HIRSCHMANN
A BELDEN BRAND

Hirschmann Automation and Control GmbH

EAGLE40-03 HiSecOS Rel. 05200

Reference Manual

Graphical User Interface

User Manual

Configuration

HIRSCHMANN
A BELDEN BRAND

Reference Manual

Graphical User Interface
Industrial Firewall
EAGLE40-03

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

You find the latest user documentation for your device at: doc.hirschmann.com

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

Contents

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 item
–	List item – second level
▶	Parameter value
☐	Task 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 prerequisite to use the Graphical User Interface of the device is a web browser with HTML5 support.

The responsive Graphical User Interface automatically adapts to the size of your screen. Consequently, you can see more details on a large, high-resolution screen than on a small screen. For example, on a high-resolution screen, the buttons have a label next to the icon. On a screen with a small width, the Graphical User Interface displays only the icon.

Note:
On a conventional screen, you click to navigate. On a device with a touchscreen, on the other hand, you tap. For simplicity, we only use "click" in our help texts.

The Graphical User Interface is divided as follows:
- Banner
- Menu pane
- Dialog area

Banner

The banner displays the following information:

Displays and hides the menu. When the web browser window is too narrow, the Graphical User Interface hides the menu pane. The banner displays the button instead.

Brand logo

Click the logo to open the website of the manufacturer of the device in a new window.

Dialog name

Displays the name of the dialog currently displayed in the dialog area.

Displays that the web browser cannot contact the device. The connection to the device is interrupted.

Displays if the settings in the volatile memory (*RAM*) differ from the settings of the "Selected" configuration profile in the non-volatile memory (*NVM*). The banner displays the icon if you have applied the settings, but not yet saved them in the non-volatile memory (*NVM*).

When you click the button, the online help opens in a new window.

When you click the button, a tooltip displays the following information:

- The summary of the *Device status* frame. See the *Basic Settings > System* dialog.
- The summary of the *Security status* frame. See the *Basic Settings > System* dialog.

A red dot next to the icon means that at least one of the values is greater than `0`.

When you click the button, a submenu opens with the following menu items:

- User account name
  The account name of the user that is currently logged in.
- *Logout* button
  When you click the button, this logs out the currently logged in user. Then the login dialog opens.

Menu pane

When the web browser window is too narrow, the Graphical User Interface hides the menu pane.

To display the menu pane, click the ☰ button in the banner.

The menu pane is divided as follows:
- Icons bar
- Menu tree

Icons bar

The icons bar displays the following information:

Device software

Displays the version number of the currently running device software that the device loaded during the last system startup.

Displays a text field to search for a keyword. When you enter a character or string, the menu tree displays a menu item only for those dialogs that are related to this keyword.

The menu tree displays a menu item only for those dialogs in which at least one parameter differs from the default setting (*Diff to default*). To display the complete menu tree again, click the  button.

Collapses the menu tree. The menu tree then displays only the menu items of the first level.

Expands the menu tree. The menu tree then displays every menu item on every level.

Menu tree

The menu tree contains one item for each dialog in the Graphical User Interface. When you click a menu item, the dialog area displays the corresponding dialog. You can change the view of the menu tree by clicking the buttons in the icons bar at the top. Furthermore, you can change the view of the menu tree by clicking the following buttons:

+

Expands the current menu item to display the menu items of the next lower level. The menu tree displays the button next to each collapsed menu item that contains menu items on the next lower level.

−

Collapses the menu item to hide the menu items of the lower levels. The menu tree displays the button next to each expanded menu item.

Dialog area

The dialog area displays the dialog that you select in the menu tree, including its controls. Here, you can monitor and change the settings of the device depending on your access role.

Below you find useful information on how to use the dialogs.

Control elements

The dialogs contain different control elements. These control elements are read-only or editable, depending on the parameter and your access role as a user.

The control elements have the following visual properties:

- Input fields
  - An editable input field has a line at the bottom.
  - A read-only input field has no special visual properties.
- Checkboxes
  - An editable checkbox has a bright color.
  - A read-only checkbox has a grey color.
- Radio buttons
  - An editable radio button has a bright color.
  - A read-only radio button has a grey color.

Modification mark

When you modify a value, the corresponding field or table cell displays a red triangle in its top-left corner. The red triangle indicates that you have not yet applied this modification. The modified settings are not yet effective.

Standard buttons

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

✓

Applies the settings you modified to the device.

Information on how the device retains the modified settings even after a reboot you find in section “Saving the settings” on page 16.

Undoes the unsaved changes in the current dialog. Resets the values in the fields to the settings applied to the device.

Saving the settings

When applying settings, the device temporarily stores the modified settings. To do this, perform the following step:

- ☐ Click the ✓ button.

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.

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

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ In the table, mark the checkbox far left in the table row of the desired configuration profile.
- ☐ When the checkbox in the *Selected* column is unmarked, click the ☰ button and then the *Select* item.
- ☐ Click the 💾 button to save your current changes.

Updating the display

If a dialog remains open 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.

Working with tables

The dialogs display numerous settings in table form. You have the option of customizing the appearance of the tables to fit your needs.

You can find useful information on how to use the tables in the following sections:

- Filtering table rows
- Sorting table rows
- Selecting multiple table rows

Filtering table rows

The filter lets you reduce the number of displayed table rows.

Displays a second table row in the table header containing a text field for every column. When you enter a string in a field, the table displays only the table rows that contain this string in the corresponding column.

Sorting table rows

You can change the order of the table rows. When you click the table header, an icon displays the sorting status.

Displays that the table rows are sorted by a criterion other than the values in this column.

Click the icon to sort the table rows in descending order based on the entries of the corresponding column. You might be able to restore the initial sorting in the table only after logging out and logging in again.

Displays that the table rows are sorted in descending order based on the entries of the corresponding column.

Click the icon to sort the table rows in ascending order based on the entries of the corresponding column. You might be able to restore the initial sorting in the table only after logging out and logging in again.

Displays that the table rows are sorted in ascending order based on the entries of the corresponding column.

Click the icon to sort the table rows in descending order based on the entries of the corresponding column. You might be able to restore the initial sorting in the table only after logging out and logging in again.

Selecting multiple table rows

You have the option of selecting multiple table rows at once and then apply an action to the selected table rows.

- ☐ To select individual table rows, mark the leftmost checkbox in the desired table row.
- ☐ To select every table row, mark the leftmost checkbox in the table header.

Once you have selected multiple table rows, you can apply an action to each of these table rows at the same time, for example:

- Entering or changing the values in one table column
- Removing multiple table rows

1 Basic Settings

The menu contains the following dialogs:

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

1.1 System

[Basic Settings > System]

This dialog displays information about the operating status of the device.

Device status

Device status

Displays the device status and the alarms that currently exist. When at least one alarm is present, the background color changes to red. Otherwise, the background color remains green.

You specify the parameters that the device monitors in the *Diagnostics > Status Configuration > Device Status* dialog. If a monitored parameter differs from the desired status, then the device triggers an alarm.

A tooltip displays the cause of the currently existing alarms and the time at which the device triggered each alarm. To display the tooltip, hover the mouse pointer over or tap the field. In the *Diagnostics > Status Configuration > Device Status* dialog, the *Status* tab displays an overview of the alarms.

Note:
If you connect only one power supply unit to a device that supports 2 redundant power supply units, then the device triggers an alarm. To avoid this alarm, deactivate the monitoring of the missing power supply units in the *Diagnostics > Status Configuration > Device Status* dialog.

Security status

Security status

Displays the security status and the alarms that currently exist. When at least one alarm is present, the background color changes to red. Otherwise, the background color remains green.

You specify the parameters that the device monitors in the *Diagnostics* > *Status Configuration* > Security Status dialog. If a monitored parameter differs from the desired status, then the device triggers an alarm.

A tooltip displays the cause of the currently existing alarms and the time at which the device triggered each alarm. To display the tooltip, hover the mouse pointer over or tap the field. In the *Diagnostics* > *Status Configuration* > *Security Status* dialog, the *Status* tab displays an overview of the alarms.

Signal contact status

The device can contain several signal contacts.

Signal contact status

Displays the signal contact status and the alarms that currently exist. When at least one alarm is present, the background color changes to red. Otherwise, the background color remains green.

You specify the parameters that the device monitors in the *Diagnostics* > *Status Configuration* > *Signal Contact* > *Signal Contact 1*/*Diagnostics* > *Status Configuration* > *Signal Contact* > *Signal Contact 2* dialog. If a monitored parameter differs from the desired status, then the device triggers an alarm.

A tooltip displays the cause of the currently existing alarms and the time at which the device triggered each alarm. To display the tooltip, hover the mouse pointer over or tap the field. In the *Diagnostics* > *Status Configuration* > *Signal Contact* > *Signal Contact 1*/*Diagnostics* > *Status Configuration* > Signal Contact > *Signal Contact 2* dialog, the *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 by which the device is known in the network.

Possible values:

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

`<device type name>-<MAC address>` (default setting)

When generating an digital certificate, 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 hostname or Fully Qualified Domain Name (FQDN). For compatibility reasons, it is recommended to use only lowercase letters, as some systems differentiate uppercase from lowercase in the FQDN. Verify that this name is unique in the entire network.

- *Syslog*

Location

Specifies the current or planned location.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

Contact person

Specifies the contact person for this device.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

Device type

Displays the product name of the device.

Power status

Displays the status of the power supply unit at the respective voltage supply connector.

Possible values:

- *present*
- *defective*
- *not installed*
- *unknown*

Uptime

Displays the time that has elapsed since the 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 threshold values in the *Diagnostics > Status Configuration > Device Status* dialog.

Upper temp. limit [°C]

Specifies the upper temperature threshold value in °C.

Possible values:

- `-99..99` (integer)
  If the temperature in the device exceeds the specified value, then the device displays an alarm.

Lower temp. limit [°C]

Specifies the lower temperature threshold value in °C.

Possible values:

- `-99..99` (integer)
  If the temperature in the device falls below the specified value, then the device displays an alarm.

LED status

For further information about the device status LEDs, see the “Installation” user manual.

Status

There is currently no device status alarm. The device status is OK.

There is currently at least one device status alarm. For details, see the *Device status* frame.

Power

Device that supports 2 redundant power supply units: Only one supply voltage is active.

Device that supports one power supply unit: The supply voltage is active.

Device that supports 2 redundant power supply units: Both supply voltages are active.

ACA

No external memory is 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 at the time of the last display update. You identify the port status from the indicator.

In the initial view, the frame only displays ports with an active link. When you click the button, the frame displays every port.

- The port speed is displayed next to the port number.
- When you hover the mouse pointer over or tap the appropriate port icon, a tooltip displays detailed port state information.

Green background color

Port with an active link.

Gray background color

Port with an inactive link.

Yellow background color

Port on which the device detected an unsupported SFP transceiver or an unsupported data rate.

1.2 Network

[Basic Settings > Network]

The menu contains the following dialogs:

- Global
- IPv4

1.2.1 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.

MAC address

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

HiDiscovery protocol v1/v2

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

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

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

Operation

Enables/disables the HiDiscovery function in the device.

Possible values:

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

Access

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

Possible values:

- `readWrite` (default setting)
  The HiDiscovery function has write access to the device. The device lets you change the IP parameters in the device using the HiDiscovery function.
- `readOnly`
  The HiDiscovery function has read-only access to the device. The device lets you view the IP parameters in the device using the HiDiscovery function.

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

1.2.2 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

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 in the *Switching > VLAN > Configuration* dialog the VLAN is already set up. Assign a VLAN 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.

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 does not overlap with any subnet connected to another interface of the device:

- router interface
- loopback interface

Netmask

Specifies the netmask.

Possible values:

- Valid IPv4 netmask

Gateway address

Specifies the IP address of a router through which the device accesses other devices outside 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:

- *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`

1.3 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 that is saved in the device.

Note:
Before you update 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 system startup.

Running version

Displays the version number and creation date of the currently running device software that the device loaded during the last system startup.

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

The device swaps the device software images and accordingly the values displayed in the fields *Stored version* and *Backup version*.

During the next system startup, the device loads the device software displayed in the *Stored version* field.

Bootcode

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

Software update

The device lets you update the device software at this place, if a suitable device software image is available outside the device. If a suitable device software image is saved on the selected external memory, use the table in the *File system* tab below.

URL

Specifies the path and the file name of the device software image that you use to update the device software.

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

- Software update from the PC

  Drag and drop the file into the area from your PC or network drive. As an alternative, click in the area to select the file.
  You can also use SCP or SFTP to transfer the file from your PC to the device. Perform the following steps:
  - ☐ On your PC, open an SCP or SFTP client, for example WinSCP.
  - ☐ Use the SCP or SFTP client to open a connection to the device.
  - ☐ Transfer the file onto the device, into the directory `/upload/firmware`.
    When the file transfer is complete, the device starts updating the device software. If the update was successful, then the device generates an `ok` file in the directory `/upload/firmware` and deletes the transferred file.
    The device loads the device software during the next system startup.
- Software update from an SCP or SFTP server
  If the file is on an SCP or SFTP server, then specify the URL in one of the following forms:
  - `scp://` or `sftp://<IP address>/<path>/<file name>`
    Click the *Start* button to open the *Credentials* window. In this window, you enter the *User name* and *Password* to log into the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

Start

Updates the device software.

- To remain logged in to the device management during the software update, move the mouse pointer occasionally. As an alternative, before you start the software update, specify a sufficiently high value in the *Device Security > Management Access > Web* dialog, *Web interface session timeout [min]* field.
- The device transfers the previously used device software to the backup memory.
- The device transfers the selected file to the flash memory, replacing the previously used device software. During the next startup, the device boots with the device software that you have transferred.

[File system]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Update Firmware

Updates the device software if a suitable device software image is saved on the external memory. The prerequisite is that a table row is selected for which the *File location* column displays the value `usb`.

- To remain logged in to the device management during the software update, move the mouse pointer occasionally. As an alternative, before you start the software update, specify a sufficiently high value in the *Device Security > Management Access > Web* dialog, *Web interface session timeout [min]* field.
- The device transfers the previously used device software to the backup memory.
- The device transfers the selected file to the flash memory, replacing the previously used device software. During the next startup, the device boots with the device software that you have transferred.

File location

Displays the storage location of the device software.

Possible values:

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

Index

Displays the index of the device software.

The index number of the device software in the flash memory has the following meaning:

- `1`
  During the next system startup, 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.

1.4 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.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Remove

Removes the configuration profile selected 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

Saves the temporarily applied settings in 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 saves a copy of the configuration profile in the external memory.

Displays a context menu with further functions for the corresponding dialog.

Save as..

Opens the *Save as..* window to copy the configuration profile selected in the table and saves it with a user-specified name in the non-volatile memory (*NVM*).

