settings on the coupling and partner coupling ports. To do this, perform the following steps:

- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ Change the *Port-VLAN ID* setting to the value of the VLAN ID configured on the ports.
- ☐ Unmark the *Ingress filtering* checkbox for both coupling ports.
- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ To tag the redundant connections for `VLAN 1` and VLAN Membership, enter the value `T` in the cells corresponding to both coupling ports on the `VLAN 1` row.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

The coupling devices send the redundancy packets with the highest priority on `VLAN 1`.

Specify the *Redundancy mode* and *Coupling mode* settings. To do this, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Ring/Network Coupling* dialog.
- ☐ In the *Configuration* frame, *Redundancy mode* option list, select one of the following radio buttons:
  - ▶ *redundant ring/network coupling*
    With this setting, either the main line or the redundant line is active. The setting lets the devices toggle between both lines.
  - ▶ *extended redundancy*
    With this setting, the main line and the redundant line are active simultaneously. The setting lets you add redundancy to the second network. When the connection between the coupling devices in the second network becomes inoperable, the coupling devices continue to transmit and receive data.

    During the reconfiguration period, packet duplications can occur. Therefore, select this setting only if your devices detect package duplications.
- ☐ In the *Configuration* frame, *Coupling mode* option list, select one of the following radio buttons:
  - ☐ If you connect to a ring network, then select the *ring coupling* radio button.
  - ☐ If you connect to a bus or mesh structure, then select the *network coupling* radio button.

  The *Coupling mode* describes the type of the backbone network to which you connect the ring network (see figure 60).
- ☐ Save the changes temporarily. To do this, click the ✓ button.

Reset the coupling settings to the default state. To do this, perform the following steps:

- ☐ Click the ≡ button and then the *Reset* item.

**Two-Switch Coupling with Control Line**

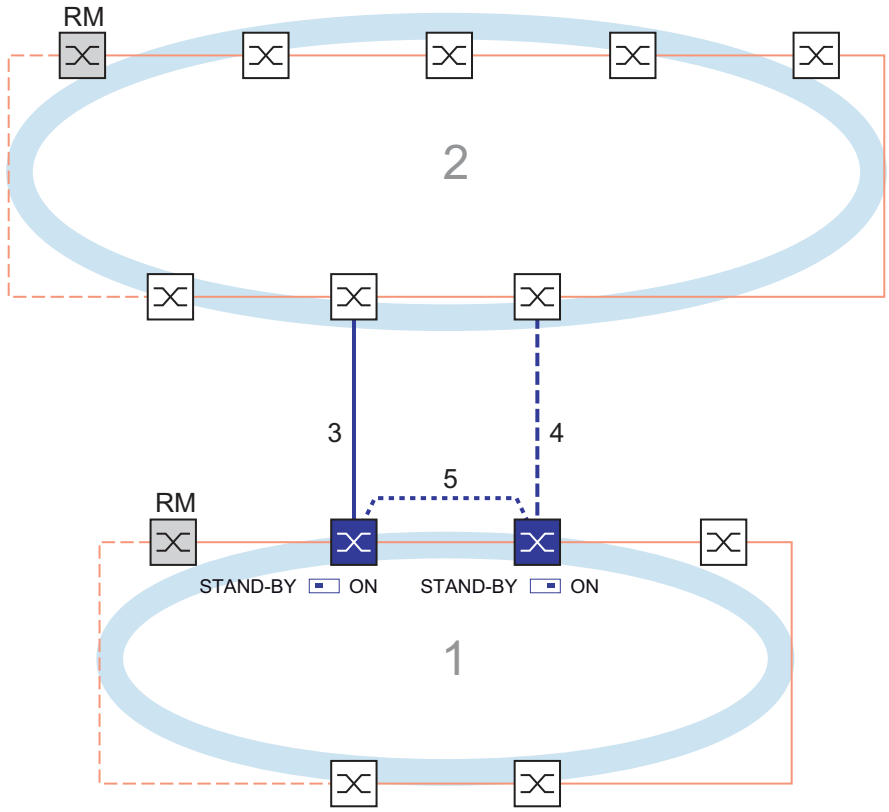



*Figure 63: Example of Two-Switch coupling with control line*
*1: Ring*
*2: Backbone*
*3: Main line*
*4: Redundant line*
*5: Control line*

The coupling between 2 networks is performed by the main line, indicated by the solid blue line. If the main line or one of the adjacent devices become inoperable, then the redundant line, indicated by the dashed blue line, takes over coupling the 2 networks. The ring coupling is performed by 2 devices.

The devices send control packets over a control line indicated by the dotted blue line in the figure below (see figure 64).

The primary device connected to the main line, and the stand-by device connected to the redundant line are partners with regard to the coupling.

☐ Connect the 2 partners using the ring ports.

### Two-Switch coupling with Control Line, Primary device

The following settings apply to the device displayed in blue in the selected graphic.

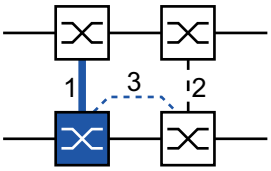



*Figure 64: Two-Switch coupling with Control Line, Primary device*
*1: Coupling port*
*2: Partner coupling port*
*3: Control line*

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Ring/Network Coupling* dialog.
- ☐ In the *Mode* frame, *Type* option list, select the `two-switch coupling with control line, master` radio button.
- ☐ In the *Coupling port* frame, select the port on which you connect the network segments in the *Port* drop-down list.
  Configure the *Coupling port* and the ring ports on different ports.
- ☐ In the *Control port* frame, select the port on which you connect the control line in the *Port* drop-down list.
  Configure the *Coupling port* and the ring ports on different ports.
- ☐ To enable the function, select the *On* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the button.
- ☐ Connect the redundant line to the Coupling port.
  In the *Coupling port* frame, the *State* field displays the status of the Coupling port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.
- ☐ Connect the control line to the Control port.
  In the *Control port* frame, the *State* field displays the status of the Control port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.

In the *Information* frame, the *Redundancy available* field displays if the redundancy is available. The *Configuration failure* field displays if the settings are complete and correct.

**Note:** If you operate the *Ring manager* function and a two-switch coupling function on the same device, then there is the possibility of creating a loop.

To help prevent continuous loops while the connections are in operation on the ring coupling ports, perform one of the following actions. The device sets the port state of the coupling port to “off”:

- disable the operation
- change the configuration

For the coupling ports, perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- ☐ For the ports selected as the coupling ports, specify the settings according to the parameters in the following table.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

*Table 39: Port settings for ring ports*

| Port type | Bit rate | Port on | Automatic configuration | Manual configuration |
|---|---|---|---|---|
| TX | 100 Mbit/s | marked | unmarked | *100 Mbit/s FDX* |
| TX | 1 Gbit/s | marked | marked | – |
| Optical | 100 Mbit/s | marked | unmarked | *100 Mbit/s FDX* |
| Optical | 1 Gbit/s | marked | marked | – |
| Optical | 2.5 Gbit/s | marked | – | *2.5 Gbit/s FDX* |
| Optical | 10 Gbit/s | marked | – | *10 Gbit/s* |

If you have configured VLANs on the coupling ports, then you specify the VLAN settings on the coupling and partner coupling ports. To do this, perform the following steps:

- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ Change the *Port-VLAN ID* setting to the value of the VLAN ID configured on the ports.
- ☐ Unmark the *Ingress filtering* checkbox for both coupling ports.
- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ To tag the redundant connections for `VLAN 1` and VLAN Membership, enter the value `T` in the cells corresponding to both coupling ports on the `VLAN 1` row.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

The coupling devices send the redundancy packets with the highest priority on `VLAN 1`.

### Two-Switch coupling with Control Line, Stand-by device

The following settings apply to the device displayed in blue in the selected graphic.

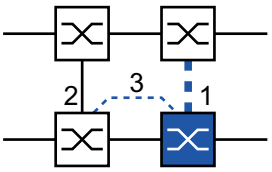



*Figure 65: Two-Switch coupling with Control Line, Stand-by device*
*1: Coupling port*
*2: Partner coupling port*
*3: Control line*

Perform the following steps:

- ☐ Open the *Switching* > *L2-Redundancy* > *Ring/Network Coupling* dialog.
- ☐ In the *Mode* frame, *Type* option list, select the `two-switch coupling with control line, slave` radio button.
- ☐ In the *Coupling port* frame, select the port on which you connect the network segments in the *Port* drop-down list.
  Configure the *Coupling port* and the ring ports on different ports.
- ☐ In the *Control port* frame, select the port on which you connect the control line in the *Port* drop-down list.
  Configure the *Coupling port* and the ring ports on different ports.
- ☐ To enable the function, select the *On* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
- ☐ Connect the redundant line to the Coupling port.
  In the *Coupling port* frame, the *State* field displays the status of the Coupling port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.
- ☐ Connect the control line to the Control port.
  In the *Control port* frame, the *State* field displays the status of the Control port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.

In the *Information* frame, the *Redundancy available* field displays if the redundancy is available. The *Configuration failure* field displays if the settings are complete and correct.

**Note:** If you operate the *Ring manager* function and a two-switch coupling function on the same device, then there is the possibility of creating a loop.

To help prevent continuous loops while the connections are in operation on the ring coupling ports, perform one of the following actions. The device sets the port state of the coupling port to “off”:

- disable the operation
- change the configuration

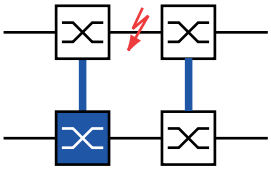
For the coupling ports, perform the following steps:

- ☐ Open the *Switching* > *VLAN* > *Port* dialog.
- ☐ Change the *Port-VLAN ID* setting to the value of the VLAN ID configured on the ports.
- ☐ Unmark the *Ingress filtering* checkbox for both coupling ports.
- ☐ Open the *Switching* > *VLAN* > *Configuration* dialog.
- ☐ To tag the redundant connections for `VLAN 1` and VLAN Membership, enter the value `T` in the cells corresponding to both coupling ports on the `VLAN 1` row.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

The coupling devices send the redundancy packets with the highest priority on `VLAN 1`.

Specify the *Redundancy mode* and *Coupling mode* settings. To do this, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Ring/Network Coupling* dialog.
- ☐ In the *Configuration* frame, *Redundancy mode* option list, select one of the following radio buttons:
  - ▶ `redundant ring/network coupling`
    With this setting, either the main line or the redundant line is active. The setting lets the devices toggle between both lines.
  - ▶ `extended redundancy`
    With this setting, the main line and the redundant line are active simultaneously. The setting lets you add redundancy to the second network. When the connection between the coupling devices in the second network becomes inoperable, the coupling devices continue to transmit and receive data.

    During the reconfiguration period, packet duplications can occur. Therefore, select this setting only if your devices detect package duplications.
- ☐ In the *Configuration* frame, *Coupling mode* option list, select one of the following radio buttons:
  - ☐ If you connect to a ring network, then select the *ring coupling* radio button.
  - ☐ If you connect to a bus or mesh structure, then select the *network coupling* radio button.

  The *Coupling mode* describes the type of the backbone network to which you connect the ring network (see figure 63).
- ☐ Save the changes temporarily. To do this, click the button.

Reset the coupling settings to the default state. To do this, perform the following steps:

- ☐ Click the button and then the *Reset* item.

# 12.12 RCP

Industrial applications require your networks to have high availability. This also involves maintaining deterministic, short interruption times for the communication in cases where a network device becomes inoperable.

A ring topology provides short transition times with a minimal use of resources. However, ring topology brings the challenge of coupling these rings together redundantly.

The Redundant Coupling Protocol *RCP* lets you couple rings that are operating with one of the following redundancy protocols:

- MRP
- HIPER ring
- RSTP

The *RCP* function also lets you couple multiple secondary rings to a primary ring (see figure 66). Only the switches which couple the rings require the *RCP* function.

You can also use devices other than Hirschmann devices within the coupled networks.

The *RCP* function uses a master and a slave device to transport data between the networks. Only the master device forwards frames between the rings.

Using Hirschmann proprietary multicast messages, the *RCP* master and slave devices inform each other about their operating state. Configure the devices in the ring which are not coupling devices to forward the following multicast addresses:

- `01:80:63:07:00:09`
- `01:80:63:07:00:0A`

Connect the master and slave devices as direct neighbors.

You use 4 ports per device to create the redundant coupling. Install the coupling devices with 2 inner and 2 outer ports in each network.

- The inner port connects the master and slave devices together.
- The outer port connects the devices to the network.

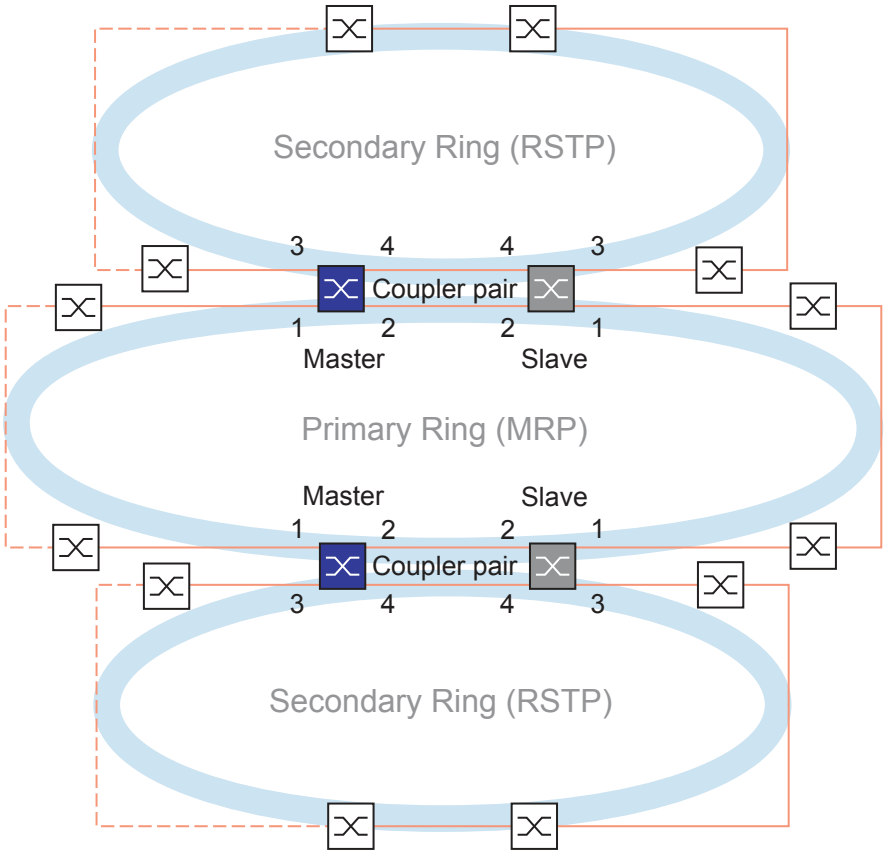



*Figure 66: Example of a two-switch redundant coupling*
*1: Outer coupling port in the primary ring*
*2: Inner coupling port in the primary ring*
*3: Outer coupling port in the secondary ring*
*4: Inner coupling port in the secondary ring*

When the role is set to the value *auto*, the coupler devices automatically selects its role as *master* or *slave*. When you want a permanent master or slave device, configure the roles manually.

If the master is no longer reachable using the inner coupling ports, then the slave device waits for the timeout period to expire before taking over the master role. During the specified timeout period, the slave attempts to reach the master using the outer coupling ports. When the master is still not reachable, the slave assumes the master role. To maintain stability in the network connected to the outer coupling ports, configure the timeout period for a longer duration than the recovery time in the coupled rings.

**Note:** Disable RSTP on the *RCP* redundant coupling inner and outer ports not connected to the RSTP ring. In the example configuration, you disable RSTP on ports 1 and 2 of every device.

### 12.12.1 Application example for RCP coupling

The Hirschmann devices support the two switch Redundant Coupling Protocol method. You can use the *RCP* function to provide a network installed in a train for example. The network provides information for the passengers about the train location or the different stops on the line. The network can also help provide passenger safety, for example using video surveillance.

The primary rings in the figure represent an *MRP* ring network within a car. The secondary rings in the figure are RSTP ring networks. Each ring contains 4 devices (see figure 67).

To simplify the train topology in the figure, the *MRP* ring ports and the *RCP* inner and outer ports are assigned the same port numbers. Specify the same values for the parameters of the ports according to their function in the network. For example, specify ports *1/1* and *1/2* on Switch 1D and 1C as MRP ring ports. Port *1/4* as an *RCP* inner port, and port *1/3* as an *RCP* outer port.

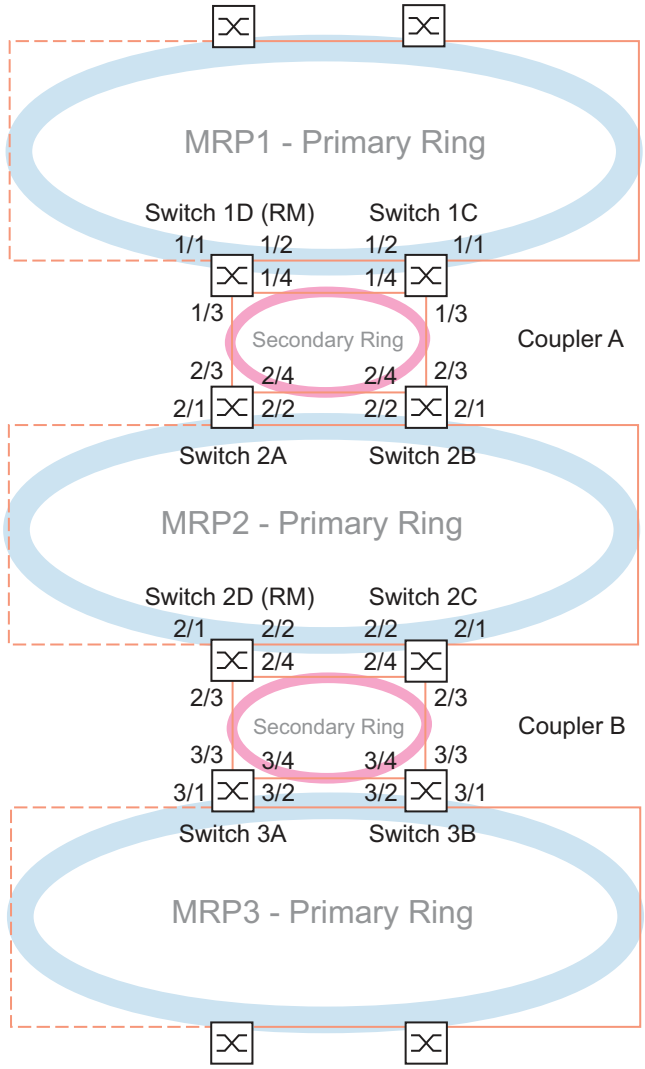



*Figure 67: Redundant Coupling Protocol Train Topology*

*The following list specifies roles of the ports on each device.*
*1: ports 1 and 2 are MRP ring ports*
*2: port 3 is an RCP outer port*
*3: port 4 is an RCP inner port*

The following steps describe how to specify the parameters for Switch 1D in Coupler A. Configure the other devices used for Coupler A and the devices used in Coupler B in the same manner.

### Disable the RSTP function in the MRP Ring

*MRP* and RSTP do not work together. Therefore, deactivate the RSTP function on the *RCP* ports used in the *MRP* ring. In the example configuration, ports `x/1` and `x/2` are used for the *MRP* ring. Activate the RSTP function only on the *RCP* inner and outer ports used in the secondary ring. For example, activate the RSTP function on ports `x/3` and `x/4`.

Perform the following steps:

- ☐ Open the *Switching* > *L2-Redundancy* > *Spanning Tree* > *Port* dialog, *CIST* tab.
- ☐ In the default setting, the RSTP function is active on the ports. To deactivate the RSTP function on the *MRP* ring ports, unmark the *STP active* checkboxes for ports `x/1` and `x/2`.
- ☐ Open the *Switching* > *L2-Redundancy* > *Spanning Tree* > *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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface x/1` | Change to the interface configuration mode of interface `x/1`. |
| `no spanning-tree mode` | Disable the *Spanning Tree* function on the port. |
| `exit` | Change to the Configuration mode. |
| `interface x/2` | Change to the interface configuration mode of interface `x/2`. |
| `no spanning-tree mode` | Disable the *Spanning Tree* function on the port. |
| `exit` | Change to the Configuration mode. |
| `spanning-tree operation` | Enable the *Spanning Tree* function. |

### Specify the Ring Master in the MRP ring

In the figure, Switch D of each *MRP* ring is designated as the ring manger (see figure 67). Specify the other switches in the rings as ring clients.

Perform the following steps:

- ☐ Open the *Switching* > *L2-Redundancy* > *MRP* dialog.
- ☐ Specify the first ring port in the *Ring port 1* frame.
  In the *Port* drop-down list, select port `x/1`.
- ☐ Specify the second ring port in the *Ring port 2* frame.
  In the *Port* drop-down list, select port `x/2`.
- ☐ To designate the device as the Ring Manager, activate the function in the *Ring manager* frame.
- ☐ To enable the function, select the *On* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `mrp domain add default-domain` | Create a new *MRP* domain with the ID `default-domain`. |
| `mrp domain modify port primary x/1` | Specify port `x/1` as ring port `1`. |
| `mrp domain modify port secondary x/2` | Specify port `x/2` as ring port `2`. |
| `mrp domain modify mode manager` | Specify that the device operates as the *Ring manager*. For the other devices in the ring, leave the default setting. |
| `mrp domain modify operation enable` | Enable the *MRP* function. |

### Specify the devices in the redundant coupler

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > RCP* dialog.
- ☐ Specify the *Inner port* in the *Primary ring/network* frame. Select port `x/2`.
- ☐ Specify the *Outer port* in the *Primary ring/network* frame. Select port `x/1`.
- ☐ Specify the *Inner port* in the *Secondary ring/network* frame. Select port `x/4`.
- ☐ Specify the *Outer port* in the *Secondary ring/network* frame. Select port `x/3`.

- ☐ To enable the function, select the *On* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `redundant-coupling port primary inner x/2` | Specify port `x/2` as the primary inner port. |
| `redundant-coupling port primary outer x/1` | Specify port `x/1` as the primary outer port. |
| `redundant-coupling port secondary inner x/4` | Specify port `x/4` as the secondary inner port. |
| `redundant-coupling port secondary outer x/3` | Specify port `x/3` as the secondary outer port. |
| `redundant-coupling operation` | Enable the *RCP* function in the device. |
| `copy config running-config nvm` | Save the current settings in the non-volatile memory (`nvm`) in the “selected” configuration profile. |

# 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, RIP, 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 40: OSI reference model*

| | | |
|---|---|---|
| 7 | Application | Access to communication services from an application program |
| 6 | Presentation | Definition of the syntax for data communication |
| 5 | Session | Set up and breakdown of connections by synchronization and organization of the dialog |
| 7 | Transport | Specification of the terminal connection, with the necessary transport quality |
| 3 | Network | Transparent data exchange between two transport entities |
| 2 | Data-Link | Access to physical media and detection of transmission errors |
| 1 | Physical | Transmission of bit strings via physical media |

What does the data exchange on the Layer 3 mean in comparison with the data exchange on the Layer 2?

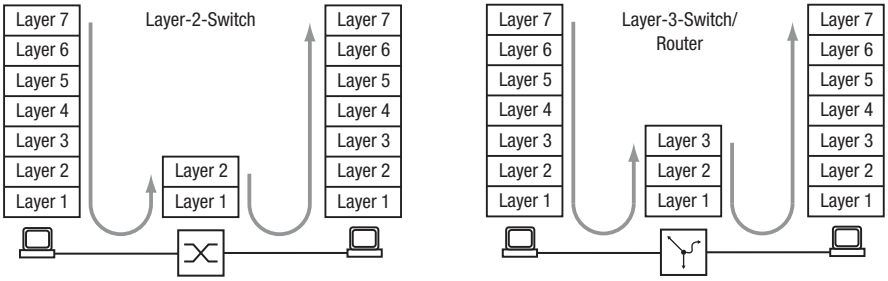



*Figure 68: Data Transport by a Switch and a Router in the OSI Reference Model's Layers*

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 247 “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 69: 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.

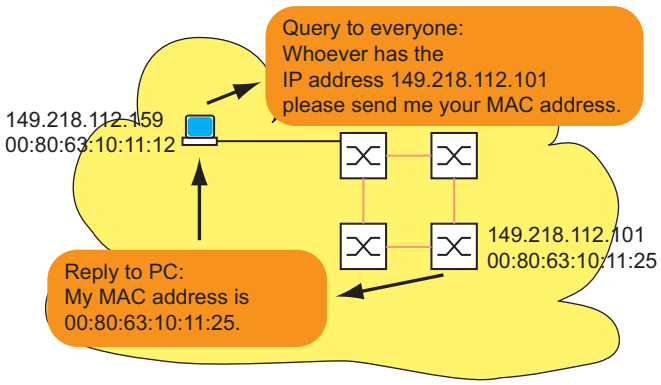



*Figure 70: ARP request and reply*

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.

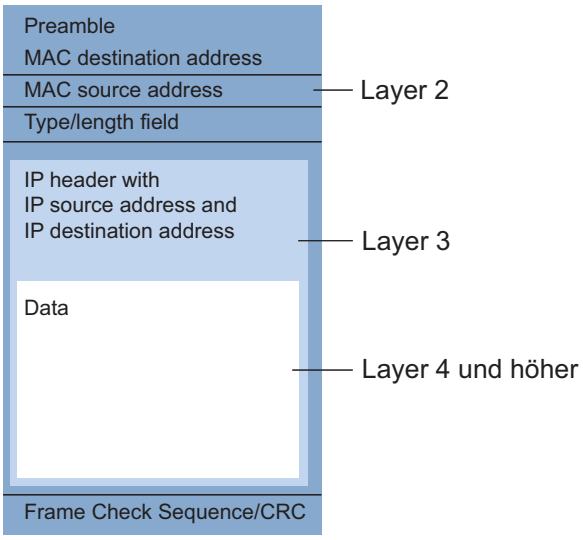



*Figure 71: Structure of a data packet from the ISO/OSI reference model perspective*

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.

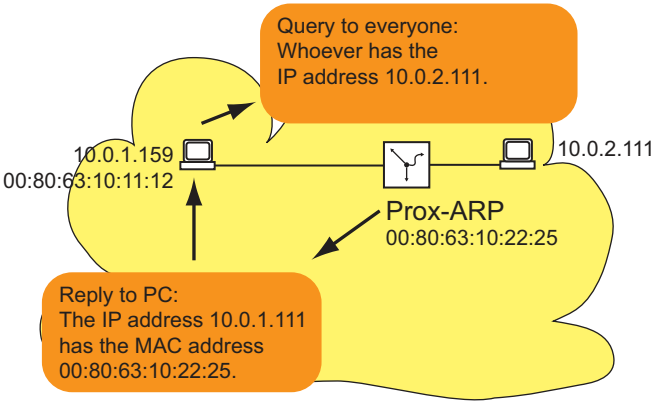



*Figure 72: Proxy ARP function*

The *Proxy ARP* function is available on the router interfaces on which you enable the proxy ARP.

### 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 41: IP address classes*

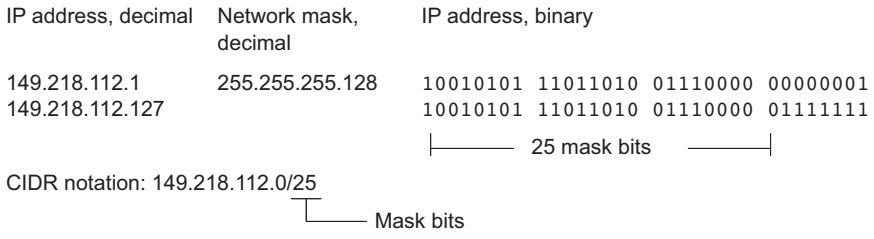
| Class | Network part | Host part | Address range |
|---|---|---|---|
| A | 1 byte | 3 bytes | 1.0.0.0 … 126.255.255.255 |
| B | 2 bytes | 2 bytes | 128.0.0.0 … 191.255.255.255 |
| C | 3 bytes | 1 byte | 192.0.0.0 … 223.255.255.255 |
| D | | | 224.0.0.0 … 239.255.255.255 |
| E | | | 240.0.0.0 … 255.255.255.255 |

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:




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 Net-directed Broadcasts

A net-directed Broadcast is an IP data packet that a device sends to the network Broadcast address of a network to contact every receiver of the network. A net-directed Broadcast is sent as a MAC Unicast packet in a transfer network. When the router locally responsible for this network supports net-directed Broadcasts, it transmits this data packet as a MAC Broadcast packet into its local network. With VLAN-based router interfaces it transmits the packet to every port that is member in the VLAN of the Router interface.[1]

Thus net-directed Broadcasts can relieve your transfer network of the multiple IP Unicasts that would be necessary to replace a net-directed Broadcast.

When the router does not support net-directed Broadcasts or you deactivate this function for a router interface, the router discards IP data packets received on the network Broadcast address of the router interface. With multinetting, this also applies to the secondary IP addresses of the router interface.

### 13.2.4 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.

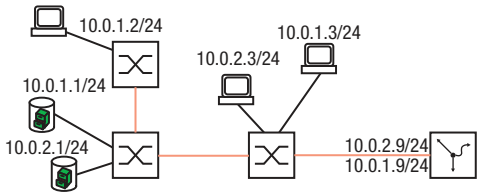



*Figure 73: Example of multinetting*

1.The device determines the Broadcast address from its interface IP address and the related netmask. For example, when a router interface has the IP address 192.168.1.1 and the netmask 255.255.255.0, it is responsible for network 192.168.1.0/24. The network Broadcast address here is 192.168.1.255.

# 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 74).

Example: Connecting two production cells

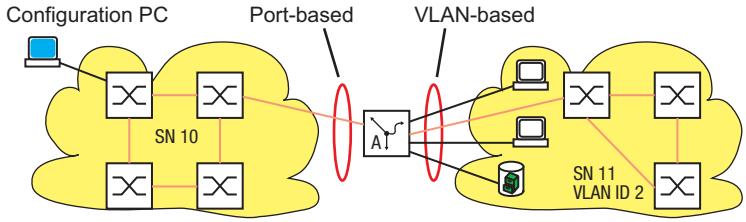



*Figure 74: Static routes*

## 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 74).

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 75) you will find an example of the simplest case of a routing application with port-based router interfaces.

### Configuration of the router interfaces

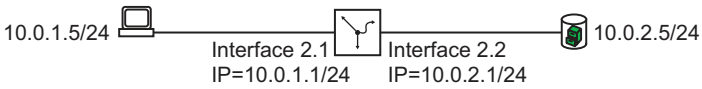



*Figure 75: Simplest case of a route*

Perform the following steps:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 2/1` | Change to the interface configuration mode of interface `2/1`. |
| `ip address primary 10.0.1.1 255.255.255.0` | Assign the interface its primary IP parameters. |
| `ip routing` | Activate the *Routing* function on this interface. |
| `exit` | Change to the Configuration mode. |
| `interface 2/2` | Change to the interface configuration mode of interface `2/2`. |
| `ip address primary 10.0.2.1 255.255.255.0` | Assign the interface its IP parameters. |
| `ip routing` | Activate the *Routing* function on this interface. |
| `ip netdirbcast` | Enable the transmission of net-directed broadcasts for this interface. |
| `no ip icmp unreachable` | Disable sending of ICMP Destination Unreachable messages on this interface. |
| `exit` | Change to the Configuration mode. |
| `ip routing` | Enable the *Routing* function globally. |
| `exit` | Change to the Privileged EXEC mode. |
| `show ip interface 2/1` | 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.................................  diabled
MAC Address...............................  EC:E5:55:F6:3E:09
IP MTU....................................  1500
ICMP Redirect.............................  enabled
ICMP Unreachable..........................  disabled
Netdirected Broadcast.....................  disabled(int2/2 enabled)
Admin State...............................  enabled
Link State................................  up
```

`show ip route all` — 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.

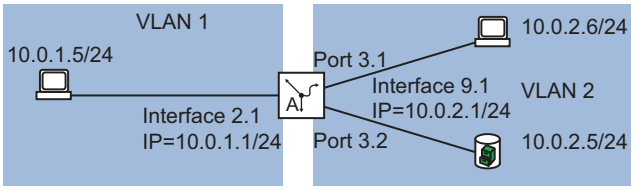



*Figure 76: VLAN-based router interface*

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` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 2` | Create a VLAN by entering the VLAN ID. The VLAN ID range is between `1` to `4042`. |
| `name 2 VLAN2` | Assign the name `VLAN2` to the VLAN. |
| `routing add 2` | Create a virtual router interface and activate the *Routing* function on this interface. |
| `exit` | Change to the Privileged EXEC mode. |
| `show ip interface` | Check the entry for the virtual router interface. |

```
Interface IP Address      IP Mask
--------- --------------- ---------------
vlan/2    0.0.0.0         0.0.0.0
```

| | |
|---|---|
| `configure` | Change to the Configuration mode. |
| `interface vlan/2` | Change to the interface configuration mode of interface `vlan/2`. |
| `ip address primary 10.0.2.1 255.255.255.0` | Assign the IP parameters to the virtual router interface. |
| `ip routing` | Activate the *Routing* function on this interface. |
| `ip netdirbcast` | Enable the transmission of net-directed broadcasts for this interface. See 248 “Net-directed Broadcasts”. |
| `exit` | Change to the Configuration mode. |

```
interface 3/1
```
Change to the interface configuration mode of interface 3/1.

```
vlan participation exclude 1
```
Remove port 3/1 from VLAN 1. In the default setting, every port is assigned to VLAN 1.

```
vlan participation include 2
```
Declare port 3/1 a member of VLAN 2.

```
vlan pvid 2
```
Specify port VLAN ID 2. Therefore, the device assigns data packets that the port receives without a VLAN tag to VLAN 2.

```
exit
```
Change to the Configuration mode.

```
interface 3/2
```
Change to the interface configuration mode of interface 3/2.

```
vlan participation exclude 1
```
Remove port 3/2 from VLAN 1. In the default setting, every port is assigned to VLAN 1.

```
vlan participation include 2
```
Declare port 3/2 a member of VLAN 2.

```
vlan pvid 2
```
Specify port VLAN ID 2. Therefore, the device assigns data packets that the port receives without a VLAN tag to VLAN 2.

```
exit
```
Change to the Configuration mode.

```
ip routing
```
Enable the *Routing* function globally.

```
exit
```
Change to the Privileged EXEC mode.

```
show vlan id 2
```
Check your entries in the static VLAN table.