- ☐ In the *Profile name* field, enter the name under which you want to save the configuration profile (maximum 32 characters).
  - ☐ To save the configuration profile under a new name, click the + button.
  - ☐ To overwrite an existing configuration profile, select the corresponding item from the drop-down list.

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”.

Note:
Before adding 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.

Activate

Loads the settings of the configuration profile selected 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 selected in the table as “Selected”. In the *Selected* column, the checkbox is then `marked`.

When applying the *Undo configuration modifications* function or during the system startup, 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.

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

☐ When *PC/URL* is selected above, in the *Import profile from PC/URL* frame you specify the configuration profile file to be imported.
- – Import from the PC

  If the file is on your PC or on a network drive, then drag and drop the file into the area.
  As an alternative, click in the area to select the file.
  You can also use SCP or SFTP to transfer the file from your PC to the device. Perform the following steps:
  On your PC, open an SCP or SFTP client, for example WinSCP.
  Use the SCP or SFTP client to open a connection to the device.
  Transfer the file onto the device, into the directory `/nv/cfg`.
- – Import from an SCP or SFTP server
  If the file is on an SCP or SFTP server, then specify the URL in one of the following forms:
  `scp://` or `sftp://<IP address>/<path>/<file name>`
  Click the *Start* button to open the *Credentials* window. In this window, you enter the *User name* and *Password* to log into 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.
From 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* field you specify the storage location for the configuration profile. The prerequisite is that from the *Select source* drop-down list the *PC/URL* item is selected.
- ▶ *RAM*
  The device saves the configuration profile in the volatile memory (*RAM*) of the device. This replaces the `running-config`, the device uses the settings of the imported configuration profile immediately. The device terminates the connection to the Graphical User Interface. Reload the Graphical User Interface. Log in again.
- ▶ *NVM*
  The device saves the configuration profile in the non-volatile memory (*NVM*) of the device.

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

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

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

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

Export...

Exports the configuration profile selected 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 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>`
    Click the *Ok* button to open the *Credentials* window. In this window, you enter the *User name* and *Password* to log into the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

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 digital 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 short time, the device reboots and then uses the default settings.

Back to default

Deletes the current operating (`running config`) settings from the volatile memory (*RAM*).

Storage

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 the system startup, 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:
  - ☐ Select the table row of 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 the *Backup config when saving* checkbox is marked.

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. To do this, select the table row of an existing configuration profile in the table, click 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.

Last modified (UTC)

Displays the Universal Time Coordinated (UTC) time a user last saved the configuration profile.

Selected

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

The device lets you designate another configuration profile as “Selected”. To do this, select 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 the system startup, the device loads the configuration profile into the volatile memory (*RAM*).
  - When you click the button, the device saves the temporarily applied settings in this configuration profile.
- `unmarked`
  Another configuration profile is designated as “Selected”.

Encryption

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.

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.

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.

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.

Verified

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

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

Possible values:

- `marked`
  The calculated and the saved checksum match.
  The saved settings are consistent.
- `unmarked`
  For the configuration profile marked as “Selected” applies:
  The calculated and the saved checksum are different.
  The configuration profile contains modified settings.
  Possible causes:
  – The file is damaged.
  – The file system in the external memory is inconsistent.
  – A user has exported the configuration profile and changed the XML file outside the device.
  For the other configuration profiles the device has not calculated the checksum.

The device verifies the checksum correctly only if the configuration profile has been saved before as follows:

- on an identical device
- with the same software version, which the device is running

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

External memory

Selected external memory

Displays the type of the external memory.

Possible values:

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

Status

Displays the operating state of the external memory.

Possible values:

- *notPresent*
  No external memory is 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* 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 adding 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 an inoperable device, 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 inoperable device.
- ☐ Install the external memory from the inoperable device in the new device.
- ☐ Restart the new device.
  During the next system startup, the device loads the configuration profile with the settings of the inoperable device from the external memory. The device copies the settings into the volatile memory (*RAM*) and into the non-volatile memory (*NVM*).

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".

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. The device thus maintains the current settings, that are only temporarily saved.

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`)

Information

NVM in sync with running config

Displays if the settings in the volatile memory (*RAM*) differ from the settings of the "Selected" configuration profile in the non-volatile memory (*NVM*).

Possible values:

- `marked`
  The settings match.
- `unmarked`

  The settings differ. Additionally, the Banner displays the icon .

External memory in sync with NVM

Displays if the settings of the"Selected" configuration profile in the external memory (ACA) differ from the settings of the "Selected" configuration profile in the non-volatile memory (*NVM*).

Possible values:

- `marked`
  The settings match.
- `unmarked`
  The settings 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.

1.5 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

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Type

Displays the type of the external memory.

Possible values:

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

Status

Displays the operating state of the external memory.

Possible values:

- *notPresent*
  No external memory is 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 system startup.

Possible values:

- `marked` (default setting)
  The device updates the device software when the following files are located in the external memory:
  - the device software image file
  - a text file `startup.txt` with the content `autoUpdate=<software_image_file_name>.bin`
- `unmarked`
  No automatic device software update during the system startup.

Config priority

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

Possible values:

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

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

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

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

Backup config when saving

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

Possible values:

- `marked` (default setting)
  Saving a copy is activated. When you click in the *Basic Settings > Load/Save* dialog the button, the device saves a copy of the configuration profile on the active external memory.
- `unmarked`
  Saving a copy is deactivated. The device does not save 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.

1.6 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]

[Configuration]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.

Name

Name of the port.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters
  The device accepts the following characters:
  - `<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.

Autoneg

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 auto-negotiation and automatically detects the assignment of the twisted-pair port connectors (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* column.
- Grayed-out display
  No automatic selection of the operating mode.

Manual configuration

Specifies the operating mode of the ports when the *Autoneg* function is disabled.

Possible values:

- `10M HDX`
  Half-duplex connection
- `10M FDX`
  Full-duplex connection
- `100M HDX`
  Half-duplex connection
- `100M FDX`
  Full-duplex connection
- `1G FDX`
  Full-duplex connection

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

Link/Current settings

Displays the operating mode which the port currently uses.

Possible values:

- `-`
  No cable connected, no link.

- `10M HDX`
  Half-duplex connection
- `10M FDX`
  Full-duplex connection
- `100M HDX`
  Half-duplex connection
- `100M FDX`
  Full-duplex connection
- `1G FDX`
  Full-duplex connection

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

Manual cable crossing

Specifies the devices connected to a twisted-pair port.

The prerequisite is that the *Autoneg* function is disabled.

Possible values:

- *mdi*
  The device interchanges the send- and receive-line pairs on the port.
- *mdix* (default setting on twisted-pair 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 twisted-pair 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 interruptions 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

Activates/deactivates the sending of SNMP traps when the device detects a change in the link up/down status on the port.

Possible values:

- `marked` (default setting)
  The sending of SNMP traps is active. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
  When the device detects a link up/down status change, the device sends an SNMP trap.
- `unmarked`
  The sending of SNMP traps is inactive.

Power state

Specifies if the port is physically enabled or disabled after you deactivated the port in the *Port on* column.

Possible values:

- `marked`
  The device keeps the port physically enabled when the *Port on* checkbox is unmarked. A device connected to this port continues to detect the link status as active.
- `unmarked` (default setting)
  The port is physically disabled. The physical status of the port is controlled only by the setting in the *Port on* column.

Power save

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.

[Statistics]

This tab displays the following overview per port:

- Number of data packets/bytes received by the device
  - *Received packets*
  - *Received octets*
  - *Received unicasts*
  - *Received multicasts*
  - *Received broadcasts*
- Number of data packets/bytes sent or forwarded by the device
  - *Transmitted packets*
  - *Transmitted octets*
  - *Transmitted unicasts*
  - *Transmitted multicasts*
  - *Transmitted broadcasts*

- Number of errors detected by the device
  - *Received fragments*
  - *Detected CRC errors*
  - *Detected collisions*
- Number of data packets per size category received by 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 column.

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.
or
☐ In the *Basic Settings > Restart* dialog, click the *Clear port statistics* button.

1.7 Restart

[Basic Settings > Restart]

This dialog lets you restart the device, reset port counters and the MAC address table (forwarding database), and delete log files.

Restart

Cold start...

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

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

- ☐ To permanently save the settings, click the *Yes* button in the *Warning* window.
- ☐ To discard the changed settings, click the *No* button in the *Warning* window.

The device restarts and goes through the following phases:

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

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

Buttons

Clear FDB

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.

Clear 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 log file

Removes the logged events from the log file.

See the *Diagnostics > Report > System Log* dialog.

Clear persistent log file

Removes the log files from the external memory.

See the *Diagnostics > Report > Persistent Logging* dialog.

Clear firewall table

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

2 Time

The menu contains the following dialogs:
- Basic Settings
- NTP

2.1 Basic Settings

[Time > Basic Settings]

After a restart, the device initializes its clock to January 1 2025, 01:00 UTC+1. Reset the time if you disconnect the device from the power supply or restart it. As an alternative, you specify that the device automatically obtains the correct time from an *SNTP* server or from a PTP clock.

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

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

[Global]

In this tab, you specify the system time and the time zone.

Configuration

System time (UTC)

Displays the date and time in Universal Time Coordinated (UTC) format.

Set time from PC

The device takes over the time from your computer as the system time.

System time

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

Time source

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

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

Possible values:

- `Local`
  System clock of the device.
- `ntp`
  The *NTP* client is enabled, and the device is synchronized by an *NTP* server. See the *Time > NTP* dialog.

Local offset [min]

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

Possible values:

- `-780..840` (default setting: `60`)

[Daylight saving time]

In this tab, you enable/disable the *Daylight saving time* function. You specify the start and end of summer time using a pre-defined profile. As an alternative, you specify these settings individually. During the summer time, the device advances the local time by one 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 sets the clock forward to summer time and back again.
- `Off` (default setting)
  The *Daylight saving time* mode is disabled.

You specify the daylight saving time settings in the *Summertime begin* and *Summertime end* frames.

Profile...

Opens the *Profile...* window to select a pre-defined profile for the start and end of summer time. Selecting a profile overwrites the settings specified in the *Summertime begin* and *Summertime end* frames.

Possible values:

- `EU`
  Daylight saving time settings as applicable in the European Union.
- `USA`
  Daylight saving time settings as applicable in the United States.

Summertime begin

In this frame, you specify the time at which the device sets the clock forward from standard time to summer time. In the first 3 fields, you specify the day for the start of summer time. In the last field, you specify the time.

Week

Specifies the week in the current month.

Possible values:

- `-` (default setting)
- *first*
- *second*
- *third*
- *fourth*
- *last*

Day

Specifies the day of the week.

Possible values:

- `-` (default setting)
- *Sunday*
- *Monday*
- *Tuesday*
- *Wednesday*
- *Thursday*
- *Friday*
- *Saturday*

Month

Specifies the month.

Possible values:

- `-` (default setting)
- *January*
- *February*
- *March*
- *April*
- *May*
- *June*
- *July*
- *August*
- *September*
- *October*
- *November*
- *December*

System time

Specifies the time at which the device sets the clock forward to summer time.

Possible values:

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

Summertime end

In this frame, you specify the time at which the device resets the clock from summer time to standard time. In the first 3 fields, you specify the day for the end of summer time. In the last field, you specify the time.

Week

Specifies the week in the current month.

Possible values:

- `-` (default setting)
- *first*
- *second*
- *third*
- *fourth*
- *last*

Day

Specifies the day of the week.

Possible values:

- `-` (default setting)
- *Sunday*
- *Monday*
- *Tuesday*
- *Wednesday*
- *Thursday*
- *Friday*
- *Saturday*

Month

Specifies the month.

Possible values:

- `-` (default setting)
- *January*
- *February*
- *March*
- *April*
- *May*

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

System time

Specifies the time at which the device resets the clock to standard time.

Possible values:

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

2.2 NTP

[Time > NTP]

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

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

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

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

The menu contains the following dialogs:

- Global
- Server

2.2.1 Global

[Time > NTP > Global]

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

- As an NTP client, the device obtains the Universal Time Coordinated (UTC) from one or more NTP servers in the network.
- As an NTP server, the device distributes the Universal Time Coordinated (UTC) to NTP clients in the subordinate network segment. The device obtains the Universal Time Coordinated (UTC) from one or more NTP servers in the network, if these were previously specified.

Client only

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

Client

Enables/disables the NTP client in the device.

Possible values:

- *On*
  The NTP client is enabled.
  The device obtains the time information from one or more NTP servers in the network.
- *Off* (default setting)
  The NTP client is disabled.

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

Mode

Specifies from where the NTP client takes the time information.

Possible values:

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

Client and server

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

Server

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

Possible values:

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

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

Mode

Specifies in which mode the NTP server works.

Possible values:

- *client-server* (default setting)
  With this setting, the device obtains the time information from NTP servers in the network and distributes it to NTP clients in the subordinate network segment.
  - The NTP client takes the time information from the unicast responses of the servers that are indicated as active in the *Time > NTP > Server* dialog.
  - The NTP server distributes the time information through unicast to the requesting clients.
- *symmetric*
  With this setting you integrate the device in a cluster of redundant NTP servers. The device synchronizes the time information with the other NTP servers in the cluster at intervals of 64 seconds.
  - ☐ In the *Time > NTP > Server* dialog, indicate the NTP servers participating in the cluster as active.
  - ☐ Specify a uniform value for the *stratum* for the NTP servers participating in the cluster.

Stratum

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

Possible values:

- 1..16 (default setting: 12)

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

The device evaluates this value under the following circumstances:

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

2.2.2 Server

[Time > NTP > Server]

In this dialog, you specify the NTP servers.

- The NTP client of the device obtains the time information from the unicast responses of the servers specified here.
- If the NTP server of the device is working in *symmetric* mode, then you specify the servers participating in the cluster here.
- The device lets you specify up to 4 NTP servers.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons


Add

Adds a table row.


Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.

When you delete a table row, this leaves a gap in the numbering. When you add a table row, the device fills the first gap.

Active

Activates/deactivates the connection to the NTP server.

Possible values:

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

IP address

Specifies the IP address of the NTP server.

Possible values:

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

Initial burst

Activates/deactivates the *Initial burst* mode.

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

Possible values:

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

Burst

Activates/deactivates the *Burst* mode.

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

Possible values:

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

Preferred

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

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

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

Possible values:

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

Status

Displays the synchronization status.

Possible values:

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

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 into the device management 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 possible consecutive unsuccessful login attempts when the user accesses the device management using the Graphical User Interface or the Command Line Interface.

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

Possible values:

▶ `0..5` (default setting: `0`)

If the user makes one more consecutive 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 into the device management.

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`)

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`)

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 the checkbox in the *Policy check* column is marked.

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.

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons


Add

Opens the *Create* window to add a table row.

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


Remove

Removes the selected table row.

User name

Displays the name of the user account.

To add a 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, to the device management, with this user name.
- `unmarked` (default setting)
  The user account is inactive. The device rejects the login of a user, to the device management, with this user name.

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

Password

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

Possible values:

- Alphanumeric ASCII character string with 6..64 characters
  The device accepts the following characters:
  - 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 access 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 to the device management. Assign this value to temporarily lock the user account. If the device detects an error when another access role is being assigned, then the device assigns this access 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 an access 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 consecutive 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 using SNMPv3.

Possible values:

- *`hmacmd5`* (default setting)
  For this user account, the device uses protocol HMACMD5.
- *`hmacsha`*
  For this user account, the device uses protocol HMACSHA.

SNMP encryption type

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

Possible values:

- *`none`*
  No encryption.
- *`des`* (default setting)
  DES encryption
- *`aesCfb128`*
  AES128 encryption

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

In the default setting the following authentication lists are available:
- `defaultLoginAuthList`
- `defaultV24AuthList`

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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

Buttons


Add

Opens the *Create* window to add a table row.
- In the *Name* field, you specify the name of the list.
  Possible values:
  ▶ Alphanumeric ASCII character string with 1..32 characters


Remove

Removes the selected table row.


Allocate applications

Opens the *Allocate applications* window. The window displays the applications that you can designate to the selected list.
- ☐ Click and select an item to designate it to the currently selected list.
  An application that is already designated to a different list the device designates to the currently selected list, after you click the *Ok* button.
- ☐ Click and deselect an item to undo its designation to the currently selected list.
  If you deselect the application `WebInterface`, then the connection to the device is lost, after you click the *Ok* button.

Name

Displays the name of the list.

To add a list, click the button.

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 user logging into the device management 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 into the device management 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 into the device management 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`.
- `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 *Device 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. The device lets you assign each application to exactly one list.

Active

Activates/deactivates the list.

Possible values:

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

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 Lightweight Directory Access Protocol (LDAP). The authentication server decides if the login data is valid and transfers the authorizations of the user to the device.

Upon successful login, the device caches the login data. This speeds up the login process when users log into the device management 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 columns *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 access role *`administrator`*. This provides you access to the device as administrator after logging into the device management through LDAP.

Possible values:

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

Configuration

Buttons

Flush cache

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

Client cache timeout [min]

Specifies for how many minutes after successfully logging into the device management 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 into 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 attempts to authenticate on the LDAP server with the user ID to find the “Distinguished Name” (DN) for the users logging into the device management. 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 into 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 into the device management.

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

To establish a secure connection, the device requires to obtain a valid digital certificate to verify the identity of the server. The prerequisite is that you have transferred the public certificate of the server onto the device. Ask the server administrator for a digital certificate in X.509 format. For security reasons, Hirschmann recommends using only digital certificates signed by a Certification Authority (CA).

URL

Specifies the path and file name of the digital certificate.

The device accepts digital certificates with the following properties:

- X.509 format
- `.PEM` file name extension
- Base64-coded and enclosed by the lines

```
-----BEGIN CERTIFICATE-----
…
-----END CERTIFICATE-----
```

The device gives you the following options for transferring the file onto the device:

- Import from the PC

  When the file is located on your PC or on a network drive, drag and drop it onto the area.
  As an alternative, click in the area to select the file.
  You can also use SCP or SFTP to transfer the file from your PC to the device. Perform the following steps:
  - ☐ On your PC, open an SCP or SFTP client, for example WinSCP.
  - ☐ Use the SCP or SFTP client to open a connection to the device.
  - ☐ Transfer the file onto the device, into the directory `/upload/ldap-cert`.
    When the file transfer is complete, the device starts installing the digital certificate. If the installation was successful, then the device generates an `ok` file in the directory `/upload/ldap-cert` and deletes the transferred file.
- Import from an SCP or SFTP server
  When the file 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>`
    Click the *Start* button to open the *Credentials* window. In this window, you enter the *User name* and *Password* to log into the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

Start

Transfers the file specified in the *URL* field onto the device.

For the changes to take effect after transferring a digital certificate into the device, disable and re-enable the *LDAP* function. See the *Operation* frame.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

 Add

Adds a table row.

 Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.

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.

If in the *Connection security* column a value other than *none* is specified and the digital certificate contains only DNS names of the server, then specify a DNS name.

Possible values:

- Valid IPv4 address (default setting: `0.0.0.0`)
- DNS name in the format `<domain>.<tld>` or `<host>.<domain>.<tld>`
  The prerequisite is that you also enable the *Client* function in the *Advanced > DNS > Client > Global* dialog.
  To establish an encrypted connection using a digital certificate, verify that the `Common Name` or `Subject Alternative Name` information in the digital certificate that you have transferred onto the device matches the value you specify here. Otherwise, the device will not be able to verify the identity of the server.
- `_ldap._tcp.<domain>.<tld>`
  Using this DNS name, the device queries the LDAP server list (SRV Resource Record) from the DNS server.

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 (2¹⁶-1)` (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 digital certificate contains only the DNS names, then you specify the DNS name of the server in the *Address* column. Enable the *Client* function in the *Advanced > DNS > Client > Global* dialog.

If the digital 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 setting.

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* column a value other than *none* is specified, then the device has verified the digital 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.

3.3.2 LDAP Role Mapping

[Device Security > LDAP > Role Mapping]

This dialog lets you set up to 64 mappings to assign an access role to users.

In the table you specify if the device assigns an access 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 into the device management, 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 access role with the more extensive authorizations or the 1st access role in the table that applies.

Configuration

Matching policy

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

Possible values:

▶ *highest* (default setting)
The device applies the access role with more extensive authorizations.

▶ *first*
The device applies the rule which has the lower value in the *Index* column to the user.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons


Add

Opens the *Create* window to add a table row.

- In the *Index* field, you specify the index number.
  Possible values:
  - `1..64`


Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates. You specify the index number when you add a table row.

Role

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

Possible values:

- *unauthorized* (default setting)
  The user is blocked, and the device rejects the user login.
  Assign this value to temporarily lock the user account. If an error is detected when another role is being assigned, then the device assigns this access role to the user account.
- *guest*
  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 specified 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`
  The role mapping is active.
- `unmarked` (default setting)
  The role mapping is inactive.

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]
- [SSH]
- [HTTP]
- [HTTPS]

[Information]

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

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

SNMPv1

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

Possible values:

- `marked`
  Server service is active.
- `unmarked`
  Server service is inactive.

SNMPv2

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

Possible values:

- `marked`
  Server service is active.
- `unmarked`
  Server service is inactive.

SNMPv3

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

Possible values:

- `marked`
  Server service is active.
- `unmarked`
  Server service is inactive.

SSH server

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

[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`
  SNMP version 1 access is active.
  - You specify the community names in the *Device Security > Management Access > SNMPv1/v2 Community* dialog.
- `unmarked` (default setting)
  SNMP version 1 access is inactive.

SNMPv2

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

Possible values:

- `marked`
  SNMP version 2 access is active.
  - You specify the community names in the *Device Security > Management Access > SNMPv1/v2 Community* dialog.
- `unmarked` (default setting)
  SNMP version 2 access is inactive.

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 (2¹⁶-1)` (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 settings.
- ☐ Restart the device.

[SSH]

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

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

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

The SSH server identifies itself to the clients using its public RSA key. When first setting up the connection, the client program displays the user the fingerprint of this key. The fingerprint contains a Base64-coded character sequence that is easy to check. When you make this character sequence available to the users through 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 generate the private and public keys (host keys) required for RSA directly in the device. As an alternative, transfer your own host key in PEM format onto the device.

As an alternative, the device lets you load the RSA key (host key) from an external memory during the system startup. 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 you disable the *SSH* server, then access to the device management is only possible using the Command Line Interface through the serial connection.

Configuration

TCP port

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

Possible values:

- `1..65535 (2¹⁶-1)` (default setting: `22`)
  Exception: Port `2222` is reserved for internal functions.

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

Sessions

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

Sessions (max.)

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

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

Possible values:

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

Session timeout [min]

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

A change in the value takes effect the next time a user logs into the device management.

Possible values:

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

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 generated:

- 2048 bit (RSA)

To get the SSH server to use the generated host key, restart the SSH server.

As an alternative, transfer your own host key in PEM format onto the device. 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.

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

RSA fingerprint

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

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

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 transferring the file onto the device:

- Import from the PC

  When the file is located on your PC or on a network drive, drag and drop it onto the  area.
  As an alternative, click in the area to select the file.
  You can also use SCP or SFTP to transfer the file from your PC to the device. Perform the following steps:
  - ☐ On your PC, open an SCP or SFTP client, for example WinSCP.
  - ☐ Use the SCP or SFTP client to open a connection to the device.
  - ☐ Transfer the file onto the device, into the directory `/upload/ssh-key`.
    When the file transfer is complete, the device starts installing the key. If the installation was successful, then the device generates an `ok` file in the directory `/upload/ssh-key` and deletes the transferred file.
- Import from an SCP or SFTP server
  When the file 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>`
    Click the *Start* button to open the *Credentials* window. In this window, you enter the *User name* and *Password* to log into the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

Start

Transfers the file specified in the *URL* field onto the device.

For the changes to take effect after transferring a digital certificate onto the device, disable and re-enable the *SSH server* function. See the *Operation* frame.

[HTTP]

This tab lets you enable/disable the Hypertext Transfer Protocol (HTTP) for the web server and specify the settings required for HTTP.

The web server provides the Graphical User Interface through an unencrypted HTTP connection. For security reasons, disable the Hypertext Transfer Protocol (HTTP) and use the Hypertext Transfer Protocol Secure (HTTPS) 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* function for the web server.

Possible values:

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

Note:
If the *HTTP* and *HTTPS* functions are disabled, then you can enable the *HTTP* function 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 (2¹⁶-1)` (default setting: `80`)
  Exception: Port `2222` is reserved for internal functions.

[HTTPS]

This tab lets you enable/disable the Hypertext Transfer Protocol Secure(HTTPS) for the web server and specify the settings required for HTTPS.

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

A digital certificate is required for the encryption of the HTTP connection. The device lets you generate this digital certificate yourself or to transfer an existing digital 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* function for the web server.

Possible values:

- *On* (default setting)
  The *HTTPS* function 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* function.
- *Off*
  The *HTTPS* function is disabled.
  When the *HTTP* function is enabled, the access to the device management is possible through an unencrypted *HTTP* connection.

Note:
If the *HTTP* and *HTTPS* functions are disabled, then you can enable the *HTTPS* function 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 (2¹⁶-1)` (default setting: `443`)
  Exception: Port `2222` is reserved for internal functions.

Certificate

If the device uses a digital certificate not signed by a Certification Authority (CA) known to the web browser, then the web browser may display a warning message before loading the Graphical User Interface.

To address the warning, you have the following possibilities:

- Transfer a digital certificate onto the device whose Certification Authority (CA) is known to your web browser. This may additionally require you to make the Certification Authority (CA) known to your web browser or operating system.
- As a workaround, you can also add an exception rule for the existing device certificate in your web browser.

Present

Displays if a digital certificate is present in the device.

Possible values:

- `marked`
  A digital certificate is present.
- `unmarked`
  The digital 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 digital certificate, restart the web server. Restarting the web server is possible only through the Command Line Interface.

As an alternative, transfer your own digital certificate onto 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 digital certificate.
- *delete*
  The device currently deletes a digital certificate.
- *generate*
  The device currently generates a digital certificate.

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 digital certificate.
- `sha256` (default setting)
  The *Fingerprint* field displays the SHA256 fingerprint of the digital certificate.

Fingerprint

Hexadecimal 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 import

URL

Specifies the path and file name of the digital certificate.

The device accepts digital certificates with the following properties:

- X.509 format
- `.PEM` file name extension
- Base64-coded and enclosed by the lines
  - `-----BEGIN PRIVATE KEY-----`
    …
    `-----END PRIVATE KEY-----`
    or
  - `-----BEGIN CERTIFICATE-----`
    …
    `-----END CERTIFICATE-----`
- RSA key with 2048 bit length

The device gives you the following options for transferring the file onto the device:

- Import from the PC

  When the file is located on your PC or on a network drive, drag and drop it onto the  area.
  As an alternative, click in the area to select the file.
  You can also use SCP or SFTP to transfer the file from your PC to the device. Perform the following steps:
  - ☐ On your PC, open an SCP or SFTP client, for example WinSCP.
  - ☐ Use the SCP or SFTP client to open a connection to the device.
  - ☐ Transfer the file onto the device, into the directory `/upload/https-cert`.
    When the file transfer is complete, the device starts installing the certificate. If the installation was successful, then the device generates an `ok` file in the directory `/upload/https-cert` and deletes the transferred file.
- Import from an SCP or SFTP server
  When the file is on an SCP or SFTP server, specify the URL for the file in the following form:
  - `scp://` or `sftp://<IP address>[:port]/<path>/<file name>`
    Click the *Start* button to open the *Credentials* window. In this window, you enter the *User name* and *Password* to log into the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>[:port]/<path>/<file name>`

Start

Transfers the file specified in the *URL* field onto the device.

For the changes to take effect after transferring a digital certificate onto the device, disable and re-enable the *HTTPS server* function. See the *Operation* frame.

3.4.2 IP Access Restriction

[Device Security > Management Access > IP Access Restriction]

This dialog lets you restrict access to the device management from a specific IP address range or through a specific physical interface for selected applications.

- If the function is disabled, then access to the device management is unrestricted. Everyone can access the device management from any IP address or through any physical interface using any application.
- If the function is enabled, then access is restricted. Everyone can access the device management only under the following conditions:
  - At least one rule is active.
    and
  - You access the device with a permitted application from a permitted IP address range or through a permitted physical interface specified in the rule.

Operation

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.

Note:
Before you enable the function, verify that the table contains at least one active rule that grants you access to the device management. Otherwise, access to the device management is only possible using the Command Line Interface through the serial connection.

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

Table

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

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

 Add

Adds a table row.

 Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.

The priority of access to the device management is based on the index number.

When you delete a table row, this leaves a gap in the numbering. When you add a table row, the device fills the first gap.

Possible values:

- `1..16`

Interface

Specifies the physical interface through which users have access to the device management.

The prerequisite is that in the *Address* and *Netmask* columns, the value `0.0.0.0` is specified.

Possible values:

- `All` (default setting)
  Users can have restricted access to the device management through every interface based on the IP address specified in the *Address* column.
- `<Port number>`
  Users can have restricted access to the device management only through the specified interface.
  The device supports the *IP Access Restriction* function only on physical interfaces, not on logical interfaces.

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.

The prerequisite is that in the *Interface* column the value `All` is specified.

Possible values:

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

Netmask

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

The prerequisite is that in the *Interface* column the value `All` is specified.

Possible values:

- Valid netmask (default setting: `0.0.0.0`)
  Example: To restrict access from a single IP address, specify the value as `255.255.255.255`.

HTTP

Activates/deactivates the HTTP access.