```
VLAN ID.............................2
VLAN Name..........................VLAN002
VLAN Creation TIme.................0 days, 01:47:17
VLAN Type..........................static

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
...
3/1         Include   Include      Untagged
3/2         Include   Include      Untagged
3/3         Exclude   Autodetect   Untagged
3/4         Exclude   Autodetect   Untagged
...
```

```
show vlan port
```
Check the VLAN-specific port settings.

```
          Port    Acceptable   IngressInterface VLAN ID Frame Types  Filtering   Priority
--------- ------- ------------ ----------- --------
...
3/1       2       admit all    disable       0
3/2       2       admit all    disable       0
3/3       1       admit all    disable       0
3/4       1       admit all    disable       0
...
```

- ☐ 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`.
- ☐ In the *Routing > Interfaces > Configuration* dialog, mark the check box in the *Netdirected broadcasts* column for router interface `vlan/2`.
- ☐ 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.

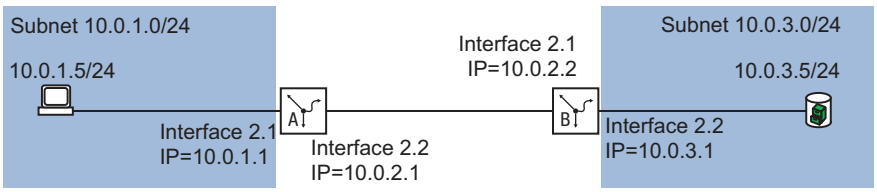



*Figure 77: Static Routing*

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 75). To do this, perform the following steps:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `ip route add 10.0.3.0 255.255.255.0 10.0.2.2` | Create the static routing entry |
| `ip routing` | Enable the *Routing* function globally. |
| `exit` | Change to the Privileged EXEC mode. |
| `show ip route all` | Verify the routing table: |

```
Network Address  Protocol Next Hop IP   Next Hop If  Pref Active
---------------  -------- ------------  ------------ ---- -------
       10.0.1.0  Local    10.0.1.1      2/1          1      [x]
       10.0.2.0  Local    10.0.2.1      2/2          1      [x]
       10.0.3.0  Static   10.0.2.2      2/2          1      [x]
```

Enter a static route for router A based on the configuration of the router interface in the previous example (see figure 75):

☐ 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.

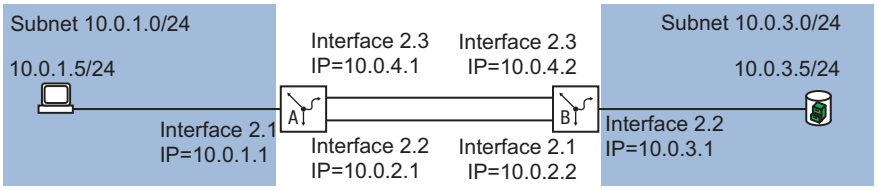



*Figure 78: Redundant static route*

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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 2/3` | Select the port at which you want to connect the redundant route. |
| `ip address primary 10.0.4.1 255.255.255.0` | Assign the IP parameters to the port. |

| | |
|---|---|
| `ip routing` | Activate the *Routing* function on this interface. |
| `exit` | Change to the Configuration mode. |
| `ip route add 10.0.3.0 255.255.255.0 10.0.4.2 preference 2` | Create the static routing entry for the redundant route. The value `2` at the end of the command indicates the Preference value.<br>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 254 “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` | Sets the default preference for static routes. (default setting: `1`) |
| `show ip route all` | Verify the routing table: |

```
Network Address  Protocol Next Hop IP   Next Hop If  Pref Active
---------------  -------- ------------  ------------ ---- -------
       10.0.1.0  Local    10.0.1.1      2/1          1      [x]
       10.0.2.0  Local    10.0.2.1      2/2          1      [x]
       10.0.3.0  Static   10.0.2.2      2/2          1      [x]
       10.0.3.0  Static   10.0.4.2      -            2      [ ]
       10.0.4.0  Local    10.0.4.1      2/3          1      [x]
```

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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `ip route modify 10.0.3.0 255.255.255.0 10.0.2.2 preference 2` | Assigns a Preference of `2` to the existing static routing entry (see on page 254 “Configuration of a simple static route”).<br>When both routes are available, the router uses both routes for the data transmission. |
| `show ip route all` | Verify the routing table: |

```
Network Address  Protocol Next Hop IP   Next Hop If  Pref Active
---------------  -------- ------------  ------------ ---- -------
       10.0.1.0  Local    10.0.1.1      2/1          1      [x]
       10.0.2.0  Local    10.0.2.1      2/2          1      [x]
       10.0.3.0  Static   10.0.2.2      2/2          2      [x]
       10.0.3.0  Static   10.0.4.2      2/3          2      [x]
       10.0.4.0  Local    10.0.4.1      2/3          1      [x]
```

## 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.

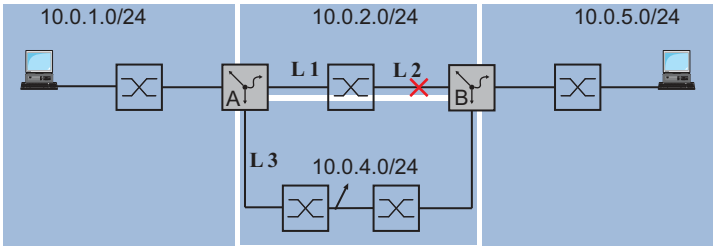



*Figure 79: Example of static route tracking*

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 80).

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:

| Parameter | Router A |
|---|---|
| IP address interface (IF) `1/1` | `10.0.4.1` |
| IP address interface (IF) `1/2` | `10.0.2.1` |
| IP address interface (IF) `1/4` | `10.0.1.112` |
| Netmask | `255.255.255.0` |

| Parameter | Router B |
|---|---|
| IP address interface (IF) `1/2` | `10.0.4.2` |
| IP address interface (IF) `1/3` | `10.0.2.53` |
| IP address interface (IF) `2/2` | `10.0.5.1` |
| Netmask | `255.255.255.0` |

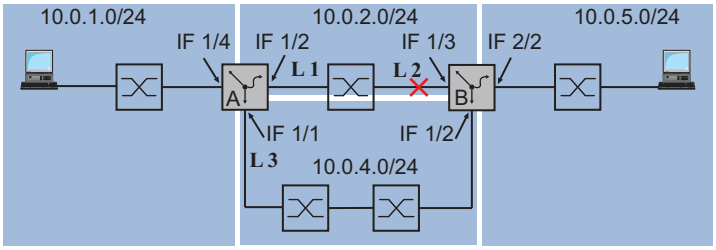



*Figure 80: Configuring static route tracking*

The following list contains prerequisites for further configuration:

- The IP parameters of the router interfaces are configured.
  (see on page 250 “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 261 “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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `track add ping 1` | Create a tracking object with track ID `1`. |
| `track modify ping 1 address 10.0.2.53` | Modify the `ping 1` entry with the IP address `10.0.2.53`. |
| `track modify ping 1 interface 1/2` | Set the source interface number of the ping tracking instance to `1/2`. |
| `track enable ping 1` | Activate the tracking object. |

| | |
|---|---|
| `track add ping 2` | Create a tracking object with track ID `2`. |
| `track modify ping 2 address 10.0.4.2` | Modify the `ping 2` entry with the IP address `10.0.4.2`. |
| `track modify ping 2 interface 1/1` | Set the source interface number of the ping tracking instance to `1/1`. |
| `track enable ping 2` | Activate the tracking object. |
| `exit` | Change to the Privileged EXEC mode. |
| `show track ping` | Verify the entries in the tracking table. |

```
Name   Interface    Intv [ms] Succ  TTL    BR-If   State Active      Inet-Address  Timeout
Miss
------ ------------ --------- ----- ------- --------  ----- ------
ping-1 1/2             1000     2     128       0  up    [x]       10.0.2.53         100     3
ping-2 1/1             1000     2     128       0  down  [x]       10.0.4.2          100     3
```

**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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `ip route add 10.0.5.0 255.255.255.0 10.0.2.53` | Create a static routing entry with the default preference. |
| `ip route add 10.0.5.0 255.255.255.0 10.0.4.2 preference 2` | Create a static routing entry with preference 2. |
| `exit` | Change to the Privileged EXEC mode. |
| `show ip route all` | Verify the routing table: |

```
Network Address  Protocol Next Hop IP   Next Hop If  Pref Active
---------------  -------- ------------  ------------ ---- -------
       10.0.1.0  Local    10.0.1.112    1/4          1      [x]
       10.0.2.0  Local    10.0.2.1      1/2          1      [x]
       10.0.5.0  Static   10.0.2.53     1/2          1      [x]
       10.0.5.0  Static   10.0.4.2      1/2          2      [x]
```

- ☐ 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 42: Static routing entries for router B*

| Destination Network | Destination Netmask | Next Hop | Preference | Track ID |
|---|---|---|---|---|
| 10.0.1.0 | 255.255.255.0 | 10.0.2.1 | 1 | 22 |
| 10.0.1.0 | 255.255.255.0 | 10.0.4.1 | 2 | |

# 13.4 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

## 13.4.1 Interface tracking

With interface tracking the device monitors the link status of:
- physical ports
- Link Aggregation interfaces
- VLAN router interfaces

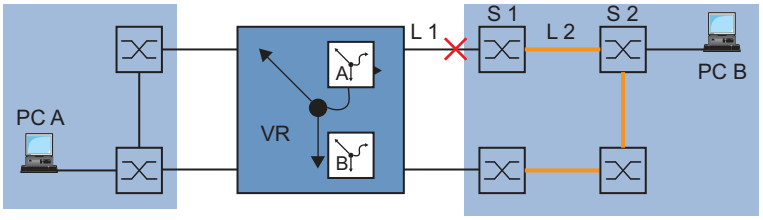



*Figure 81: Monitoring a line with interface tracking*

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.

### 13.4.2 Ping tracking

With ping tracking, the device uses ping requests to monitor the link status to other devices.

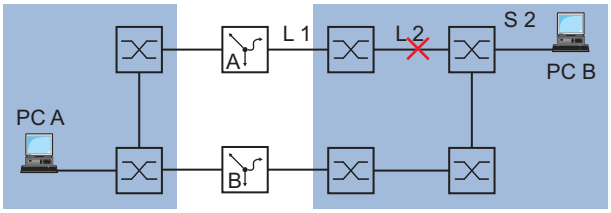



*Figure 82: Monitoring a line with ping tracking*

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.

### 13.4.3 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 264 “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.

### 13.4.4 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 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.

```
enable                                          Change to the Privileged EXEC mode.
configure                                       Change to the Configuration mode.
track add interface 11                          Enter a tracking object in the table.
track modify interface 11 ifnumber 1/1          Specify the parameters for this tracking object.
link-up-delay 3 link-down-delay 0
track enable interface 11                       Activate the tracking object.
Tracking ID interface-11 created  Target interface set to 1/1
  Link Up Delay for target interface set to 3 sec
  Link Down Delay for target interface set to 0 sec
Tracking ID 11 activated
exit                                            Change to the Privileged EXEC mode.
show track interface                            Display the configured tracks.
Name     If-Number  Link-Up-Delay  Link-Down-Delay  State  Active
-------- ---------- -------------  ---------------  -----  ------
if-11     1/1                   0                3   up       [x]
```

### Application example for ping tracking

While the interface tracking monitors the directly connected link (see figure 81), the ping tracking monitors the entire link to device S2 (see figure 82).

☐ 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.

```
enable                                          Change to the Privileged EXEC mode.
configure                                       Change to the Configuration mode.
track add ping 21                               Enter a tracking object in the table.
track modify ping 21    ifnumber  1/2           Specify the parameters for this tracking object.
   address   10.0.2.53
   interval  500
   miss      3
   success   2
   timeout   100
```

```
track enable ping 21                          Activate the tracking object.
Tracking ID ping-21 created
  Target IP address set to 10.0.2.53
  Interface used for sending pings to target set to 1/2
  Ping interval for target set to 500 ms
  Max. no. of missed ping replies from target set to 3
  Min. no. of received ping replies from target set to 2
  Timeout for ping replies from target set to 100 ms
Tracking ID 21 activated
exit                                          Change to the Privileged EXEC mode.
show track                                    Display the configured tracks.
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 14:00:03
Description..................................
```

### Application example for logical tracking

The figure (see figure 83) 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:

| Parameter | Value |
|---|---|
| Operand No. 1 (track ID) | 21 |
| Operand No. 2 (track ID) | 22 |

Prerequisites for further configuration:

- The ping tracking objects for operands 1 and 2 are configured (see on page 263 “Application example for ping tracking”).

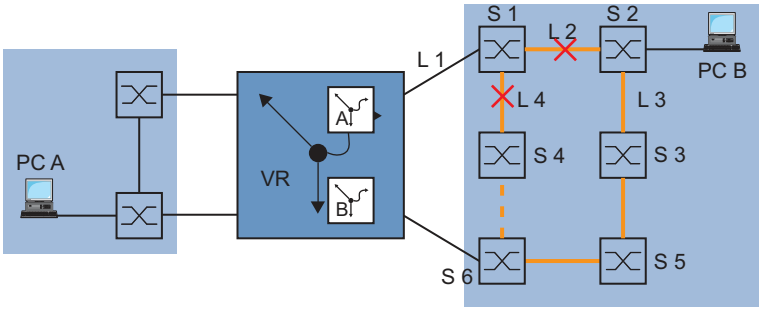



*Figure 83: Monitoring the accessibility of a device in a redundant ring*

☐ Set up a logical tracking object as an OR link. To do this, perform the following steps:

☐ Open the *Routing > Tracking > Configuration* dialog.

☐ 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `track add logical 31` | Enter a tracking object in the table. |
| `track modify logical 31 ping-21 or ping-22` | Enter the parameters for the tracking object. |
| `track enable logical 31` | Activate the tracking object. |

```
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` | Change to the Privileged EXEC mode. |
| `show track ping 21` | Display the configured tracks. |

```
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` Display the configured tracks.

```
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` Display the configured tracks.

```
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..................................
```

### Application example for logical tracking

The figure (see figure 83) 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:

| Parameter | Value |
|---|---|
| Operand No. 1 (track ID) | 21 |
| Operand No. 2 (track ID) | 22 |

Prerequisites for further configuration:

- The ping tracking objects for operands 1 and 2 are configured (see on page 263 “Application example for ping tracking”).

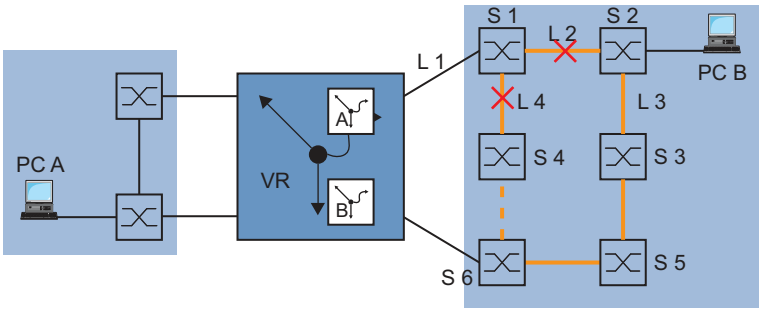



*Figure 84: Monitoring the accessibility of a device in a redundant ring*

☐ Set up a logical tracking object as an OR link. To do this, perform the following steps:

☐ Open the *Routing > Tracking > Configuration* dialog.

☐ 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `track add logical 31` | Enter a tracking object in the table. |
| `track modify logical 31 ping-21 or ping-22` | Enter the parameters for the tracking object. |
| `track enable logical 31` | Activate the tracking object. |

```
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
```

Change to the Privileged EXEC mode.

```
show track ping 21
```

Display the configured tracks.

```
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
```

Display the configured tracks.

```
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
```

Display the configured tracks.

```
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..................................
```

# 13.5 VRRP/HiVRRP

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.

In many cases, such as Voice over IP, Video over IP, or industrial controllers these long failover times are unacceptable.

Hirschmann has further developed VRRP into the Hirschmann Virtual Router Redundancy Protocol (HiVRRP). With the appropriate configuration, HiVRRP provides a maximum failover time of 400 milliseconds.

Thanks to this failover time, HiVRRP helps to enable the use of “gateway redundancy” in time-sensitive applications. Even in tunnel controllers that require failover times of less than 1 second, you improve the network availability with this form of “gateway redundancy”.

**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.

## 13.5.1 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.

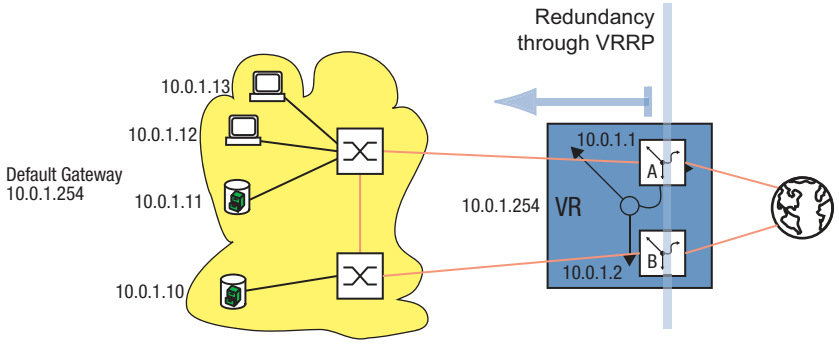



*Figure 85: Illustration of the virtual router*

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.

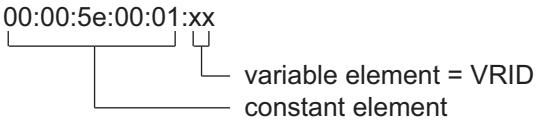



*Figure 86: Virtual MAC address*

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 43: Who shall be the master?*

| | |
|---|---|
| 1. | The IP address owner as it has the higher VRRP priority (255) by definition. |
| 2. | The VRRP router with the higher VRRP priority. |
| 3. | When the priorities are the same, the VRRP router with the higher IP address. |

**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.
- Virtual router MAC address
  The MAC address of the virtual router instance (see figure 86).
- 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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `ip routing` | Enable the *Routing* function globally. |
| `ip vrrp operation` | Enables VRRP globally. |
| `interface 1/3` | Change to the interface configuration mode of interface `1/3`. |
| `ip address primary 10.0.1.1 255.255.255.0` | Specifies the primary IP address and the netmask of the router interface. |
| `ip routing` | Enables the *Routing* function on this interface. |
| `ip vrrp add 1` | Creates the VRID for the first virtual router on this port. |
| `ip vrrp virtual-address add 1 10.0.1.100` | Assigns virtual router `1` its IP address. |
| `ip vrrp 1 priority 200` | Assigns virtual router `1` the router priority `200`. |

- ☐ You specify every active VRRP port the same way.
- ☐ You also perform the same configuration on the backup router.

### 13.5.2 HiVRRP

HiVRRP provides a number of mechanisms for shortening the failover times or reducing the number of Multicasts:

- shorter advertisement intervals
- link-down notification
- pre-empt delay
- Unicast advertisement
- domains

As defined in RFC 3768, the VRRP master sends IP Multicast messages (advertisements) at intervals of 1 second to the backup routers. When 3 intervals pass without the backup routers receiving an advertisement, the backup routers initiate a master router election process to select a new master. VRRP has a typical failover time of 3 to 4 seconds.

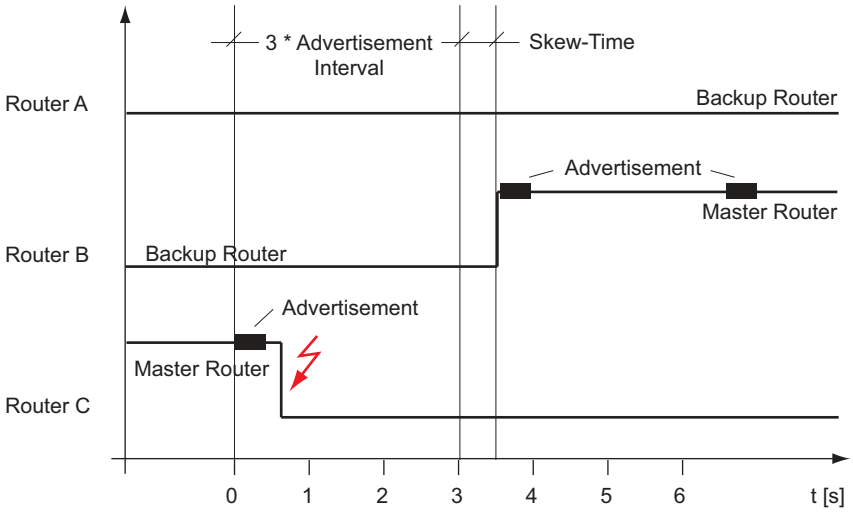



*Figure 87: Master router <-> backup router failover times according to RFC 2338*
*VRRP priority router A = 64*
*VRRP priority router B = 128*
*VRRP priority router C = 254*

To be able to achieve faster failover times, Hirschmann developed HiVRRP which shortens the cycle for sending the IP Multicast message to as little as 0.1 seconds. You thus achieve failover times that are up to 10 times faster than VRRP.

The router supports up to 16 VRRP router interfaces with this shortened sending cycle.

- HiVRRP skew time
  The HiVRRP skew time uses the VRRP priority of the master router to determine how long a HiVRRP backup router waits, after declaring the HiVRRP master down, until it initiates the master router election process.
  HiVRRP skew time = (256 - VRRP priority) / 256 * advertisement interval
  Times displayed in milliseconds.
- HiVRRP master down interval
  The HiVRRP master down interval uses the advertisement interval of the HiVRRP master router to specify the time the elapse before a HiVRRP backup router declares the HiVRRP master down.
  HiVRRP master down interval = 3 * advertisement interval + HiVRRP skew time
  Times displayed in milliseconds.

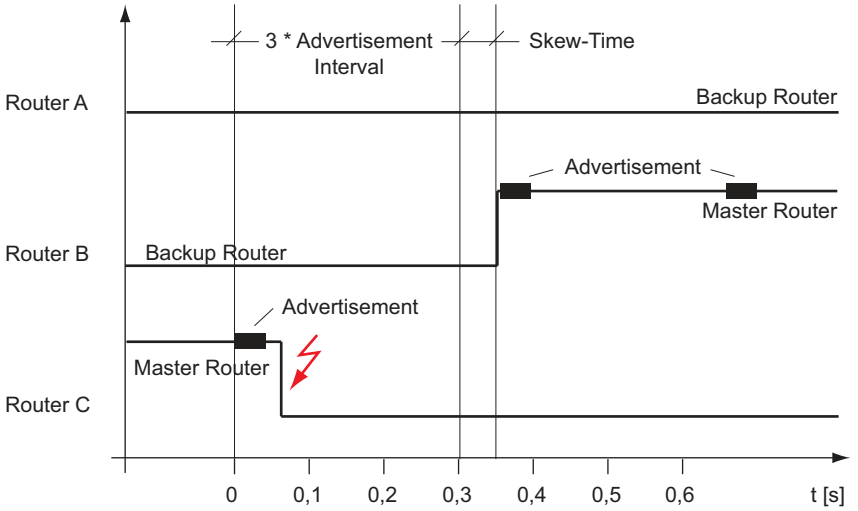



*Figure 88: Master router <-> backup router failover times according to HiVRRP*
*VRRP priority router A = 64*
*VRRP priority router B = 128*
*VRRP priority router C = 254*

Another option provided by HiVRRP for shortening the failover times dramatically is the link-down notification. When the virtual router consists of 2 VRRP routers, you use this function. When 2 VRRP routers are participating, it is sufficient to send the link-down notification in the form of a Unicast message. In contrast to the Multicast message, the Unicast message travels beyond the boundaries of the subnetwork. This means that in cases where the data link is down to your own subnetwork, the link-down notification also travels through other subnetworks to reach the second router of the virtual router.

As soon as HiVRRP detects that the data link is down, it sends the link-down notification to the second router through a different route. The second router takes over the master function immediately after receiving the link-down notification.

In the pre-empt mode, the backup router takes over the master role from the master router as soon as the backup router receives an advertisement from the master router in which the VRRP priority of the master router is lower than its own.

Thus, the pre-empt mode enables a failover to a better router. However, dynamic routing procedures take a certain amount of time to react to changed routes and refill their routing table.

To help protect against losing packets during this time, delayed failover (pre-empt delay) from the master router to the backup router enables the dynamic routing procedure to fill the routing tables.

HiVRRP provides an additional advantage for networks with devices that have difficulties with higher volumes of Multicasts. When using up to 2 HiVRRP routers, instead of sending advertisements in the form of Multicasts, HiVRRP sends the advertisements in the form of Unicast data packets on the VRRP destination address.

**Note:** When you want the advantages of HiVRRP, only use VRRP routers equipped with the HiVRRP function from Hirschmann in the virtual router.

### 13.5.3 HiVRRP Domains

Large HiVRRP domains with a flat network structure enable you to:
- use the HiVRRP routers very rapid failover for redundancy
- use the available bandwidth more effectively
- specify more than 16 VRRP router interfaces for each router using HiVRRP
- operate Multicast-sensitive end devices in large HiVRRP networks

An HiVRRP instance is a router interface specified as HiVRRP with functions that HiVRRP contains. In an HiVRRP domain you combine multiple HiVRRP instances of the routers into one administrative unit. You nominate one HiVRRP instance as the supervisor of the HiVRRP domain. This supervisor regulates the behavior of the HiVRRP instances in its domain.
- The supervisor sends its advertisements on behalf of every HiVRRP instance in its domain.
- The supervisor assigns itself the master role and the other HiVRRP instances the backup role.

See figure 89 for an example of a flat network structure. Every cross-VLAN data stream passes through the ring.

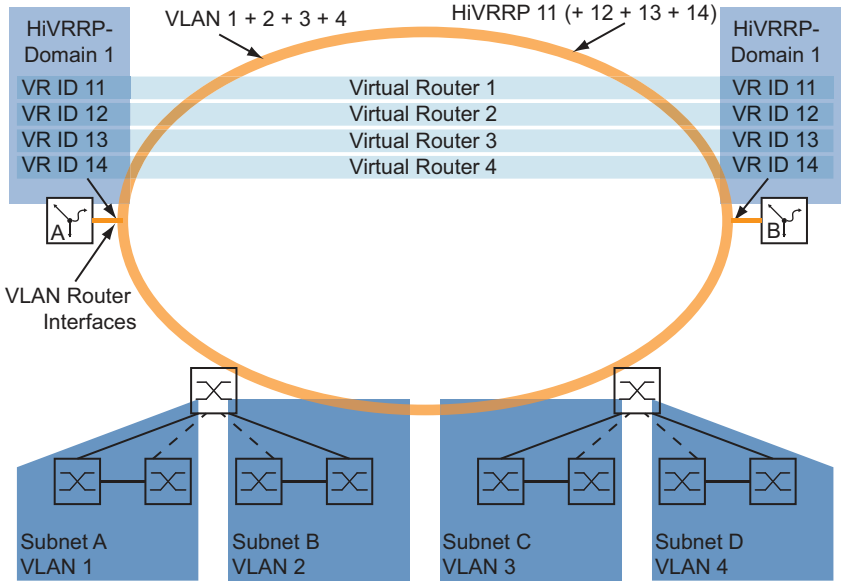



*Figure 89: Example of how a HiVRRP domain is used*

#### Configuration of HiVRRP domains

The configuration of HiVRRP domains consists of the following steps:
- Create VLANs
- Specify VLAN router interfaces
- Assign the IP addresses to the router interfaces

- Specify HiVRRP instances
  - Activate every VRRP instance
  - Assign an IP address to every instance
    Within a router, you either specify every instance as IP address owners, or every instance as an IP address non-owner.
  - Assign a priority to the supervisor
    Assign the supervisors different priorities so that the VRRP routers agree on a master router.
  - Enable every HiVRRP instance
  - Assign an interface to the domain for every instance
  - Specify the sending interval of the supervisor
- Configure the HIPER-Ring for applications as in the above example
- Define the Ring ports as members of the VLANs
- Enable the *Routing* and *VRRP* functions globally

### Example of configuration of HiVRRP domains

Example of possible settings for the application in figure 89:

*Table 44: Configuration of the Switches in the subnetwork*

| Subnetwork | IP address range | VLAN | VLAN ID |
|---|---|---|---|
| A | 10.0.11.0/24 | 1 | 11 |
| B | 10.0.12.0/24 | 2 | 12 |
| C | 10.0.13.0/24 | 3 | 13 |
| D | 10.0.14.0/24 | 4 | 14 |

*Table 45: Configuration of the 2 routers*

| Virtual router | VR ID | IP address of the virtual router | Router interface of router A: IP address | Router interface of router B: IP address | VLAN ID |
|---|---|---|---|---|---|
| 1 | 11 | 10.0.11.1/24 | 10.0.11.2/24 | 10.0.11.3/24 | 11 |
| 2 | 12 | 10.0.12.1/24 | 10.0.12.2/24 | 10.0.12.3/24 | 12 |
| 3 | 13 | 10.0.13.1/24 | 10.0.13.2/24 | 10.0.13.3/24 | 13 |
| 4 | 14 | 10.0.14.1/24 | 10.0.14.2/24 | 10.0.14.3/24 | 14 |

☐ Set up the VLAN router interface and assign an IP address. To do this, perform the following steps:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 11` | Create a VLAN by entering the VLAN ID. |
| `name 11 VLAN1` | Assign the name `VLAN1` to the VLAN `11`. |
| `routing add 11` | Specify VLAN `11` as a routing VLAN. |
| `exit` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `ip address primary 10.0.11.2 255.255.255.0` | Assigns the interface its IP parameters. |
| `ip routing` | Enables the *Routing* function on this interface. |
| `exit` | Change to the Configuration mode. |
| `interface vlan/11` | Change to the interface configuration mode of interface `vlan/11`. |
| `ip address primary 10.0.12.2 255.255.255.0` | Assigns the interface its IP parameters. |
| `ip routing` | Enables the *Routing* function on this interface. |
| `exit` | Change to the Configuration mode. |

☐ Set up the virtual router and configure the port. To do this, perform the following steps:

| | |
|---|---|
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `ip vrrp add 1` | Creates the VRID for the first virtual router on this port. |
| `ip vrrp 1 virtual-address add 1 10.0.11.1` | Assigns virtual router `1` its IP address. |
| `ip vrrp modify 1 priority 200` | Assigns virtual router `1` the router priority `200`. |
| `ip vrrp modify 1 domain-id 1` | Assigns the HiVRRP instance to domain `1`. |
| `ip vrrp modify 1 domain-role supervisor` | Assigns the HiVRRP domain role to the interface. |
| `ip vrrp modify 1 interval 100` | Assigns the HiVRRP notification interval to the interface. |
| `ip vrrp enable 1` | Enables the first virtual router on this port. |
| `exit` | Change to the Configuration mode. |

```
exit                                                    Change to the Privileged EXEC mode.
show ip vrrp interface 1/1 1                            Displays the configuration of VLAN 11.
VRRP instance information
-------------------------
Admin State..................................... enabled
State........................................... init
Virtual MAC Address............................ 00:00:5e:00:01:01
Base Priority.................................. 100
Current Priority............................... 100
Advertisement Interval (milliseconds).......... 100
Pre-empt Mode.................................. enable
Accept ICMP Echo Requests...................... enable
Preeption Delay (seconds)...................... 0
Advertisement Address.......................... 224.0.0.18
Notification Address........................... 0.0.0.0
Current Master Address......................... 0.0.0.0
Master Candidate Address....................... 0.0.0.0
Domain ID...................................... 1
Domain Role.................................... supervisor
Domain Status.................................. supervisor down
```

☐ Set up the Ring port as a member of the VLAN. To do this, perform the following steps:

```
enable                                                  Change to the Privileged EXEC mode.
configure                                               Change to the Configuration mode.
interface 1/2                                           Change to the interface configuration mode of
                                                        interface 1/2.
vlan participation include 11                           Assign the interface to the VLAN.
exit                                                    Change to the Configuration mode.
exit                                                    Change to the Privileged EXEC mode.
show vlan id 11                                         Displays the configuration of VLAN 11.
VRRP preferences
-------------------------
VLAN ID........................ 11
VLAN Name.....................  VLAN1
VLAN Type...................... static
VLAN Creation Time.............  0 days, 00:00:06 (System Uptime)

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         -         Autodetect   Untagged
1/2         Include   Include      Untagged
1/3         -         Autodetect   Untagged
1/4         -         Autodetect   Untagged
```

Enable the *Routing* and *VRRP* functions globally. To do this, perform the following steps:

```
enable                                                  Change to the Privileged EXEC mode.
configure                                               Change to the Configuration mode.
ip routing                                              Enable the Routing function globally.
ip vrrp                                                 Enables VRRP globally.
```

### 13.5.4 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.

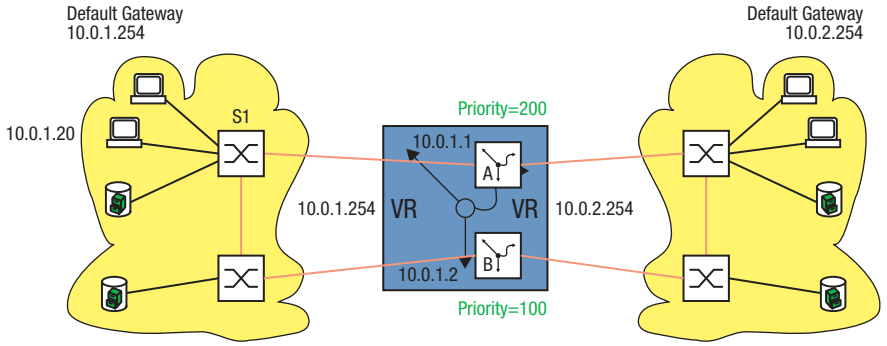



*Figure 90: Virtual router with load sharing*

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.

### 13.5.5 VRRP with Multinetting

The router lets you combine VRRP with Multinetting.

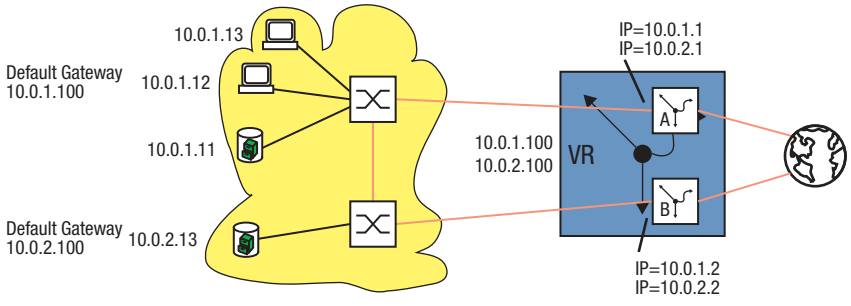



*Figure 91: Virtual router with multinetting*

Configure VRRP with multinetting on the basis of an existing VRRP configuration (see figure 85).
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.

| | |
|---|---|
| `Interface 2/3` | Select the port at which you want to configure multinetting. |
| `ip address secondary 10.0.2.1 255.255.255.0` | Assign the second IP address to the port. |
| `ip vrrp virtual-address add 1 10.0.2.100` | Assign a second IP address to the virtual router with the VRID `1`. |

- ☐ Perform the same configuration on the backup router.

# 13.6 RIP

The Routing Information Protocol (RIP) is a routing protocol based on the distance vector algorithm. It is used for the dynamic creation of the routing table for routers.

When you start a router, the router only knows the networks directly connected to it, and it sends this routing table to the neighboring routers. At the same time, it requests the routing tables of its neighboring routers. The router adds this information to its routing table and thus learns which networks can be accessed via which routers, and how much effort is involved in this. In order to detect changes in the network (when a router fails or starts), the routers regularly exchange the routing tables, usually every 30 seconds.

The costs, also known as the metric, refer to the work involved in reaching a particular network. RIP uses the Hop count for this, which describes the number of routers that are traversed along the path to the destination network. The name 'distance vector' is derived from the fact that the distance (metric) is the criterion for determining the route, and the direction is specified by the next hop (vector). The next hop refers to the neighboring router along the path to the destination address.

An entry in the routing table consists of the address of the next hop, the destination address and the metric. The RIP routing table contains the direct route to the destination. This is the route with the smallest metric and the longest suitable network mask prefix.

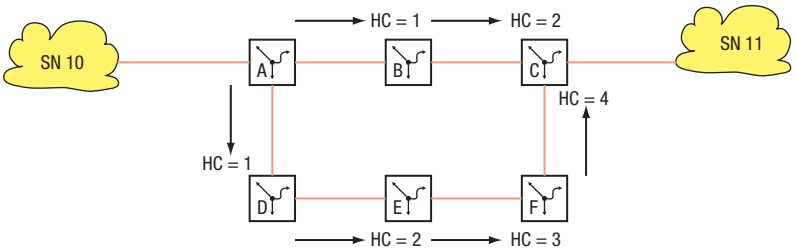



*Figure 92: Counting Hops*

*Table 46: Routing table to the figure above*

| Router A | | | Router B | | | Router D | | |
|---|---|---|---|---|---|---|---|---|
| Destination | Next Hop | Metric | Destination | Next Hop | Metric | Destination | Next Hop | Metric |
| SN 10 | local | 0 | SN 10 | Router A | 1 | SN 10 | Router A | 1 |
| SN 11 | Router B | 2 | SN 11 | Router C | 1 | SN 11 | Router E | 3 |

In contrast to OSPF, a RIP router regularly exchanges the content of its entire routing table with its direct neighbor. Every router knows only its own routes and the routes of its neighbor. Thus it only has a local perspective.

When changes are made in the network, it takes a while until the routers have the same uniform view of the network. The process of achieving this condition is known as convergence.

### 13.6.1 Convergence

How does RIP react to changes in the topography?

In the following example of a line interruption between router B and router C, you can see the resulting changes in the address table:

Assumptions:
- The interruption occurs 5 seconds after router B sent its routing table.
- The routers send their routing table every 30 seconds (= factory setting).
- The interval between the time router A sends its routing table and router B sends its routing table is 15 seconds.

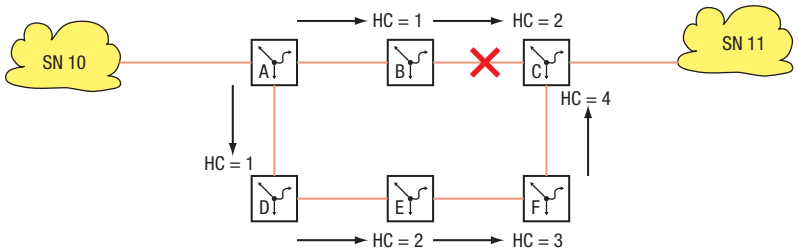



*Figure 93: Hop count*

Time elapsing before convergence:

0 seconds:

Interruption

Link down between Router B and C identified, RIPv2 sends triggered updates

After 10 seconds:

Router A sends its routing table:

| **Router A** | | |
|---|---|---|
| Destination | Next Hop | Metric |
| SN 10 | local | 0 |
| SN 11 | Router B | 2 |

Using the routing table from router A, router B sees that router A knows a connection to destination SN 11 with a metric of 2. Because it does not have its own connection to router C as the next hop to SN 11, router B changes its entry to destination SN 11. It enters router A as the next hop and increases the metric from router A by 1 to 3 (distance = learned distance + 1).

After 25 seconds router B sends its routing table:

| **Router B** | | |
|---|---|---|
| Destination | Next Hop | Metric |
| SN 10 | Router A | 1 |
| SN 11 | Router A | 3 |

Using the routing table from router B, router A sees that router B knows a connection to SN 11 with a metric of 3. So router A increases its metric for SN 11 by 1 to 4.

After 40 seconds router A sends its routing table:

| **Router A** | | |
|---|---|---|
| Destination | Next Hop | Metric |
| SN 10 | local | 1 |
| SN 11 | Router B | 4 |

Using the routing table from router A, router B sees that router A knows a connection to destination SN 11 with a metric of 4. So router B increases its metric for SN 11 by 1 to 5.

After 55 seconds router B sends its routing table:

| **Router B** | | |
|---|---|---|
| Destination | Next Hop | Metric |
| SN 10 | Router A | 1 |
| SN 11 | Router A | 5 |

Using the routing table from router B, router A sees that router B knows a connection to SN 11 with a metric of 5. So router A increases its metric for SN 11 by 1 to 6. Because router A can see in the routing table from router D that router D has a connection to SN 11 with the smaller metric of 3, router A changes its entry for SN 11.

After 70 seconds router A sends its routing table:

| **Router A** | | |
|---|---|---|
| Destination | Next Hop | Metric |
| SN 10 | Router A | 1 |
| SN 11 | Router D | 4 |

After 70 seconds, convergence has been achieved again.

### 13.6.2 Maximum Network Size

The main disadvantage of RIP is that routers only know their neighbors directly. This results in long convergence times and the count-to-infinity problem. Infinity refers to the inaccessibility of a destination, and it is designated by Hop count 16 in RIP. If the above example did not contain the parallel path via routers D, E and F, then routers A and B would keep sending their routing tables until the metric reached a value of 16. Then the routers recognize that the destination is inaccessible.

Using the “split horizon” approach decreases possible looping problems between two neighboring routers. Split horizon has two operating modes.

| | |
|---|---|
| Simple split horizon | When sending the routing table to a neighbor, simple split horizon omits the entries known by the neighbor. |
| Simple split horizon with poison reverse | Sends the routing table to a neighbor with the entries known by this neighbor, but denotes these entries with the infinity metric (=16). |

Thus the Hop count 16 specifies the maximum size of a network with RIP as the routing procedure. The longest paths can pass through up to 15 routers.

### 13.6.3 General Properties of RIP

The RFC 1058 from June 1988 specifies RIP version 1. Version 1 has the following restrictions:
- Use of broadcasts for protocol messages.
- Does not support subnetworks/CIDR.
- No authentication.

The standardization of RIP version 2 in the RFC 2453 in 1998 does away with the above restrictions.

RIP V2 sends its protocol messages as a multicast with the destination address 224.0.0.9, and supports subnetwork masks and authentication.

However, the restrictions relating to the size of the network remain.

*Table 47: Advantages and disadvantages of Vector Distance Routing*

| Advantages | Disadvantages |
|---|---|
| Easy to implement | Routing tables in large networks very comprehensive |
| Easy to administrate | Routing information is distributed slowly, because there are fixed sending intervals. This applies in particular to connections that have elapsed, since the routing table only contains existing paths. |
| | Count-to-infinity |

### 13.6.4 Configuring the RIP

The advantage of RIP is the simple configuration. After the router interface is defined and the RIP is switched on, RIP automatically enters the required routes in the routing table.

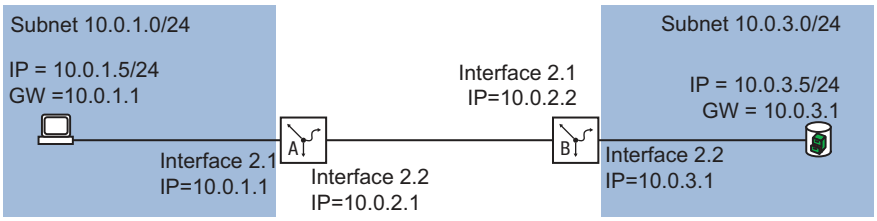



*Figure 94: Example of the configuration of RIP*

Configure the *RIP* functions. To do this, perform the following steps:

- Configure router interfaces – assign IP address and network mask.
- Activate RIP on the port.
- Enable RIP globally.
- Enable routing globally (if this has not already been done).

#### Configuration for Router B

Perform the following steps:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 2/2` | Change to the interface configuration mode of interface `2/2`. |
| `ip address primary 10.0.3.1 255.255.255.0` | Assign the IP parameters to the interface. |
| `ip routing` | Activate the *Routing* function on this interface. |
| `exit` | Change to the Configuration mode. |
| `interface 2/1` | Change to the interface configuration mode of interface `2/1`. |
| `ip address primary 10.0.2.2 255.255.255.0` | Assign the IP parameters to the interface. |
| `ip routing` | Activate the *Routing* function on this interface. |
| `ip rip opertion` | Activate RIP on this interface. |
| `exit` | Change to the Configuration mode. |
| `show ip rip interface 2/1` | Verify the settings for the RIP configuration. |

```
Admin mode..................................... active
IP address..................................... 10.0.2.2
Send version................................... ripv2
Receive version................................ both
Athentication Type............................. none
```

**Note:** The IP address entries remain at `0.0.0.0` as long as the *Routing* function is globally inactive.

```
ip rip re-distribute connected
```
Tell RIP to send the routes of the locally connected interfaces along with the learned routes in the RIP information

```
ip rip operation
```
Activate RIP globally.

```
ip routing
```
Enable the *Routing* function globally.

```
show ip rip interface
```
Verify the settings for the RIP configuration.

```
Interface IP Address Send Version Receive Version Authent Active
---------  --------- ------------ --------------- ------- -----
2/1        10.0.2.2  ripv2        both            none     [x]
```

```
show ip route all
```
Verify the routing table:

```
Network Address  Protocol  Next Hop IP  Next Hop IF  Pref Active
---------------  --------  -----------  -----------  ---- ------
    10.0.1.0/24  RIP       10.0.2.1     2/1          0     [x]
    10.0.2.0/24  Local     10.0.2.2     2/1          0     [x]
    10.0.3.0/24  Local     10.0.3.1     2/2          0     [x]
```

☐ Also perform the corresponding configuration on the other RIP routers.

# 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 48: Advantages and disadvantages of Link State Routing*

| Advantages | Disadvantages |
|---|---|
| Every router calculates its routes independently of the other routers. | Complicated to implement |
| The routers have the same basic information. | Complex administration due to the large number of options. |
| Rapid detection of link interruptions and rapid calculation of alternative routes. | |
| 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. | |
| Optimal path selection through evaluation of the link quality. | |

OSPF is a routing protocol based on the states of the links between the routers.

Using the link states collected from every router and the Shortest Path First algorithm, an OSPF router dynamically creates its routing 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.

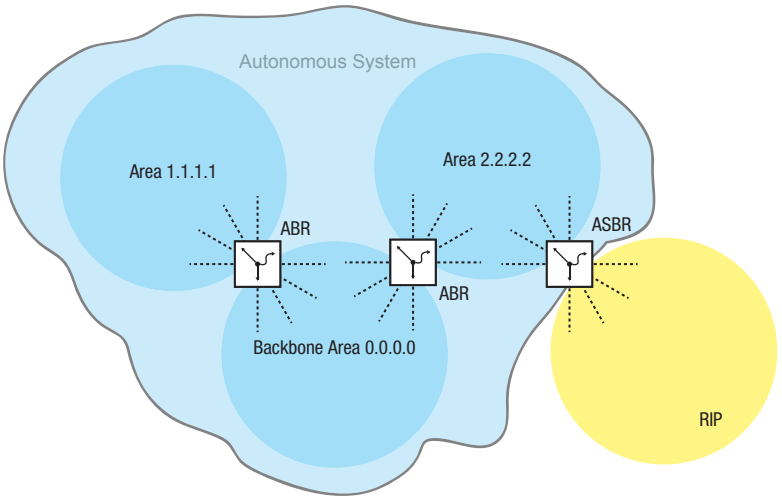



*Figure 95: Autonomous System*

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 96 on page 289. 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.

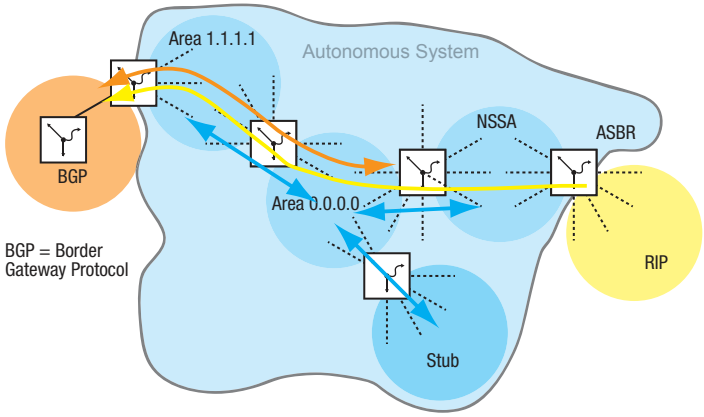



*Figure 96: LSA distribution into the area types*

Perform the following steps:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `ip ospf area 2.2.2.2 nssa add import-nssa` | Specifies area `2.2.2.2` as NSSA. |
| `ip ospf area 3.3.3.3 stub add 0` | Specifies area `3.3.3.3` as stub area. |
| `ip ospf area 3.3.3.3 stub modify 0 default-cost 10` | Instruct the ABR to inject the default route with the metric `10` into the stub area. |

### 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 98 on page 290.. A VL even lets you connect an area that is connected with the backbone area via another area.

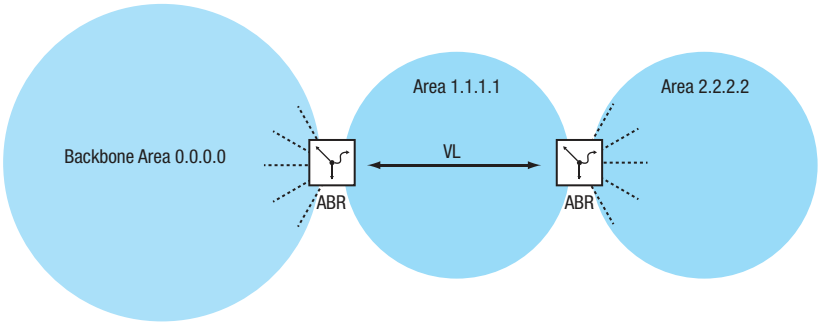



*Figure 97: Linking a remote area to the backbone area using a virtual link (VL)*

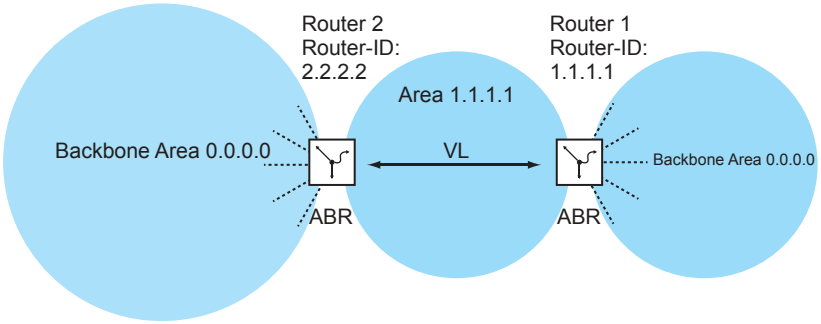



*Figure 98: Expanding the backbone area using a virtual link (VL)*

Configuration for expanding the backbone area (see figure 98):

Configure router 1. To do this, perform the following steps:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `ip ospf area 1.1.1.1 virtual-link add 2.2.2.2` | 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:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `ip ospf area 1.1.1.1 virtual-link add 1.1.1.1` | Enter the neighboring router ID for a virtual link in area `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)
  - RIP

### 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 293 “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 288.

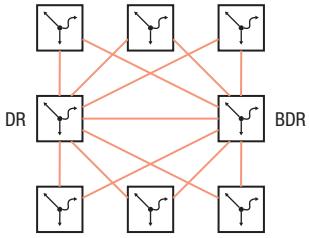



*Figure 99: LSA distribution with designated router and backup designated router*

To exchange information, OSPF uses reserved multicast addresses.

*Table 49: OSPF - multicast addresses*

| Destination | Multicast IP address | Mapped Multicast MAC address |
|---|---|---|
| Every OSPF router | 224.0.0.5 | 01:00:5E:00:00:05 |
| Designated routers | 224.0.0.6 | 01:00:5E:00:00:06 |

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:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface 1/1. |
| `ip ospf hello-interval 20` | Specifies the Hello interval as 20 seconds. |
| `ip ospf dead-interval 60` | Specifies the Dead interval as 60 seconds. |
| `exit` | Change to the Configuration mode. |

```
exit                                    Change to the Privileged EXEC mode.
show ip ospf neighbor 1/1               Displays the Adjacencies of the router.
Neighbor ID       IP Address    Interface    State    Dead Time
------------      -----------   -----------  ------   ----------
192.168.1.1        10.0.1.1        1/1       Full
192.168.1.2        11.0.1.1        1/2       Full
192.168.1.3        12.0.1.1        1/3       Full
192.168.1.4        13.0.1.1        1/4       Full
```

The following list contains the states of the Adjacencies:

| | |
|---|---|
| `Down` | No Hello packets received yet |
| `Init` | Receiving Hello packets |
| `2-way` | Bidirectional communication, determination of the DR and the BDR |
| `Exstart` | Determination of master/slave for LSA exchange |
| `Exchange` | LSAs are exchanged or flooded |
| `Loading` | Completion of the LSA exchange |
| `Full` | Data basis complete and uniform in the area. Routes can now be calculated |

### 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                                  Change to the Privileged EXEC mode.
show ip ospf database internal          Displays the internal Adjacencies of the router.
```

```
LSDB type       Link ID
Area ID         Adv Router       Age    Sequence   Checksum
-----------     ---------------  -----  --------   ------
router link     192.168.1.1      122    80000007   0x5380
0.0.0.0         192.168.1.1
router link     192.169.1.1      120    80000007   0xbf0e
1.1.1.1         192.169.1.1
```

`show ip ospf database external` — Displays the external Adjacencies of the router.

```
Area ID         Adv Router       Age    Sequence   Checksum
-----------     ---------------  -----  --------   ------
1.1.1.1         192.169.1.1      178    80000002   0xcalc
```

### 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:

Metric = *Autocost reference bandwidth*/ bandwidth (bits/sec)

For Ethernet, this leads to the following costs:

| | |
|---|---|
| 10 Mbit | 10 |
| 100 Mbit | 1 |
| 1000 Mbit | 1 (0.1 rounded up to 1) |

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:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `ip ospf cost 2` | Assigns the value `1/1` to port `2` for the OSPF costs. |

### 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.

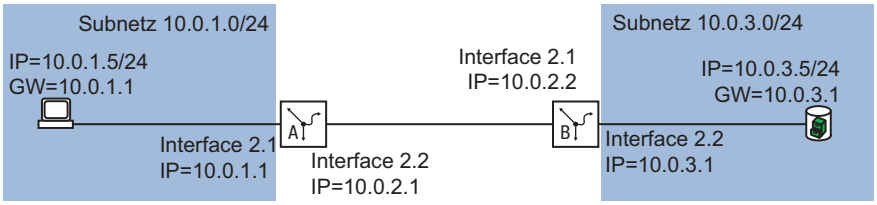



*Figure 100: Example of the configuration of OSPF*

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:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 2/2` | Change to the interface configuration mode of interface `2/2`. |
| `ip address primary 10.0.3.1 255.255.255.0` | Assign the IP parameters to the port. |
| `ip routing` | Activate routing on this port. |
| `ip ospf operation` | Activate OSPF on this port. |
| `exit` | Change to the Configuration mode. |
| `interface 2/1` | Change to the interface configuration mode of interface `2/1`. |
| `ip address primary 10.0.2.2 255.255.255.0` | Assign the IP parameters to the port. |
| `ip routing` | Activate routing on this port. |
| `ip ospf operation` | Activate OSPF on this port. |
| `exit` | Change to the Configuration mode. |
| `ip ospf router-id 10.0.2.2` | Assign router ID `10.0.2.2` to router B. |
| `ip ospf operation` | Enable OSPF globally. |
| `ip ospf re-distribute connected [subnets]` | Specify the OSPF parameters for the following actions:<br>▶ send the routes of the locally connected interfaces along with the routes learned from the RIP information<br>▶ include subnetworks without OSPF in OSPF (CIDR). |
| `exit` | Change to the Configuration mode. |
| `exit` | Change to the Privileged EXEC mode. |
| `show ip ospf global` | Display the settings for the global OSPF 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 settings for the OSPF interface configuration.

```
IP address................................... 10.0.2.2
OSPF admin mode.............................. enabled
OSPF area ID................................. 1.1.1.1
Transmit delay............................... 1
Hello interval............................... 10
Dead interval................................ 40
Re-transmit interval......................... 5
Authentification type........................ none
OSPF interface type.......................... broadcast
Status....................................... not Ready
Designated Router............................ 0.0.0.0
Backup designated Router..................... 0.0.0.0
State........................................ down
MTU ignore flag.............................. disabled
Metric cost.................................. 1
```

```
configure
```

Change to the Configuration mode.

```
ip routing
```

Enable the *Routing* function globally.

```
exit
```

Change to the Privileged EXEC mode.

☐ Also perform the corresponding configuration on the other OSPF routers.

```
show ip ospf neighbor brief
```

Display the OSPF Adjacencies.

```
Neighbor ID       IP Address    Interface    State    Dead Time
------------      -----------   -----------  ------   ----------
10.0.2.1          10.0.2.1        2/1        Full
```

```
show ip route all
```

Display the router table:

```
Network Address   Protocol  Next Hop IP   Next Hop If   Pref  Active
---------------   --------  --- -------   -----------   ----  ------
10.0.1.0          OSPF     10.0.2.1     2/1           110    [x]
```

### 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.

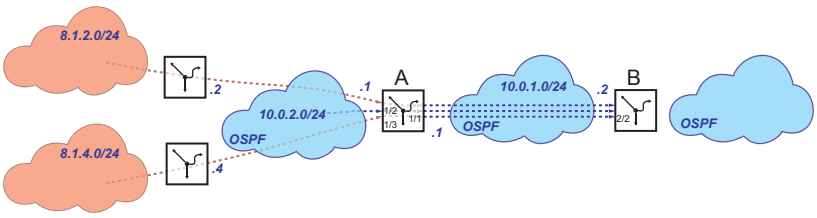
Using IP rules, you specify which routes the device distributes to other devices in OSPF:
- To distribute a few routes in OSPF, you use the explicit `permit` rules. Using the `permit` rules, you specify exactly which routes the device distributes in OSPF.
- To distribute many routes in OSPF, you use 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                                  Change to the Privileged EXEC mode.
configure                               Change to the Configuration mode.
ip routing                              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                           Change to the interface configuration mode of
                                        interface 1/1.
ip address primary 10.0.1.1             Specify the IP address and subnet mask.
255.255.255.0
ip routing                              Activate routing.
ip ospf operation                       Activate OSPF on the router interface.
exit                                    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                           Change to the interface configuration mode of
                                        interface 1/2.
ip address primary 10.0.2.1             Specify the IP address and subnet mask.
255.255.255.0
ip routing                              Activate routing.
ip ospf operation                       Activate OSPF on the router interface.
exit                                    Change to the Configuration mode.
```

☐ Enable OSPF globally.

```
ip ospf router-id 10.0.1.1              Assign the router ID (for example 10.0.1.1).
ip ospf operation                       Enable OSPF globally.
show ip route all

Network Address  Protocol  Next Hop IP      Next Hop If  Pref  Active
---------------  --------  --------------  -----------  ----  ------
10.0.1.0/24      Local     10.0.1.1        1/1          0       [x]
10.0.2.0/24      Local     10.0.2.1        1/2          0       [x]
```

☐ Configure and distribute static routes

```
enable                                  Change to the Privileged EXEC mode.
configure                               Change to the Configuration mode.
```

| | |
|---|---|
| `ip route add 8.1.2.0 255.255.255.0 10.0.2.2` | Configure the static route `8.1.2.0` through the gateway `10.0.2.2`. |
| `ip route add 8.1.4.0 255.255.255.0 10.0.2.4` | Configure the static route `8.1.4.0` through the gateway `10.0.2.4`. |
| `ip ospf re-distribute static subnets enable` | Distribute the configured routes in OSPF. |

**Router B**

☐ Enable routing globally.

```
enable                                  Change to the Privileged EXEC mode.
configure                               Change to the Configuration mode.
ip routing                              Enable routing globally.
```

☐ Setting up the router interface 10.0.1.2/24.
Activate routing.
Activate OSPF on the router interface.

```
interface 2/2                           Change to the interface configuration mode of
                                        interface 2/2.
ip address primary 10.0.1.2             Specify the IP address and subnet mask.
255.255.255.0
ip routing                              Activate routing.
ip ospf operation                       Activate OSPF on the router interface.
exit                                    Change to the Configuration mode.
show ip route all
Network Address  Protocol     Next Hop IP   Next Hop If  Pref  Active
---------------  --------    ------------  -----------  ----  ------
10.0.1.0/24      Local         10.0.1.2      2/2          0       [x]
```

☐ Enable OSPF globally.

```
ip ospf router-id 10.0.1.2              Assign the router ID (for example 10.0.1.2).
ip ospf operation                       Enable OSPF globally.
```

☐ 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.

```
show ip ospf neighbor                   Checking the router table:
Neighbor ID     IP address      Interface   State          Dead Time
--------------- --------------  ----------  -------------- ---------
10.0.1.1        10.0.1.1        2/2         full           00:00:34
```

☐ Check the distribution of the routes configured on router A
Router A distributes both configured routes.

```
show ip route all                       Checking the router table:
Network Address  Protocol     Next Hop IP   Next Hop If  Pref  Active
---------------  --------    ------------  -----------  ----  ------
8.1.2.0/24       OSPF          10.0.1.2      2/2          0       [x]
8.1.4.0/24       OSPF          10.0.1.2      2/2          0       [x]
10.0.1.0/24      Local         10.0.1.2      2/2          0       [x]
10.0.2.0/24      OSPF          10.0.1.2      2/2          0       [x]
```

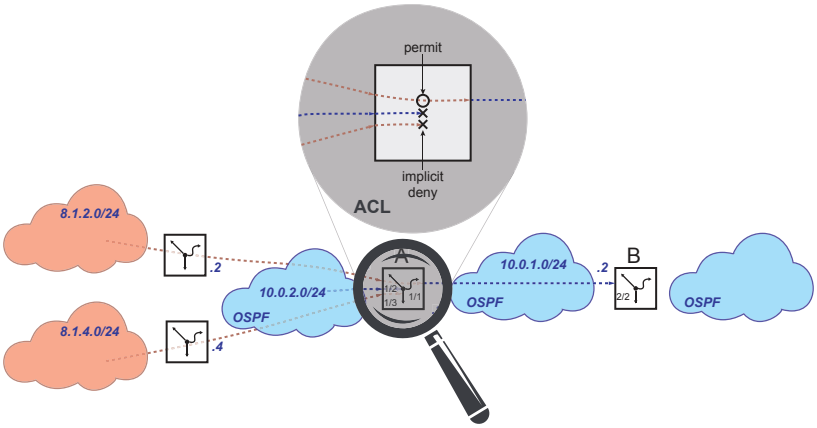
To explicitly enable a route with a `permit` rule, refer to the “Explicitly enabling a route using a permit rule” on page 303 section.

To explicitly disable a route with a `deny` rule, refer to the “Explicitly disabling a route using a deny rule” on page 305 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.

```
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.

```
show access-list ip
```

Display the configured Access Control Lists and rules.

```
Index  AclName                      RuleNo  Action  SrcIP
                                                    DestIP
-----  ---------------------------  ------  ------  -----------
1000   OSPF-rule                    1       Permit  8.1.2.0
                                                      255.255.255.0
```

```
show access-list ip OSPF-rule 1
```

Display the rule `1` (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...............1
Action..................................Permit
Match every ............................False
Protocol................................IP
Source IP address.......................8.1.2.0
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
```

☐ Apply the Access Control List to OSPF.

```
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.

Checking the router table:

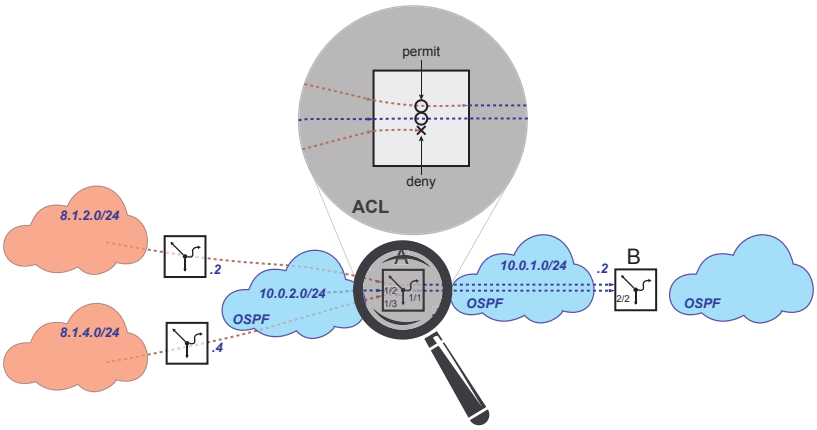
```
show ip route all
```

| Network Address | Protocol | Next Hop IP | Next Hop If | Pref | Active |
|---|---|---|---|---|---|
| 8.1.2.0/24 | OSPF | 10.0.1.2 | 2/2 | 0 | [x] |
| 10.0.1.0/24 | Local | 10.0.1.2 | 2/2 | 0 | [x] |
| 10.0.2.0/24 | OSPF | 10.0.1.2 | 2/2 | 0 | [x] |

### 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 303.

| | |
|---|---|
| `no ip ospf distribute-list out static OSPF-rule` | Separate the `OSPF-rule` Access Control List from OSPF. |
| `ip access-list extended del OSPF-rule` | Delete the Access Control List `OSPF-rule` and the associated rules. |

☐ 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` | Create the `OSPF-rule` Access Control List and set up a `deny` rule for the `8.1.4.0` subnet.<br>• `src 8.1.4.0-0.0.0.0` = address of the destination network and inverse mask<br>• `dst 255.255.255.0-0.0.0.0` = mask of the destination network and inverse mask<br>The device lets you assign the address and mask of the destination network with bit-level accuracy using the inverse mask. |

☐ Apply the Access Control List to OSPF.

| | |
|---|---|
| `ip ospf distribute-list out static OSPF-rule` | Apply the `OSPF-rule` rule to OSPF. |

**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` — Checking the router table:

| Network Address | Protocol | Next Hop IP | Next Hop If | Pref | Active |
|---|---|---|---|---|---|
| 8.1.2.0/24 | OSPF | 10.0.1.2 | 2/2 | 0 | [x] |
| 10.0.1.0/24 | Local | 10.0.1.2 | 2/2 | 0 | [x] |
| 10.0.2.0/24 | OSPF | 10.0.1.2 | 2/2 | 0 | [x] |

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.

```
Index  AclName                     RuleNo  Action  SrcIP
                                                   DestIP
-----  --------------------------  ------  ------  -----------
1000   OSPF-rule                   1       Deny    8.1.4.0
                                                       255.255.255.0
1000   OSPF-rule                   2       Permit  0.0.0.0
                                                   0.0.0.0
```

```
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.

Checking the router table:

```
show ip route all
```

| Network Address | Protocol | Next Hop IP | Next Hop If | Pref | Active |
|---|---|---|---|---|---|
| 8.1.2.0/24 | OSPF | 10.0.1.2 | 2/2 | 0 | [x] |
| 10.0.1.0/24 | Local | 10.0.1.2 | 2/2 | 0 | [x] |
| 10.0.2.0/24 | OSPF | 10.0.1.2 | 2/2 | 0 | [x] |

# 13.8 Protocol-based VLANs

Along with port-based VLANs based on IEEE 802.1Q, the device also supports protocol-based VLANs based on IEEE 802.1v.

With port-based VLANs, the device uses the port VLAN ID of the receiving port to determine which VLAN a data packet belongs to in cases where it is received without a VLAN tag.

With protocol-based VLANs, the router uses the protocol of the received data packet to determine which VLAN a data packet belongs to in cases where it is received without a VLAN tag.

The router lets you use the following protocols by name.
- IP
- ARP
- IPX

The device also supports other protocols using their numerical value. When the router receives data packets from protocols for which a rule does not exist, the router assigns the packets to the port VLAN.

For VLAN assignment, the router takes the following items into account in the order in which they are listed:
- the VLAN tag
- the protocol to which the data packet belongs
- the port VLAN ID

Protocol-based VLANs enable you to transfer data packets not relevant to routing across IP subnetwork boundaries. Data packets relevant to routing are IP and ARP data packets.

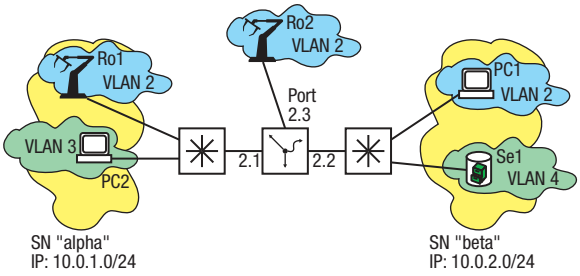



*Figure 101: Example of a protocol-based VLAN*

In the example, PC2 and Se1 communicate via IP. These data packets are routed.

The devices Ro1, Ro2 and PC1 communicate via other Ethernet-based protocols. These data packets are forwarded in VLAN 2.

Thus, every IP data packet remains in its subnetwork, apart from the IP data packets that are meant for a different subnetwork.