Possible values:

- `marked` (default setting)
  HTTP access is active. Access is possible from the adjacent IP address range or through the adjacent physical interface.
- `unmarked`
  HTTP access is inactive.

HTTPS

Activates/deactivates the HTTPS access.

Possible values:

- `marked` (default setting)
  HTTPS access is active. Access is possible from the adjacent IP address range or through the adjacent physical interface.
- `unmarked`
  HTTPS access is inactive.

SNMP

Activates/deactivates the SNMP access.

Possible values:

- `marked` (default setting)
  SNMP access is active. Access is possible from the adjacent IP address range or through the adjacent physical interface.
- `unmarked`
  SNMP access is inactive.

SSH

Activates/deactivates the SSH access.

Possible values:

- `marked` (default setting)
  SSH access is active. Access is possible from the adjacent IP address range or through the adjacent physical interface.
- `unmarked`
  SSH access is inactive.

Active

Activates/deactivates the table row.

Possible values:

- `marked`
  The table row is active. The device restricts the access to the device management from the specified IP address range or through the specified interface for the selected applications.
- `unmarked` (default setting for new table row)
  The table row is inactive. The device does not restrict access to the device management from the specified IP address range or through the specified interface for the selected applications.

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 into the device management.

Possible values:

- `0..160` (default setting: `5`)

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

3.4.4 Command Line Interface

[Device Security > Management Access > CLI]

In this dialog, you specify settings for the Command Line Interface. For further information about the Command Line Interface, see 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 to activate automatic closing of inactive Command Line Interface sessions through the serial connection.

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
  – `%s` short product name
  – `%t` time
Default setting: `(EAGLE)`

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

Serial interface timeout [min]

Specifies the time in minutes after which the device automatically closes the session of an inactive user logged into the device management using the Command Line Interface through the serial connection.

Possible values:

▶ `0..160` (default setting: `5`)
The value `0` deactivates the function, and the user remains logged into the device management when inactive.

A change in the value takes effect the next time a user logs into the device management.

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

[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 into the device management through 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>`

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 using SNMPv1/v2 with a community name in the SNMP data packet header. Depending on the community name (see *Community* column), the application gets *read-only* authorization or *read and write* authorization.

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

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Community

Displays the authorization for SNMPv1/v2 access to the device.

Possible values:

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

Name

Specifies the community name for the adjacent authorization.

Possible values:

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

  `private` (default setting for *read and write* authorization)
  `public` (default setting for *read-only* authorization)

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 into the device management.

The users see this text in the login dialog of the Graphical User Interface and of the Command Line Interface. Users logging into the device management 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, the device saves this text.

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>`

4 Network Security

The menu contains the following dialogs:

- Network Security Overview
- RADIUS
- Asset
- Protocol
- Packet Filter
- Deep Packet Inspection
- DoS

4.1 Network Security Overview

[Network Security > Overview]

This dialog displays an overview over the network security rules used in the device.

Overview

The top level displays:

- The ports to which a network security rule is assigned
- The VLANs to which a network security rule is assigned

The subordinate levels display:

- The set-up *Packet filter L3* rules
  See the *Network Security > Packet Filter > Routed Firewall Mode* dialog.
- The set-up *Packet filter L2* rules
  See the *Network Security > Packet Filter > Transparent Firewall Mode* dialog.
- The set-up *Destination NAT* rules
  See the *Routing > NAT > Destination NAT* dialog.
- The set-up *Double NAT* rules
  See the *Routing > NAT > Double NAT* dialog.
- The set-up *Masquerading NAT* rules
  See the *Routing > NAT > Masquerading NAT* dialog.
- The set-up *1:1 NAT* rules
  See the *Routing > NAT > 1:1 NAT* dialog.

Buttons

Displays a text field to search for a keyword. When you enter a character or string, the overview displays only items related to this keyword.

Collapses the levels. The overview then displays only the first level of the items.

Expands the levels. The overview then displays every level of the items.

Expands the current item and displays the items of the next lower level.

Collapses the item and hides the items of the underlying levels.

4.2 RADIUS

[Network Security > RADIUS]

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

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

- Authentication
  The authentication server authenticates the users when the RADIUS client at the access point forwards the login data of the users to the server.
- Authorization
  The authentication server authorizes logged in users for selected services by assigning various parameters for the relevant end device to the RADIUS client at the access point.

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

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

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

The menu contains the following dialogs:

- RADIUS Global
- RADIUS Authentication Server
- RADIUS Authentication Statistics

4.2.1 RADIUS Global

[Network Security > RADIUS > Global]

This dialog lets you specify basic settings for RADIUS.

RADIUS configuration

Buttons

Reset

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

Retransmits (max.)

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

Possible values:

- `1..15` (default setting: `4`)

Timeout [s]

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

Possible values:

- `1..30` (default setting: `5`)

NAS IP address (attribute 4)

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

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).

4.2.2 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

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

 Add

Opens the *Create* window to add a table row.

- In the *Index* field, you specify the index number.
- In the *Address* field, you specify the IP address of the server.

 Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates. You specify the index number when you add a table row.

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`)
  You can specify the same name for several servers. When several servers have the same name, the setting in the *Primary server* column applies.

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 (2¹⁶-1)` (default setting: `1812`)
  Exception: Port `2222` is reserved for internal functions.

Secret

Displays ****** (asterisks) when you specify a password with which the device logs into 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.

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.
  This setting applies only if more than one server in the table has the same value in the *Name* column.
- `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 columns *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.

4.2.3 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 table row.

To delete the statistic, click in the *Network Security > RADIUS > Global* dialog the button.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Name

Displays the name of the server.

IP 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 requests

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.

4.3 Asset

[Network Security > Asset]

This dialog lets you specify the settings for managing the assets. An asset can represent a physical device, such as a PLC (Programmable Logic Controller), a computer or a network device. An asset can also represent a virtual object, such as a multicast address range, or a multicast address. Assets provide flexibility when setting up and maintaining firewall rules. The device lets you set up to 100 assets.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons


Add

Opens the *Create* window to add a table row.

- In the *Name* field, you specify a unique name for the asset.
  Possible values:
  ▶ Alphanumeric ASCII character string with 1..32 characters, excluding the character `any`
  When you click the *Ok* button, the device adds the table row. The device assigns the name specified in the *Name* field to the table row.


Remove

Removes the selected table row.

Index

Displays the sequential number of the asset to which the table row relates. The device automatically assigns the value when you add a table row.

Name

Specifies a unique name for the asset.

Possible values:

▶ Alphanumeric ASCII character string with 1..32 characters, excluding the character `any`

Description

Specifies a description for the asset.

Possible values:

▶ Alphanumeric ASCII character string with 0..128 characters

Type

Specifies the type of the asset.

Possible values:

▶ *computer* (default setting)
▶ *controller*
▶ *device*
▶ *network*
▶ *network-equipment*
▶ *broadcast*
▶ *multicast*

Manufacturer

Specifies the manufacturer of the asset.

Possible values:

- Alphanumeric ASCII character string with 0..128 characters

Model

Specifies the model of the asset.

Possible values:

- Alphanumeric ASCII character string with 0..128 characters

General location

Specifies a general location for the asset.

Possible values:

- Alphanumeric ASCII character string with 0..128 characters

Specific location

Specifies a specific location for the asset.

Possible values:

- Alphanumeric ASCII character string with 0..128 characters

Asset tag

Specifies a tag for the identification of the user-defined asset.

Possible values:

- Alphanumeric ASCII character string with 0..128 characters

IP address

Specifies the IP address of the asset.

Possible values:

- `any` (default setting)
  The device accepts any IP address associated with the asset.
- Valid IPv4 address
  The device applies the specified IP address to the asset.
- Valid IPv4 address and netmask in CIDR notation
  The device applies the specified IP address in the specified subnet to the asset.
  Example: `192.168.112.0/25`
- An exclamation mark (`!`) preceding the IP address reverses the expression into its opposite. The device accepts any IP address or the subnet associated with the asset excluding the specified IP address or the subnet.
  Example: `!1.1.1.1` or `!192.168.112.0/25`

MAC address

Specifies the MAC address of the asset.

Possible values:

- `any` (default setting)
  The device accepts any MAC address associated with the asset.
- Valid MAC address
  The device applies the specified MAC address to the asset.

4.4 Protocol

[Network Security > Protocol]

This dialog lets you specify basic settings for the user-defined protocol. The device lets you set up to 50 user-defined protocols.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

 Add

Opens the *Create* window to add a table row. In the *Protocol name* field, you specify a unique name for the protocol.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters, excluding the following characters:
  - any
  - icmp
  - igmp
  - ipip
  - tcp
  - udp
  - esp
  - ah
  - icmpv6

  When you click the *Ok* button, the device adds the table row. The device assigns the name specified in the *Protocol name* field to the table row.

 Remove

Removes the selected table row.

Index

Displays the sequential number of the protocol to which the table row relates. The device automatically assigns the value when you add a table row.

Protocol name

Specifies a unique name for the protocol.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters, excluding the following characters:
  - any
  - icmp
  - igmp
  - ipip
  - tcp

- udp
- esp
- ah
- icmpv6

Description

Specifies a description for the protocol.

Possible values:

- Alphanumeric ASCII character string with 0..128 characters

Protocol type

Specifies the protocol type for the user-defined protocol, which the device applies in the packet filter rule.

Possible values:

- *any* (default setting)
- *ethernet*
- *icmp*
- *tcp*
- *udp*

Ethertype

Specifies the *Ethertype* keyword of the data packets, which the Layer 2 packet filter uses.

Possible values:

- *custom* (default setting)
- *appletalk*
- *arp*
- *ibmsna*
- *ipv4*
- *ipv6*
- *ipxold*
- *mplsmcast*
- *mplsucast*
- *netbios*
- *novell*
- *pppoedisc*
- *rarp*
- *pppoesess*
- *ipxnew*
- *profinet*
- *powerlink*
- *ethercat*
- *vlan8021q*

Ethertype custom value

Specifies the *Ethertype* value of the data packets in a decimal notation, which the Layer 2 packet filter uses. The prerequisite is that in the *Ethertype* column the value `custom` is specified.

Possible values:

- `1536..65535 (2¹⁶-1)` (default setting: `0`)

Protocol number

Specifies the protocol number for the user-defined protocol which the IPv4 header uses. The prerequisite is that in the *Protocol type* column a value other than `ethernet` is specified.

Possible values:

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

Port

Specifies the destination port that the device evaluates in the data packet. The prerequisite is that in the *Protocol type* column the value `TCP` or `UDP` is specified.

Possible values:

- `any` (default setting)
  The device applies the rule to every data packet without evaluating the destination port.
- `1..65535 (2¹⁶-1)`
  The device applies the rule only to data packets containing the specified destination port.
  The field lets you specify the following options:
  - You specify a port with a single numerical value, for example `21`.
  - You specify multiple individual ports with numerical values separated by commas, for example `21,80,110`.
  - You specify a port range with numerical values connected by dashes, for example `2000-3000`.
  - You can also combine ports and port ranges, for example `21,2000-3000,65535`.
    The field lets you specify up to 15 numerical values. When you enter `21,2000-3000,65535`, for example, you use 4 of 15 numerical values.

4.5 Packet Filter

[Network Security > Packet Filter]

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

The menu contains the following dialogs:
- Routed Firewall Mode
- Transparent Firewall Mode

4.5.1 Routed Firewall Mode

[Network Security > Packet Filter > Routed Firewall Mode]

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

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

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

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

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

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

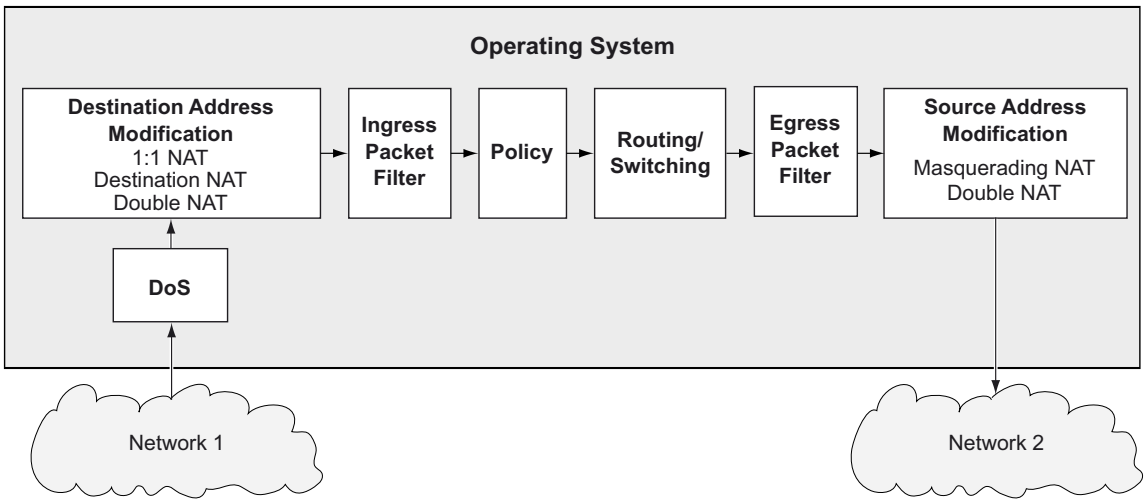


Figure 1: Processing sequence of the data packets in the device

The menu contains the following dialogs:

- Global
- Firewall Learning Mode
- Packet Filter Rule
- Packet Filter Assignment
- Packet Filter Overview

4.5.1.1 Global

[Network Security > Packet Filter > Routed Firewall Mode > Global]

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

Configuration

Buttons

Commit changes

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

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

Note:
While the device is activating the saved rules, you cannot establish any new communication connections.

Allowed rules for L3 firewalling (max.)

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

Default policy

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

Possible values:

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

Validate checksum

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

Possible values:

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

Logging

Log

Activates/deactivates the logging in the System Log file for cases when the device applies the *default policy* to a data packet. This happens whenever no *Packet Filter* rule exists or no data packet matches the set up rules.

Possible values:

- `marked`
  Logging is active.
  The device places an entry in the System Log file when the device applies the *default policy* to the data packets. See the *Diagnostics > Report > System Log* dialog.
- `unmarked` (default setting)
  Logging is inactive.

Information

Uncommitted changes present

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

Possible values:

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

4.5.1.2 Firewall Learning Mode

[Network Security > Packet Filter > Routed Firewall Mode > FLM]

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

The maximum number of rules that you can specify using the *FLM* function depends on the number of rules already set up in the *Network Security > Packet Filter > Routed Firewall Mode > Rule* dialog. The device lets you specify up to 2048 rules.

The *FLM* function only applies to packets that pass through the device matching the *FORWARD* chain. The *FLM* function does not apply to the packets that the device receives on the *INPUT* chain and to those that the device generates on the *OUTPUT* chain. During the learning phase the device retains SSH, SNMP, and GUI access.

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

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

Note:
During the learning phase the network is temporarily exposed, because the *FLM* function sets up rules to accept every data packet on the selected ports.

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

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

[Configuration]

The tab lets you enable the *FLM* function. The device monitors up to 4 interfaces to discover what type of data packets the device forwards through the interfaces into the network.

Operation

Operation

Enables/disables the *FLM* function.

Possible values:

- *On*
  The *FLM* function is enabled.
- *Off* (default setting)
  The *FLM* function is disabled.

Information

Buttons

 Start

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

 Stop

Stops the learning phase.

 Clear

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

Status

Displays the state of the running *FLM* application.

Possible values:

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

Information

Displays the status of *FLM* application memory.

Interfaces selected for learning

Displays the interfaces that the *FLM* function actively monitors. The maximum number of interfaces that the device monitors is 4.

Additional information

Displays a special status message.

Learned entries

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

Free memory for learning data [%]

Displays the percentage of free memory available for learning data.

[Rules]

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

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

Learned entries table

Buttons

 Add

Opens the *Create* window to add a rule when the *Learned entries* table displays at least one table row. The *Packet filter rules* table displays the added rule:

- In the *Description* field, you specify a name for the rule.
- In the *Source address* field, you specify the source address of the data packets.
- In the *Destination address* field, you specify the destination address of the data packets.
- From the *Protocol* drop-down list, you select the protocol type of the data packets.
- In the *Destination port* field, you specify the destination port of the data packets.
- In the *Ingress interface* field, you specify if the device applies the rule to data packets received or sent on a router interface.

Source address

Displays the source address of the packets.

Destination address

Displays the destination address of the packet.

Protocol

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

Destination port

Displays the destination port of the packet.

Ingress interface

Displays the interface that received the packet.

Egress interface

Displays the interface that sent the packet.

First occurence

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

Connections by Rule Set

Displays the number of connections that match the rules set in the table below.

Connections by Selection

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

Packet filter rules table

Buttons

Remove

Removes the selected table row.

Edit

Opens the *Edit* window to edit the parameters of the selected table row.

Rule index

Displays the sequential number of the *Packet Filter* rule.

Description

Specifies a name for the rule.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters

Source address

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

Possible values:

- `any` (default setting)
  The device applies the *Packet Filter* rule to data packets with any source address.
- Valid IPv4 address
  The device applies the rule to data packets with the specified source address.
- Valid IPv4 address and netmask in CIDR notation
  The device applies the rule to data packets with the specified source address in the specified subnet.

Destination address

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

Possible values:

- `any` (default setting)
  The device applies the *Packet Filter* rule to data packets with any destination address.

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

Protocol

Specifies the protocol type of the data packets to which the device applies the rule. The device applies the rule only to data packets that contain the specified value in the *Protocol* field.

Possible values:

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

Destination port

Specifies the destination port of the data packets to which the device applies the rule. The prerequisite is that in the *Protocol* column the value `TCP` or `UDP` is specified.

Possible values:

- `any` (default setting)
  The device applies the *Packet Filter* rule to every data packet without evaluating the destination port.
- `1..65535 (2¹⁶-1)`
  The device applies the *Packet Filter* rule only to data packets containing the specified destination port.
  The field lets you specify the following options:
  - You specify a port with a single numerical value, for example `21`.
  - You specify multiple individual ports with numerical values separated by commas, for example `21,80,110`.
  - You specify a port range with numerical values connected by dashes, for example `2000-3000`.
  - You can also combine ports and port ranges, for example `21,2000-3000,65535`.
    The field lets you specify up to 15 numerical values. When you enter `21,2000-3000,65535`, for example, you use 4 of 15 numerical values.

Action

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

Possible values:

- *accept* (default setting)
  The device accepts the data packets according to the ingress rules. Afterwards, the device applies the egress rules before the port sends the data packets.
- *drop*
  The device discards the data packet without informing the sender.
- *reject*
  The device discards the data packet and informs the sender.
- *enforce-modbus*
  The device applies the rule specified in the *DPI profile index* column to the data packets.
- *enforce-opc*
  The device applies the rule specified in the *DPI profile index* column to the data packets.
- *enforce-dnp3*
  The device applies the rule specified in the *DPI profile index* column to the data packets.
- *enforce-iec104*
  The device applies the rule specified in the *DPI profile index* column to the data packets.
- *enforce-ethernetip*
  The device applies the rule specified in the *DPI profile index* column to the data packets.

Ingress interface

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

Possible values:

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

Active

Activates/deactivates the rule.

Possible values:

- marked
  The rule is active.
- unmarked (default setting)
  The rule is inactive.

4.5.1.3 Packet Filter Rule

[Network Security > Packet Filter > Routed Firewall Mode > Rule]

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

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

 Add

Adds a table row.

 Remove

Removes the selected table row.

Rule index

Displays the sequential number of the *Packet Filter* rule. The device automatically assigns the value when you add a table row.

Description

Specifies a name for the rule.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters

Source address

Specifies the asset name or the source address of the data packets to which the device applies the rule. Select an item from the drop-down list or specify the source address. You specify the asset name in the *Network Security > Asset* dialog.

Possible values:

- `any` (default setting)
  The device applies the rule to data packets with any asset name or source address.
- Valid IPv4 address
  The device applies the rule to data packets with the specified source address.
- Valid IPv4 address and netmask in CIDR notation
  The device applies the rule to data packets with the specified source address in the specified subnet.
  Example: `192.168.112.0/25`

- An exclamation mark (`!`) preceding the IP address reverses the expression into its opposite. The device applies the rule to data packets with any source address or subnet excluding the specified source address or the subnet.
  Example: `!1.1.1.1` or `!192.168.112.0/25`
- Name of the asset
  Alphanumeric ASCII character string with 1..32 characters

Destination address

Specifies the asset name or the destination address of the data packets to which the device applies the rule. Select an item from the drop-down list or specify the destination address. You specify the asset name in the *Network Security > Asset* dialog.

Possible values:

- `any` (default setting)
  The device applies the rule to data packets with any asset name or destination address.
- Valid IPv4 address
  The device applies the rule to data packets with the specified destination address.
- Valid IPv4 address and netmask in CIDR notation
  The device applies the rule to data packets with the specified destination address in the specified subnet.
  Example: `192.168.112.0/25`
- An exclamation mark (`!`) preceding the IP address reverses the expression into its opposite. The device applies the rule to data packets with any destination address or subnet excluding the specified destination address or the subnet.
  Example: `!1.1.1.1` or `!192.168.112.0/25`
- Name of the asset
  Alphanumeric ASCII character string with 1..32 characters

Protocol

Specifies the IP protocol or Layer 4 protocol type of the data packets to which the device applies the rule. The device applies the rule only to data packets that contain the specified value in the *Protocol* field.

Possible values:

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

- *icmpv6*
  Internet Control Message Protocol for IPv6 (RFC 4443)
- <user-defined protocols>
  The device also processes user-defined protocols. You specify user-defined protocols in the *Network Security > Protocol* dialog.

Source port

Specifies the L4 source port of the data packets to which the device applies the rule. The prerequisite is that in the *Protocol* column the value *tcp* or *udp* is specified.

Possible values:

- any (default setting)
  The device applies the *Packet Filter* rule to every data packet without evaluating the L4 source port.
- 1..65535 (2^{16}-1)
  The device applies the *Packet Filter* rule only to data packets containing the specified L4 source port.
  The field lets you specify the following options:
  - You specify a port with a single numerical value, for example 21.
  - You specify multiple individual ports with numerical values separated by commas, for example 21,80,110.
  - You specify a port range with numerical values connected by dashes, for example 2000-3000.
  - You can also combine ports and port ranges, for example 21,2000-3000,65535.
    The field lets you specify up to 15 numerical values. When you enter 21,2000-3000,65535, for example, you use 4 of 15 numerical values.

Destination port

Specifies the L4 destination port of the data packets to which the device applies the rule. The prerequisite is that in the *Protocol* column the value *tcp* or *udp* is specified.

Possible values:

- any (default setting)
  The device applies the *Packet Filter* rule to every data packet without evaluating the L4 destination port.
- 1..65535 (2^{16}-1)
  The device applies the *Packet Filter* rule only to data packets containing the specified L4 destination port.
  The field lets you specify the following options:
  - You specify a port with a single numerical value, for example 21.
  - You specify multiple individual ports with numerical values separated by commas, for example 21,80,110.
  - You specify a port range with numerical values connected by dashes, for example 2000-3000.
  - You can also combine ports and port ranges, for example 21,2000-3000,65535.
    The field lets you specify up to 15 numerical values. When you enter 21,2000-3000,65535, for example, you use 4 of 15 numerical values.

Parameters

Specifies additional parameters for this rule.

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

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

Possible values:

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

Action

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

Possible values:

- *accept* (default setting)
  The device accepts the data packets according to the ingress rules. Afterwards, the device applies the egress rules before the port sends the data packets.
- *drop*
  The device discards the data packet without informing the sender.
- *reject*
  The device discards the data packet and informs the sender.
- *enforce-modbus*
  The device applies the rule specified in the *DPI profile index* column to the data packets. The prerequisite is that in the *Source address*, *Destination address* and *Destination port* columns a value other than `any` is specified.
  The value is only available in the software level IN/SU/UN. Refer to the *Software level* characteristic value in the product code.
- *enforce-opc*
  The device applies the rule specified in the *DPI profile index* column to the data packets. The prerequisite is that in the *Source address*, *Destination address* and *Destination port* columns a value other than `any` is specified.
  The value is only available in the software level IN/UN. Refer to the *Software level* characteristic value in the product code.

- *enforce-dnp3*
  The device applies the rule specified in the *DPI profile index* column to the data packets. The prerequisite is that in the *Source address*, *Destination address* and *Destination port* columns a value other than `any` is specified.
  The value is only available in the software level SU/UN. Refer to the *Software level* characteristic value in the product code.
- *enforce-iec104*
  The device applies the rule specified in the *DPI profile index* column to the data packets. The prerequisite is that in the *Source address*, *Destination address* and *Destination port* columns a value other than `any` is specified.
  The value is only available in the software level SU/UN. Refer to the *Software level* characteristic value in the product code.
- *enforce-ethernetip*
  The device applies the rule specified in the *DPI profile index* column to the data packets. The prerequisite is that in the *Source address*, *Destination address* and *Destination port* columns a value other than `any` is specified.
  The value is only available in the software level IN/UN. Refer to the *Software level* characteristic value in the product code.
- *enforce-s7*
  The device applies the rule specified in the *DPI profile index* column to the data packets.
  Prerequisites:
  - In the *Source address* column, a value other than `any` is specified.
  - In the *Destination address* column, a value other than `any` is specified.
  - In the *Protocol* column, the value *tcp* is specified.
  - In the *Destination port* column, a value other than `any` is specified.

  The value is only available in the software level UN. Refer to the *Software level* characteristic value in the product code.

Log

Activates/deactivates the logging in the log file.

Possible values:

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

Trap

Activates/deactivates the sending of SNMP traps when the device applies a *Packet Filter* rule to a data packet.

Possible values:

- `marked`
  The sending of SNMP traps is active. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
  If the device applies the *Packet Filter* rule to a data packet, then the device sends an SNMP trap.
- `unmarked` (default setting)
  The sending of SNMP traps is inactive.

DPI profile index

Specifies which rule the device applies to the data packets.

The prerequisite is that in the *Action* column one of the following values is specified:

- *enforce-modbus*
- *enforce-opc*
- *enforce-dnp3*
- *enforce-iec104*
- *enforce-ethernetip*
- *enforce-s7*

Possible values:

- `0` (default setting)
  The device does not apply any rule to the data packets.
- `1..32`
  The device applies the rule with the specified Index number to the data packets.

Active

Activates/deactivates the rule.

To apply the settings to the data stream, perform the following steps:

- ☐ Click the ✓ button to save the current settings.
- ☐ Open the *Network Security > Packet Filter > Routed Firewall Mode > Global* dialog, or the *Network Security > Packet Filter > Routed Firewall Mode > Assignment* dialog.
- ☐ Click the ⬆ button.

Possible values:

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

4.5.1.4 Packet Filter Assignment

[Network Security > Packet Filter > Routed Firewall Mode > Assignment]

This dialog lets you assign one or more *Packet Filter* rules to the router interfaces of the device. You set up router interfaces in the *Routing > Interfaces > Configuration* dialog.

Information

Assignments

Displays how many rules are active for the ports.

Uncommitted changes present

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

Possible values:

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

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the *Create* window to assign a rule to a router interface.

- From the *Rule index* drop-down list, you select the rule that you assign to the router interface.
- From the *Direction* drop-down list, you select if the device applies the rule to received or sent data packets or to both.
- From the *Interface* drop-down list, you select the router interface on which the device applies the rule.

Remove

Removes the selected table row.

Commit changes

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

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

Note:
While the device is activating the saved rules, you cannot establish any new communication connections.

Description

Displays the name of the rule. You specify the description in the *Network Security > Packet Filter > Routed Firewall Mode > Rule* dialog.

Rule index

Displays the sequential number of the *Packet Filter* rule. You specify the rule index when you add a table row.

Interface

Displays the router interface on which the device applies the rule. You specify the interface number when you add a table row.

Direction

Displays if the device applies the *Packet Filter* rule to received or sent data packets or to both.

Possible values:

- `ingress`
  The device applies the *Packet Filter* rule to data packets received on the router interface.
- `egress`
  The device applies the *Packet Filter* rule to data packets sent on the router interface.
- `both`
  The device applies the *Packet Filter* rule to data packets sent and received on the router interface.

Priority

Specifies the priority of the *Packet Filter* rule.

Using the priority, you specify the sequence in which the device applies the rules to the data stream. The device applies the rules in ascending order which starts with priority `0`.

Possible values:

- `0..4294967295 (2³²-1)` (default setting: `1`)

Active

Activates/deactivates the rule.

To apply the settings to the data stream, perform the following steps:

- ☐ Click the ✓ button to save the current settings.
- ☐ Open the *Network Security > Packet Filter > Routed Firewall Mode > Global* dialog, or the *Network Security > Packet Filter > Routed Firewall Mode > Assignment* dialog.
- ☐ Click the ⬆ button.

Possible values:

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

4.5.1.5 Packet Filter Overview

[Network Security > Packet Filter > Routed Firewall Mode > Overview]

This dialog gives you an overview of the specified *Packet Filter* rules.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Description

Displays the name of the rule. You specify the description in the *Network Security* > *Packet Filter* > Routed Firewall Mode > *Rule* dialog.

Rule index

Displays the sequential number of the *Packet Filter* rule.

Interface

Displays the router interface on which the device applies the rule.

Direction

Displays if the device applies the *Packet Filter* rule to received or sent data packets or to both.