## 13.8.1 General Configuration

- ☐ Create a VLAN protocol group for each subnetwork.
- ☐ Assign the protocols to the VLAN protocol group for each subnetwork.
- ☐ Create the VLANs.
- ☐ Activate VLAN routing on the VLANs affected and thus creating the virtual router interfaces.

- ☐ Assign the VLAN protocol groups to the VLANs.
- ☐ Configure the port interfaces:
  - VLAN membership
  - Port VLAN ID for non-ARP/IP data packets
  - Port of a VLAN protocol group and thus assign to a VLAN
- ☐ Configure the virtual router interfaces:
  - Assign IP address.
  - Activate routing.
- ☐ Enable routing globally.

### 13.8.2 Configuration of the Example

Perform the following steps:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 3` | Create the VLAN `3`. |
| `vlan add 4` | Create the VLAN `4`. |
| `name 3 VLAN3` | Assign the name `VLAN3` to the VLAN `3`. |
| `name 4 VLAN4` | Assign the name `VLAN4` to the VLAN `4`. |
| `vlan protocol group add 1 name alpha vlan-id 3` | Create VLAN protocol group `1` for the `alpha` subnet and assign the group to VLAN `3`. |
| `vlan protocol group add 2 name beta vlan-id 4` | Create VLAN protocol group `2` for the `alpha` subnet and assign the group to VLAN `4`. |
| `exit` | Change to the Privileged EXEC mode. |
| `show port protocol` | Display the VLAN protocol groups created. |

```
Idx Group name          VLAN  Protocol(s)
                              Interface(s)
--- ------------------  ----  ---------------------------------
1   alpha               3
2   beta                4
```

| | |
|---|---|
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan protocol group add 1 ethertype ip` | Add the IP protocol to VLAN protocol group `1`. |
| `vlan protocol group add 1 ethertype arp` | Add the ARP protocol to VLAN protocol group `1`. |
| `vlan protocol group add 2 ethertype ip` | Add the IP protocol to VLAN protocol group `2`. |
| `vlan protocol group add 2 ethertype arp` | Add the ARP protocol to VLAN protocol group `2`. |
| `exit` | Change to the Privileged EXEC mode. |
| `show port protocol` | Display the protocols assigned to the protocol groups. |

```
Idx Group name          VLAN  Protocol(s)
                              Interface(s)
--- ------------------  ----  ---------------------------------
1   alpha               3     ip,  arp
2   beta                4     ip,  arp
```

| | |
|---|---|
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 2` | Create the VLAN `2`. |
| `name 2 VLAN 2` | Assign the name `VLAN2` to the VLAN `2`. |

| | |
|---|---|
| `routing add 3` | Create a virtual router interface and activate the *Routing* function on this interface. |
| `routing add 4` | Create a virtual router interface and activate the *Routing* function on this interface. |
| `exit` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 2/1` | Change to the interface configuration mode of interface `2/1`. |
| `vlan participation exclude 1` | Remove port `2/1` from VLAN `1`. |
| `vlan participation include 2` | Declare port `2/1` a member of VLAN `2`. |
| `vlan participation include 3` | Declare port `2/1` a member of VLAN `3`. |
| `vlan pvid 2` | Specify port VLAN ID `2`. Therefore, the device assigns non-IP/ARP data packets to VLAN `2`. |
| `protocol vlan group 1` | Assign VLAN protocol group `1` to interface `2/1`, which means that the device assigns non-IP/ARP data packets to VLAN `3`. |
| `exit` | Change to the Configuration mode. |
| `interface 2/2` | Change to the interface configuration mode of interface `2/2`. |
| `vlan participation exclude 1` | Remove port `2/2` from VLAN `1`. |
| `vlan participation include 2` | Declare port `2/2` a member of VLAN `2`. |
| `vlan participation include 4` | Declare port `2/2` a member of VLAN `4`. |
| `vlan pvid 2` | Specify port VLAN ID `2`. Therefore, the device assigns non-IP/ARP data packets to VLAN `2`. |
| `protocol vlan group 2` | Assign VLAN protocol group `2/2` to interface `2`, which means that the device assigns non-IP/ARP data packets to VLAN `4`. |
| `exit` | Change to the Configuration mode. |
| `interface 2/3` | Change to the interface configuration mode of interface `2/3`. |
| `vlan participation exclude 1` | Remove port `2/3` from VLAN `1`. |
| `vlan participation include 2` | Declare port `2/3` a member of VLAN `2`. |
| `vlan pvid 2` | Specify port VLAN ID `2`. Therefore, the device assigns data packets that the port receives without a VLAN tag to VLAN `2`. |
| `exit` | Change to the Configuration mode. |
| `interface vlan/3` | Change to the interface configuration mode of interface `vlan/3`. |
| `ip address primary 10.0.1.1 255.255.255.0` | Assign the IP parameters to the router interface. |
| `ip routing` | Activate the *Routing* function on this interface. |
| `exit` | Change to the Configuration mode. |
| `interface vlan/4` | Change to the interface configuration mode of interface `vlan/4`. |
| `ip address primary 10.0.2.1 255.255.255.0` | Assign the IP parameters to the router interface. |
| `ip routing` | Activate the *Routing* function on this interface. |
| `exit` | Change to the Configuration mode. |

```
show ip interface
```

Display the entries of the virtual router interface.

```
Interface IP Address      IP Mask
--------- --------------- ---------------
vlan/3    10.0.1.1        255.255.255.0
vlan/4    10.0.2.1        255.255.255.0
```

```
ip routing operation
```

Enable the *Routing* function globally.

# 13.9 Multicast Routing

Multicast data streams are data packets that a source sends to multiple recipients. To reduce the network load, the source uses a multicast address. The source thus sends each packet only once to the multicast address instead of sending it to each recipient individually. The recipients recognize a multicast data stream intended for them by the multicast address.

A common reason for introducing subnetworks is the restriction of broadcast data streams. Switches flood broadcast/multicast data streams to every port, while routers block broadcast/ multicast data streams. Multicast routing enables you to accurately transmit multicast data streams beyond the boundaries of subnetworks. Accurate transmission means sending data streams with specified multicast addresses only to those devices that have requested the multicast data stream.

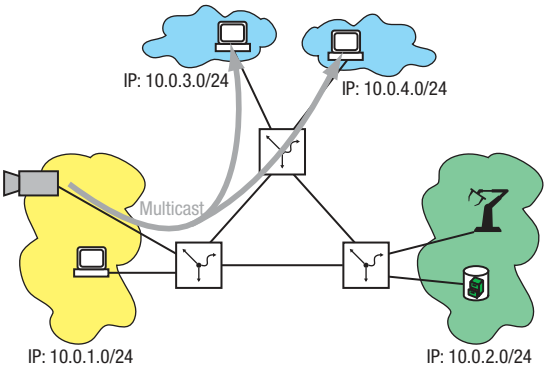



*Figure 102: Example of a multicast application*

When using multicast routing observe the following guidelines:

- Defined multicast addresses
- Defined a protocol for multicast group registration that organizes the exchange of information by means of multicast data streams (for example IGMP). This information relates to reporting the network participants who request to receive multicast data streams and querying the request by means of intermediate devices.
- Defined a protocol that guides the multicast data streams in accordance with the information contained in the multicast datagrams (for example PIM, DVMRP).

## 13.9.1 Multicast Addresses

### IP Multicast Addresses

The Internet Assigned Numbers Authority (IANA) defined the IP addresses of the class D IP address space as multicast addresses. IP multicast addresses are in the range from 224.0.0.0 to 239.255.255.255.

*Table 50: Assignment of the IP multicast address range*

| IP address range | Assignment |
|---|---|
| 224.0.0.0 | Base address, reserved |
| 224.0.0.1 - 224.0.0.255 | Local Network Control Block, reserved for routing protocols, IGMP, etc.<br>For example:<br>224.0.0.1 - every host of a subnetwork<br>224.0.0.2 - every router of a subnetwork<br>224.0.0.4 - every DVMRP router<br>224.0.0.5 - every OSPF router<br>224.0.0.6 - every OSPF DR router<br>224.0.0.9 - every RIP v2 router<br>224.0.0.13 - every PIM router<br>224.0.0.18 - every VRRP router<br>224.0.0.22 - every IGMP v3 report |
| 224.0.1.0 - 224.0.1.255 | Internetwork Control Block |
| 224.0.2.0 - 224.0.255.255 | AD HOC Block |
| 224.1.0.0 - 238.255.255.255 | Various organizations, protocols, applications, reservations.<br>For example:<br>232.0.0.0-232.255.255.255 - Source-Specific Multicasts |
| 239.0.0.0 - 239.255.255.255 | Administratively scoped IP v4 multicast space<br>These multicast addresses are not transferred by any router beyond the local boundaries and into the internet. Therefore the administrator can assign these addresses any way he wants within these local boundaries. |

The administratively scoped IP v4 multicast area is subdivided further by the IANA:

*Table 51: Assignment of the administratively scoped IP v4 multicast area*

| IP address range | Assignment |
|---|---|
| 239.000.000.000 - 239.191.255.255 | Reserved [IANA] |
| 239.192.000.000 - 239.251.255.255 | Organization-local scope [Meyer, RFC2365] |
| 239.252.000.000 - 239.254.255.255 | Site-local scope (reserved) [Meyer, RFC2365] |
| 239.255.000.000 - 239.255.255.255 | Site-local scope [Meyer, RFC2365] |

In the end, the following multicast IP adress ranges are left over for disposal by an organization's administrator:

- 239.192.000.000 - 239.251.255.255
  for the local areas of an organization.
- 239.255.000.000 - 239.255.255.255
  for the local areas of an organization.

**Note:** When selecting the multicast IP addresses, verify that they can be uniquely mapped onto MAC multicast addresses (see on page 316 “Mapping IP MAC Multicast Addresses”).

### MAC Multicast Addresses

The IEEE calls the 48-bit MAC address an “Extended Unique Identifier”. It is the unique identifier of a device. The first 24 bits of the MAC address (Organizationally Unique Identifier, OUI) is assigned by the IEEE to the manufacturer. The manufacturer uses the last 24 bits to uniquely identify their device interfaces.

A number of MAC addresses are reserved for specific applications:

*Table 52: Examples of reserved MAC addresses*

| MAC-Address | Type | Use |
|---|---|---|
| 01-00-5E-00-00-00 | 0800 | Internet multicast [RFC1112] |
| 01-80-C2-00-00-00 | -802- | Spanning tree (for bridges) |
| FF-FF-FF-FF-FF-FF | 0806 | ARP (for IP and CHAOS) as needed |
| FF-FF-FF-FF-FF-FF | 8035 | Reverse ARP |

### Mapping IP MAC Multicast Addresses

When IP data packets are sent via an ethernet, the IP address is assigned to a MAC address, and therefore IP multicast addresses are also mapped to MAC multicast addresses.

The 23 lower-value bits of the 32-bit IP multicast address make up the 23 lower-value bits of the 48-bit MAC multicast address.

Of the remaining 9 bits of the IP multicast address, 4 bits are used as the class D identification for the multicast address.

The remaining 5 bits help ensure that 32 IP multicast addresses can be mapped to one and the same MAC multicast address.

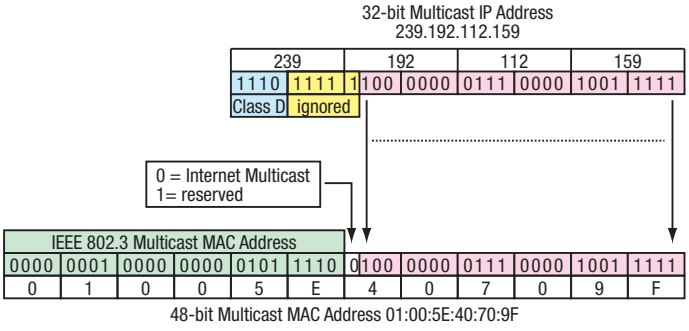



*Figure 103: Conversion of the IP address to the MAC address*

## 13.9.2 Multicast Group Registration

The Internet Group Management Protocol (IGMP) describes the distribution of multicast information between routers and end devices on Layer 3.

Routers with an active *IGMP* function periodically send queries to find out which IP multicast group members are connected to the LAN, or to find out who is interested in becoming a group member.

Multicast group members reply with a Report message. The Report message contains the parameters required by the IGMP. The router records the IP multicast group address from the Report message in its routing table. The result of this is that it transfers frames with this IP multicast group address in the target address field only in accordance with the routing table.

Devices which no longer want to be members of a multicast group can cancel their membership by means of a Leave message (from IGMP version 2), and they do not transmit any more Report messages. When the router does not receive any Report messages from a device within a specified period of time (aging time), the router removes it from the routing table.

When there are multiple routers with an active *IGMP* function in the subnetwork, the following rules apply:

- for IGMP version 1, every router in this subnetwork periodically sends a query
- for IGMP versions 2 and 3, the routers decide which router takes over the query function (Querier Election).

*Table 53: Standards which describe the Multicast Group Membership Discovery*

| Protocol | Standard |
|---|---|
| IGMP v1 | RFC 1112 |
| IGMP v2 | RFC 2236 |
| IGMP v3 | RFC 3376 |

An advantage that IGMP version 2 has over IGMP version 1 is that a multicast recipient can cancel his membership in a multicast group, thus freeing up his bandwidth more quickly. Another advantage is the introduction of the Querier Election.

IGMP version 3 provides more security with the Source Filtering option. Multicast recipients can define the sources from which they want to receive multicast data streams. The router blocks multicast data streams with other source addresses.

The different versions of IGMP are backwards compatible.

This means that an IGMP version 3 router can also process version 1 and version 2. When there are different IGMP versions in a subnetwork, the participating routers agree on the earliest version.

### 13.9.3 Scoping

In the multicast transmission, the protocol provides two options for limiting the expansion of the multicast data stream:

- Multicast Address Scoping / Boundary
  In the multicast Address Scoping, the administrator assigns a multicast IP address range to a router interface (see table 51). The router interface blocks the multicast data streams with addresses within this address range.
  Example:
  ```
  ip mcast boundary 239.193.122.0 255.255.255.0
  ```
  In this example, the router interface blocks multicast data streams with a multicast IP address in the range 239.193.122.0-239.193.122.255.
- TTL Scoping
  Every multicast data packet contains a Time To Live (TTL)
  When a router re-transmits a multicast data packet, the router decreases the TTL counter by 1.
  In TTL Scoping, the administrator assigns a TTL threshold to an interface. The router interface blocks every multicast data packet for which the TTL is below the TTL threshold.
  Example:
  ```
  ip multicast ttl-threshold 64
  ```
  In this example, the router interface blocks multicast data streams with a TTL whose value is less than 64.

*Table 54: Usual scope for TTLs*

| TTL | Range |
|---|---|
| 0 | Restricted to the same host |
| 1 | Restricted to the same subnetwork |
| < 32 | Restricted to a particular location, organization or department |
| < 64 | Restricted to the same region |
| < 128 | Restricted to the same continent |
| < 255 | Unrestricted, global |

# 13.10 Entering the IP Parameters

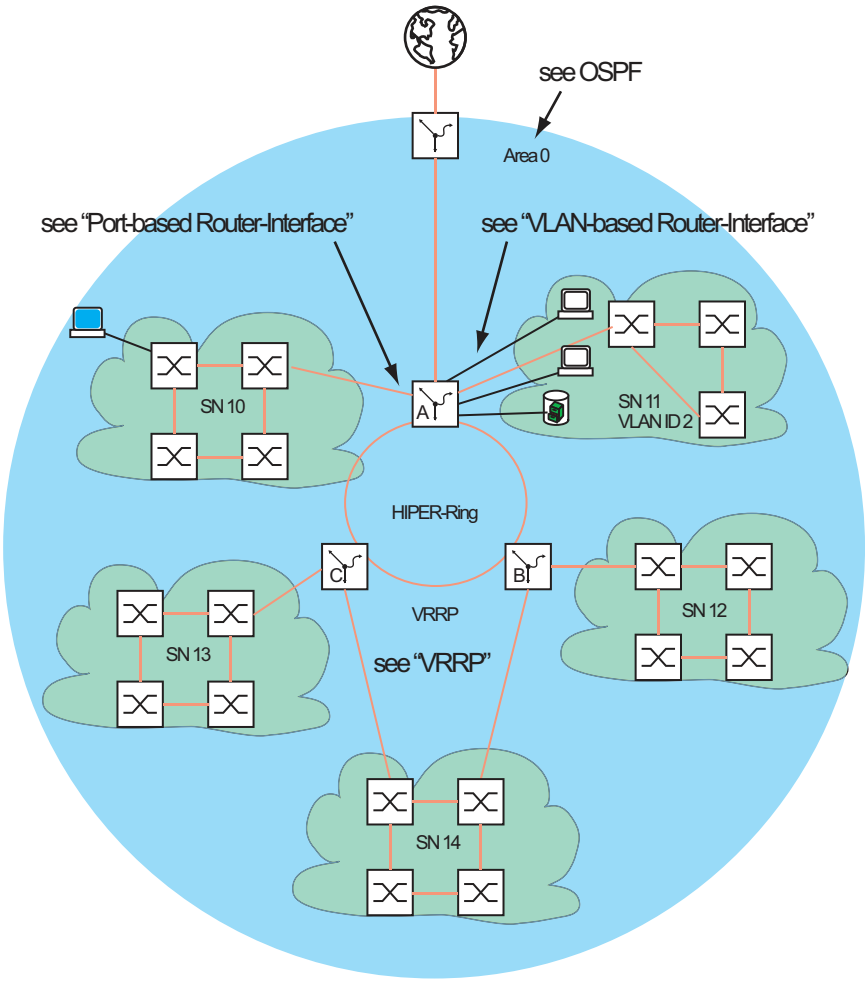



*Figure 104: Network plan*

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 and HIPER ring). To help avoid loops in the configuration phase, close the redundant connections only after the configuration phase.

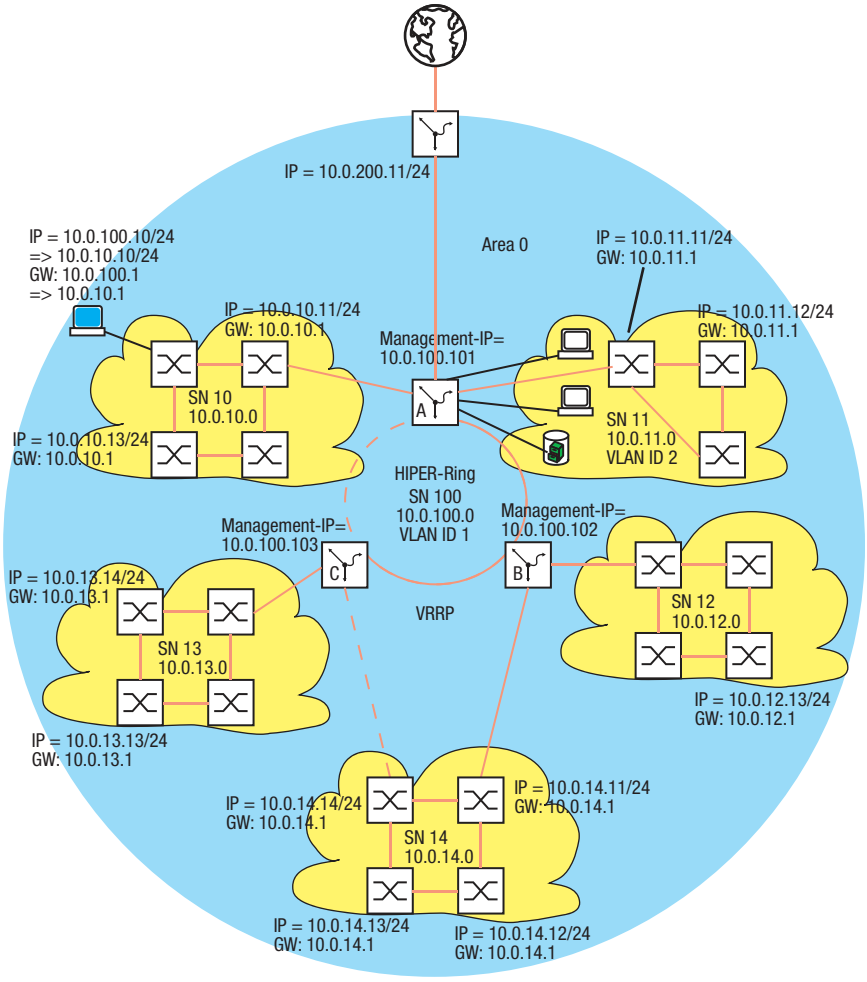



*Figure 105: Network plan with management IP addresses*

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.

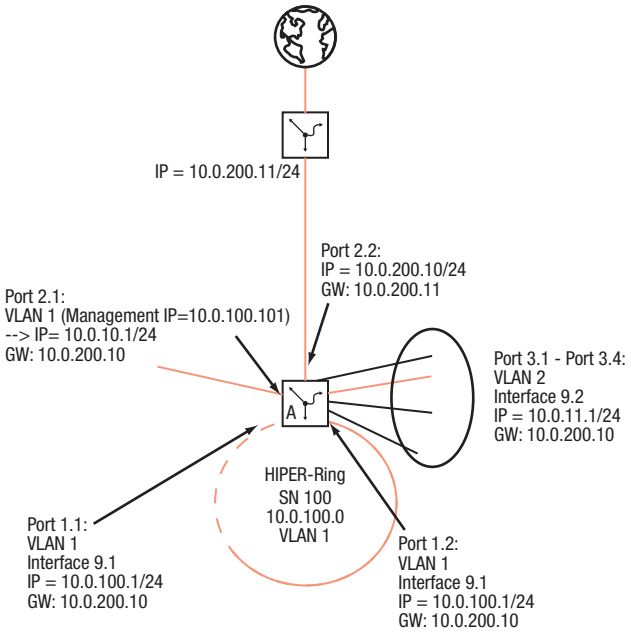



*Figure 106: IP parameters for Layer 3 device A*

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 106).

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
- Help protect against layer 2 network 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.

### 14.1.1 List of SNMP traps

The following table displays possible SNMP traps sent by the device.

*Table 55: Possible SNMP traps*

| Name of the SNMP trap | Meaning |
|---|---|
| authenticationFailure | When a station attempts to access an agent without authorisation, this trap is sent. |
| coldStart | Sent after a restart. |
| hm2DevMonSenseExtNvmRemoval | When the external memory has been removed, this trap is sent. |
| linkDown | When the connection to a port is interrupted, this trap is sent. |
| linkUp | When connection is established to a port, this trap is sent. |
| hm2DevMonSensePSState | When the status of a power supply unit changes, this trap is sent. |
| hm2SigConStateChange | When the status of the signal contact changes in the operation monitoring, this trap is sent. |
| newRoot | When the sending agent becomes the new root of the spanning tree, this trap is sent. |
| topologyChange | When the port changes from blocking to forwarding or from forwarding to blocking, this trap is sent. |
| alarmRisingThreshold | When the RMON input exceeds its upper threshold, this trap is sent. |
| alarmFallingThreshold | When the RMON input goes below its lower threshold, this trap is sent. |
| hm2AgentPortSecurityViolation | When a MAC address detected on this port does not match the current settings of the parameter hm2AgentPortSecurityEntry, this trap is sent. |
| hm2DiagSelftestActionTrap | When a self test for the four categories “task”, “resource”, “software”, and “hardware” is performed according to the configured settings, this trap is sent. |
| hm2MrpReconfig | When the configuration of the MRP ring changes, this trap is sent. |
| hm2DiagIfaceUtilizationTrap | When the threshold of the interface exceeds or undercuts the upper or lower threshold specified, this trap is sent. |
| hm2LogAuditStartNextSector | When the audit trail after completing one sector starts a new one, this trap is sent. |
| hm2PtpSynchronizationChance | When the status of the PTP synchronization has been changed, this trap is sent. |
| hm2ConfigurationSavedTrap | After the device has successfully saved its configuration locally, this trap is sent. |
| hm2ConfigurationChangedTrap | When you change the configuration of the device for the first time after it has been saved locally, this trap is sent. |
| hm2PlatformStpInstanceLoopInconsistentStartTrap | When the port in this STP instance changes to the “loop inconsistent” status, this trap is sent. |
| hm2PlatformStpInstanceLoopInconsistentEndTrap | When the port in this STP instance leaves the “loop inconsistent” status receiving a BPDU packet, this trap is sent. |

### 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
- *Basic Settings > Power over Ethernet > Global* dialog
- *Network Security > Port Security* dialog
- *Switching > L2-Redundancy > Link Aggregation* dialog
- *Routing > OSPF > Global* dialog
- *Routing > Tracking > Configuration* dialog
- *Routing > L3-Redundancy > VRRP > Configuration* dialog
- *Diagnostics > Status Configuration > Device Status* dialog
- *Diagnostics > Status Configuration > Security Status* dialog
- *Diagnostics > Status Configuration > Signal Contact* dialog
- *Diagnostics > Status Configuration > MAC Notification* dialog
- *Diagnostics > System > IP Address Conflict Detection* dialog
- *Diagnostics > System > Selftest* dialog
- *Diagnostics > Ports > Port Monitor* 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
- Loss of the redundancy (in ring manager mode)
- 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.
- The removal of a module

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 56: Device Status events*

| Name | Meaning |
|---|---|
| *Temperature* | Monitors in case the temperature exceeds or falls below the value specified. |
| *Ring redundancy* | When ring redundancy is present, enable this function. |
| *Connection errors* | Enable this function to monitor every port link event in which the *Propagate connection error* checkbox is active. |
| *Ethernet module removal* | Enable this global function to monitor the removal of a module. Also enable the individual module to monitor. |
| *External memory removal* | Enable this function to monitor the presence of an external storage device. |
| *External memory not in sync* | The device monitors synchronization between the device configuration and the configuration stored in the external memory (*ENVM*). |
| *Power supply* | Enable this function to monitor the power supply. |

### 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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `device-status trap` | When the device status changes, send an SNMP trap. |
| `device-status monitor envm-not-in-sync` | Monitors the configuration profiles in the device and in the external memory.<br>The *Device status* changes to `error` in the following situations:<br>• The configuration profile only exists in the device.<br>• The configuration profile in the device differs from the configuration profile in the external memory. |
| `device-status monitor envm-removal` | Monitors the active external memory. When you remove the active external memory from the device, the value in the *Device status* frame changes to `error`. |
| `device-status monitor power-supply 1` | Monitors the power supply unit `1`. When the device has a detected power supply fault, the value in the *Device status* frame changes to `error`. |
| `device-status monitor ring-redundancy` | Monitors the ring redundancy.<br>The *Device status* changes to `error` in the following situations:<br>• The redundancy function becomes active (loss of redundancy reserve).<br>• The device is a normal ring participant and detects an error in its settings. |

| | |
|---|---|
| `device-status monitor temperature` | Monitors the temperature in the device. When the temperature exceeds or falls below the specified limit, the value in the *Device status* frame changes to `error`. |
| `device-status monitor module-removal` | Monitors the modules. When you remove a module from the device, the value in the *Device status* frame changes to `error`. |
| `device-status module 1` | Monitors module `1`. When you remove the module `1` from the device, the value in the *Device status* frame changes to `error`. |

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.
- ☐ 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `device-status monitor link-failure` | Monitors the ports/interfaces link. When the link interrupts on a monitored port/interface, the value in the *Device status* frame changes to `error`. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `device-status link-alarm` | Monitors the port/interface link. When the link interrupts on the port/interface, the value in the *Device status* frame changes to `error`. |

**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 57: Security Status events*

| Name | Meaning |
|---|---|
| *Password default settings unchanged* | After installation change the passwords to increase security. When active and the default passwords remain unchanged, the device displays an alarm. |
| *Min. password length < 8* | Create passwords more than 8 characters long to maintain a high security posture. When active, the device monitors the *Min. password length* setting. |
| *Password policy settings deactivated* | The device monitors the settings located in the *Device Security* > User Management dialog for password policy requirements. |
| *User account password policy check deactivated* | The device monitors the settings of the *Policy check* checkbox. When *Policy check* is inactive, the device sends an SNMP trap. |
| *Telnet server active* | The device monitors when you enable the *Telnet* function. |
| *HTTP server active* | The device monitors when you enable the *HTTP* function. |
| *SNMP unencrypted* | The device monitors when you enable the *SNMPv1* or *SNMPv2* function. |
| *Access to system monitor with serial interface possible* | The device monitors the System Monitor status. |
| *Saving the configuration profile on the external memory possible* | The device monitors the possibility to save configurations to the external non-volatile memory. |
| *Link interrupted on enabled device ports* | The device monitors the link status of active ports. |

*Table 57: Security Status events (cont.)*

| Name | Meaning |
|---|---|
| *Access with HiDiscovery possible* | The device monitors when you enable the HiDiscovery read/ write access function. |
| *Load unencrypted config from external memory* | The device monitors the security settings for loading the configuration from the external NVM. |
| *Self-signed HTTPS certificate present* | The device monitors the HTTPS server for self-created digital certificates. |

### 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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `security-status monitor pwd-change` | Monitors the password for the locally set up user accounts `user` and `admin`. When the password for the `user` or `admin` user accounts is the default setting, the value in the *Security status* frame changes to `error`. |
| `security-status monitor pwd-min-length` | Monitors the value specified in the *Min. password length* policy. When the value for the *Min. password length* policy is less than `8`, the value in the *Security status* frame changes to `error`. |
| `security-status monitor pwd-policy-config` | Monitors the password policy settings. When the value for at least one of the following policies is specified as `0`, the value in the *Security status* frame changes to `error`.<br>• *Upper-case characters (min.)*<br>• *Lower-case characters (min.)*<br>• *Digits (min.)*<br>• *Special characters (min.)* |
| `security-status monitor pwd-policy-inactive` | Monitors the password policy settings. When the value for at least one of the following policies is specified as `0`, the value in the *Security status* frame changes to `error`. |
| `security-status monitor telnet-enabled` | Monitors the Telnet server. When you enable the Telnet server, the value in the *Security status* frame changes to `error`. |

| | |
|---|---|
| `security-status monitor http-enabled` | Monitors the HTTP server. When you enable the HTTP server, the value in the *Security status* frame changes to `error`. |
| `security-status monitor snmp-unsecure` | Monitors the SNMP server.<br>When at least one of the following conditions applies, the value in the *Security status* frame changes to `error`:<br>• The *SNMPv1* function is enabled.<br>• The *SNMPv2* function is enabled.<br>• 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 the System Monitor function 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. |

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 > Security Status* dialog, *Global* tab.
- ☐ For the *Link interrupted on enabled device ports* parameter, mark the checkbox in the *Monitor* column.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
- ☐ Open the *Diagnostics > Status Configuration > Device Status* dialog, *Port* tab.
- ☐ For the *Link interrupted on enabled device ports* parameter, mark the checkbox in the column of the ports to be monitored.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `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:

☐ 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
- Events for ring redundancy
  Loss of the redundancy (in ring manager mode)
  In the default setting, ring redundancy monitoring is inactive. The device is a normal ring participant and detects an error in the local configuration.
- 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.
- The removal of a module

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 ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |

| | |
|---|---|
| `signal-contact 1 mode manual` | Select the manual setting mode for signal contact 1. |
| `signal-contact 1 state open` | Open signal contact 1. |
| `signal-contact 1 state closed` | 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `signal-contact 1 monitor temperature` | Monitors the temperature in the device. When the temperature exceeds / falls below the threshold values, the signal contact opens. |

| | |
|---|---|
| `signal-contact 1 monitor ring-redundancy` | Monitors the ring redundancy.<br>The signal contact opens in the following situations:<br>• The redundancy function becomes active (loss of redundancy reserve).<br>• The device is a normal ring participant and detects an error in its settings. |
| `signal-contact 1 monitor link-failure` | Monitors the ports/interfaces link. When the link interrupts on a monitored port/interface, the signal contact opens. |
| `signal-contact 1 monitor envm-removal` | Monitors the active external memory. When you remove the active external memory from the device, the signal contact opens. |
| `signal-contact 1 monitor envm-not-in-sync` | Monitors the configuration profiles in the device and in the external memory.<br>The signal contact opens in the following situations:<br>• The configuration profile only exists in the device.<br>• The configuration profile in the device differs from the configuration profile in the external memory. |
| `signal-contact 1 monitor power-supply 1` | Monitors the power supply unit `1`. When the device has a detected power supply fault, the signal contact opens. |
| `signal-contact 1 monitor module-removal 1` | Monitors module `1`. When you remove module `1` from the device, the signal contact opens. |
| `signal-contact 1 trap` | Enables the device to send an SNMP trap when the status of the operation monitoring changes. |
| `no signal-contact 1 trap` | Disabling the SNMP trap |

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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `signal-contact 1 monitor link-failure` | Monitors the ports/interfaces link. When the link interrupts on a monitored port/interface, the signal contact opens. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `signal-contact 1 link-alarm` | Monitors the port/interface link. When the link interrupts on the port/interface, the signal contact opens. |

### Events which can be monitored

*Table 58: Device Status events*

| Name | Meaning |
|---|---|
| *Temperature* | When the temperature exceeds or falls below the value specified. |
| *Ring redundancy* | When ring redundancy is present, enable this function to monitor. |
| *Connection errors* | Enable this function to monitor every port link event in which the *Propagate connection error* checkbox is active. |
| *Ethernet module removal* | Enable this global function to monitor the removal of a module. Also enable the individual module to monitor. |
| *External memory not in sync with NVM* | The device monitors synchronization between the device configuration and the configuration stored in the external memory (*ENVM*). |
| *External memory removed* | Enable this function to monitor the presence of an external storage device. |
| *Power supply* | Enable this function to monitor the power supply. |

### 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:

☐ 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.

```
show signal-contact 1 all
```

Displays signal contact settings for the specified signal contact.

# 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 59: Symbols identifying the status of the ports*

| Criterion | Symbol |
|---|---|
| Bandwidth of the port | 10 Mbit/s<br>Port activated, connection okay, full-duplex mode<br>100 Mbit/s<br>Port activated, connection okay, full-duplex mode<br>1000 Mbit/s<br>Port activated, connection okay, full-duplex mode |
| Operating state | Half-duplex mode enabled<br>See the *Basic Settings > Port* dialog, *Configuration* tab, *Automatic configuration* checkbox, *Manual configuration* field and *Manual cable crossing (Auto. conf. off)* field.<br>Autonegotiation enabled<br>See the *Basic Settings > Port* dialog, *Configuration* tab, *Automatic configuration* checkbox.<br>The port is blocked by a redundancy function. |
| AdminLink | The port is deactivated, connection okay<br>The port is deactivated, no connection set up<br>See the *Basic Settings > Port* dialog, *Configuration* tab, *Port on* checkbox and *Link/Current settings* field. |

# 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 60: Examples indicating known weaknesses*

| Counter | Indication of known possible weakness |
|---|---|
| Received fragments | • Non-functioning controller of the connected device<br>• Electromagnetic interference in the transmission medium |
| CRC Error | • Non-functioning controller of the connected device<br>• Electromagnetic interference in the transmission medium<br>• Inoperable component in the network |
| Collisions | • Non-functioning controller of the connected device<br>• Network over extended/lines too long<br>• Collision or a detected fault with a data packet |

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.

- 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 61: Evaluation of non-matching of the duplex mode*

| No. | Automatic configuration | Current duplex mode | Detected error events (≥ 10 after link up) | Duplex modes | Possible causes |
|---|---|---|---|---|---|
| 1 | marked | Half duplex | None | OK | |
| 2 | marked | Half duplex | Collisions | OK | |
| 3 | marked | Half duplex | Late Collisions | Duplex problem detected | Duplex problem, EMI, network extension |
| 4 | marked | Half duplex | CRC Error | OK | EMI |
| 5 | marked | Full duplex | None | OK | |
| 6 | marked | Full duplex | Collisions | OK | EMI |
| 7 | marked | Full duplex | Late Collisions | OK | EMI |
| 8 | marked | Full duplex | CRC Error | OK | EMI |
| 9 | unmarked | Half duplex | None | OK | |
| 10 | unmarked | Half duplex | Collisions | OK | |
| 11 | unmarked | Half duplex | Late Collisions | Duplex problem detected | Duplex problem, EMI, network extension |
| 12 | unmarked | Half duplex | CRC Error | OK | EMI |
| 13 | unmarked | Full duplex | None | OK | |
| 14 | unmarked | Full duplex | Collisions | OK | EMI |
| 15 | unmarked | Full duplex | Late Collisions | OK | EMI |
| 16 | unmarked | Full duplex | CRC Error | Duplex problem detected | Duplex problem, EMI |

# 14.7 Auto-Disable

The device can disable a port due to several configurable reasons. Each reason causes the port to “shut down”. In order to recover the port from the shut down state, you can manually clear the condition which caused the port to shut down or specify a timer to automatically re-enable the port.

If the configuration displays a port as enabled, but the device detects an error or change in the condition, then the software shuts down that port. In other words, the device software disables the port because of a detected error or change in the condition.

If a port is auto-disabled, then the device effectively shuts down the port and the port blocks traffic. The port LED blinks green 3 times per period and identifies the reason for the shutdown. In addition, the device creates a log file entry which lists the causes of the deactivation. When you re-enable the port after a timeout using the *Auto-Disable* function, the device generates a log entry.

The *Auto-Disable* function provides a recovery function which automatically enables an auto-disabled port after a user-defined time. When this function enables a port, the device sends an SNMP trap with the port number, but without a value for the *Reason* parameter.

The *Auto-Disable* function serves the following purposes:
- It assists the network administrator in port analysis.
- It reduces the possibility that this port causes the network to be instable.

The *Auto-Disable* function is available for the following functions:
- *Link flap* (*Port Monitor* function)
- *CRC/Fragments* (*Port Monitor* function)
- Duplex Mismatch detection (*Port Monitor* function)
- *DHCP Snooping*
- *Dynamic ARP Inspection*
- *Spanning Tree*
- *Port Security*
- *Overload detection* (*Port Monitor* function)
- *Link speed/Duplex mode detection* (*Port Monitor* function)

In the following example, you configure the device to disable a port due to detected violations to the thresholds specified the *Diagnostics > Ports > Port Monitor* dialog, *CRC/Fragments* tab, and then automatically re-enable the disabled port.

Perform the following steps:

- ☐ Open the *Diagnostics > Ports > Port Monitor* dialog, *CRC/Fragments* tab.
- ☐ Verify that the thresholds specified in the table concur to your preferences for port `1/1`.
- ☐ Open the *Diagnostics > Ports > Port Monitor* dialog, *Global* tab.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ To allow the device to disable the port due to detected errors, mark the checkbox in the *CRC/Fragments on* column for port `1/1`.

- In the *Action* column you can choose how the device reacts to detected errors. In this example, the device disables port `1/1` for threshold violations and then automatically re-enables the port.
  - To allow the device to disable and automatically re-enable the port, select the value `auto-disable` and configure the *Auto-Disable* function. The value `auto-disable` only works in conjunction with the *Auto-Disable* function.

  The device can also disable a port without auto re-enabling.
  - To allow the device to disable the port only, select the value `disable port`. To manually re-enable a disabled port, highlight the port.

    Click the ☰ button and then the *Reset* item.
  - When you configure the *Auto-Disable* function, the value `disable port` also automatically re-enables the port.
- Open the *Diagnostics > Ports > Port Monitor* dialog, *Auto-disable* tab.
- To allow the device to auto re-enable the port after it was disabled due to detected threshold violations, mark the checkbox in the *CRC error* column.
- Open the *Diagnostics > Ports > Port Monitor* dialog, *Port* tab.
- Specify the delay time as 120 s in the *Reset timer [s]* column for the ports you want to enable.

**Note:** The *Reset* item lets you enable the port before the time specified in the *Reset timer [s]* column counts down.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `port-monitor condition crc-fragments count 2000` | Specifying the CRC-Fragment counter to 2000 parts per million. |
| `port-monitor condition crc-fragments interval 15` | Sets the measure interval to 15 seconds for CRC-Fragment detection. |
| `auto-disable timer 120` | Specifies the waiting period of `120` seconds, after which the *Auto-disable* function re-enables the port. |
| `exit` | Change to the Configuration mode. |
| `auto-disable reason crc-error` | Activate the auto-disable CRC function. |
| `port-monitor condition crc-fragments mode` | Activate the CRC-Fragments condition to trigger an action. |
| `port-monitor operation` | Activate the *Port Monitor* function. |

When the device disables a port due to threshold violations, the device lets you use the following commands to manually reset the disabled port.

Perform the following steps:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `auto-disable reset` | Lets you enable the port before the Timer counts down. |

# 14.8 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:

1. Open the *Diagnostics > Ports > SFP* dialog.

# 14.9 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 neighbor 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.

## 14.9.1 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.

### 14.9.2 LLDP-Med

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices. Endpoints include devices such as IP phones, or other Voice over IP (VoIP) devices or servers and network devices such as switches. It specifically provides support for VoIP applications. LLDP-MED provides this support using an additional set of common type-length-value (TLV) advertisement messages, for capabilities discovery, network policy, Power over Ethernet, inventory management and location information.

The device supports the following TLV messages:

- capabilities TLV
  Lets the LLDP-MED endpoints determine the capabilities that the connected device supports and what capabilities the device has enabled.
- Network policy TLV
  Lets both network connectivity devices and endpoints advertise VLAN configurations and associated attributes for the specific application on that port. For example, the device notifies a phone of the VLAN number. The phone connects to a switch, obtain its VLAN number, and then starts communicating with the call control.

LLDP-MED provides the following functions:

- Network policy discovery, including VLAN ID, 802.1p priority and Diffserv code point (DSCP)
- Device location and topology discovery based on LAN-level MAC/port information
- Endpoint move detection notification, from network connectivity device to the associated VoIP management application
- Extended device identification for inventory management
- Identification of endpoint network connectivity capabilities, for example, multi-port IP Phone with embedded switch or bridge capability
- Application level interactions with the LLDP protocol elements to provide timely startup of LLDP to support rapid availability of an Emergency Call Service
- Applicability of LLDP-MED to Wireless LAN environments, support for Voice over Wireless LAN

# 14.10 Detecting loops

Loops in the network cause connection interruptions or data loss. This also applies to temporary loops. The automatic detection and reporting of this situation lets you detect it faster and diagnose it more easily.

An incorrect configuration causes loops, for example, deactivating Spanning Tree.

The device lets you detect the effects typically caused by loops and report this situation automatically to the network management station. You have the option here to specify the magnitude of the loop effects that trigger the device to send a report.

BPDU frames sent from the designated port and received on either a different port of the same device or the same port within a short time, is a typical effect of a loop.

To check if the device has detected a loop, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *CIST* tab.
- ☐ Check the value in the *Port state* and *Port role* fields. If the *Port state* field displays the value `discarding` and the *Port role* field displays the value `backup`, then the port is in a loop status.
  or
- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *Guards* tab.
- ☐ Check the value in the *Loop state* column. If the field displays the value `true`, then the port is in a loop status.

# 14.11 Help protect against layer 2 network loops

The device helps protect against layer 2 network loops.

A network loop can lead to a standstill of the network due to overload. A possible reason is the continuous duplication of data packets due to a misconfiguration. The cause could be, for example, an incorrectly plugged cable or faulty settings in the device.

For example, a layer 2 network loop can occur in the following cases, if no redundancy protocols are active:
- Two ports of the same device are directly connected to each other.
- More than one active connection is established between two devices.

## 14.11.1 Application example

The figure displays examples for possible layer 2 loops in a network. The *Loop Protection* function is enabled in every device.
- **A**: *Active mode*
  Ports that are intended to connect end devices operate in the *active* mode. The device evaluates and sends *loop detection* packets on these ports.
- **P**: *Passive mode*
  Ports which belong to the redundant rings operate in the *passive* mode. The device only evaluates *loop detection* packets on these ports.
- **Loop 1**..**Loop 4**
  Unintentionally configured layer 2 network loops.

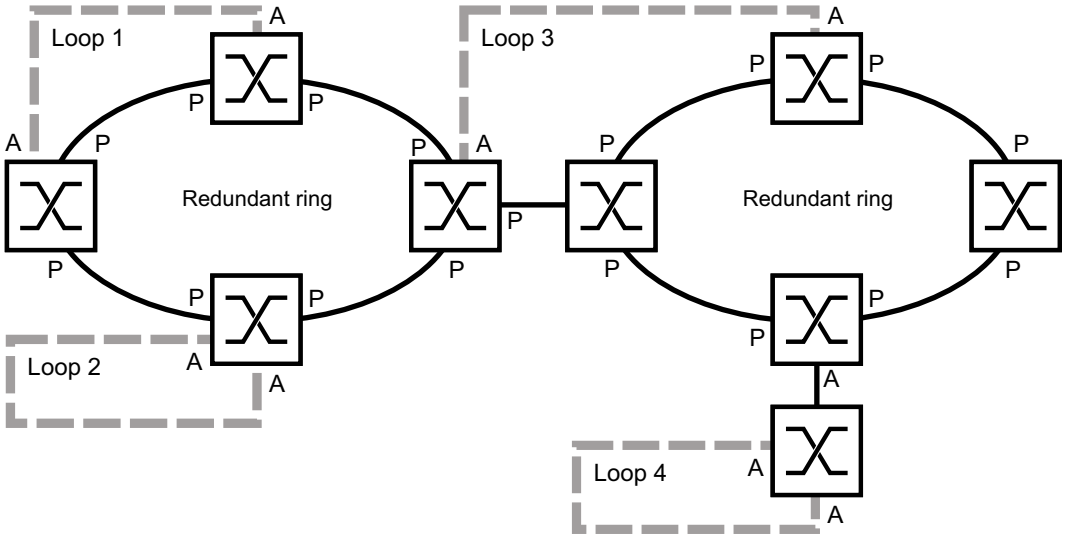



*Figure 107: Examples for unintended layer 2 network loops*

### Assign the Loop Protection settings to the ports

For each *active* and each *passive* port, assign the settings of the *Loop Protection* function.

Perform the following steps:

- ☐ Open the *Diagnostics > Loop Protection* dialog.
- ☐ In the *Global* frame, *Transmit interval* field, adjust the value, if necessary.
- ☐ In the *Global* frame, *Receive threshold* field, adjust the value, if necessary.
- ☐ In the *Mode* column, specify the behavior of the *Loop Protection* function on the port:
  - `active` for ports that are intended to connect end devices
  - `passive` for ports which belong to the redundant rings
- ☐ In the *Action* column, specify the value *all*.
  When the device detects a layer 2 loop on this port, then it sends a trap and disables the port using the *Auto-Disable* function. If necessary, adjust the value.
- ☐ In the *Active* column, mark the checkbox.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `loop-protection tx-interval 5` | Specify the transmit interval, if necessary. |
| `loop-protection rx-threshold 1` | Specify the receive threshold, if necessary. |
| `interface 1/1` | Change to the Interface mode.<br>Example: port *1/1*. |
| `loop-protection mode active` | Specify the mode `active` for ports that are intended to connect end devices. |
| `loop-protection mode passive` | Specify the mode `passive` for ports which belong to the redundant rings. |
| `loop-protection action all` | Specify the action that the device performs when it detects a layer 2 network loop on this port. |
| `loop-protection operation` | Activate the *Loop Protection* function on the port. |
| `exit` | Change to the Configuration mode. |

### Activate the Auto-Disable function

After you assigned the *Loop Protection* settings to the ports, activate the *Auto-Disable* function.

Perform the following steps:

- ☐ In the*Configuration* frame, mark the *Auto-disable* checkbox.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `loop-protection auto-disable` | Activate the *Auto-Disable* function. |

#### Enable the Loop Protection function in the device

When finished, enable the *Loop Protection* function in the device.

Perform the following steps:

- ☐ In the*Operation* frame, select the *On* radio button.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `loop-protection operation` | Enable the *Loop Protection* function in the device. |

### 14.11.2 Recommendations for redundant ports

Depending on the *Loop Protection* settings, the device disables ports using the *Auto-Disable* function when the device detects a layer 2 network loop.

If any redundancy function is active on a port, then do not activate the *active* mode on this port. Otherwise, port shutdowns on redundant network paths can be the result. In the example above these are the ports which belong to the redundant rings.

Verify that a redundant network path is available as backup media. The device changes to the redundant path in case of the outage of the primary path.

The following settings help avoid port shutdowns on redundant network paths:
- ☐ Disable the *Loop Protection* function on redundant ports.
  or
- ☐ Enable the *passive* mode on redundant ports.

The *Loop Protection* function and the *Spanning Tree* function have an effect on each other. The following steps help avoid unexpected behavior of the device:
- ☐ Disable the *Spanning Tree* function on the port on which you want to enable the *Loop Protection* function. See the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *STP active* column.
- ☐ Disable the*Spanning Tree* function on the connected port of each connected device. See the *Switching > L2-Redundancy > Spanning Tree* dialog.

# 14.12 Using the Email Notification function

The device lets you inform users by email about events that have occurred. Prerequisite is that a mail server is available through the network on which the device transfers the emails.

To set up the device to send emails, perform the steps in the following chapters:
- ☐ Specify the sender address
- ☐ Specify the triggering events
- ☐ Specify the recipients
- ☐ Specify the mail server
- ☐ Enable/disable the Email Notification function
- ☐ Send a test email

## 14.12.1 Specify the sender address

The sender address is the email address that indicates the device which sent the email. In the device, the default setting is `switch@hirschmann.com`.

Change the preset value. To do this, perform the following steps:

- ☐ Open the *Diagnostics > Email Notification > Global* dialog.
- ☐ In the *Sender* frame, change the value in the *Address* field. Add a valid email address.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `logging email from-addr <user@doma.in>` | Changes the sender address. |

## 14.12.2 Specify the triggering events

The device differentiates between the following severities:

*Table 62: Meaning of the severities for events*

| Severity | Meaning |
|---|---|
| `emergency` | Device not ready for operation |
| `alert` | Immediate user intervention required |
| `critical` | Critical status |
| `error` | Error status |
| `warning` | Warning |
| `notice` | Significant, normal status |
| `informational` | Informal message |
| `debug` | Debug message |

You have the option of specifying the events of which the device informs you. For this, assign the desired minimum severity to the notification levels of the device.

The device informs the recipients as follows:

- *Notification immediate*
  When an event of the severity assigned or more severe occurs, the device sends an email immediately.
- *Notification periodic*
  - When an event of the severity assigned or more severe occurs, the device logs the event in a buffer.
  - The device sends an email with the log file periodically or if the buffer is full.
  - When an event of a lower severity occurs, the device does not log this event.

Perform the following steps:

☐ Open the *Diagnostics > Email Notification > Global* dialog.

In the *Notification immediate* frame, you specify the settings for emails which the device sends immediately.

☐ In the *Severity* field, you specify the minimum severity.

☐ In the *Subject* field, you specify the subject of the email.

In the *Notification periodic* frame, you specify the settings for emails which the device sends periodically.

☐ In the *Severity* field, you specify the minimum severity.

☐ In the *Subject* field, you specify the subject of the email.

☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `logging email severity immediate <level>` | Specifies the minimum severity for events for which the device sends an email immediately. |
| `logging email severity periodic <level>` | Specifies the minimum severity for events for which the device sends an email periodically. |
| `logging email subject add <immediate \| periodic> TEXT` | Creates a subject line with the content `TEXT`. |

### 14.12.3 Change the send interval

The device lets you specify in which interval it sends emails with the log file. The default setting is `30` minutes.

Perform the following steps:

☐ Open the *Diagnostics > Email Notification > Global* dialog.

In the *Notification periodic* frame, you specify the settings for emails which the device sends periodically.

☐ Change the value in the *Sending interval [min]* field to change the interval.

☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `logging email duration <30..1440>` | Specifies the interval at which the device sends emails with log file. |

### 14.12.4 Specify the recipients

The device lets you specify up to 10 recipients.

Perform the following steps:

- ☐ Open the *Diagnostics > Email Notification > Recipients* dialog.
- ☐ To add a table entry, click the button.
- ☐ In the *Notification type* column, specify if the device sends the emails to this recipient immediately or periodically.
- ☐ In the *Address* column, specify the email address of the recipient.
- ☐ In the *Active* column, mark the checkbox.
- ☐ Save the changes temporarily. To do this, click the button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `logging email to-addr add <1..10> addr <user@doma.in> msgtype <immediately \| periodically>` | Specifies the recipient with the email address `user@doma.in`. The device manages the settings in memory `1..10`. |

### 14.12.5 Specify the mail server

The device supports encrypted and unencrypted connections to the mail server.

Perform the following steps:

- ☐ Open the *Diagnostics > Email Notification > Mail Server* dialog.
- ☐ To add a table entry, click the button.
- ☐ In the *IP address* column, specify the IP address or the DNS name of the server.
- ☐ In the *Encryption* column, specify the protocol which encrypts the connection between the device and the mail server.
- ☐ When the mail server uses a port other than the well-known port, specify the TCP port in the *Destination TCP port* column.

When the mail server requests an authentication:

- ☐ In the *User name* and *Password* columns, specify the account credentials which the device uses to authenticate on the mail server.

- ☐ In the *Description* column, enter a meaningful name for the mail server.
- ☐ In the *Active* column, mark the checkbox.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `logging email mail-server add <1..5> addr <IP ADDRESS> [security <none\|tlsv1>] [username <USER NAME>] [password <PASSWORD>] [port <1..65535>]` | Specifies the mail server with the IP address `IP ADDRESS`. The device manages the settings in memory `1..5`. |

### 14.12.6 Enable/disable the Email Notification function

Perform the following steps:

- ☐ Open the *Diagnostics > Email Notification > 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `logging email operation` | Enables the sending of emails. |
| `no logging email operation` | Disables the sending of emails. |

### 14.12.7 Send a test email

The device lets you check the settings by sending a test email.

Prerequisite:
- ▶ The email settings are completely specified.
- ▶ The *Email Notification* function is enabled.

Perform the following steps:

- ☐ Open the *Diagnostics > Email Notification > Mail Server* dialog.
- ☐ Click the ≡ button and then the *Connection test* item.
  The dialog displays the *Connection test* window.
- ☐ In the *Recipient* drop-down list, select to which recipients the device sends the test email.
- ☐ In the *Message text* field, specify the text of the test email.
- ☐ Click the *Ok* button to send the test email.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `logging email test msgtype <urgent\|non-urgent> TEXT` | Sends an email with the content `TEXT` to the recipients. |

When you do not see any error messages and the recipients obtain the email, the device settings are correct.

# 14.13 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.

## 14.13.1 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.

### 14.13.2 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 TCP or 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `logging host add 1 addr 10.0.1.159 severity 3` | Adds 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`. |
| `logging syslog operation` | Enable the *Syslog* function. |
| `exit` | Change to the Privileged EXEC mode. |
| `show logging host` | Display the Syslog host settings. |

```
No.    Server IP      Port   Max. Severity   Type        Status
-----  -------------- -----  --------------  ----------  -------
1      10.0.1.159     514    error           systemlog   active
```

| | |
|---|---|
| `configure` | Change to the Configuration mode. |

```
logging snmp-requests get operation
```
Logs SNMP GET requests.

```
logging snmp-requests get severity 5
```
The value `5` specifies the severity level of the event that the device logs in case of SNMP GET requests. The value `5` means `notice`.

```
logging snmp-requests set operation
```
Logs SNMP SET requests.

```
logging snmp-requests set severity 5
```
The value `5` specifies the severity level of the event that the device logs in case of SNMP SET requests. The value `5` means `notice`.

```
exit
```
Change to the Privileged EXEC mode.

```
show logging snmp
```
Display the SNMP logging settings.

```
Log SNMP GET requests              : enabled
Log SNMP GET severity              : notice
Log SNMP SET requests              : enabled
Log SNMP SET severity              : notice
```

### 14.13.3 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.

### 14.13.4 Syslog over TLS

The Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating computer applications.

After initiating a connection with a Syslog server, using a TLS handshake, the device validates the certificate received from the server. For this purpose, you transfer the PEM certificate from a remote server or from the external memory onto the device. Verify that the configured IP address or DNS name of the server matches the information provided in the certificate. You find the information in the Common Name or in the Subject Alternative Name fields of the certificate.

The device sends the TLS encrypted Syslog messages over the TCP port specified in the *Destination UDP port* column.

**Note:** Specify the IP address or DNS name on the server to match the IP Address or DNS name provided in the server certificate. You find the values entered in the certificate as the Common Name or the Subject Alternative Name.

### Example

The given example describes the configuration of the *Syslog* function. By following these steps, the device lets you send the TLS encrypted Syslog messages over the TCP port specified in the *Destination UDP port* column.

The Syslog messages that are sent from a device to a syslog server can pass through unsecured networks. To configure a Syslog server over TLS, transfer the Certificate Authority (CA) certificate onto the device.

**Note:** In order for the changes to take effect after loading a new certificate, restart the *Syslog* function.

Perform the following steps:

- ☐ Open the *Diagnostics > Syslog* dialog.
- ☐ To initiate a connection with the Syslog servers, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

The device validates the certificate received. The device also authenticates the server and starts sending Syslog messages.

- ☐ Transfer the PEM certificate from the remote server or from the external memory onto the device.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `logging host add 1 addr 192.168.3.215` | Add index `1` to the Syslog server with IPv4 address `192.168.3.215`. |
| `logging host modify 1 port 6512 type systemlog` | Specifying the port number `6512` and logging the events in the system log. |
| `logging host modify 1 transport tls` | Specify the type of transmission as `tls`. |
| `logging host modify 1 severity informational` | Specifying the type of event to log into the system log as `informational`. |
| `exit` | Change to the Privileged EXEC mode. |
| `copy syslogcacert evmm` | Copy CA certificates from external memory to the device. |
| `show logging host` | Display the Syslog host settings. |

## 14.13.5 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
- 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

# 14.14 Network analysis with TCPdump

Tcpdump is a packet-sniffing UNIX utility used by network administrators to sniff and analyze traffic on a network. A couple of reasons for sniffing traffic on a network is to verify connectivity between hosts, or to analyze the traffic traversing the network.

TCPDump in the device provides the possibility to decode or capture packets received and transmitted by the Management CPU. This function is available using the `debug` command. Refer to the “Command Line Interface” reference manual for further information about the TCPDump function.

# 14.15 Monitoring the data traffic

The device lets you forward data packets that pass through the device to a destination port. There you can monitor and evaluate the data packets.

The device provides you with the following options:

- Port Mirroring
- VLAN mirroring
- Remote SPAN

## 14.15.1 Port Mirroring

The *Port Mirroring* function lets you copy data packets from physical source ports to a physical destination port.

You monitor the data traffic on the source ports in the sending and receiving directions with a management tool connected on the destination port, for example an RMON probe. The function has no affect on the data traffic running on the source ports.

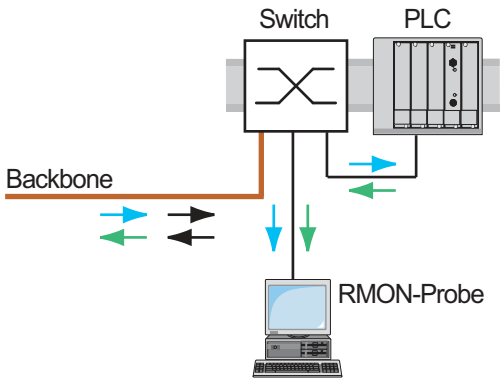



*Figure 108: Example*

On the destination port, the device only forwards the data packets copied from the source ports.

Before you switch on the *Port Mirroring* function, mark the checkbox *Allow management* to access the device management via the destination port. The device lets users access the device management via the destination port without interrupting the active *Port Mirroring* session.

**Note:** The device duplicates multicasts, broadcasts and unknown unicasts on the destination port.

The VLAN settings on the destination port remain unchanged. Prerequisite for access to the device management on the destination port is that the destination port is a member of the device management VLAN.

### Enabling the Port Mirroring function

Perform the following steps:

- ☐ Open the *Diagnostics > Ports > Port Mirroring* dialog.
- ☐ Specify the source ports.
  Mark the checkbox in the *Enabled* column for the relevant ports.
- ☐ Specify the destination port.
  In the *Destination port* frame, select the desired port in the *Primary port* drop-down list.
  The drop-down list only displays available ports. Ports that are already specified as source ports are unavailable.
- ☐ When needed, specify a second destination port.
  In the *Destination port* frame, select the desired port in the *Secondary port* drop-down list.
  The prerequisite is that you have already specified the primary destination port.
- ☐ In order to access the device management via the destination port:
  In the *Destination port* frame, mark the *Allow management* checkbox.
- ☐ Save the changes temporarily. To do this, click the button.

To deactivate the *Port Mirroring* function and restore the default settings, click the button and then the *Reset config* item.

## 14.15.2 VLAN mirroring

The *VLAN mirroring* function lets you mirror the received data stream that matches a specific VLAN to a selected destination port. The device only copies the data on the VLAN, and sends the original data to the intended recipients. For example, the device can mirror data to a network analyzer connected to the destination port.

Only one of the functions, either the *VLAN mirroring* function or the *Port Mirroring* function, can be active at the same time. When you select VLAN 0 as the source VLAN, the *VLAN mirroring* function is inactive. To disable the *VLAN mirroring* function, unmark the checkbox in the *Enabled* column for the source port.

If the data stream received on the mirrored VLAN exceeds the maximum bandwidth of the destination port, then the device drops some packets to accommodate the maximum bandwidth of the destination port. Even though the device drops some packets, the device continues to mirror packets that match the specified VLAN.

When you specify the PVID on a port as the source VLAN ID, the device mirrors the untagged packets received, but without a VLAN tag. In this case, the device mirrors the packet exactly as it received the packet.

### Example configuration

In this example configuration, Sw 4 mirrors data received on VLAN 20 to a network analyzer on the destination port.

To configure VLAN mirroring on Sw 4 use the following steps:
- ☐ Create the mirrored VLAN.
- ☐ Configure VLAN mirroring

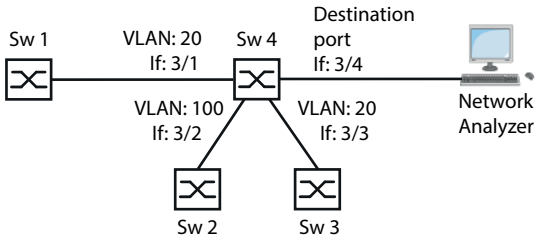



*Figure 109: VLAN Mirroring Example Configuration*

Perform the following steps:

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Add the VLAN:
  - ☐ Click the button.
    The dialog displays the *Create* window.
  - ☐ In the *VLAN ID* field, specify the value `20`.
  - ☐ Click the *Ok* button.
  - ☐ In the *Name* column, enter the value `VLAN mirroring port`.
- ☐ Save the changes temporarily. To do this, click the button.
- ☐ Open the *Diagnostics > Ports > Port Mirroring* dialog.
- ☐ Deactivating the *Port Mirroring* function:
  Unmark every checkbox in the *Enabled* column.
- ☐ Specifying the destination port:
  In the *Destination port* frame, specify the value `3/4`.
- ☐ Specifying the data source:
  In the *VLAN mirroring* frame, *Source VLAN ID* field, specify the value `20`.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 20` | Create VLAN `20` in the device. |
| `name 20 VLAN mirroring port` | Assign the name `20` to the VLAN `VLAN mirroring port`. |
| `exit` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |

| | |
|---|---|
| `monitor session 1 source vlan 20` | Creates VLAN mirroring session `1`, the source is VLAN `20`. |
| `monitor session 1 destination interface 3/4` | Specifies port `3/4` as the destination port. |
| `monitor session 1 mode` | Activates VLAN mirroring session `1`. |

### 14.15.3 Remote SPAN

Remote Switch Port Analysis (RSPAN) lets the network administrator forward mirrored data across multiple devices to a destination port. The network administrator can then analyze the data or diagnose detected errors on the network from a central location. The device lets the network administrator analyze data from a single source or from multiple sources.

The mirrored data traverses the network on a specified VLAN. Each RSPAN device uses the same RSPAN VLAN to forward mirrored data. Furthermore, any port, except the mirrored ports, can be a member of the RSPAN VLAN.

Depending on the amount of data and the port bandwidth, the device can drop some of the mirrored data. To reduce the loss of mirrored data packets, use Gigabit ports and/or LAG interfaces to forward the RSPAN data to the destination device.

The network administrator configures the devices, used for RSPAN, depending on the various roles. RSPAN uses the following device configurations:

- A Source device mirrors and tags the data with the RSPAN VLAN ID and forwards the data only to the destination port of the source device. On the source device, specify the RSPAN VLAN in the *Destination VLAN ID* field.
  IF the source device forwards the uplink data and the RSPAN data on the same link, then the device requires a Reflector port. The reflector port tags the RSPAN VLAN data with the RSPAN VLAN ID. The device then forwards the tagged data to the destination device. In order to accomplish this task, the network administrator connects 2 ports on the source device together with an Ethernet cable.
- The Destination device aggregates the data tagged with the RSPAN VLAN ID and then forwards the data to the destination port. On the destination device, specify the RSPAN VLAN in the *Source VLAN ID* field. The normal data stream can share the port with the RSPAN VLAN data.
- An Intermediate device floods the data tagged with the RSPAN VLAN ID to the ports with RSPAN VLAN membership. On an intermediate device, specify the RSPAN VLAN in the *VLAN ID* field. The device can transmit the RSPAN VLAN data over a LAG link toward the RSPAN destination device.

The device can forward RSPAN data to the destination device over an MRP ring network as long as the destination ring device is not a ring member. The device can also forward RSPAN data over a LAG instance as long as the LAG ports are not destination ports.

**Note:** To help prevent erroneous loop detection in case you use the *RSPAN* function. If you connect to the neighboring devices using separate paths for uplink and RSPAN data, then verify that the Spanning-Tree Protocol is inactive on both ports of the RSPAN data links. If you use a reflector port, then verify that the Spanning-Tree protocol is inactive on the links forwarding the RSPAN data.

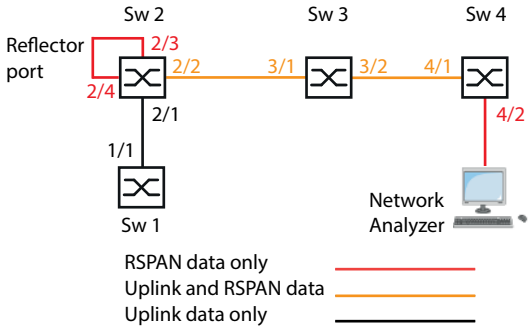
In the following examples the network administrator desires to mirror the data stream to a network analyzer located somewhere in the network. The examples demonstrate the various ways to integrate the source device in your network.

In the examples, the network administrator desires to mirror the data packets received from switch 1, on port `2/1` of switch 2 to the network analyzer connected to switch 4. The network administrator has specified VLAN 30 as the RSPAN VLAN ID.

**Note:** Use only RSPAN-aware devices to forward the RSPAN data.

### Example 1

In the example, you configure a reflector port on switch 2. Connect the ports `2/3` and `2/4` together with an ethernet cable. The links between switch 2, switch 3 and switch 4 carry both the RSPAN and the uplink data stream. Afterwards, perform the following steps:




Configure switch 2 as a port mirroring source.

Perform the following steps:

- ☐ Open the *Switching* > *VLAN* > *Configuration* dialog.
- ☐ Add the VLAN:
  Click the button.
  The dialog displays the *Create* window.
  In the *VLAN ID* field, specify the value `30`.
  Click the *Ok* button.
  In the *Name* column, specify the value `RSPAN_VLAN`.
- ☐ Specifying port `2/2` as a member of the RSPAN VLAN:
  For VLAN `30`, specify in the *2/2* column the value `T`.
- ☐ Block management packets from being forwarded to port `2/4`.
  For VLAN `1`, specify in the *2/4* column the value `-`.
- ☐ Save the changes temporarily. To do this, click the button.
- ☐ Open the *Diagnostics* > *Ports* > *Port Mirroring* dialog.
- ☐ Specifying the destination port:
  In the *Destination port* frame, specify the value `2/3`.
- ☐ Specifying the RSPAN VLAN:
  In the *RSPAN* frame, *VLAN ID* field, specify the value `30`.
- ☐ Specifying the destination VLAN:
  In the *RSPAN* frame, *Destination VLAN ID* field, specify the value `30`.
- ☐ Specifying the data source:
  For port `2/1`, mark the checkbox in the *Enabled* column.
- ☐ Specifying the direction:
  For port `2/1`, specify in the *Type* column the value `txrx`.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the button.