Possible values:

- `ingress`
  The device applies the *Packet Filter* rule to data packets received on the router interface.
- `egress`
  The device applies the *Packet Filter* rule to data packets sent on the router interface.
- `both`
  The device applies the *Packet Filter* rule to data packets sent and received on the router interface.

Priority

Displays the priority of the *Packet Filter* rule. The device applies the rules in ascending order which starts with priority `0`.

Source address

Displays the asset name or the source address of the data packets to which the device applies the rule.

Source port

Displays the source TCP or UDP port of the data packets to which the device applies the rule.

Destination address

Displays the asset name or the destination address of the data packets to which the device applies the rule.

Destination port

Displays the destination TCP or UDP port of the data packets to which the device applies the rule.

Protocol

Displays the IP protocol to which the *Packet Filter* rule is restricted. The device applies the *Packet Filter* rule only to data packets with the specified IP protocol.

Parameters

Displays additional parameters for this rule.

Action

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

DPI profile index

Displays the profile index of the *DPI enforcer* function. You specify the profile index in the *Network Security > Packet Filter > Routed Firewall Mode > Rule* dialog.

Log

Displays if the device places an entry in the log file when the device applies the rule to a data packet.

Trap

Displays if the device sends an SNMP trap when the device applies the rule to a data packet.

4.5.2 Transparent Firewall Mode

[Network Security > Packet Filter > Transparent Firewall Mode]

In this menu, you specify the settings for the *Transparent Firewall Mode* packet filter. The *Transparent Firewall Mode* packet filter contains rules which the device applies successively to the data stream on its non-routing ports or VLAN interfaces. The *Transparent Firewall Mode* packet filter evaluates every data packet that passes through the firewall based on the connection status as mentioned below:

- For IPv4, evaluation is *stateful*.
- For other Layer 2 and Layer 3 protocols, evaluation is *stateless*.

The device filters the undesired data packets selectively while the connection is unknown.

- If a data packet matches the criteria of one or more rules, then the device applies the action specified in the first applicable rule to the data stream. The device ignores the rules that follow the first applicable rule.
- If no rule matches, then the device applies the default rule. In the default setting, the default rule has the value `accept`. The device lets you change the default rule in the *Network Security > Packet Filter > Transparent Firewall Mode > Global* dialog.

The device provides a multi-step approach to set up and apply the *Packet Filter* rules:

- You add a rule.
- You assign the rule to a non-routing port or VLAN.
  Up to this step, changes have no effect on the behavior of the device and the data stream.
- You apply the rule to the data stream.

The device processes data packets in the following sequence:

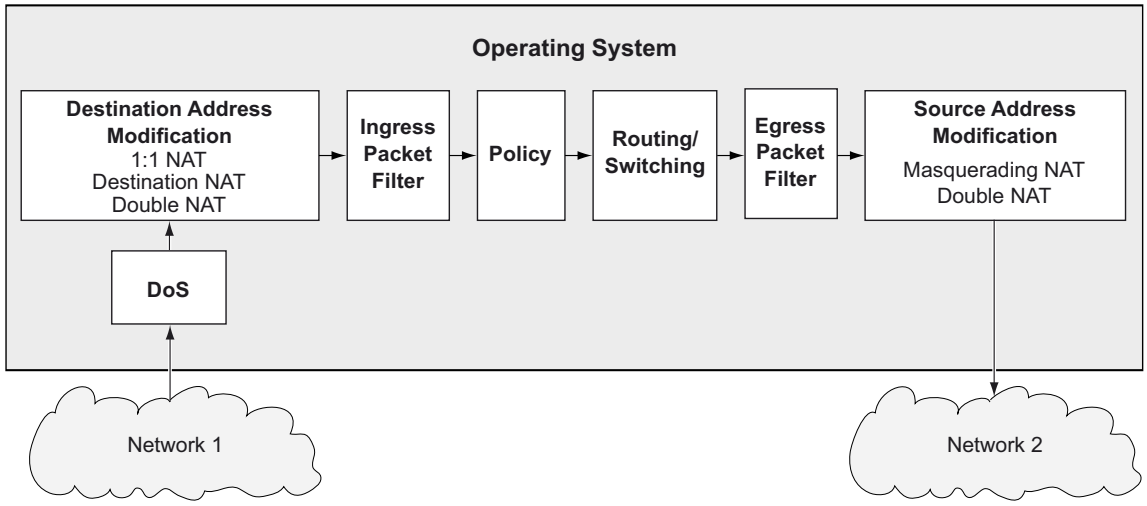


Figure 2: Processing sequence of the data packets in the device

The menu contains the following dialogs:

- Packet Filter Global
- Packet Filter Rule
- Packet Filter Assignment
- Packet Filter Overview

4.5.2.1 Packet Filter Global

[Network Security > Packet Filter > Transparent Firewall Mode > Global]

In this dialog, you specify the global settings for the *Transparent Firewall Mode* packet filter.

Configuration

Buttons

Commit changes

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

Note:
While the device is activating the saved rules, you cannot establish any new communication connections.

Allowed rules for L2 firewalling (max.)

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

Default policy

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

Possible values:

- *accept* (default setting)
  The device accepts the data packets.
- *drop*
  The device discards the data packets.
  In further progress, note when you assign any rule to a port or VLAN interface: The device accepts ARP packets implicitly, regardless of the data packet type.

Validate FCS

Specifies if the firewall evaluates the *Frame Check Sequence* of data packets.

Possible values:

- `marked` (default setting)
  The device evaluates the *Frame Check Sequence* in the data packet. If the value is invalid, then the device drops the data packet.
- `unmarked`
  The device ignores the *Frame Check Sequence*. The device forwards the data packet even if the value is invalid.

Information

Uncommitted changes present

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

Possible values:

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

4.5.2.2 Packet Filter Rule

[Network Security > Packet Filter > Transparent Firewall Mode > Rule]

This dialog lets you set up rules for the packet filter. You assign the rules specified here to the desired non-routing ports or VLANs in the *Network Security > Packet Filter > Transparent Firewall Mode > Assignment* dialog.

Table

For information on how to customize the appearance of the table, see "Working with tables" on page 16.

Buttons

Add

Adds a table row.

Remove

Removes the selected table row.

Index

Displays the sequential number of the *Packet Filter* rule. The device automatically assigns the value when you add a table row.

Description

Specifies a name for the rule.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters

Action

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

Possible values:

- `accept` (default setting)
  The device accepts the data packets according to the ingress rules. Afterwards, the device applies the egress rules before the port sends the data packets.
- `drop`
  The device discards the data packet without informing the sender.
- `enforce-modbus`
  The device applies the rule specified in the *DPI profile index* column to the data packets. The prerequisite is that in the *Source IP address*, *Destination IP address* and *Destination port* columns a value other than `any` is specified.
  The value is only available in the software level IN/SU/UN. Refer to the *Software level* characteristic value in the product code.

- *enforce-opc*
  The device applies the rule specified in the *DPI profile index* column to the data packets. The prerequisite is that in the *Source IP address*, *Destination IP address* and *Destination port* columns a value other than `any` is specified.
  The value is only available in the software level IN/UN. Refer to the *Software level* characteristic value in the product code.
- *enforce-iec104*
  The device applies the rule specified in the *DPI profile index* column to the data packets. The prerequisite is that in the *Source IP address*, *Destination IP address* and *Destination port* columns a value other than `any` is specified.
  The value is only available in the software level SU/UN. Refer to the *Software level* characteristic value in the product code.
- *enforce-dnp3*
  The device applies the rule specified in the *DPI profile index* column to the data packets. The prerequisite is that in the *Source IP address*, *Destination IP address* and *Destination port* columns a value other than `any` is specified.
  The value is only available in the software level SU/UN. Refer to the *Software level* characteristic value in the product code.
- *enforce-ethernetip*
  The device applies the rule specified in the *DPI profile index* column to the data packets. The prerequisite is that in the *Source IP address*, *Destination IP address* and *Destination port* columns a value other than `any` is specified.
  The value is only available in the software level IN/UN. Refer to the *Software level* characteristic value in the product code.
- *enforce-amp*
  The device applies the rule specified in the *DPI profile index* column to the data packets. The prerequisite is that in the *Source IP address*, *Destination IP address* and *Destination port* columns a value other than `any` is specified.
  The value is only available in the software level IN/UN. Refer to the *Software level* characteristic value in the product code.
- *enforce-s7*
  The device applies the rule specified in the *DPI profile index* column to the data packets.
  Prerequisites:
  - In the *Ethertype* column, the value *ipv4* is specified.
  - In the *Source IP address* column, a value other than `any` is specified.
  - In the *Destination IP address* column, a value other than `any` is specified.
  - In the *Protocol* column, the value *tcp* is specified.
  - In the *Destination port* column, a value other than `any` is specified.

  The value is only available in the software level UN. Refer to the *Software level* characteristic value in the product code.

Source MAC address

Specifies the asset name or the source address of the MAC data packets to which the device applies the rule. Select an item from the drop-down list or specify the source address. You specify the asset name in the *Network Security > Asset* dialog.

Possible values:

- `any` (default setting)
  The device applies the rule to MAC data packets with any asset name or source address.
- Valid MAC address
  The device applies the rule to MAC data packets with the specified source address.
  Example: `00:11:22:33:44:55`
- Name of the asset
  Alphanumeric ASCII character string with 1..32 characters

Destination MAC address

Specifies the asset name or the destination address of the MAC data packets to which the device applies the rule. Select an item from the drop-down list or specify the destination address. You specify the asset name in the *Network Security > Asset* dialog.

Possible values:

- `any` (default setting)
  The device applies the rule to MAC data packets with any asset name or destination address.
- Valid MAC address
  The device applies the rule to MAC data packets with the specified destination address.
  Example: `00:11:22:33:44:55`
- Name of the asset
  Alphanumeric ASCII character string with 1..32 characters

Ethertype

Specifies the *Ethertype* keyword of the MAC data packets to which the device applies the rule.

Possible values:

- *custom* (default setting)
  The device applies the value specified in the *Ethertype custom value* column.
- *appletalk*
- *arp*
- *ibmsna*
- *ipv4*
- *ipv6*
- *ipxold*
- *mplsmcast*
- *mplsucast*
- *netbios*
- *novell*
- *pppoedisc*
- *rarp*
- *pppoesess*
- *ipxnew*
- *profinet*
- *powerlink*
- *ethercat*
- *vlan8021q*

Ethertype custom value

Specifies the *Ethertype* value of the MAC data packets to which the device applies the rule. The prerequisite is that in the *Ethertype* column the value *custom* is specified.

Possible values:

- `0` (default setting)
  The device applies the rule to every MAC data packet without evaluating the *Ethertype* value.

- `1..5ff`
  The device applies the rule to Logical Link Control (LLC) data packets whose length field contains the specified the value. These values are available only for port-based rules.
- `600..ffff`
  The device applies the rule only to MAC data packets that contain the *Ethertype* value specified here.

VLAN ID

Specifies the VLAN ID of the data packets to which the device applies the rule. The prerequisite is that in the *Ethertype* column the value *vlan8021q* is specified.

Possible values:

- `any` (default setting)
  The device applies the rule to every data packet without evaluating the VLAN ID.
- `1..4042`
  The device applies the rule only to data packets containing the specified VLAN ID.

Source IP address

Specifies the asset name or the source address of the IP data packets to which the device applies the rule. Select an item from the drop-down list or specify the source address. You specify the asset name in the *Network Security > Asset* dialog.

Prerequisites:

- In the *Ethertype* column, the value *ipv4* is specified.
- In the *Action* column, a value other than *enforce-goose* is specified.

Possible values:

- `any` (default setting)
  The device applies the rule to IP data packets with any asset name or source address.
- Valid IPv4 address and netmask in CIDR notation
  The device applies the rule to data packets with the specified source address in the specified subnet.
  Example: `192.168.112.0/25`
- An exclamation mark (`!`) preceding the IP address reverses the expression into its opposite. The device applies the rule to data packets with any source address or subnet excluding the specified source address or the subnet.
  Example: `!1.1.1.1` or `!192.168.112.0/25`
- Name of the asset
  Alphanumeric ASCII character string with 1..32 characters

Destination IP address

Specifies the asset name or the destination address of the IP data packets to which the device applies the rule. Select an item from the drop-down list or specify the destination address. You specify the asset name in the *Network Security > Asset* dialog.

Prerequisites:

- In the *Ethertype* column, the value *ipv4* is specified.
- In the *Action* column, a value other than *enforce-goose* is specified.

Possible values:

- `any` (default setting)
  The device applies the rule to IP data packets with any asset name or destination address.

- Valid IPv4 address and netmask in CIDR notation
  The device applies the rule to data packets with the specified destination address in the specified subnet.
  Example: `192.168.112.0/25`
- An exclamation mark (`!`) preceding the IP address reverses the expression into its opposite. The device applies the rule to data packets with any destination address or subnet excluding the specified destination address or the subnet.
  Example: `!1.1.1.1` or `!192.168.112.0/25`
- Name of the asset
  Alphanumeric ASCII character string with 1..32 characters

Protocol

Specifies the IP protocol or Layer 4 protocol type of the data packets to which the device applies the rule. The device applies the rule only to data packets that contain the specified value in the *Protocol* field.

Possible values:

- *any* (default setting)
  The device applies the rule to every data packet without evaluating the protocol.
- *icmp*
  Internet Control Message Protocol (RFC 792)
- *igmp*
  Internet Group Management Protocol
- *ipip*
  IP in IP tunneling (RFC 2003)
- *tcp*
  Transmission Control Protocol (RFC 793)
- *udp*
  User Datagram Protocol (RFC 768)
- *esp*
  IPsec Encapsulated Security Payload (RFC 2406)
- *ah*
  IPsec Authentication Header (RFC 2402)
- *icmpv6*
  Internet Control Message Protocol for IPv6
- `<user-defined protocols>`
  The device also processes user-defined protocols. You specify user-defined protocols in the *Network Security > Protocol* dialog.

TOS priority

Specifies the *IP Precedence (ToS)* value in the header of the IP data packets to which the device applies the rule.

Possible values:

- `0` (default setting)
  The device applies the rule to every IP data packet without evaluating the *ToS* value.
- `1..255`
  The device applies the rule only to IP data packets containing the specified *ToS* value.

DPI profile index

Specifies which rule the device applies to the data packets.

The prerequisite is that in the *Action* column one of the following values is specified:

- *enforce-modbus*
- *enforce-opc*
- *enforce-dnp3*
- *enforce-iec104*
- *enforce-amp*
- *enforce-ethernetip*
- *enforce-s7*

Possible values:

▶ `0` (default setting)
The device does not apply any rule to the data packets.

▶ `1..32`
The device applies the rule with the specified Index number to the data packets.

Source port

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

Prerequisites:

- In the *Protocol* column, the value *tcp* or *udp* is specified.
- In the *Action* column, a value other than *enforce-goose* is specified.

Possible values:

▶ `any` (default setting)
The device applies the rule to every data packet without evaluating the source port.