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.
- ☐ Deactivating the *Spanning Tree* function on port 2/4:
  For port 2/4, unmark the checkbox in the *STP active* column.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 30` | Create VLAN 30 in the device. |
| `name 30 RSPAN_VLAN` | Assign the name 30 to the VLAN RSPAN_VLAN. |
| `rspan-vlan 30` | Specify VLAN 30 as the RSPAN VLAN. |
| `exit` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `monitor session 1 source add interface 2/1` | Add port 2/1 to session 1 as a source port. |
| `monitor session 1 destination interface 2/3` | Add port 2/3 to session 1 as a source port. |
| `monitor session 1 destination remote vlan 30` | Create VLAN mirroring session 1. The source is VLAN 30. |
| `monitor session 1 mode` | Activate the VLAN mirroring session 1. |
| `interface 2/2` | Change to the interface configuration mode of interface 2/2. |
| `vlan participation include 30` | Specify that port 2/2 is a member of VLAN 30. |
| `vlan tagging 30` | Specify that port 2/2 forwards VLAN 30 data. |
| `exit` | Change to the Configuration mode. |
| `interface 2/4` | Change to the interface configuration mode of interface 2/4. |
| `vlan participation auto 1` | When requested, the port participates in this VLAN. |
| `spanning-tree mode disable` | Deactivate STP on the port. |
| `exit` | Change to the Configuration mode. |

Configure switch 3 as an intermediate device.

Perform the following steps:

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Add the VLAN:
  Click the button.
  The dialog displays the *Create* window.
  In the *VLAN ID* field, specify the value 30.
  Click the *Ok* button.
  In the *Name* column, specify the value RSPAN_VLAN.
- ☐ Specifying port 3/2 as a member of the RSPAN VLAN:
  For VLAN 30, specify in the *3/2* column the value T.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 30` | Create VLAN `30` in the device. |
| `name 30 RSPAN_VLAN` | Assign the name `30` to the VLAN `RSPAN_VLAN`. |
| `rspan-vlan 30` | Specify VLAN `30` as the RSPAN VLAN. |
| `exit` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 3/2` | Change to the interface configuration mode of interface `3/2`. |
| `vlan participation include 30` | Specify that port `3/2` is a member of VLAN `30`. |
| `vlan tagging 30` | Specify that port `3/2` forwards VLAN `30` data. |
| `exit` | Change to the Configuration mode. |

Configure switch 4 as the destination device.

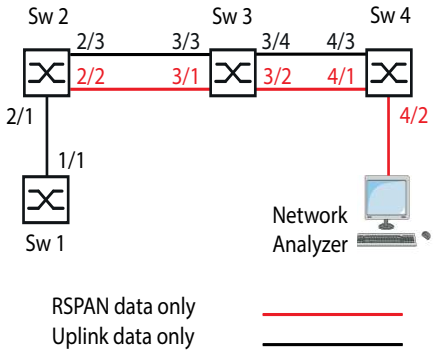
Perform the following steps:

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Add the VLAN:
  Click the button.
  The dialog displays the *Create* window.
  In the *VLAN ID* field, specify the value `30`.
  Click the *Ok* button.
  In the *Name* column, specify the value `RSPAN_VLAN`.
- ☐ Save the changes temporarily. To do this, click the button.
- ☐ Open the *Diagnostics > Ports > Port Mirroring* dialog.
- ☐ Specifying the destination port:
  In the *Destination port* frame, specify the value `4/2`.
- ☐ Specifying the RSPAN VLAN:
  In the *RSPAN* frame, *VLAN ID* field, specify the value `30`.
- ☐ Specifying the data source:
  In the *RSPAN* frame, *Source VLAN ID* field, specify the value `30`.
- ☐ To enable the function, select the *On* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 30` | Create VLAN `30` in the device. |
| `name 30 RSPAN_VLAN` | Assign the name `30` to the VLAN `RSPAN_VLAN`. |
| `rspan-vlan 30` | Specify VLAN `30` as the RSPAN VLAN. |
| `exit` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `monitor session 1 source remote vlan 30` | Specify VLAN `30` as the RSPAN data source. |
| `monitor session 1 destination interface 4/2` | Specify port `4/2` as the destination port. |
| `monitor session 1 mode` | Activate the VLAN mirroring session `1`. |

### Example 2

In this example, the network forwards the RSPAN data and the uplink data on parallel paths from the source device to the destination device.




Configure switch 2 as a port mirroring source.

Perform the following steps:

- ☐ Open the *Switching* > *VLAN* > *Configuration* dialog.
- ☐ Add the VLAN:
  Click the button.
  The dialog displays the *Create* window.
  In the *VLAN ID* field, specify the value `30`.
  Click the *Ok* button.
  In the *Name* column, specify the value `RSPAN_VLAN`.
- ☐ Specifying port `2/3` as a non-member of the RSPAN VLAN:
  For VLAN `30`, specify in the *2/3* column the value `-`.
- ☐ Save the changes temporarily. To do this, click the button.
- ☐ Open the *Diagnostics* > *Ports* > *Port Mirroring* dialog.
- ☐ Specifying the destination port:
  In the *Destination port* frame, specify the value `2/2`.
- ☐ Specifying the destination VLAN:
  In the *RSPAN* frame, *Destination VLAN ID* field, specify the value `30`.
- ☐ Specifying the data source:
  For port `2/1`, mark the checkbox in the *Enabled* column.
- ☐ Specifying the direction:
  For port `2/1`, specify in the *Type* column the value `txrx`.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 30` | Create VLAN `30` in the device. |
| `name 30 RSPAN_VLAN` | Assign the name `30` to the VLAN `RSPAN_VLAN`. |
| `rspan-vlan 30` | Specify VLAN `30` as the RSPAN VLAN. |
| `exit` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |

| | |
|---|---|
| `monitor session 1 source add interface 2/1` | Add port `2/1` to session `1` as a source port. |
| `monitor session 1 destination interface 2/3` | Add port `2/3` to session `1` as a source port. |
| `monitor session 1 destination remote vlan 30` | Create VLAN mirroring session `1`. The source is VLAN `30`. |
| `monitor session 1 mode` | Activate the VLAN mirroring session `1`. |
| `interface 2/3` | Change to the interface configuration mode of interface `2/3`. |
| `vlan participation auto 30` | When requested, the port participates in this VLAN. |
| `exit` | Change to the Configuration mode. |

Configure switch 3 as an intermediate device.

Perform the following steps:

- ☐ Open the *Switching* > *VLAN* > *Configuration* dialog.
- ☐ Add the VLAN:
  Click the button.
  The dialog displays the *Create* window.
  In the *VLAN ID* field, specify the value `30`.
  Click the *Ok* button.
  In the *Name* column, specify the value `RSPAN_VLAN`.
- ☐ Specifying port `3/1` as a non-member of the management VLAN:
  For VLAN `1`, specify in the *3/1* column the value `-`.
- ☐ Specifying port `3/2` as a non-member of the management VLAN:
  For VLAN `1`, specify in the *3/2* column the value `-`.
- ☐ Specifying port `3/2` as a member of the RSPAN VLAN:
  For VLAN `30`, specify in the *3/2* column the value `T`.
- ☐ Specifying port `3/3` as a non-member of the RSPAN VLAN:
  For VLAN `30`, specify in the *3/3* column the value `-`.
- ☐ Specifying port `3/4` as a non-member of the RSPAN VLAN:
  For VLAN `30`, specify in the *3/4* column the value `-`.
- ☐ Save the changes temporarily. To do this, click the button.
- ☐ Open the *Switching* > *L2-Redundancy* > *Spanning Tree* > *Port* dialog.
- ☐ Deactivating the *Spanning Tree* function on port `3/1`:
  For port `3/1`, unmark the checkbox in the *STP active* column.
- ☐ Deactivating the *Spanning Tree* function on port `3/2`:
  For port `3/2`, unmark the checkbox in the *STP active* column.
- ☐ Save the changes temporarily. To do this, click the button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 30` | Create VLAN `30` in the device. |
| `name 30 RSPAN_VLAN` | Assign the name `30` to the VLAN `RSPAN_VLAN`. |
| `rspan-vlan 30` | Specify VLAN `30` as the RSPAN VLAN. |
| `exit` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |

| | |
|---|---|
| `interface 3/1` | Change to the interface configuration mode of interface `3/1`. |
| `vlan participation auto 1` | When requested, the port participates in this VLAN. |
| `spanning-tree mode disable` | Deactivate STP on the port. |
| `exit` | Change to the Configuration mode. |
| `interface 3/2` | Change to the interface configuration mode of interface `3/2`. |
| `vlan participation include 30` | Specify that port `3/2` is a member of VLAN `30`. |
| `vlan tagging 30` | Specify that port `3/2` forwards VLAN `30` data. |
| `vlan participation auto 1` | When requested, the port participates in this VLAN. |
| `spanning-tree mode disable` | Deactivate STP on the port. |
| `exit` | Change to the Configuration mode. |
| `interface 3/3` | Change to the interface configuration mode of interface `3/3`. |
| `vlan participation auto 30` | When requested, the port participates in this VLAN. |
| `exit` | Change to the Configuration mode. |
| `interface 3/4` | Change to the interface configuration mode of interface `3/4`. |
| `vlan participation auto 30` | When requested, the port participates in this VLAN. |
| `exit` | Change to the Configuration mode. |

Configure switch 4 as the destination device.

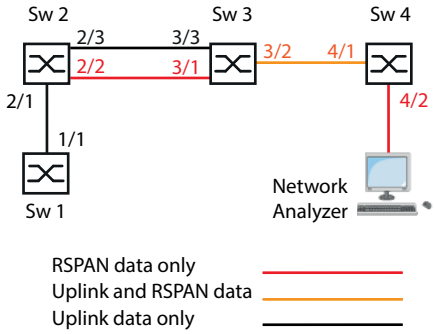
Perform the following steps:

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Add the VLAN:
  Click the button.
  The dialog displays the *Create* window.
  In the *VLAN ID* field, specify the value `30`.
  Click the *Ok* button.
  In the *Name* column, specify the value `RSPAN_VLAN`.
- ☐ Save the changes temporarily. To do this, click the button.
- ☐ Open the *Diagnostics > Ports > Port Mirroring* dialog.
- ☐ Specifying the destination port:
  In the *Destination port* frame, specify the value `4/2`.
- ☐ Specifying the data source:
  In the *RSPAN* frame, *Source VLAN ID* field, specify the value `30`.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the button.
- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.
- ☐ Deactivating the *Spanning Tree* function on port `4/1`:
  For port `4/1`, unmark the checkbox in the *STP active* column.
- ☐ Save the changes temporarily. To do this, click the button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 30` | Create VLAN `30` in the device. |
| `name 30 RSPAN_VLAN` | Assign the name `30` to the VLAN `RSPAN_VLAN`. |
| `rspan-vlan 30` | Specify VLAN `30` as the RSPAN VLAN. |
| `exit` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `monitor session 1 destination interface 4/2` | Specify port `4/2` as the destination port. |
| `monitor session 1 source remote vlan 30` | Specify VLAN `30` as the RSPAN data source. |
| `monitor session 1 mode` | Activate the VLAN mirroring session `1`. |
| `interface 4/1` | Change to the interface configuration mode of interface `4/1`. |
| `spanning-tree mode disable` | Deactivate STP on the port. |
| `exit` | Change to the Configuration mode. |

### Example 3

In the example, the source device switch 2 sends the uplink data and the RSPAN data to the intermediate device switch 3. The intermediate device switch 3 then forwards the combined traffic on a single link to the destination device switch 4.




Configure switch 2 as a port mirroring source.

Perform the following steps:

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Add the VLAN:
  Click the button.
  The dialog displays the *Create* window.
  In the *VLAN ID* field, specify the value `30`.
  Click the *Ok* button.
  In the *Name* column, specify the value `RSPAN_VLAN`.
- ☐ Specifying port `2/3` as a member of the RSPAN VLAN:
  For VLAN `30`, specify in the *2/3* column the value `-`.
- ☐ Save the changes temporarily. To do this, click the button.
- ☐ Open the *Diagnostics > Ports > Port Mirroring* dialog.

- ☐ Specifying the destination port:
  In the *Destination port* frame, specify the value `2/2`.
- ☐ Specifying the destination VLAN:
  In the *RSPAN* frame, *Destination VLAN ID* field, specify the value `30`.
- ☐ Specifying the data source:
  For port `2/1`, mark the checkbox in the *Enabled* column.
- ☐ Specifying the direction:
  For port `2/1`, specify in the *Type* column the value `txrx`.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 30` | Create VLAN `30` in the device. |
| `name 30 RSPAN_VLAN` | Assign the name `30` to the VLAN `RSPAN_VLAN`. |
| `rspan-vlan 30` | Specify VLAN `30` as the RSPAN VLAN. |
| `exit` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `monitor session 1 destination interface 2/2` | Add port `2/3` to session `1` as a source port. |
| `monitor session 1 destination remote vlan 30` | Create VLAN mirroring session `1`. The source is VLAN `30`. |
| `monitor session 1 source add interface 2/1` | Add port `2/1` to session `1` as a source port. |
| `monitor session 1 mode` | Activate the VLAN mirroring session `1`. |
| `interface 2/3` | Change to the interface configuration mode of interface `2/3`. |
| `vlan participation auto 30` | When requested, the port participates in this VLAN. |
| `exit` | Change to the Configuration mode. |

Configure switch 3 as an intermediate device.

Perform the following steps:

- ☐ Open the *Switching* > *VLAN* > *Configuration* dialog.
- ☐ Add the VLAN:
  Click the button.
  The dialog displays the *Create* window.
  In the *VLAN ID* field, specify the value `30`.
  Click the *Ok* button.
  In the *Name* column, specify the value `RSPAN_VLAN`.
- ☐ Specifying port `3/1` as a non-member of the management VLAN:
  For VLAN `1`, specify in the *3/1* column the value `-`.
- ☐ Specifying port `3/2` as a member of the RSPAN VLAN:
  For VLAN `30`, specify in the *3/2* column the value `T`.
- ☐ Specifying port `3/3` as a non-member of the management VLAN:
  For VLAN `1`, specify in the *3/3* column the value `-`.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.
- ☐ Deactivating the *Spanning Tree* function on port `3/1`:
  For port `3/1`, unmark the checkbox in the *STP active* column.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 30` | Create VLAN `30` in the device. |
| `name 30 RSPAN_VLAN` | Assign the name `30` to the VLAN `RSPAN_VLAN`. |
| `rspan-vlan 30` | Specify VLAN `30` as the RSPAN VLAN. |
| `exit` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 3/1` | Change to the interface configuration mode of interface `3/1`. |
| `vlan participation auto 1` | When requested, the port participates in this VLAN. |
| `spanning-tree mode disable` | Deactivate STP on the port. |
| `exit` | Change to the Configuration mode. |
| `interface 3/2` | Change to the interface configuration mode of interface `3/2`. |
| `vlan participation include 30` | Specify that port `3/2` is a member of VLAN `30`. |
| `vlan tagging 30` | Specify that port `3/2` forwards VLAN `30` data. |
| `exit` | Change to the Configuration mode. |
| `interface 3/3` | Change to the interface configuration mode of interface `3/3`. |
| `vlan participation auto 30` | When requested, the port participates in this VLAN. |
| `exit` | Change to the Configuration mode. |

Configure switch 4 as the destination device.

Perform the following steps:

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Add the VLAN:
  Click the button.
  The dialog displays the *Create* window.
  In the *VLAN ID* field, specify the value `30`.
  Click the *Ok* button.
  In the *Name* column, specify the value `RSPAN_VLAN`.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
- ☐ Open the *Diagnostics > Ports > Port Mirroring* dialog.
- ☐ Specifying the destination port:
  In the *Destination port* frame, specify the value `4/2`.
- ☐ Specifying the data source:
  In the *RSPAN* frame, *Source VLAN ID* field, specify the value `30`.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `vlan add 30` | Create VLAN `30` in the device. |
| `name 30 RSPAN_VLAN` | Assign the name `30` to the VLAN `RSPAN_VLAN`. |
| `rspan-vlan 30` | Specify VLAN `30` as the RSPAN VLAN. |
| `exit` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `monitor session 1 destination interface 4/2` | Specify port `4/2` as the destination port. |
| `monitor session 1 source remote vlan 30` | Specify VLAN `30` as the RSPAN data source. |
| `monitor session 1 mode` | Activate the VLAN mirroring session `1`. |

# 14.16 Self-test

The device checks its assets during the boot process and occasionally thereafter. The device checks system task availability or termination and the available amount of memory. Furthermore, the device checks for application functionality and any hardware degradation in the chip set.

If the device detects a loss in integrity, then the device responds to the degradation with a user-defined action. The following categories are available for configuration.

- `task`
  Action to be taken in case a task is unsuccessful.
- `resource`
  Action to be taken due to the lack of resources.
- `software`
  Action taken for loss of software integrity; for example, code segment checksum or access violations.
- `hardware`
  Action taken due to hardware degradation

Configure each category to produce an action in case the device detects a loss in integrity. The following actions are available for configuration.

- `log only`
  This action writes a message to the logging file.
- `send trap`
  Sends an SNMP trap to the trap destination.
- `reboot`
  If activated, then an error in the category will cause the device to reboot

Perform the following steps:

- ☐ Open the *Diagnostics > System > Selftest* dialog.
- ☐ In the *Action* column, specify the action to perform for a cause.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `selftest action task log-only` | To send a message to the event log when a task is unsuccessful. |
| `selftest action resource send-trap` | When there are insufficient resources, send an SNMP trap. |
| `selftest action software send-trap` | When the software integrity has been lost, send an SNMP trap. |
| `selftest action hardware reboot` | To reboot the device when hardware degradation occurs. |

Disabling these functions lets you decrease the time required to restart the device after a cold start. You find these options in the *Diagnostics > System > Selftest* dialog, *Configuration* frame.

- *RAM test*
  Activates/deactivates the *RAM test* function during a cold start.

- *SysMon1 is available*
  Activates/deactivates the System Monitor function during a cold start.
- *Load default config on error*
  Activates/deactivates the loading of the default device configuration in case no readable configuration is available during a restart.

The following settings block your access to the device permanently in case the device does not detect any readable configuration profile at restart.
- The *SysMon1 is available* checkbox is unmarked.
- The *Load default config on error* checkbox is unmarked.

This is the case, for example, when 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.

Perform the following steps:

| | |
|---|---|
| `selftest ramtest` | Enable RAM selftest on cold start. |
| `no selftest ramtest` | Disable the "ramtest“ function. |
| `selftest system-monitor` | Enable the "SysMon1“ function. |
| `no selftest system-monitor` | Disable the "SysMon1“ function. |
| `show selftest action` | Show status of the actions to be taken in the event of device degradation. |
| `show selftest settings` | Display the settings for "ramtest" and "SysMon" settings in event of a cold start. |

# 14.17 Copper cable test

Use this feature to test copper cables attached to an interface for a short or open circuit. The test interrupts traffic flow, when in progress, on this port.

The table displays the state and lengths of each individual pair. The device returns a result with the following meaning:

- normal - indicates that the cable is operating properly
- open - indicates an interruption in the cable
- short circuit - indicates a short circuit in the cable
- untested - indicates an untested cable
- Unknown - cable unplugged

# 14.18 Network monitoring with sFlow

*SFlow* is a standard protocol for monitoring networks. The device provides this function for visibility into network activity, enabling effective management and control of network resources.

The *SFlow* monitoring system consists of an *SFlow* agent, embedded in the device and a central *SFlow* collector. The agent uses sampling technology to capture traffic statistics. *SFlow* instances associated with individual data sources within the agent perform packet flow and counter sampling. Using *SFlow* datagrams the agent forwards the sampled traffic statistics to an *SFlow* collector for analysis.

The agent uses 2 forms of sampling, a statistical packet based sampling of packet flows and a timed based sampling of counters. An *SFlow* datagram contains both types of samples. Packet flow sampling, based on a sampling rate, sends a steady, but random stream of datagrams to the collector. For time-based sampling, the agent polls the counters at set intervals to fill the datagrams.

The device implements datagram version 5 for the *SFlow* agent.

The user-defined *SFlow* functions are:

- Sampler configuration, packet flow sampling:
  - data source port number, to sample physical ports
  - receiver index associated with the sampler
  - Sampling rate
    The device counts the packets of received data. When the count reaches the user-defined number, the agent samples the packet.
    Range: `256..65535`
    `0` = function inactive
  - Header size in bytes to sample
    Range: `20..256`
- Poller configuration, counter sampling:
  - data source port number, available for physical ports
  - receiver index associated with the poller
  - Interval, in seconds, between samples
    Range: `0..86400`
- Receiver configuration, up to 8 entries:
  - Owner name, to claim an *SFlow* entry
  - timeout, in seconds, until sampling is stopped and the device releases the receiver along with the sampler and the poller
  - datagram size
  - IP address
  - port number

To configure the *SFlow* agent for a monitoring session, first configure an available receiver. Then, configure a sampling rate to perform packet flow sampling. Additionally configure a polling interval for counter sampling.

For example, Company XYZ wishes to monitor data flow on a device. The IP address for the remote server containing the sFlow collector, is `10.10.10.10`. XYZ requires a sample of the first 256 bytes of every 300th packet. Furthermore, XYZ requires counter polling every 400 s.

Perform the following steps:

- ☐ Open the *Diagnostics > SFlow > Receiver* dialog.
- ☐ For the name of the person or organization controlling the receiver, enter the value `XYZ` in the *Name* column.
- ☐ For the remote server IP Address, on which the *SFlow* collector software runs, enter the value `10.10.10.10` in the *IP address* column.
- ☐ Open the *Diagnostics > SFlow > Configuration* dialog, *Sampler* tab.
- ☐ In the *Receiver* column, select the index number of the receiver specified in the previous steps.
- ☐ In the *Sampling rate* column, specify the value `300`.
- ☐ In the *Max. header size [byte]* column, specify the value `256`.
- ☐ Open the *Diagnostics > SFlow > Configuration* dialog, *Poller* tab.
- ☐ In the *Receiver* column, select the index number of the receiver specified in the previous steps.
- ☐ In the *Interval [s]* column, specify the value `400`.
- ☐ Save the changes temporarily. To do this, click the ✔ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `sflow receiver 1 owner XYZ ip 10.10.10.10` | Configure an *SFlow* receiver |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `sflow sampler receiver 1 rate 300` | To assign the *SFlow* sampler on the port to the previously configured receiver with a sampling rate of `300`. |
| `sflow sampler maxheadersize 256` | To configure the maximum header size of the *SFlow* sampler to the value `256`. |
| `sflow poller receiver 1interval 400` | To assign the *SFlow* poller to the previously configured receiver and to sample data for `400` s. |

# 15 Advanced functions of the device

## 15.1 Using the device as a DHCP server

A DHCP server ("Dynamic Host Configuration Protocol") assigns IP addresses, Gateways, and other networking definitions such as DNS and NTP parameters to clients.

The DHCP operations fall into 4 basic phases: IP discovery, IP lease offer, IP request, and IP lease acknowledgment. Use the acronym DORA which stands for Discovery, Offer, Request, and Acknowledgement to help remember the phases. The server receives client data on UDP port 67 and forwards data to the client on UDP port 68.

The DHCP server provides an IP address pool or "pool", from which it allocates IP addresses to clients. The pool consists of a list of entries. An entry defines either a specific IP address or an IP address range.

The device lets you activate the DHCP server globally and per interface.

### 15.1.1 IP Addresses assigned per port or per VLAN

The DHCP server assigns a static IP address or dynamic range of IP addresses to a client connected to a port or a VLAN. The device lets you create entries for either a port or a VLAN. When creating an entry to assign an IP address to a VLAN, the port entry grays out. When creating an entry to assign an IP address to a port, the VLAN entry grays out.

Static allocation means that the DHCP server assigns the same IP address to a specific client. The DHCP server identifies the client using a unique hardware ID. A static address entry contains one IP address, and applies it to a port or VLAN on which the server receives a request from a specific client. For static allocation, create a pool entry for the ports or one specific port, enter the IP address, and leave the *Last IP address* column empty. Specify a hardware ID with which the DHCP server uniquely identifies the client. This ID is either a MAC address, a client ID, a remote ID, or a circuit ID. When a client contacts the server with the configured hardware ID, the DHCP server allocates the static IP address.

When routing is enabled, the *DHCP Server* function for a specific DHCP pool only takes effect if one of the following prerequisites is met:

- The device has a router interface in the subnet of the respective DHCP pool.
- The device management is located in the subnet of the respective DHCP pool.

The device also lets you assign a dynamic IP address range to ports or VLANs from which the DHCP server allocates a free IP address from a pool. To add a dynamic pool entry for the ports or VLANs, specify the first and last IP addresses for the IP address range, leaving the *MAC address*, *Client ID*, *Remote ID*, and *Circuit ID* columns empty. Creating multiple pool entries lets you have IP address ranges that contain gaps.

### 15.1.2 DHCP server static IP address example

In this example, configure the device to allocate a static IP address to a port. The device recognizes clients with unique hardware identification. The Hardware ID in this case is the client MAC address `00:24:E8:D6:50:51`. To do this, perform the following steps:

- ☐ Open the *Advanced > DHCP Server > Pool* dialog.
- ☐ To add a table entry, click the button.
- ☐ In the *IP address* column, specify the value `192.168.23.42`.
- ☐ In the *Port* column, specify the value `1/1`.
- ☐ In the *MAC address* column, specify the value `00:24:E8:D6:50:51`.
- ☐ To assign the IP address to the client infinitely, in the *Lease time [s]* column, specify the value `4294967295`.
- ☐ Mark the checkbox in the *Active* column.
- ☐ Open the *Advanced > DHCP Server > Global* dialog.
- ☐ For port `1/1`, mark the checkbox in the *DHCP server 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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `dhcp-server pool add 1 static 192.168.23.42` | Creating an entry with index `1` and adding the IP address `192.168.23.42` to the static pool. |
| `dhcp-server pool modify 1 mode interface 1/1` | Assign the static address in index `1` to interface `1/1`. |
| `dhcp-server pool modify 1 mode mac 00:24:E8:D6:50:51` | Assign the IP address in index `1` to the device with the MAC address `00:24:E8:D6:50:51`. |
| `dhcp-server pool mode 1` | Enable the index `1` pool entry. |
| `dhcp-server pool modify 1 leasetime infinite` | To allocate the IP address to the client infinitely, modify the entry with index `1`. |
| `dhcp-server operation` | Enable the DHCP server globally. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `dhcp-server operation` | Activate the *DHCP Server* server function on this port. |

### 15.1.3 DHCP server dynamic IP address range example

The device lets you create dynamic IP address ranges. Leave the *MAC address*, *Client ID*, *Remote ID* and *Circuit ID* fields empty. To create dynamic IP address ranges with gaps between the ranges add several entries to the table. To do this, perform the following steps:

- ☐ Open the *Advanced* > *DHCP Server* > *Pool* dialog.
- ☐ To add a table entry, click the button.
- ☐ In the *IP address* column, specify the value `192.168.23.92`. This is the first IP address of the range.
- ☐ In the *Last IP address* column, specify the value `192.168.23.142`. This is the last IP address of the range.

In the *Lease time [s]* column, the default setting is 60 days.

- ☐ In the *Port* column, specify the value `1/2`.
- ☐ Mark the checkbox in the *Active* column.
- ☐ Open the *Advanced* > *DHCP Server* > *Global* dialog.
- ☐ For port `1/2`, mark the checkbox in the *DHCP server 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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `dhcp-server pool add 2 dynamic 192.198.23.92 192.168.23.142` | Add a dynamic pool with an IP range from `192.168.23.92` to `192.168.23.142`. |
| `dhcp-server pool modify 2 leasetime {seconds \| infinite}` | Entering the Lease Time in seconds or infinite. |
| `dhcp-server pool add 3 dynamic 192.198.23.172 192.168.23.180` | Add a dynamic pool with an IP range from `192.168.23.172` to `192.168.23.180`. |
| `dhcp-server pool modify 3 leasetime {seconds \| infinite}` | Entering the Lease Time in seconds or infinite. |
| `dhcp-server pool mode 2` | Enable the index `2` pool entry. |
| `dhcp-server pool mode 3` | Enable the index `3` pool entry. |
| `dhcp-server operation` | Enable the DHCP server globally. |
| `interface 2/1` | Change to the interface configuration mode of interface `2/1`. |
| `dhcp-server operation` | Activate the *DHCP Server* server function on this port. |

# 15.2 DHCP L2 Relay

A network administrator uses the DHCP Layer 2 *Relay Agent* to add DHCP client information. This information is required by Layer 3 *Relay Agents* and DHCP servers to assign an address and configuration to a client.

When a DHCP client and server are in the same IP subnet, they exchange IP address requests and replies directly. However, having a DHCP server on each subnet is expensive and often impractical. An alternative to having a DHCP server in every subnet is to use the network devices to relay packets between a DHCP client and a DHCP server located in a different subnet.

A Layer 3 *Relay Agent* is generally a router that has IP interfaces in both the client and server subnets and routes traffic between them. However, in Layer 2 switched networks, there are one or more network devices, switches for example, between the client and the Layer 3 *Relay Agent* or DHCP server. In this case, this device provides a Layer 2 *Relay Agent* to add the information that the Layer 3 *Relay Agent* and DHCP server require to perform their roles in address and configuration assignment.

The following list contains the default settings for this function:
- Global setting:
  - Active setting: disable
- Interface settings:
  - Active setting: disable
  - Trusted Port: disable
- VLAN settings:
  - Active setting: disable
  - *Circuit ID*: enable
  - *Remote ID* Type: mac
  - *Remote ID*: blank

## 15.2.1 Circuit and Remote IDs

In an IPv4 environment, before forwarding the request of a client to the DHCP server, the device adds the *Circuit ID* and the *Remote ID* to the *Option 82* field of the DHCP request packet.
- The *Circuit ID* stores on which port the device received the request of the client.
- The *Remote ID* contains the MAC address, the IP address, the system name, or a user-defined character string. Using it, the participating devices identify the *Relay Agent* that received the request of the client.

The device and other *Relay Agents* use this information to re-direct the answer from the DHCP *Relay Agent* to the original client. The DHCP server is able to analyze this data for example to assign the client an IP address from a specific address pool.

Also, the replay packet of the DHCP server contains the *Circuit ID* and the *Remote ID*. Before forwarding the answer to the client, the device removes the information from the *Option 82* field.

### 15.2.2 DHCP L2 Relay configuration

The *Advanced > DHCP L2 Relay > Configuration* dialog lets you activate the function on the active ports and on the VLANs. In the *Operation* frame, select the *On* radio button. Then click the ✓ button.

The device forwards DHCPv4 packets with *Option 82* information on those ports for which the checkbox in the *DHCP L2 Relay* column and in the *Trusted port* column is marked. Typically, these are ports in the network of the DHCP server.

The ports to which the DHCP clients are connected, you activate the *DHCP L2 Relay* function, but leave the *Trusted port* checkbox unmarked. On these ports, the device discards DHCPv4 packets with *Option 82* information.

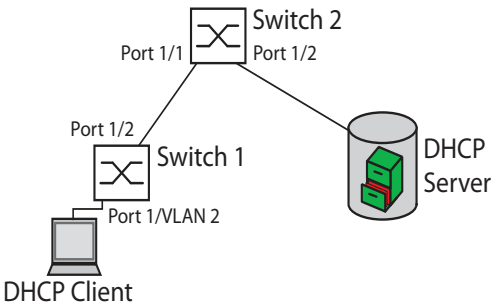



*Figure 110: DHCP Layer 2 Example Network*

Perform the following steps on Switch 1:

- ☐ Open the *Advanced > DHCP L2 Relay > Configuration* dialog, *Interface* tab.
- ☐ For port `1/1`, specify the settings as follows:
  - Mark the checkbox in the *Active* column.
- ☐ For port `1/2`, specify the settings as follows:
  - Mark the checkbox in the *Active* column.
  - Mark the checkbox in the *Trusted port* column.
- ☐ Open the *Advanced > DHCP L2 Relay > Configuration* dialog, *VLAN ID* tab.
- ☐ Specify the settings for VLAN 2 as follows:
  - Mark the checkbox in the *Active* column.
  - Mark the checkbox in the *Circuit ID* column.
  - To use the IP address of the device as the *Remote ID*, in the *Remote ID type* column, specify the value `ip`.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

Perform the following steps on Switch 2:

- ☐ Open the *Advanced > DHCP L2 Relay > Configuration* dialog, *Interface* tab.
- ☐ For port `1/1` and `1/2`, specify the settings as follows:
  - Mark the checkbox in the *Active* column.
  - Mark the checkbox in the *Trusted port* column.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

Verify that VLAN 2 is present. Then perform the following steps on Switch 1:

☐ Configure VLAN 2, and specify port 1/1 as a member of VLAN 2.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `vlan database` | Change to the VLAN configuration mode. |
| `dhcp-l2relay circuit-id 2` | Activate the Circuit ID and the DHCP Option 82 on VLAN 2. |
| `dhcp-l2relay remote-id ip 2` | Specify the IP address of the device as the Remote ID on VLAN 2. |
| `dhcp-l2relay mode 2` | Activate the *DHCP L2 Relay* function on VLAN 2. |
| `exit` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface 1/1. |
| `dhcp-l2relay mode` | Activate the *DHCP L2 Relay* function on the port. |
| `exit` | Change to the Configuration mode. |
| `interface 1/2` | Change to the interface configuration mode of interface 1/2. |
| `dhcp-l2relay trust` | Specify the port as *Trusted port*. |
| `dhcp-l2relay mode` | Activate the *DHCP L2 Relay* function on the port. |
| `exit` | Change to the Configuration mode. |
| `dhcp-l2relay mode` | Enable the *DHCP L2 Relay* function in the device. |

Perform the following steps on Switch 2:

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface 1/1. |
| `dhcp-l2relay trust` | Specify the port as *Trusted port*. |
| `dhcp-l2relay mode` | Activate the *DHCP L2 Relay* function on the port. |
| `exit` | Change to the Configuration mode. |
| `interface 1/2` | Change to the interface configuration mode of interface 1/2. |
| `dhcp-l2relay trust` | Specify the port as *Trusted port*. |
| `dhcp-l2relay mode` | Activate the *DHCP L2 Relay* function on the port. |
| `exit` | Change to the Configuration mode. |
| `dhcp-l2relay mode` | Enable the *DHCP L2 Relay* function in the device. |

# 15.3 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 configure the DNS client from the DHCP server using the device management VLAN. The device also 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
- static hostname to IP address mapping, with space for 64 configurable static hosts
- host cache, with space for 128 entries

## 15.3.1 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `dns client source user` | Specifying that the user manually configures the DNS client settings. |
| `dns client domain-name devicel` | Specifying the string `device1` as a unique domain name for the device. |
| `dns client servers add 1 ip 192.168.3.5` | To add a DNS name server with an IPv4 address of `192.168.3.5` as index `1`. |
| `dns client adminstate` | Enable the *DNS Client* function globally. |

Configure the DNS client to map static hosts with IP addresses. To do this, perform the following steps:

- ☐ Open the *Advanced > DNS > Client > Static Hosts* dialog.
- ☐ To add a table entry, click the button.
- ☐ In the *Name* column, enter the value `example.com`.
  This is a name of a device in the network.
- ☐ In the *IP address* column, specify the value `192.168.3.9`.
- ☐ Mark the checkbox in the *Active* column.
- ☐ Save the changes temporarily. To do this, click the button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `dns client host add 1 name example.com ip 192.168.3.9` | Add `example.com` as a static host with an IP address of `192.168.3.9`. |
| `dns client adminstate` | Enable the *DNS Client* function globally. |

# 15.4 GARP

The Generic Attribute Registration Protocol (*GARP*) is defined by the IEEE to provide a generic framework so switches can register and deregister attribute values, such as VLAN identifiers and Multicast group membership.

If an attribute for a participant is registered or deregistered according to the *GARP* function, then the participant is modified according to specific rules. The participants are a set of reachable end stations and network devices. The defined set of participants at any given time, along with their attributes, is the reachability tree for the subset of the network topology. The device forwards the data frames only to the registered end stations. The station registration helps prevent attempts to send data to the end stations that are unreachable.

## 15.4.1 Configuring GMRP

The GARP Multicast Registration Protocol (*GMRP*) is a Generic Attribute Registration Protocol (*GARP*) that provides a mechanism allowing network devices and end stations to dynamically register group membership. The devices register group membership information with the devices attached to the same LAN segment. The *GARP* function also lets the devices disseminate the information across the network devices that support extended filtering services.

**Note:** Before you enable the *GMRP* function, verify that the *MMRP* function is disabled.

The following example describes the configuration of the *GMRP* function. The device provides a constrained multicast flooding facility on a selected port. To do this, perform the following steps:

- ☐ Open the *Switching* > *GARP* > *GMRP* dialog.
- ☐ To provide constrained Multicast Flooding on a port, mark the checkbox in the *GMRP active* column.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `garp gmrp operation` | Enabling the *GMRP* function on the port. |
| `exit` | Change to the Configuration mode. |
| `garp gmrp operation` | Enabling the *GMRP* function globally. |

### 15.4.2 Configuring GVRP

You use the *GVRP* function to allow the device to exchange VLAN configuration information with other *GVRP* devices. Thus reducing unnecessary Broadcast and unknown Unicast traffic. Besides the *GVRP* function dynamically creates and manages VLANs on devices connected through 802.1Q trunk ports.

The following example describes the configuration of the *GVRP* function. The device lets you exchange VLAN configuration information with other *GVRP* devices. To do this, perform the following steps:

- ☐ Open the *Switching* > *GARP* > *GVRP* dialog.
- ☐ To exchange VLAN configuration information with other *GVRP* devices, mark checkbox in the *GVRP active* column for the port.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 3/1` | Change to the interface configuration mode of interface `3/1`. |
| `garp gvrp operation` | Enabling the *GVRP* function on the port. |
| `exit` | Change to the Configuration mode. |
| `garp gvrp operation` | Enabling the *GVRP* function globally. |

# 15.5 MRP-IEEE

The IEEE 802.1ak amendment to the IEEE 802.1Q standard introduced the Multiple Registration Protocol (MRP) to replace the Generic Attribute Registration Protocol (*GARP*). The IEEE also modified and replaced the *GARP* applications, *GARP* Multicast Registration Protocol (*GMRP*) and *GARP* VLAN Registration Protocol (*GVRP*), with the Multiple MAC Registration Protocol (*MMRP*) and the Multiple VLAN Registration Protocol (*MVRP*).

To confine traffic to the required areas of a network, the MRP applications distribute attribute values to MRP enabled devices across a LAN. The MRP applications register and de-register Multicast group memberships and VLAN identifiers.

**Note:** The Multiple Registration Protocol (MRP) requires a loop free network. To help prevent loops in your network, use a network protocol such as the Media Redundancy Protocol, Spanning Tree Protocol, or Rapid Spanning Tree Protocol with MRP.

## 15.5.1 MRP operation

Each participant contains an applicant component and an MRP Attribute Declaration (MAD) component. The applicant component is responsible for forming the attribute values and their registration and de-registration. The MAD component generates MRP messages for transmission and processes messages received from other participants. The MAD component encodes and transmits the attributes to other participants in MRP Data Units (MRPDU). In the switch, an MRP Attribute Propagation (MAP) component distributes the attributes to participating ports.

A participant exists for each MRP application and each LAN port. For example, a participant application exists on an end device and another application exists on a switch port. The Applicant state machine records the attribute and port for each MRP participant declaration on an end device or switch. Applicant state machine variable changes trigger the transmission of MRPDUs to communicate the declaration or withdrawal.

To establish an *MMRP* instance, an end device first sends a Join empty (JoinMt) message with the appropriate attributes. The switch then floods the JoinMt to the participating ports and to the neighboring switches. The neighboring switches flood the message to their participating port, and so on, establishing a path for the group traffic.

## 15.5.2 MRP timers

The default timer settings help prevent unnecessary attribute declarations and withdraws. The timer settings allow the participants to receive and process MRP messages before the Leave or LeaveAll timers expire.

When you reconfigure the timers, maintain the following relationships:

- To allow for re-registration after a Leave or LeaveAll event, although there is a lost message, set the value of the LeaveTime as follows: ≥ (2x JoinTime) + 60 in 1/100 s
- To minimize the volume of rejoining traffic generated following a LeaveAll, specify the value for the LeaveAll timer larger than the LeaveTime.

The following list contains various MRP events that the device transmits:
- Join - Controls the interval for the next Join message transmission
- Leave - Controls the length of time that a switch waits in the Leave state before changing to the withdraw state
- LeaveAll - Controls the frequency with which the switch generates LeaveAll messages

When expired, the Periodic timer initiates a Join request MRP message that the switch sends to participants on the LAN. The switches use this message to help prevent unnecessary withdraws.

## 15.5.3 MMRP

When a device receives Broadcast, Multicast or unknown traffic on a port, the device floods the traffic to the other ports. This process causes unnecessary use of bandwidth on the LAN.

The Multiple MAC Registration Protocol (*MMRP*) lets you control the traffic flooding by distributing an attribute declaration to participants on a LAN. The attribute values that the MAD component encodes and transmits on the LAN in MRP messages are Group service requirement information and 48-bit MAC addresses.

The switch stores the attributes in a filtering database as MAC address registration entries. The forwarding process uses the filtering database entries only to transmit data through those ports necessary to reach Group member LANs.

Switches facilitate the group distribution mechanisms based on the Open Host Group concept, receiving packets on the active ports and forwarding only to ports with group members. This way, any *MMRP* participants requiring packets transmitted to a particular group or groups, requests membership in the group. MAC service users send packets to a particular group from anywhere on the LAN. A group receives these packets on the LANs attached to registered *MMRP* participants. *MMRP* and the MAC Address Registration Entries thus restrict the packets to required segments of a loop-free LAN.

In order to maintain the registration and deregistration state and to receive traffic, a port declares interest periodically. Every device on a LAN with the *MMRP* function enabled maintains a filtering database and forwards traffic having the group MAC addresses to listed participants.

### MMRP example

In this example, Host A intends to listen to traffic destined to group G1. Switch A processes the *MMRP* Join request received from host A and sends the request to both of the neighboring switches. The devices on the LAN now recognize that there is a host interested in receiving traffic destined for group G1. When Host B starts transmitting data destined for group G1, the data flows on the path of registrations and Host A receives it.

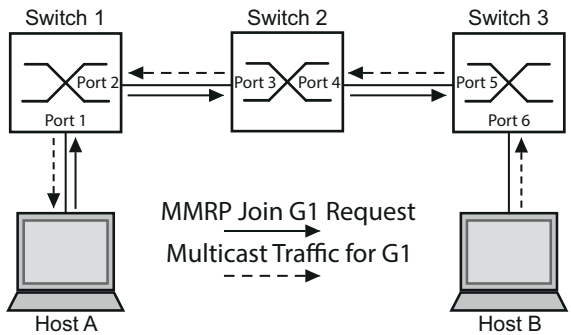



*Figure 111: MMRP Network for MAC address Registration*

Enable the *MMRP* function on the switches. To do this, perform the following steps:

- Open the *Switching* > *MRP-IEEE* > *MMRP* dialog, *Configuration* tab.
- To activate port `1` and port `2` as *MMRP* participants, mark the checkbox in the *MMRP* column for port `1` and port `2` on switch 1.
- To activate port `3` and port `4` as *MMRP* participants, mark the checkbox in the *MMRP* column for port `3` and port `4` on switch 2.
- To activate port `5` and port `6` as *MMRP* participants, mark the checkbox in the *MMRP* column for port `5` and port `6` on switch 3.
- To send periodic events allowing the device to maintain the registration of the MAC address group, enable the *Periodic state machine*. Select the `On` radio button in the *Configuration* frame.
- Save the changes temporarily. To do this, click the button.

To enable the *MMRP* ports on switch 1, use the following commands. Substituting the appropriate interfaces in the commands, enable the *MMRP* functions and ports on switches 2 and 3.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |
| `mrp-ieee mmrp operation` | Enabling the *MMRP* function on the port. |
| `interface 1/2` | Change to the interface configuration mode of interface `1/2`. |
| `mrp-ieee mmrp operation` | Enabling the *MMRP* function on the port. |
| `exit` | Change to the Configuration mode. |
| `mrp-ieee mrp periodic-state-machine` | Enabling the *Periodic state machine* function globally. |
| `mrp-ieee mmrp operation` | Enabling the *MMRP* function globally. |

### 15.5.4 MVRP

The Multiple VLAN Registration Protocol (*MVRP*) is an MRP application that provides dynamic VLAN registration and withdraw services on a LAN.

The *MVRP* function provides a maintenance mechanism for the Dynamic VLAN Registration Entries, and for transmitting the information to other devices. This information lets *MVRP*-aware devices establish and update their VLAN membership information. When members are present on a VLAN, the information indicates through which ports the switch forwards traffic to reach those members.

The main purpose of the *MVRP* function is to allow switches to discover some of the VLAN information that you otherwise manually set up. Discovering this information lets switches overcome the limitations of bandwidth consumption and convergence time in large VLAN networks.

### MVRP example

Set up a network comprised of MVRP aware switches (1 - 4) connected in a ring topology with end device groups, A1, A2, B1, and B2 in 2 different VLANs, A and B. With STP enabled on the switches, the ports connecting switch 1 to switch 4 are in the discarding state, helping prevent a loop condition.

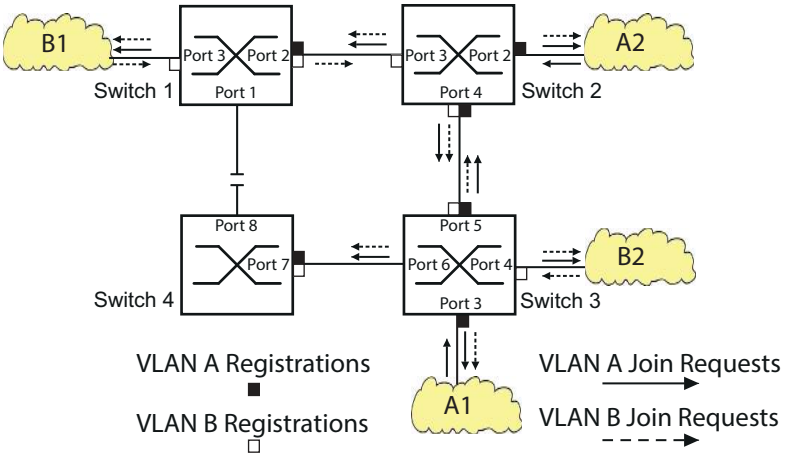



*Figure 112: MVRP Example Network for VLAN Registration*

In the MVRP example network, the LANs first send a Join request to the switches. The switch enters the VLAN registration in the forwarding database for the port receiving the frames.

The switch then propagates the request to the other ports, and sends the request to the neighboring LANs and switches. This process continues until the switches have registered the VLANs in the forwarding database of the receive port.

Enable MVRP on the switches. To do this, perform the following steps:

- ☐ Open the *Switching > MRP-IEEE > MVRP* dialog, *Configuration* tab.
- ☐ To activate the ports `1` through `3` as *MVRP* participants, mark the checkbox in the *MVRP* column for the ports `1` through `3` on switch 1.
- ☐ To activate the ports `2` through `4` as *MVRP* participants, mark the checkbox in the *MVRP* column for the ports `2` through `4` on switch 2.
- ☐ To activate the ports `3` through `6` as *MVRP* participants, mark the checkbox in the *MVRP* column for the ports `3` through `6` on switch 3.
- ☐ To activate port `7` and port `8` as *MVRP* participants, mark the checkbox in the *MVRP* column for port `7` and port `8` on switch 4.
- ☐ To maintain the registration of the VLANs, enable the *Periodic state machine*. Select the `On` radio button in the *Configuration* frame.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

To enable the *MVRP* ports on switch 1, use the following commands. Substituting the appropriate interfaces in the commands, enable the *MVRP* functions and ports on switches 2, 3 and 4.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `interface 1/1` | Change to the interface configuration mode of interface `1/1`. |

| | |
|---|---|
| `mrp-ieee mvrp operation` | Enabling the *MVRP* function on the port. |
| `interface 1/2` | Change to the interface configuration mode of interface `1/2`. |
| `mrp-ieee mvrp operation` | Enabling the *MVRP* function on the port. |
| `exit` | Change to the Configuration mode. |
| `mrp-ieee mvrp periodic-state-machine` | Enabling the *Periodic state machine* function globally. |
| `mrp-ieee mvrp operation` | Enabling the *MVRP* function globally. |

# 16 Industry Protocols

For a long time, automation communication and office communication were on different paths. The requirements and the communication properties were too different.

Office communication moves large quantities of data with low demands with respect to the transfer time. Automation communication moves small quantities of data with high demands with respect to the transfer time and availability.

While the transmission devices in the office are usually kept in temperature-controlled, relatively clean rooms, the transmission devices used in automation are exposed to wider temperature ranges. Dirty, dusty and damp ambient conditions make additional demands on the quality of the transmission devices.

With the continued development of communication technology, the demands and the communication properties have moved closer together. The high bandwidths now available in Ethernet technology and the protocols they support enable large quantities to be transferred and exact transfer times to be specified.

With the creation of the first optical LAN to be active worldwide, at the University of Stuttgart in 1984, Hirschmann laid the foundation for industry-compatible office communication devices. Thanks to Hirschmann's initiative with the world's first rail hub in the 1990s, Ethernet transmission devices such as switches, routers and firewalls are now available for the toughest automation conditions.

The desire for uniform, continuous communication structures encouraged many manufacturers of automation devices to come together and use standards to aid the progress of communication technology in the automation sector. This is why we now have protocols that enable us to communicate via Ethernet from the office right down to the field level.

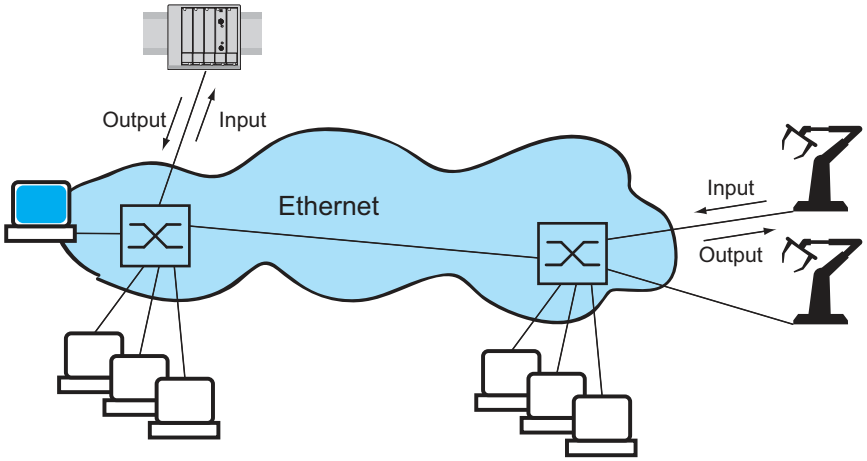



*Figure 113: Example of communication.*

# 16.1 OPC UA Server

The *Open Platform Communications United Architecture* (*OPC UA*) is a protocol for industrial communication, and describes a variety of *OPC UA* information models. The *OPC UA* protocol is a standardized protocol for the secure and reliable exchange of data in the industrial automation space and in other industries.

The *OPC UA* protocol provides a very flexible and adaptable mechanism for transferring the data between industrial automation equipment, monitoring devices, and sensors. The *OPC UA* protocol uses a standard interface, for example, *HTTPS* that makes the protocol simple to integrate into existing management systems. The device operating as an *OPC UA* server transmits the data of the connected end devices, ranging from simple uptime status to large amounts of complex industrial data.

The following figure displays the *OPC UA* information model data of the connected end devices available to the *OPC UA* client.

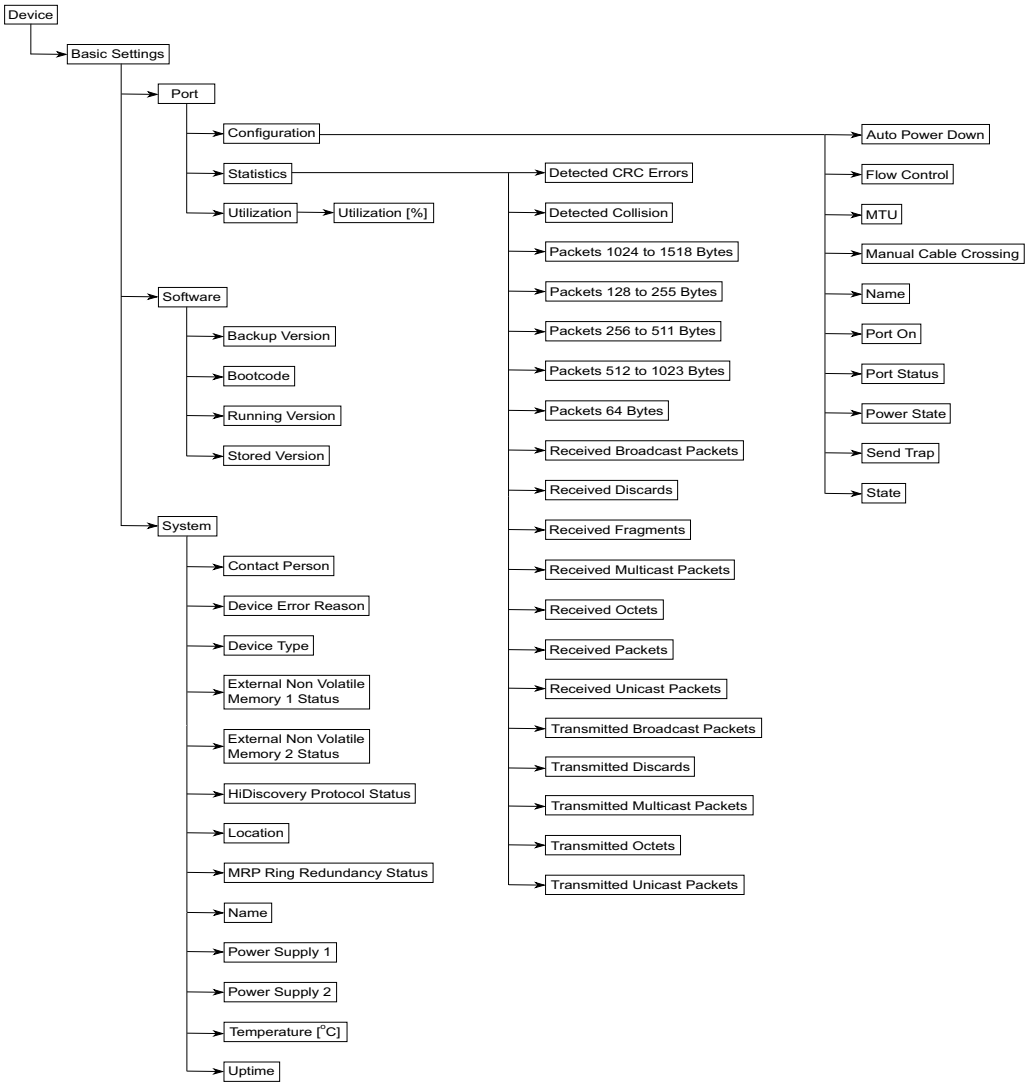



*Figure 114: OPC UA information model*

*Table 63: Objects in the OPC UA information model*

| Object | Description |
|---|---|
| *Auto power down* | Specifies how the port behaves when no cable is connected. |
| *Port on* | Activates/deactivates the 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. |
| *State* | Displays if the port is currently physically enabled or disabled. |
| *Port status* | Displays the link status of the port. |

*Table 64: Object values in the OPC UA information model*

| Object | Value | Description |
|---|---|---|
| Device Error Reason | 1 | None |
| | 2 | Power supply |
| | 3 | Link failure |
| | 4 | Temperature |
| | 5 | Fan failure |
| | 6 | Module removal |
| | 7 | External non volatile memory removal |
| | 8 | External non volatile memory not in synchronization |
| | 9 | Ring redundancy |
| External Non Volatile Memory 1 Status | 1 | Not present |
| | 2 | Removed |
| | 3 | Ok |
| | 4 | Out of memory |
| | 5 | Generic error |
| External Non Volatile Memory 2 Status | 1 | Not present |
| | 2 | Removed |
| | 3 | Ok |
| | 4 | Out of memory |
| | 5 | Generic error |
| HiDiscovery Protocol Status | 1 | Enabled |
| | 2 | Disabled |
| MRP Ring Redundancy Status | 1 | Available |
| | 2 | Not available |
| Power Supply 1 | 1 | Present |
| | 2 | Defective |
| | 3 | Not installed |
| | 4 | Unknown |
| Power Supply 2 | 1 | Present |
| | 2 | Defective |
| | 3 | Not installed |
| | 4 | Unknown |

*Table 64: Object values in the OPC UA information model*

| Object | Value | Description |
|---|---|---|
| Auto Power Down | 1 | Auto power down |
| | 2 | No power save |
| | 3 | Energy efficient ethernet |
| | 4 | Unsupported |
| Flow Control | 1 | Enabled |
| | 2 | Disabled |
| Manual Cable Crossing | 1 | Medium dependent interface |
| | 2 | Medium dependent interface crossover |
| | 3 | Auto medium dependent interface crossover |
| | 4 | Unsupported |
| Port On | 1 | Up |
| | 2 | Down |
| | 3 | Testing |
| Power State | 1 | Enabled |
| | 2 | Disabled |
| Send Trap | 1 | Enabled |
| | 2 | Disabled |
| State | 1 | Up |
| | 2 | Down |
| Port Status | 1 | Up |
| | 2 | Down |
| | 3 | Testing |
| | 4 | Unknown |
| | 5 | Dormant |
| | 6 | Not present |
| | 7 | Lower layer down |

The device operating as an *OPC UA* server processes the *OPC UA* information model data and transmits it securely to the *OPC UA* client application. The *OPC UA* server and *OPC UA* client communicate through a session.

The device operating as an *OPC UA* server shares the monitored data of the *OPC UA* information model. The user of the *OPC UA* client selects the items to be monitored in the *OPC UA* client application from a list of the International Electrotechnical Commission (IEC) variables. The *OPC UA* client application requests the *OPC UA* information model data from the device operating as an *OPC UA* server using the specified *OPC UA* user account data.

The device sets up an *OPC UA* session by first negotiating the policy for a secure connection. Over this secure connection, the *OPC UA* client sends the login credentials of the *OPC UA* user account. The *OPC UA* server in the device then authenticates the *OPC UA* client. When the login credentials are valid, the device grants the *OPC UA* client access to its *OPC UA Server* function.

The device offers a role-based authentication and encryption concept to specifically control the access to its *OPC UA* server. The *OPC UA* client can use commands and functions associated with the *OPC UA* user account set up in the device.

### 16.1.1 Enabling the OPC UA server

In the default setting, the *OPC UA Server* function is disabled. The *Advanced > Industrial Protocols > OPC UA Server* dialog lets you enable the *OPC UA Server* function. You can also specify the max. number of simultaneous *OPC UA* sessions. In the default setting, the values for the *Listening port* and *Sessions (max.)* fields are already specified. You specify the authentication and encryption protocol for *OPC UA* users at global level.

Perform the following steps:

- ☐ Open the *Advanced > Industrial Protocols > OPC UA Server* dialog.
- ☐ To enable the *OPC UA Server* function, select the *On* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
- ☐ In the *Listening port* field, change the TCP port number, if necessary.
- ☐ In the *Sessions (max.)* field, change the number of *OPC UA* sessions that can be established simultaneously, if necessary.
- ☐ In the *Security policy* field, select the authentication and encryption protocol.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
  The dialog displays the *To apply the changes, restart the OPC/UA server. Restart now?* window.
- ☐ To apply the changes, click the *Yes* button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `opc-ua operation` | Enable the *OPC UA Server* server. |
| `opc-ua port <1..65535>` | Change the TCP port number, if necessary. |
| `opc-ua sessions <1..5>` | Specify the number of *OPC UA* connections that can be established simultaneously. |
| `opc-ua security-policy none \| basic128rsa15 \| basic256 \| basic256sha256` | Specify the authentication and encryption protocol. |
| `show opc-ua global` | Display the *OPC UA* Server settings. |

```
IEC62541 - OPC/UA server settings
-------------------------
IEC62541 - OPC/UA server operation.........enabled
Listening port.............................4840
Number of concurrent sessions..............5
Configured security-policy.................none
```

### 16.1.2 Setting up an OPC UA user account

The device lets you manage the *OPC UA* user accounts required to access the device using a *OPC UA* client application. Every *OPC UA* client user requires an active *OPC UA* user account to gain access to the *OPC UA* server of the device.

In the following example, we will set up an *OPC UA* user account for the *OPC UA* client user `USER` which has read access. Then the user `USER` is authorized to monitor the *OPC UA* information model data. To do this, perform the following steps:

- ☐ Open the *Advanced > Industrial Protocols > OPC UA Server* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ Enter the name `USER` in the *User name* field.
- ☐ Click the *Ok* button.
- ☐ In the *Password* field, enter a password of at least 6 characters.
  In this example, we give the user account the password `SECRET`.
- ☐ In the *Access role* column, select the *readOnly* item.
- ☐ Save the changes temporarily. To do this, click the button.
  The dialog displays the *To apply the changes, restart the OPC/UA server. Restart now?* window.
- ☐ To apply the changes, click the *Yes* button.
  The dialog displays the *OPC UA* user accounts that are set up.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `users add USER` | Create the *OPC UA* user account `USER`. |
| `opc-ua users modify USER password`<br>`Enter NEW password: ****** (SECRET)`<br>`Confirm NEW password: ****** (SECRET)` | Enter and confirm the password `SECRET` for the *OPC UA* user account `USER`. Enter a password of at least 6 characters. |
| `opc-ua users modify USER access-role read-only` | Assign the access role *`readOnly`* to the *OPC UA* user account `USER`. |
| `opc-ua users enable USER` | Activate the user account `USER`. |
| `show opc-ua users` | Display the user accounts that are set up. |

```
User Name                Access-Role      Status
------------------------ ---------------- ------
user                     read-only        [x]
```

**Note:** When you set up a new *OPC UA* user account, remember to set the password.

### 16.1.3 Deactivating an OPC UA user account

After you deactivate the *OPC UA* user account, the user cannot access the device using the *OPC UA Server* function. Deactivating an *OPC UA* user account lets you keep the account settings and reuse them in the future. To do this, perform the following steps:

- ☐ Open the *Advanced > Industrial Protocols > OPC UA Server* dialog.
  The dialog displays the *OPC UA* user accounts that are set up.
- ☐ In the row for the relevant *OPC UA* user account, unmark the checkbox in the *Active* column.
- ☐ Save the changes temporarily. To do this, click the button.
  The dialog displays the *To apply the changes, restart the OPC/UA server. Restart now?* window.
- ☐ To apply the changes, click the *Yes* button.

```
enable                                  Change to the Privileged EXEC mode.
configure                               Change to the Configuration mode.
opc-ua users disable USER               Disable the user account USER.
show opc-ua users                       Display the user accounts that are set up.
User Name                 Access-Role   Status
------------------------- ------------- ------
user                      read-only     [ ]
save                                    Save the settings in the non-volatile memory (nvm)
                                        in the “selected” configuration profile.
```

### 16.1.4 Delete an OPC UA user account

To permanently deactivate the *OPC UA* user account settings, you delete the *OPC UA* user account. To do this, perform the following steps:

- ☐ Open the *Advanced > Industrial Protocols > OPC UA Server* dialog.
  The dialog displays the *OPC UA* user accounts that are set up.
- ☐ Highlight the row for the relevant *OPC UA* user account.
- ☐ Click the button.
- ☐ Save the changes temporarily. To do this, click the button.
  The dialog displays the *To apply the changes, restart the OPC/UA server. Restart now?* window.
- ☐ To apply the changes, click the *Yes* button.

```
enable                                  Change to the Privileged EXEC mode.
configure                               Change to the Configuration mode.
opc-ua users delete USER                Delete the user account USER.
show opc-ua users                       Display the user accounts that are set up.
User Name                 Access-Role   Status
------------------------- ------------- ------

save                                    Save the settings in the non-volatile memory (nvm)
                                        in the “selected” configuration profile.
```

# A Setting up the configuration environment

## A.1 Setting up a DHCP/BOOTP server

The following example describes the configuration of a DHCP server using the haneWIN DHCP Server software. This shareware software is a product of IT-Consulting Dr. Herbert Hanewinkel. You can download the software from www.hanewin.net. You can test the software for 30 calendar days from the date of the first installation, and then decide if you want to purchase a license.

Perform the following steps:

- ☐ Install the DHCP server on your PC.
  To carry out the installation, follow the installation assistant.
- ☐ Start the *haneWIN DHCP Server* program.

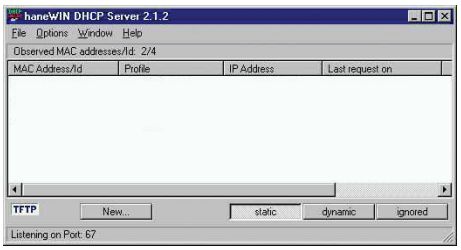



*Figure 115: Start window of the haneWIN DHCP Server program*

**Note:** When Windows is activated, the installation procedure includes a service that is automatically started in the basic configuration. This service is also active although the program itself has not been started. When started, the service responds to DHCP queries.

- ☐ In the menu bar, click the items *Options > Preferences* to open the program settings window.
- ☐ Select the *DHCP* tab.
- ☐ Specify the settings displayed in the figure.

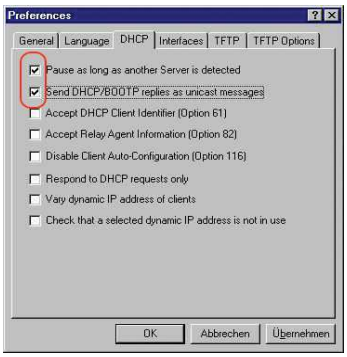



*Figure 116: DHCP setting*

- ☐ Click the *OK* button.
- ☐ To enter the configuration profiles, click in the menu bar the items *Options > Configuration Profiles*.

☐ Specify the name for the new configuration profile.

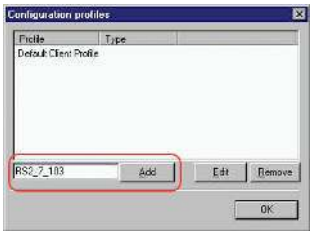



*Figure 117: Adding configuration profiles*

☐ Click the *Add* button.
☐ Specify the netmask.

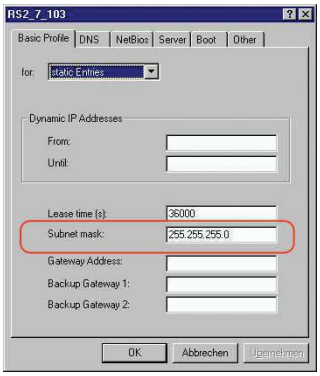



*Figure 118: Netmask in the configuration profile*

☐ Click the *Apply* button.
☐ Select the *Boot* tab.
☐ Enter the IP address of your tftp server.
☐ Enter the path and the file name for the configuration file.

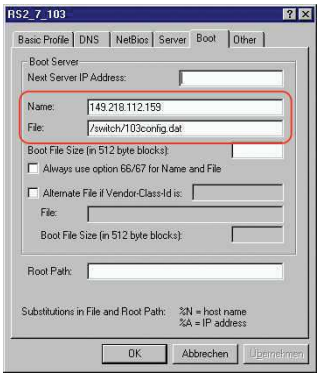



*Figure 119: Configuration file on the tftp server*

☐ Click the *Apply* button and then the *OK* button.

☐ Add a profile for each device type.
When devices of the same type have different configurations, you add a profile for each configuration.

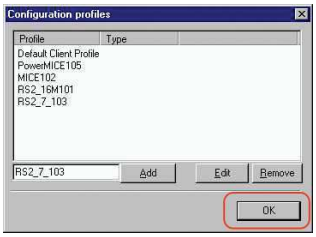



*Figure 120: Managing configuration profiles*

☐ To complete the addition of the configuration profiles, click the *OK* button.
☐ To enter the static addresses, in the main window, click the *Static* button.

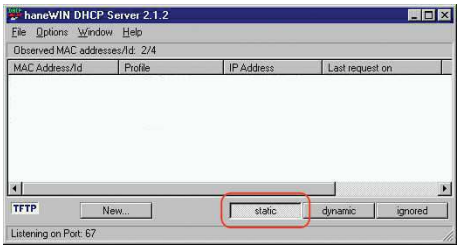



*Figure 121: Static address input*

☐ Click the *Add* button.

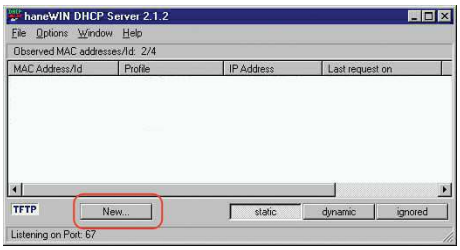



*Figure 122: Adding static addresses*

☐ Enter the MAC address of the device.
☐ Enter the IP address of the device.

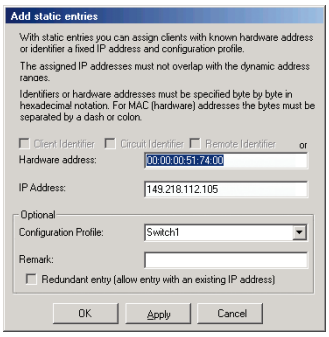



*Figure 123: Entries for static addresses*

☐ Select the configuration profile of the device.