▶ `1..65535 (2¹⁶-1)`
The device applies the rule only to data packets containing the specified source port.
The field lets you specify the following options:
– You specify a port with a single numerical value, for example `21`.
– You specify multiple individual ports with numerical values separated by commas, for example `21,80,110`.
– You specify a port range with numerical values connected by dashes, for example `2000-3000`.
– You can also combine ports and port ranges, for example `21,2000-3000,65535`.
The column lets you specify up to 15 numerical values. When you enter `21,2000-3000,65535`, for example, you use 4 of 15 numerical values.

Destination port

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

Prerequisites:

- In the *Protocol* column, the value *tcp* or *udp* is specified.
- In the *Action* column, a value other than *enforce-goose* is specified.

Possible values:

- `any` (default setting)
  The device applies the rule to every data packet without evaluating the destination port.
- `1..65535 (2¹⁶-1)`
  The device applies the rule only to data packets containing the specified destination port.
  The field lets you specify the following options:
  - You specify a port with a single numerical value, for example `21`.
  - You specify multiple individual ports with numerical values separated by commas, for example `21,80,110`.
  - You specify a port range with numerical values connected by dashes, for example `2000-3000`.
  - You can also combine ports and port ranges, for example `21,2000-3000,65535`.
    The column lets you specify up to 15 numerical values. When you enter `21,2000-3000,65535`, for example, you use 4 of 15 numerical values.

Rate limit

Specifies the data rate limit for the non-routing port or VLAN. The limit applies to the sum of the sizes of data packets sent and received.

Possible values:

- `0` (default setting)
  No limitation of the data transfer rate.
- `1..10000000 (10⁷)`
  If the data transfer rate on the port exceeds the value specified, then the device discards superfluous IP data packets. The prerequisite is that in the *Burst size* column a value >`0` is specified. You specify the measurement unit of the limit in the *Unit* column.

Burst size

Specifies the limit in KByte for the data volume during temporary bursts.

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 superfluous MAC data packets.

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

Unit

Specifies the measurement unit for the data transfer rate specified in the *Rate limit* column.

Possible values:

- *pps* (default setting)
  Data packets per second
- *kbps*
  kBytes per second

Trap

Activates/deactivates the sending of SNMP traps when the device applies a *Packet Filter* rule to a data packet.

Possible values:

- `marked`
  The sending of SNMP traps is active. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
  If the device applies the *Packet Filter* rule to a data packet, then the device sends an SNMP trap.
- `unmarked` (default setting)
  The sending of SNMP traps is inactive.

Log

Activates/deactivates the logging in the log file.

Possible values:

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

Active

Activates/deactivates the rule.

To apply the settings to the data stream, perform the following steps:

- ☐ Click the ✓ button to save the current settings.
- ☐ Open the *Network Security > Packet Filter > Transparent Firewall Mode > Global* dialog, or the *Network Security > Packet Filter > Transparent Firewall Mode > Assignment* dialog.
- ☐ Click the ⬆ button.

Possible values:

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

4.5.2.3 Packet Filter Assignment

[Network Security > Packet Filter > Transparent Firewall Mode > Assignment]

This dialog lets you assign one or more *Packet Filter* rules to the non-routing ports or VLANs.

Information

Assignments

Displays how many rules are active for the non-routing ports or VLANs.

Uncommitted changes present

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

Possible values:

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

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the *Create* window to assign a rule to a non-routing port or VLAN.

- From the *Port/VLAN* drop-down list, you select the non-routing port or the VLAN to which the device applies the rule. If you select the `VLAN:1` item from the drop-down list, the device applies the rule to all the ports associated with VLAN 1.
- From the *Direction* drop-down list, you select if the device applies the rule to received or sent data packets.
- From the *Index* drop-down list, you select the rule that you assign to the non-routing port or VLAN.

Remove

Removes the selected table row.

Commit changes

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

Note:
While the device is activating the saved rules, you cannot establish any new communication connections.

Description

Displays the name of the rule. You specify the description in the *Network Security > Packet Filter > Transparent Firewall Mode > Rule* dialog.

Index

Displays the sequential number of the *Packet Filter* rule. You specify the index number when you add a table row.

Type

Displays where the device applies the rule to.

Possible values:

- *Port*
  The device already applies the *Packet Filter* rule to a non-routing port.
  You find the corresponding port number in the *Port/VLAN* column.
- *VLAN*
  The device already applies the *Packet Filter* rule to a non-routing VLAN interface.
  You find the corresponding VLAN ID in the *Port/VLAN* column.

Port/VLAN

Displays the number of the non-routing port or the VLAN to which the device applies the rule. To specify the port number or VLAN ID, click the button.

Possible values:

- `<Port number>`
  Number of the non-routing port.
- `VLAN: <VLAN ID>`
  ID of the VLAN.

Direction

Displays if the device applies the *Packet Filter* rule to received or sent data packets.

Possible values:

- *ingress*
  The device applies the *Packet Filter* rule to data packets received on the non-routing port or VLAN interface.
- *egress*
  The device applies the *Packet Filter* rule to data packets sent on the non-routing port or VLAN interface.

Priority

Specifies the priority of the *Packet Filter* rule.

Using the priority, you specify the sequence in which the device applies the rules to the data stream. The device applies the rules in ascending order which starts with priority `0`.

Possible values:

- `0..4294967295 (2³²-1` (default setting: `1`)

Active

Activates/deactivates the rule.

To apply the settings to the data stream, perform the following steps:

- ☐ Click the ✓ button to save the current settings.
- ☐ Open the *Network Security > Packet Filter > Transparent Firewall Mode > Global* dialog, or the *Network Security > Packet Filter > Transparent Firewall Mode > Assignment* dialog.
- ☐ Click the ⬆ button.

Possible values:

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

4.5.2.4 Packet Filter Overview

[Network Security > Packet Filter > Transparent Firewall Mode > Overview]

This dialog gives you an overview of the specified *Packet Filter* rules.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Description

Displays the name of the rule. You specify the description in the *Network Security* > *Packet Filter* > Transparent Firewall Mode > *Rule* dialog.

Index

Displays the sequential number of the *Packet Filter* rule.

Direction

Displays if the device applies the *Packet Filter* rule to received or sent data packets.

Possible values:

- *ingress*
  The device applies the *Packet Filter* rule to data packets received on the non-routing port or VLAN interface.
- *egress*
  The device applies the *Packet Filter* rule to data packets sent on the non-routing port or VLAN interface.

Priority

Displays the priority of the *Packet Filter* rule. The device applies the rules in ascending order which starts with priority `0`.

Type

Displays where the device applies the rule to.

Port/VLAN

Displays the number of the non-routing port or the VLAN to which the device applies the rule.

Source MAC address

Displays the asset name or source address of the MAC data packets to which the device applies the rule.

Destination MAC address

Displays the asset name or destination address of the MAC data packets to which the device applies the rule.

Ethertype

Displays the *Ethertype* keyword of the MAC data packets to which the device applies the rule.

Ethertype custom value

Displays the *Ethertype* value of the MAC data packets to which the device applies the rule. The prerequisite is that in the *Ethertype* column the value `custom` is specified.

Source IP address

Displays the asset name or source address of the IP data packets to which the device applies the rule.

Destination IP address

Displays the asset name or destination address of the IP data packets to which the device applies the rule.

Protocol

Displays the IP protocol to which the *Packet Filter* rule is restricted. The device applies the *Packet Filter* rule only to data packets of the specified IP protocol.

TOS priority

Displays the *IP Precedence (ToS)* value in the header of the IP data packets to which the device applies the rule.

Action

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

DPI profile index

Displays the profile index of the *DPI enforcer* function. You specify the profile index in the *Network Security > Packet Filter > Transparent Firewall Mode > Rule* dialog.

Source port

Displays the source TCP or UDP port of the data packets to which the device applies the rule.

Destination port

Displays the destination TCP or UDP port of the data packets to which the device applies the rule.

Rate limit

Displays the data rate limit for the non-routing port or VLAN. The limit applies to the sum of the sizes of data packets sent and received.

Burst size

Displays the limit in KByte for the data volume during temporary bursts.

Unit

Displays the measurement unit for the data transfer rate specified in the *Rate limit* column.

Trap

Displays if the device sends an SNMP trap when the device applies the rule to a data packet.

Log

Displays if the device places an entry in the log file when the device applies the rule to a data packet.

Active

Displays if the rule is active or inactive.

4.6 Deep Packet Inspection

[Network Security > DPI]

The *DPI* function lets you monitor and filter data packets. The function supports you in protecting the network from undesirable content, such as spam or viruses.

The *DPI* function inspects data packets for undesirable characteristics and protocol violations. The protocol inspects the header and the payload of the data packets.

This dialog lets you specify the *DPI* settings. The device blocks the data packets that violate the specified profiles. If an error is detected, then the device terminates the data connection upon user request.

The menu contains the following dialogs:

- Deep Packet Inspection - Modbus Enforcer
- Deep Packet Inspection - OPC Enforcer
- Deep Packet Inspection - DNP3 Enforcer
- Deep Packet Inspection - IEC104 Enforcer
- Deep Packet Inspection - AMP Enforcer
- Deep Packet Inspection - ENIP Enforcer
- Deep Packet Inspection - S7 Enforcer

4.6.1 Deep Packet Inspection - Modbus Enforcer

[Network Security > DPI > Modbus Enforcer]

This dialog lets you specify the *Modbus Enforcer* settings and define the *Modbus TCP* specific profiles.

The profiles specify *function codes* and register or coil addresses. The *function code* in the protocol Modbus TCP specifies the purpose of the data transfer. The device blocks the data packets that violate the specified profiles. If an error is detected, then the device terminates the data connection upon user request. The predefined *function code* lists and the *function code* generator support you when specifying the *function codes*.

When the *Modbus Enforcer* profile is active (checkbox in the *Profile active* column is marked), the device applies the profiles to the data stream.

- The device permits data packets containing only the *function codes* specified in the *Function code* column.
- The device rejects the data packets containing any other *function codes* that are not specified in the *Function code* column.

Information

Uncommitted changes present

Displays if the *Modbus Enforcer* profiles applied to the data stream differ from the profiles saved in the device.

Possible values:

▶ `marked`
At least one of the active *Modbus Enforcer* profiles saved in the device contains modified settings.

To apply the pending profiles to the data stream, click the ⬆ button.

Note:
If there are uncommitted changes on the device, the device commits them during the next system startup.

▶ `unmarked`
The *Modbus Enforcer* profiles applied to the data stream match the profiles saved in the device.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons


Add

Opens the *Create* window to add a table row.

- In the *Index* field, you specify the number of the profile.
  Possible values:
  ▶ `1..32`

When you click the *Ok* button, the device adds the table row. The device assigns the number specified in the *Index* field to the table row.


Remove

Removes the selected table row.

If you mark the *Profile active* checkbox for the profile, then the device stops you from removing the profile.


Copy

Opens the *Copy* window to copy an existing table row. The prerequisite is that the table row for the profile to be copied is selected.

- In the *Index* field, you specify a new number which identifies the copied profile.
  Possible values:
  ▶ `1..32`

When you click the *Ok* button, the device adds the table row. The device assigns the number specified in the *Index* field to the table row.


Commit changes

The device applies the specified profiles to the data stream.

If you changed the value in the *Function type* field, then the device applies the change to the *Function code* list and refreshes the display in the *Function code* column.

Index

Displays the sequential number of the profile to which the table row relates. You specify the index number when you add a table row.

Description

Specifies a name for the profile.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters
  (default setting: `modbus`)

Function type

Specifies the function type for the *Modbus Enforcer* profile. After clicking the ✓ button, the device assigns the corresponding *type IDs*.

Possible values:

- `readOnly` (default setting)
  Assigns the *function codes* for the *read* function of the *Modbus TCP* protocol.
  `1,2,3,4,7,11,12,17,20,24`
- `readWrite`
  Assigns the *function codes* for the *read/write* functions of the *Modbus TCP* protocol.
  `1,2,3,4,5,6,7,11,12,15,16,17,20,21,22,23,24`
- `programming`
  Assigns the *function codes* for the *programming* functions of the *Modbus TCP* protocol.
  `1,2,3,4,5,6,7,11,12,15,16,17,20,21,22,23,24,40,42,90, 125,126`
- `all`
  Assigns the *function codes* for every function of the *Modbus TCP* protocol.
  `1,2,..,254,255`
- `advanced`
  Lets you specify user-defined values in the *Function code* column.

Note:
If you have specified the value `advanced`, then for your own security the device does not allow any subsequent changes to be made to the value. The device helps prevent a change to `readOnly`, `readWrite` or `programming`. This helps avoid overwriting the manually specified values in the *Function code* column. To specify a table row with the value `readOnly`, `readWrite` or `programming`, add a table row.

Function code

Displays the *function codes* for the *Modbus Enforcer* profile. The device permits data packets with the specified properties.

The column displays different values depending on the value specified in the *Function type* column:

- If in the *Function type* column the value `readOnly`, `readWrite` or `programming` is specified, then the device automatically enters the related *function codes*.
- If in the *Function type* column the value `advanced` is specified, then the device lets you specify user-defined *function codes*. To do this, perform the following steps:
  - ☐ For the relevant profile, click into the *Function code* column.
    The dialog displays the *Function code* window. See “[Function code]” on page 156.
  - ☐ From the *Function code* drop-down list, select the desired *function code* item.
  - ☐ Click the *Add* button.
  - ☐ To add multiple *function codes*, repeat the previously described steps.
  - ☐ Click the *Ok* button.

Possible values:

- `<FC>|<AR>,<FC>|<AR>,…`
  The device lets you specify multiple *function codes* and for some *function codes* an additional address range. You find the meaning of the numbers in section “Meaning of the Function code values” on page 157.
  - *Function code* `<FC>` = `1..255`
    You separate each *function code* with a comma, for example `1,2,3`.
    For some *function codes* the device lets you specify an additional address range. You separate the address range from the *function code* with a vertical bar (pipe), for example `1|128-255`.
  - *Address range* `<AR>` = `0..65535` or `0..65535|0..65535` (for *function codes* that require read and write address ranges)
    You join the start value and end value of the range with a hyphen, for example `128-255`.
    The device also lets you specify a single value as an address range. For example, specifying the address range `5-5` is equivalent to the single address `5`.

Unit identifier

Specifies the *Modbus TCP* identification unit for the *Modbus Enforcer* profile.

Possible values:

- `none` (default setting)
  The device permits data packets without an identification unit.
- `0..255`
  The device permits data packets with the specified identification unit.
  The field lets you specify the following options:
  - A single *Modbus TCP* identification unit with a single numerical value, for example `1`.
  - Multiple *Modbus TCP* identification units with numerical values separated by a comma, for example `1,2,3`.

Sanity check

Activates/deactivates the plausibility check for the data packets.