- ☐ Click the *Apply* button and then the *OK* button.
- ☐ Add an entry for each device that will get its parameters from the DHCP server.

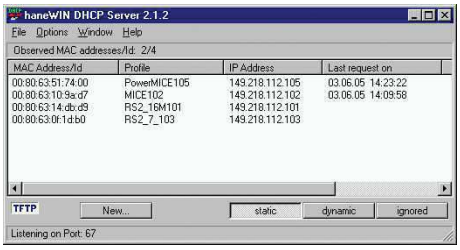



*Figure 124: DHCP server with entries*

# A.2 Setting up a DHCP server with Option 82

The following example describes the configuration of a DHCP server using the haneWIN DHCP Server software. This shareware software is a product of IT-Consulting Dr. Herbert Hanewinkel. You can download the software from www.hanewin.net. You can test the software for 30 calendar days from the date of the first installation, and then decide if you want to purchase a license.

Perform the following steps:

- ☐ Install the DHCP server on your PC.
  To carry out the installation, follow the installation assistant.
- ☐ Start the *haneWIN DHCP Server* program.

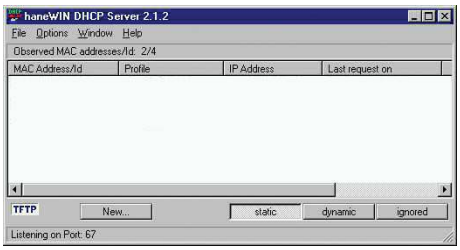



*Figure 125: Start window of the haneWIN DHCP Server program*

**Note:** When Windows is activated, the installation procedure includes a service that is automatically started in the basic configuration. This service is also active although the program itself has not been started. When started, the service responds to DHCP queries.

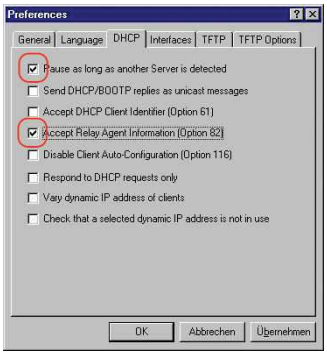



*Figure 126: DHCP setting*

- ☐ To enter the static addresses, click the *Add* button.

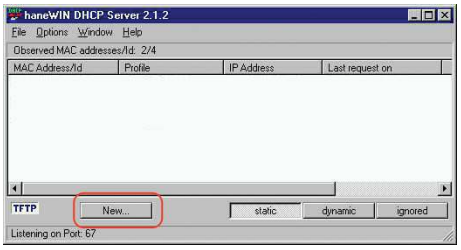



*Figure 127: Adding static addresses*

- ☐ Mark the *Circuit Identifier* checkbox.
- ☐ Mark the *Remote Identifier* checkbox.

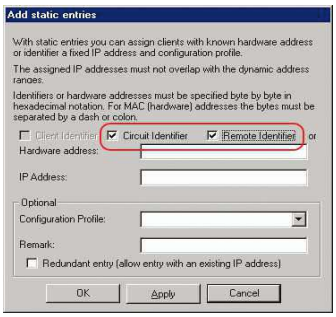



*Figure 128: Default setting for the fixed address assignment*

- ☐ In the *Hardware address* field, specify the value *Circuit Identifier* and the value *Remote Identifier* for the switch and port.
  The DHCP server assigns the IP address specified in the *IP address* field to the device that you connect to the port specified in the *Hardware address* field.
  The hardware address is in the following form:
  `ciclhhvvvvssmmpprirlxxxxxxxxxxxx`
  - `ci`
    Sub-identifier for the type of the Circuit ID
  - `cl`
    Length of the Circuit ID.
  - `hh`
    Hirschmann identifier:
    `01` when a Hirschmann device is connected to the port, otherwise `00`.
  - `vvvv`
    VLAN ID of the DHCP request.
    Default setting: `0001` = VLAN 1
  - `ss`

Socket of device at which the module with that port is located to which the device is connected. Specify the value `00`.

- `mm`
  Module with the port to which the device is connected.
- `pp`
  Port to which the device is connected.
- `ri`
  Sub-identifier for the type of the Remote ID
- `rl`
  Length of the Remote ID.
- `xxxxxxxxxxxx`
  Remote ID of the device (for example MAC address) to which a device is connected.

*Figure 129: Specifying the addresses*

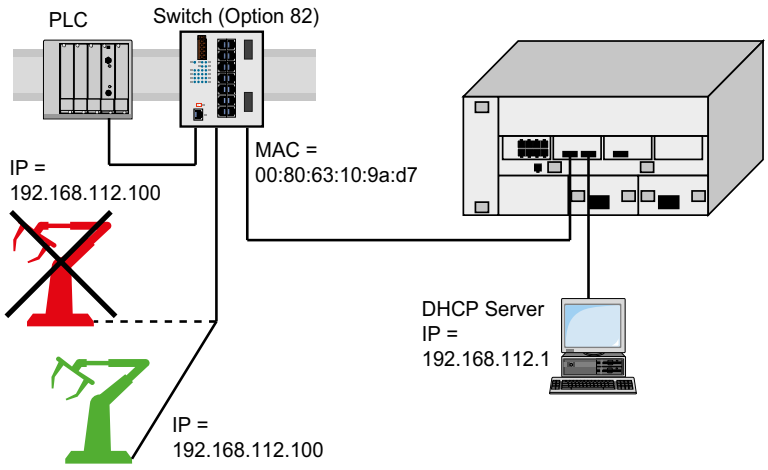



*Figure 130: Application example of using Option 82*

# A.3 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.3.1 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.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
- ☐ To create a RSA key, in the *Signature* frame, click the *Create* button.
- ☐ To enable the SSH server, select the *On* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `ssh key rsa generate` | Generate a new RSA key. |

## A.3.2 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 ''
rsaparam -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.
- ☐ 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.

- ☐ Click the *Start* button in the *Key import* frame to load the key onto the device.
- ☐ To enable the SSH server, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

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.3.3 Preparing the SSH client program

The *PuTTY* program lets you access the device using SSH. You can download the software from www.putty.org.

Perform the following steps:
- ☐ Start the program by double-clicking on it.

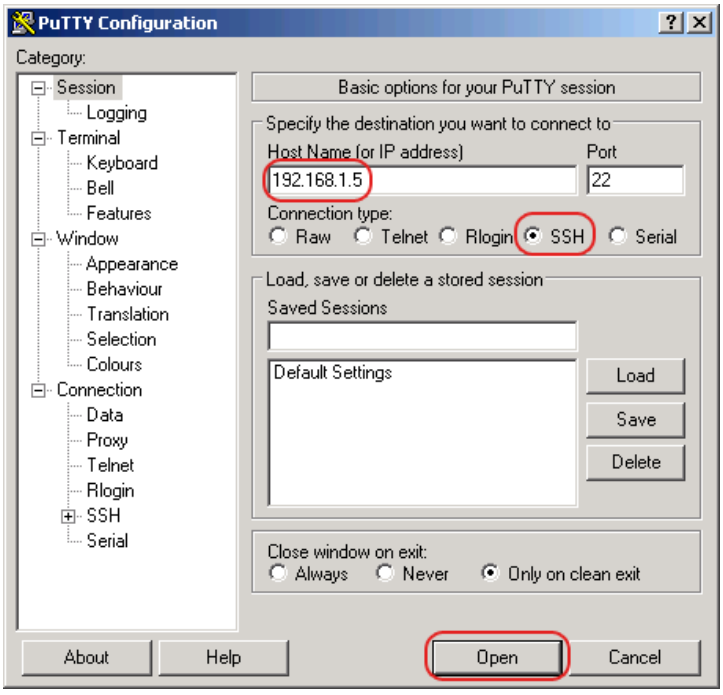



*Figure 131: PuTTY input screen*

- ☐ 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.

Before the connection is established, the *PuTTY* program displays a security alarm message and lets you check the key fingerprint.

*Figure 132: 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.4 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.4.1 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` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `https certificate generate` | Generate a https X.509/PEM Certificate. |
| `no https server` | Disable the *HTTPS* function. |
| `https server` | Enable the *HTTPS* function. |

☐ The device also enables you to transfer an externally generated X.509/PEM certificate onto the device:

- ☐ 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` | Change to the Privileged EXEC mode. |
| `copy httpscert envm <file name>` | Copy HTTPS certificate from external non-volatile memory device. |

| | |
|---|---|
| `configure` | Change to the Configuration mode. |
| `no https server` | Disable the *HTTPS* function. |
| `https server` | Enable the *HTTPS* function. |

**Note:** To activate the certificate after you created or transfered it, reboot the device or restart the HTTPS server. Restart the HTTPS server using the Command Line Interface.

### A.4.2 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.

| | |
|---|---|
| `enable` | Change to the Privileged EXEC mode. |
| `configure` | Change to the Configuration mode. |
| `https port 443` | Specifies the number of the TCP port on which the web server receives HTTPS requests from clients. |
| `https server` | Enable the *HTTPS* function. |
| `show https` | Displays the status of the *HTTPS* server and the port number. |

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.

# B 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
  ISBN 978-1-119-52791-6 (Print), ISBN 978-1-119-52799-2 (eBook)
  Get your free PDF copy on 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
  ISBN 978-1-449-31921-2 (Print)
- TCP/IP Illustrated, Volume 1: The Protocols (2nd Edition) (in English)
  W. R. Stevens and Kevin R. Fall
  Addison Wesley, 2011
  ISBN 978-0-321-33631-6
- Measurement, Control and Communication Using IEEE 1588 (in English)
  John C. Eidson
  Springer, 2006
  ISBN 978-1-84628-250-8 (Print), ISBN 978-1-84628-251-5 (eBook)
- 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:** | |
|---|---|
| Integer | An integer in the range $-2^{31}$ - $2^{31}$-1 |
| IP address | `xxx.xxx.xxx.xxx`<br>(`xxx` = integer in the range `0..255`) |
| MAC address | 12-digit hexadecimal number in accordance with ISO/IEC 8802-3 |
| Object Identifier | x.x.x.x… (for example 1.3.6.1.1.4.1.248...) |
| Octet String | ASCII character string |
| PSID | Power supply identifier (number of the power supply unit) |
| TimeTicks | Stopwatch, Elapsed time = numerical value / 100 (in seconds)<br>numerical value = integer in the range 0-$2^{32}$-1 |
| Timeout | Time value in hundredths of a second<br>time value = integer in the range 0-$2^{32}$-1 |
| Type field | 4-digit hexadecimal number in accordance with ISO/IEC 8802-3 |
| Counter | Integer (0-$2^{32}$-1), when certain events occur, the value increases by `1`. |

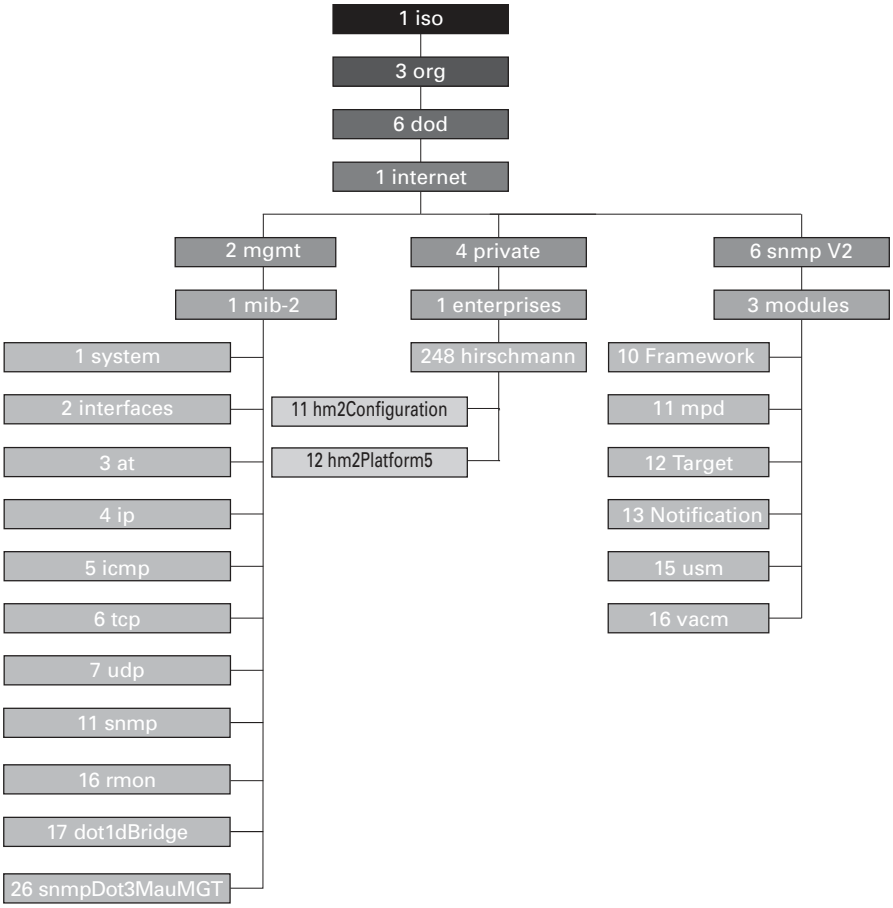



*Figure 133: Tree structure of the Hirschmann MIB*

A description of the MIB can be found on the product CD provided with the device.

# B.4 List of RFCs

| | |
|---|---|
| RFC 768 | UDP |
| RFC 783 | TFTP |
| RFC 791 | IP |
| RFC 792 | ICMP |
| RFC 793 | TCP |
| RFC 826 | ARP |
| RFC 854 | Telnet |
| RFC 855 | Telnet Option |
| RFC 951 | BOOTP |
| RFC 1112 | IGMPv1 |
| RFC 1157 | SNMPv1 |
| RFC 1155 | SMIv1 |
| RFC 1191 | Path MTU Discovery |
| RFC 1212 | Concise MIB Definitions |
| RFC 1213 | MIB2 |
| RFC 1256 | IRDP (ICMP router discovery) |
| RFC 1493 | Dot1d |
| RFC 1542 | BOOTP-Extensions |
| RFC 1643 | Ethernet-like -MIB |
| RFC 1757 | RMON |
| RFC 1812 | Requirements for IP Version 4 Routers |
| RFC 1867 | Form-Based File Upload in HTML |
| RFC 1901 | Community based SNMP v2 |
| RFC 1905 | Protocol Operations for SNMP v2 |
| RFC 1906 | Transport Mappings for SNMP v2 |
| RFC 1945 | HTTP/1.0 |
| RFC 2068 | HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03 |
| RFC 2082 | RIP v1/v2 |
| RFC 2131 | DHCP |
| RFC 2132 | DHCP-Options |
| RFC 2233 | The Interfaces Group MIB using SMI v2 |
| RFC 2236 | IGMPv2 |
| RFC 2246 | The TLS Protocol, Version 1.0 |
| RFC 2328 | OSPF v2 |
| RFC 2346 | AES Ciphersuites for Transport Layer Security |
| RFC 2365 | Administratively Scoped IP Multicast |
| RFC 2453 | RIP v1/v2 |
| RFC 2474 | Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers |
| RFC 2475 | An Architecture for Differentiated Service |
| RFC 2578 | SMIv2 |
| RFC 2579 | Textual Conventions for SMI v2 |
| RFC 2580 | Conformance statements for SMI v2 |

| | |
|---|---|
| RFC 2613 | SMON |
| RFC 2618 | RADIUS Authentication Client MIB |
| RFC 2620 | RADIUS Accounting MIB |
| RFC 2644 | Changing the Default for Directed Broadcasts in Routers |
| RFC 2674 | Dot1p/Q |
| RFC 2818 | HTTP over TLS |
| RFC 2851 | Internet Addresses MIB |
| RFC 2863 | The Interfaces Group MIB |
| RFC 2865 | RADIUS Client |
| RFC 2866 | RADIUS Accounting |
| RFC 2868 | RADIUS Attributes for Tunnel Protocol Support |
| RFC 2869 | RADIUS Extensions |
| RFC 2869bis | RADIUS support for EAP |
| RFC 2933 | IGMP MIB |
| RFC 3164 | The BSD Syslog Protocol |
| RFC 3376 | IGMPv3 |
| RFC 3410 | Introduction and Applicability Statements for Internet Standard Management Framework |
| RFC 3411 | An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks |
| RFC 3412 | Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) |
| RFC 3413 | Simple Network Management Protocol (SNMP) Applications |
| RFC 3414 | User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) |
| RFC 3415 | View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) |
| RFC 3418 | Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) |
| RFC 3580 | 802.1X RADIUS Usage Guidelines |
| RFC 3584 | Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework |
| RFC 3621 | Power Ethernet MIB |
| RFC 3768 | VRRP |
| RFC 4022 | Management Information Base for the Transmission Control Protocol (TCP) |
| RFC 4113 | Management Information Base for the User Datagram Protocol (UDP) |
| RFC 4188 | Definitions of Managed Objects for Bridges |
| RFC 4251 | SSH protocol architecture |
| RFC 4252 | SSH authentication protocol |
| RFC 4253 | SSH transport layer protocol |
| RFC 4254 | SSH connection protocol |
| RFC 4293 | Management Information Base for the Internet Protocol (IP) |
| RFC 4318 | Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol |
| RFC 4330 | Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI |
| RFC 4363 | Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions |

| | |
|---|---|
| RFC 4541 | Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches |
| RFC 4836 | Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs) |
| RFC 5321 | Simple Mail Transfer Protocol |

# B.5 Underlying IEEE Standards

| | |
|---|---|
| IEEE 802.1AB | Station and Media Access Control Connectivity Discovery |
| IEEE 802.1D | MAC Bridges (switching function) |
| IEEE 802.1Q | Virtual LANs (VLANs, MRP, Spanning Tree) |
| IEEE 802.1X | Port Authentication |
| IEEE 802.3 | Ethernet |
| IEEE 802.3ac | VLAN Tagging |
| IEEE 802.3x | Flow Control |
| IEEE 802.3af | Power over Ethernet |

# B.6 Underlying IEC Norms

| | |
|---|---|
| IEC 62439 | High availability automation networks<br>MRP – Media Redundancy Protocol based on a ring topology |

# B.7 Underlying ANSI Norms

| | |
|---|---|
| ANSI/TIA-1057 | Link Layer Discovery Protocol for Media Endpoint Devices, April 2006 |

# B.8 Technical Data

### 16.1.5 Switching

| | |
|---|---|
| Size of the MAC address table (incl. static filters) | 32768 |
| Max. number of statically configured MAC address filters | 100 |
| Max. number of MAC address filters learnable through IGMP Snooping | 1024 |
| Max. number of MAC address entries (MMRP) | 512 |
| Number of priority queues | 8 Queues |
| Port priorities that can be set | 0..7 |
| MTU (Max. allowed length of packets a port can receive or transmit) | 12288 Bytes |

### 16.1.6 VLAN

| | |
|---|---|
| VLAN ID range | 1..4042 |
| Number of VLANs | max. 512 simultaneously per device<br>max. 512 simultaneously per port |

### 16.1.7 Access Control Lists (ACL)

| | |
|---|---|
| Max. number of ACLs | 100 |
| Max. number of rules per ACL | 1023 |
| Max. number of rules per port | 1023 |
| Number of total configurable rules | 16368 (16 × 1023) |
| Max. number of VLAN assignments | 48 |
| Max. number of rules which log an event | 128 |
| Max. number of Ingress rules | 3584 (7168) |
| Max. number of Egress rules | 1024 (2048) |

### 16.1.8 Routing/Switching

| | |
|---|---|
| MTU (Max. allowed length of over-long packets a router interface can receive or transmit) | 12266 |
| Number of loopback interfaces | 8 |
| Max. number of Secondary IP addresses (Multinetting) | 31 |
| Max. number of VLAN router interfaces | 128 |
| Max. number of static routing entries | 1280 |
| Max. number of total IPv4 Unicast routing entries | 12288 (Routing profiles `ipv4RoutingDefault`, `ipv4RoutingUnicast` and `ipv4RoutingMulticast`)<br>8160 (Routing profile `ipv4DataCenter`) |
| Max. number of IPv4 Multicast routing entries | 2048 (Routing profiles `ipv4RoutingDefault` and `ipv4DataCenter`)<br>0 (Routing profile `ipv4RoutingUnicast`)<br>4095 (Routing profile `ipv4RoutingMulticast`) |
| Max. number of ARP entries | 12288 (Routing profiles `ipv4RoutingDefault` and `ipv4DataCenter`)<br>16384 (Routing profile `ipv4RoutingUnicast`)<br>8192 (Routing profile `ipv4RoutingMulticast`) |
| Max. number of ECMP Next Hop entries | 4 (Routing profiles `ipv4RoutingDefault`, `ipv4RoutingUnicast` and `ipv4RoutingMulticast`)<br>16 (Routing profile `ipv4DataCenter`) |

# B.9 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.10 Abbreviations used

| | |
|---|---|
| ACA | Name of the external memory |
| ACL | Access Control List |
| BOOTP | Bootstrap Protocol |
| CLI | Command Line Interface |
| DHCP | Dynamic Host Configuration Protocol |
| EUI | Extended Unique Identifier |
| FDB | Forwarding Database |
| GUI | Graphical User Interface |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| ICMP | Internet Control Message Protocol |
| IEEE | Institute of Electrical and Electronics Engineers |
| IGMP | Internet Group Management Protocol |
| IP | Internet Protocol |
| LED | Light Emitting Diode |
| LLDP | Link Layer Discovery Protocol |
| MAC | Media Access Control |
| MIB | Management Information Base |
| MRP | Media Redundancy Protocol |
| MSTP | Multiple Spanning Tree Protocol |
| NMS | Network Management System |
| PC | Personal Computer |
| PTP | Precision Time Protocol |
| QoS | Quality of Service |
| RFC | Request For Comment |
| RM | Redundancy Manager |
| RSTP | Rapid Spanning Tree Protocol |
| SCP | Secure Copy |
| SFP | Small Form-factor Pluggable |
| SFTP | SSH File Transfer Protocol |
| SNMP | Simple Network Management Protocol |
| SNTP | Simple Network Time Protocol |
| TCP | Transmission Control Protocol |
| TFTP | Trivial File Transfer Protocol |
| TP | Twisted Pair |
| UDP | User Datagram Protocol |
| URL | Uniform Resource Locator |
| UTC | Coordinated Universal Time |
| VLAN | Virtual Local Area Network |

# C Index

**0-9**
802.1X . . . . . 59

**A**
ABR . . . . . 289, 291
Access roles . . . . . 63
Access security . . . . . 109
Address Resolution Protocol . . . . . 245
Adjacency . . . . . 293
Advanced Mode . . . . . 179, 180
Advertisement . . . . . 270
Advertisement interval . . . . . 271
AF . . . . . 151
Aging time . . . . . 134, 317
Alarm . . . . . 325
Alarm messages . . . . . 323
Alternate port . . . . . 199, 205
APNIC . . . . . 44
Area Border Router . . . . . 289, 291
ARIN . . . . . 44
ARP . . . . . 46, 245, 246
ARP data packet . . . . . 310
ASBR . . . . . 288, 291
Assured Forwarding . . . . . 151
Authentication list . . . . . 59
Automatic configuration . . . . . 110
Autonomous System Area Border Router . . . . . 291
Autonomous System Boundary Router . . . . . 288

**B**
Backbone Area . . . . . 289
Backup Designated Router . . . . . 293, 294
Backup port . . . . . 200, 205
Backup router . . . . . 271
Bandwidth . . . . . 154
BDR . . . . . 293
Best Master Clock algorithm . . . . . 87
BOOTP . . . . . 43
Boundary . . . . . 318
Boundary clock (PTP) . . . . . 86
BPDU . . . . . 193
BPDU guard . . . . . 204, 205
Bridge Identifier . . . . . 191
Bridge Protocol Data Unit . . . . . 193
Broadcast . . . . . 244

**C**
CA certificate . . . . . 359
CIDR . . . . . 46, 247, 287
Class Selector . . . . . 151
Classless inter domain routing . . . . . 46
Classless Inter-Domain Routing . . . . . 247, 287
Closed circuit . . . . . 335
Command Line Interface . . . . . 18
Command tree . . . . . 29
Configuration file . . . . . 54
Configuration modifications . . . . . 323
Convergence . . . . . 281
Count-to-infinity . . . . . 284

**D**
Data traffic . . . . . 123
Daylight saving time . . . . . 81
Default gateway . . . . . 269, 270
Delay (PTP) . . . . . 87
Delay measurement (PTP) . . . . . 87
Delay time (MRP) . . . . . 179
Denial of Service . . . . . 123
Denial of service . . . . . 123
Designated bridge . . . . . 199
Designated port . . . . . 199, 204
Designated Router . . . . . 293, 294
Destination table . . . . . 323
Device status . . . . . 327
DHCP . . . . . 43
DHCP L2 Relay . . . . . 386
DHCP server . . . . . 80, 84, 407, 411
Diameter (Spanning Tree) . . . . . 193
Differentiated services . . . . . 151
DiffServ . . . . . 140
DiffServ Codepoint . . . . . 151
Disabled port . . . . . 200
Distance . . . . . 254, 255
Distance vector algorithm . . . . . 281
DoS . . . . . 123
DR . . . . . 293
DSCP . . . . . 140, 148, 151

**E**
Edge port . . . . . 199, 204
EF . . . . . 151
Email notification . . . . . 351
Event log . . . . . 359
Expedited Forwarding . . . . . 151
Extended Unique Identifier . . . . . 316

**F**
FAQ . . . . . 441
Faulty device replacement . . . . . 15
First installation . . . . . 43
Flow control . . . . . 154

**G**
GARP . . . 391
Gateway . . . 44, 48
Generic object classes . . . 421
Global Config mode . . . 26, 27
GMRP . . . 391
Grandmaster (PTP) . . . 87

**H**
HaneWin . . . 407, 411
Hardware reset . . . 323
Hello . . . 293
HiDiscovery . . . 43
HIPER-Ring . . . 188
HiView . . . 58
HiVRRP . . . 269
Hop count . . . 281, 284
Host address . . . 44

**I**
IANA . . . 44, 315
IAS . . . 59
IEEE 802.1X . . . 59
IEEE MAC Adresse . . . 345
IGMP . . . 316
IGMP snooping . . . 134
Importance . . . 256
Industrial HiVision . . . 13
Infinity . . . 284
Instantiation . . . 421
Integrated authentication server . . . 59
Interface tracking . . . 260, 262, 263
Interface tracking object . . . 261
Internal router . . . 291
Internet Group Management Protocol . . . 316
IP . . . 245
IP address . . . 44, 48, 54, 270
IP address owner . . . 270, 271
IP data packet . . . 310
IP header . . . 140, 142, 151
ISO/OSI layer model . . . 46
ISO/OSI reference model . . . 244

**L**
LACNIC . . . . . 44
LDAP . . . . . 59
Leave message . . . . . 134, 317
Link Aggration . . . . . 176
Link Aggregation interface . . . . . 260
Link down delay . . . . . 261
Link monitoring . . . . . 327, 335
Link State Advertisement . . . . . 291
Link State Database . . . . . 294
Link up delay . . . . . 261
Link-down notification . . . . . 274
Load sharing . . . . . 255
Logical tracking . . . . . 260, 262, 264, 266
Login dialog . . . . . 17
Loop guard . . . . . 205, 207
Loops . . . . . 228, 230, 233, 235
LSA . . . . . 291, 294
LSD . . . . . 294

**M**
MAC address . . . . . 270
MAC address filter . . . . . 131
MAC destination address . . . . . 46
Mail notification . . . . . 351
Master router . . . . . 270
MaxAge . . . . . 193
Memory (RAM) . . . . . 89
Message . . . . . 323
Metric . . . . . 281
Mode . . . . . 110
MRP . . . . . 176, 178, 179
MRP over LAG . . . . . 184
Multicast . . . . . 134, 244
Multicast address . . . . . 293, 314
Multicast routing . . . . . 314
Multinetting . . . . . 248

**N**
Netdirected Broadcasts . . . . . 248
Netdirected broadcasts (port based) . . . . . 250
Netdirected broadcasts (VLAN based) . . . . . 251
Netmask . . . . . 44, 48
Network load . . . . . 190, 191
Network management . . . . . 55
Network plan . . . . . 243
Next Hop . . . . . 281
Non-volatile memory (NVM) . . . . . 89
Not So Stubby Area . . . . . 289
NSSA . . . . . 289
NVM (non-volatile memory) . . . . . 89

**O**

Object classes . . . 421
Object description . . . 421
Object ID . . . 421
Open Shortest Path First . . . 287
OpenSSH-Suite . . . 21
Operand . . . 265, 267
Operation monitoring . . . 335
Operators . . . 262
Option 82 . . . 411
Ordinary clock (PTP) . . . 87
Organizationally Unique Identifier . . . 316
OSI reference model . . . 244
OSPF . . . 243, 281, 287
OUI . . . 316

**P**

Password . . . 20, 22, 24
Path costs . . . 191, 195
PHB . . . 151
Ping response . . . 261
Ping tracking . . . 256, 260, 261
Polling . . . 323
Port Identifier . . . 191, 192
Port mirroring . . . 363
Port number . . . 192
Port priority . . . 147
Port priority (Spanning Tree) . . . 192
Port roles (RSTP) . . . 199
Port State . . . 200
Port-based router interface . . . 249
Precedence . . . 151
Preempt delay . . . 274
Preempt mode . . . 274
Primary ring (RCP) . . . 237
Priority . . . 142
Priority queue . . . 143
Priority tagged frames . . . 142
Privileged Exec mode . . . 26
Protection functions (guards) . . . 204
Protocol-based VLAN . . . 310
Proxy ARP . . . 246
PTP . . . 79
PTP domain . . . 88
PuTTY . . . 18

**Q**

QoS . . . 141
Querier Election . . . 317
Query . . . 134

**R**

RADIUS . . . . . 59
RAM (memory) . . . . . 89
Rapid Spanning Tree . . . . . 176, 199
RCP . . . . . 176
Real time . . . . . 140
Reconfiguration . . . . . 191
Reconfiguration time (MRP) . . . . . 179
Redistributing . . . . . 289
Redistribution . . . . . 288
Redundancy . . . . . 190
Redundant static route . . . . . 254
Reference time source . . . . . 79, 84, 87
Relay contact . . . . . 335
Remote diagnostics . . . . . 335
Report . . . . . 356
Report message . . . . . 134, 317
RFC . . . . . 423
Ring . . . . . 178, 184
Ring Manager . . . . . 184
Ring manager . . . . . 178
Ring/Network coupling . . . . . 176
RIP . . . . . 243, 281
RIPE NCC . . . . . 44
RM function . . . . . 178, 184
RMON probe . . . . . 363
Root Bridge . . . . . 195
Root guard . . . . . 204, 207
Root path . . . . . 196, 197
Root Path Cost . . . . . 191
Root port . . . . . 199, 205
Route Summarization . . . . . 289
Route tracking . . . . . 256
Router . . . . . 44
Router ID . . . . . 293
Router priority . . . . . 293
Routing Information Protocol . . . . . 281
Routing table . . . . . 250, 256, 281
Routing tables . . . . . 274
RST BPDU . . . . . 199, 201
RSTP . . . . . 202

**S**

Scoping . . . 318
Secondary ring (RCP) . . . 237
Secure shell . . . 18, 21
Segmentation . . . 323
Serial interface . . . 18, 23
Service . . . 356
Service shell . . . 26
Service Shell deactivation . . . 39
Setting the time . . . 79
SFP module . . . 344
Shortest Path First . . . 295
Signal contact . . . 335
Skew time . . . 271
SNMP . . . 323
SNMP trap . . . 323, 325
SNTP . . . 79
Software version . . . 103
Source filtering . . . 317
SPF . . . 295
Split horizon . . . 284
SSH . . . 18, 21
Starting the graphical user interface . . . 17
Static route tracking . . . 256
Static routes . . . 243
Static routing . . . 260
Store-and-forward . . . 131
STP-BPDU . . . 193
Strict Priority . . . 143
Stub Area . . . 289
Subidentifier . . . 421
Subnet . . . 48
Subring . . . 176, 214
Sub-ring Manager . . . 221
Sub-ring Redundant Manager . . . 221
Syslog over TLS . . . 359
System requirements (Graphical User Interface) . . . 17

**T**

Tab Completion . . . 36
TCN guard . . . 205, 207
Technical questions . . . 441
Time to Live. . . . 318
Topology Change flag . . . 205
ToS . . . 140, 142, 151
Tracking . . . 256
Tracking (VRRP) . . . 260
Traffic class . . . 143, 148
Traffic shaping . . . 149
Training courses . . . 441
Transmission reliability . . . 323
Transparent clock (PTP) . . . 86
Trap . . . 323, 325
Trap destination table . . . 323
Tree structure (Spanning Tree) . . . 195, 198
TTL . . . 318
Two-Switch coupling, Primary device . . . 228
Two-Switch coupling, Stand-by device . . . 229
Type of Service . . . 142

**U**

Update . . . . . 41
User Exec mode . . . . . 26
User name . . . . . 19, 22, 24

**V**

Variable Length Subnet Mask . . . . . 287
Video . . . . . 143
virtual link . . . . . 290
Virtual MAC address . . . . . 270
Virtual router . . . . . 270
Virtual router ID . . . . . 270
Virtual router interface . . . . . 311
Virtual router IP address . . . . . 271
Virtual router MAC address . . . . . 271
VLAN . . . . . 157
VLAN (HIPER-Ring) . . . . . 188
VLAN priority . . . . . 147
VLAN protocol group . . . . . 310
VLAN router interface . . . . . 260
VLAN routing . . . . . 310
VLAN tag . . . . . 142, 157
VLSM . . . . . 287
VoIP . . . . . 143
VRID . . . . . 270, 271
VRRP . . . . . 260, 269
VRRP priority . . . . . 271
VRRP router . . . . . 270
VRRP Tracking . . . . . 260
VT100 . . . . . 24

**W**

Weighted Fair Queuing . . . . . 143
Weighted Round Robin . . . . . 143

# 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.

### Customer Innovation Center

The Customer Innovation 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.belden.com/solutions/customer-innovation-center.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Customer Innovation 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:

| | Very Good | Good | Satisfactory | Mediocre | Poor |
|---|---|---|---|---|---|
| Precise description | O | O | O | O | O |
| Readability | O | O | O | O | O |
| Understandability | O | O | O | O | O |
| Examples | O | O | O | O | O |
| Structure | O | O | O | O | O |
| Comprehensive | O | O | O | O | O |
| Graphics | O | O | O | O | O |
| Drawings | O | O | O | O | O |
| Tables | O | O | O | O | O |

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

HIRSCHMANN

A BELDEN BRAND