Possible values:

- `marked` (default setting)
  The plausibility check is active.
  The device checks the plausibility of the data packets regarding format and specification.
- `unmarked`
  The plausibility check is inactive.

Exception

Activates/deactivates the sending of an *exception* response in case of a protocol violation or if the plausibility check identifies errors.

Possible values:

- `marked`
  The sending of an *exception* response is active.
  If the device identifies a protocol violation or a plausibility check error, then the device sends an *exception* response to the end points and terminates the *Modbus TCP* connection.
- `unmarked` (default setting)
  The sending of an *exception* response is inactive. The *Modbus TCP* connection remains established.

TCP reset

Activates/deactivates the resetting of the TCP connection in case of a protocol violation or if the plausibility check detects an error.

Possible values:

- `marked` (default setting)
  The resetting of the TCP connection is active.
  If the device identifies a protocol violation or detects a plausibility check error, then the device terminates the TCP connection.
- `unmarked`
  The resetting of the TCP connection is inactive. The TCP connection remains established.

Profile active

Activates/deactivates the profile.

Possible values:

- `marked`
  The profile is active.
  The device applies the *Modbus Enforcer* profiles specified in this table row to the data stream.
- `unmarked` (default setting)
  The profile is inactive.

[Function code]

Function code

Specifies the *function codes* for the relevant *Modbus Enforcer* profile.

You find the meaning of the numbers in section “Meaning of the Function code values” on page 157.

Read address range

Specifies the read address range for certain *function codes*. See section “Meaning of the Function code values” on page 157.

Possible values:

- `0..65535 (2¹⁶-1)`

Write address range

Specifies the write address range for certain *function codes*. See section “Meaning of the Function code values” on page 157.

Possible values:

- `0..65535 (2¹⁶-1)`

Add

Adds the items you selected from the drop-down list to the *Function code* field.

Deletes the item from the *Function code* field.

Meaning of the Function code values

#	Meaning	Address range (read)	Address range (write)
1	Read Coils	<0..65535>	-
2	Read Discrete Inputs	<0..65535>	-
3	Read Holding Registers	<0..65535>	-
4	Read Input Registers	<0..65535>	-
5	Write Single Coil	-	<0..65535>
6	Write Single Register	-	<0..65535>
7	Read Exception Status	-	-
8	Diagnostic	-	-
11	Get Comm Event Counter	-	-
12	Get Comm Event Log	-	-
13	Program (584/984)	-	-
14	Poll (584/984)	-	-
15	Write Multiple Coils	-	<0..65535>
16	Write Multiple Registers	-	<0..65535>
17	Report Slave ID	-	-
20	Read File Record	-	-
21	Write File Record	-	-
22	Mask Write Register	-	<0..65535>
23	Read/Write Multiple Registers	<0..65535>	<0..65535>
24	Read FIFO Queue	<0..65535>	-
40	Program (Concept)	-	-
42	Concept Symbol Table	-	-
43	Encapsulated Interface Transport	-	-
48	Advantech Co. Ltd. - Management Functions	-	-
66	Scan Data Inc. - Expanded Read Holding Registers	-	-
67	Scan Data Inc. - Expanded Write Holding Registers	-	-
90	Unity Programming/OFS	-	-
100	Scattered Register Read	-	-
125	Schneider Electric - Firmware	-	-

4.6.2 Deep Packet Inspection - OPC Enforcer

[Network Security > DPI > OPC Enforcer]

This dialog lets you specify the *OPC Enforcer* (*OLE for Process Control Enforcer*) settings and define the *OPC Enforcer* specific profiles.

The *OPC* is an integration protocol for industrial environments. The *OPC Enforcer* is a function that supports the network security. The device blocks the data packets that violate the specified profiles. Upon user request, the device verifies the data packets for their plausibility and their fragment characteristics. The device verifies and observes *OPC* data connections and helps protect against invalid or fake data packets. The function dynamically activates TCP ports for each data connection. When requested by an *OPC* server, the device sets up the data connection only between the *OPC* server and the related *OPC* client.

The prerequisite is that *authentication level 5* or lower is set up in your end device to perform the Deep Packet Inspection (DPI). The end device can be a computer or any other equipment capable of sending *OPC* data packets. The *authentication level* defines the type of authentication required for an *OPC* client to connect with an *OPC* server.

The device removes the state information from the packet filter on the following events:
- When applying the profiles saved in the device to the data stream.
- When activating/deactivating the *Routing* function on a router interface.

This includes potential *DCE RPC* information of the *OPC Enforcer*. In the process, the device interrupts open communication connections.

Operation

Uncommitted changes present

Displays if the *OPC Enforcer* profiles applied to the data stream differ from the profiles saved in the device.

Possible values:

▶ `marked`
At least one of the active *OPC Enforcer* profiles saved in the device contains modified settings.

To apply the pending profiles to the data stream, click the ⤒ button.

Note:
If there are uncommitted changes on the device, the device commits them during the next system startup.

▶ `unmarked`
The *OPC Enforcer* profiles applied to the data stream match the profiles saved in the device.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

 Add

Opens the *Create* window to add a table row.

- In the *Index* field, you specify the number of the profile.
  Possible values:
  ▶ `1..32`

When you click the *Ok* button, the device adds the table row. The device assigns the number specified in the *Index* field to the table row.

 Remove

Removes the selected table row.

If you mark the *Profile active* checkbox for the profile, then the device stops you from removing the profile.

 Copy

Opens the *Copy* window to copy an existing table row. The prerequisite is that the table row for the profile to be copied is selected.

- In the *Index* field, you specify the number of the profile.
  Possible values:
  ▶ `1..32`

When you click the *Ok* button, the device adds the table row. The device assigns the number specified in the *Index* field to the table row.

 Commit changes

The device applies the specified profiles to the data stream.

Index

Displays the sequential number of the profile to which the table row relates. You specify the index number when you add a table row.

Description

Specifies a name for the profile.

Possible values:

▶ Alphanumeric ASCII character string with 0..64 characters
(default setting: `opc`)

Sanity check

Activates/deactivates the plausibility check for the data packets.

Possible values:

- `marked` (default setting)
  The plausibility check is active.
  The device checks the plausibility of the data packets regarding format and specification.
  The device blocks the data packets that violate the specified profiles.
- `unmarked`
  The plausibility check is inactive.

Fragment check

Activates/deactivates the fragment check for the data packets.

Possible values:

- `marked` (default setting)
  The fragment check is active.
  The device checks the data packets for fragment characteristics.
- `unmarked`
  The fragment check is inactive.

Timeout at connect

Specifies the time in seconds after which the device removes the dynamic TCP ports, if there is no longer an active *OPC* data connection on the dynamic TCP ports.

Possible values:

- `1..300` (default setting: `5`)
- `0`
  The value `0` deactivates the function. The *OPC* data connection remains set up without a time limit.

Profile active

Activates/deactivates the profile.

Possible values:

- `marked`
  The profile is active.
  The device applies the *OPC Enforcer* profiles specified in this table row to the data stream.
- `unmarked`
  The profile is inactive.

4.6.3 Deep Packet Inspection - DNP3 Enforcer

[Network Security > DPI > DNP3 Enforcer]

This dialog lets you specify the *DNP3 Enforcer* (*Distributed Network Protocol v3 Enforcer*) settings and define the *DNP3 Enforcer* specific profiles.

The *DNP3* protocol is designed to help ensure reliable communication between components in process automation systems. The protocol provides multiplexing, error checking, link control, prioritization, and layer 2 addressing services for user data. The *DNP3 Enforcer* function activates the Deep Packet Inspection (DPI) firewall capabilities for the *DNP3* data stream. The device blocks the data packets that violate the specified profiles. Upon user request, the device verifies the data packets for their plausibility and their fragment characteristics. The device verifies and monitors *DNP3* data connections and helps protect against invalid or falsified data packets.

When the *DNP3 Enforcer* profile is active (checkbox in the *Profile active* column is marked), the device applies the profiles to the data stream.

- The device permits data packets containing only the *function codes* specified in the *Function code list* column.
- The device rejects the data packets containing any other *function codes* that are not specified in the *Function code list* column.

The menu contains the following dialogs:

- DNP3 Profile
- DNP3 Object

4.6.3.1 DNP3 Profile

[Network Security > DPI > DNP3 Enforcer > Profile]

This dialog lets you set up profiles for the *DNP3 Enforcer* function. The profile lets you forward or discard data packets based on the specified values.

Information

Uncommitted changes present

Displays if the *DNP3 Enforcer* profiles applied to the data stream differ from the profiles saved in the device.

Possible values:

- `marked`
  At least one of the active *DNP3 Enforcer* profiles saved in the device contains modified settings.
  To apply the pending profiles to the data stream, click the button.

  Note:
  If there are uncommitted changes on the device, the device commits them during the next system startup.

- `unmarked`
  The *DNP3 Enforcer* profiles applied to the data stream match the profiles saved in the device.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the *Create* window to add a table row.

- In the *Index* field, you specify the number of the profile.
  Possible values:
  - `1..32`

When you click the *Ok* button, the device adds the table row. The device assigns the number specified in the *Index* field to the table row.

Remove

Removes the selected table row.

Copy

Opens the *Copy* window to copy an existing table row. The prerequisite is that the table row for the profile to be copied is selected.

- In the *Index* field, you specify a new number which identifies the copied profile.
  Possible values:
  ▶ `1..32`

When you click the *Ok* button, the device adds the table row. The device assigns the number specified in the *Index* field to the table row.

Commit changes

The device applies the specified profiles to the data stream.

Index

Displays the sequential number of the profile to which the table row relates. You specify the index number when you add a table row.

Description

Specifies a name for the profile.

Possible values:

▶ Alphanumeric ASCII character string with 0..32 characters
(default setting: `dnp3`)

Function code list

Displays the *function codes* for the *DNP3 Enforcer* profile. The device permits data packets with the specified properties.

The device lets you specify multiple *function codes*. To do this, perform the following steps:

☐ For the relevant profile, click into the *Function code list* column.
The dialog displays the *Function code list* window. See “[Function code list]” on page 165.
☐ From the *Function code list* drop-down list, select the desired *function code* item.
☐ Click the *Add* button.
☐ To add multiple *function codes*, repeat the previously described steps.
☐ Click the *Ok* button.

Possible values:

▶ `0..255`
You find the meaning of the numbers in section “Meaning of the Function code list values” on page 165.

Index of Default Object List

Specifies the *index numbers* used in the *default object list*.

Possible values:

▶ `all` (default setting)
The device applies the *DNP3 Enforcer* profile to every data packet regardless of the *index number*.

- `1..317`
  The device applies the *DNP3 Enforcer* profile only to data packets containing the specified *index number*.
  The field lets you specify the following options:
  - A single *index number* with a single numerical value, for example `1`.
  - Multiple *index numbers* with numerical values separated by a comma, for example `1,2,3`.
  - A range with numerical values joined by a dash, for example `7-25`.
  - You can also combine single numerical values and ranges, for example `2,7-25,56`.
- `none`
  The device does not apply the *index number* to the *DNP3 Enforcer* profile.

CRC check

Activates/deactivates the CRC check for the data packets to validate the checksum contained in the *DNP3* data packets.

Possible values:

- `marked` (default setting)
  The CRC check is active.
  The device calculates the checksum and compares it with the checksum field in the *DNP3* data packets.
- `unmarked`
  The CRC check is inactive.

Sanity check

Activates/deactivates the plausibility check for the data packets.

Possible values:

- `marked` (default setting)
  The plausibility check is active.
  The device checks the plausibility of the data packets regarding format and specification. The device blocks the data packets that violate the specified profiles.
- `unmarked`
  The plausibility check is inactive.

Check outstation traffic

Activates/deactivates the checking of the data packets that originate at an *outstation*.

Possible values:

- `marked`
  The checking of data packets from an *outstation* is active.
- `unmarked`
  The checking of data packets from an *outstation* is inactive.

TCP reset

Activates/deactivates the resetting of the TCP connection in case of a protocol violation or if the plausibility check detects an error.

Possible values:

- `marked` (default setting)
  The resetting of the TCP connection is active.
  If the device identifies a protocol violation or detects a plausibility check error, then the device terminates the TCP connection.
- `unmarked`
  The resetting of the TCP connection is inactive. The TCP connection remains established.

Profile active

Activates/deactivates the profile.

Possible values:

- `marked`
  The profile is active.
  The device applies the *DNP3 Enforcer* profiles specified in this table row to the data stream.
- `unmarked`
  The profile is inactive.

[Function code list]

Function code list

Specifies the *function codes* for the relevant *DNP3 Enforcer* profile.

You find the meaning of the numbers in section “Meaning of the Function code list values” on page 165.

Add

Adds the items you selected from the drop-down list to the *Function code list* field.

Deletes the item from the *Function code list* field.

Meaning of the Function code list values

#	Meaning
0	Confirm
1	Read
2	Write
3	Select
4	Operate
5	Direct Operate

#	Meaning
6	Direct Operate-No Response Required
7	Freeze
8	Freeze-No Response Required
9	Freeze Clear
10	Freeze Clear-No Response Required
11	Freeze at Time
12	Freeze at Time-No Response Required
13	Cold Restart
14	Warm Restart
15	Initialize Data
16	Initialize Application
17	Start Application
18	Stop Application
19	Save Configuration
20	Enable Unsolicited Messages
21	Disable Unsolicited Messages
22	Assign Class
23	Delay Measurement
24	Record Current Time
25	Open File
26	Close File
27	Delete File
28	Get File Information
29	Authenticate File
30	Abort File Transfer
31	Active Configuration
32	Authentication Request
33	Authenticate Request-No Acknowledgment
129	Response
130	Unsolicited Response
131	Authentication Response

4.6.3.2 DNP3 Object

[Network Security > DPI > DNP3 Enforcer > Object]

The *DNP3* function uses objects to transmit values and information between devices. The *DNP3* function uses group numbers to categorize the data type and variation numbers to specify how the data within the group is encoded. Each instance of an encoded information element that defines a unique group and variation in the message, is a *DNP3* object.

This window lets you add custom *DNP3* objects and also lets you view the previously added custom *DNP3* objects. To verify that an added *DNP3* object is valid in a particular *request message*/ *response message*, check the following parameters:

- *Type*
- *Group no.*
- *Variation*
- *Function*
- *Qualifier*
- *Length*
- *Function name*

Based on the IEEE 1815-2012 standard, the *DNP3 Enforcer* function permits by default the data stream containing *DNP3* objects which are available in the *default object list*.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

 Add

Opens the *Create* window to add a table row.

- From the *Index* drop-down list, you select the profile *index number*.
- In the *Object index* field, you specify the *index number* of the object.
  Possible values:
  ▶ `1..256`
- From the *Type* drop-down list, you select the type of the message.
  Possible values:
  ▶ *request*
  ▶ *response*
- In the *Group no.* field, you specify a means of classifying the type or the types of data packets in a message. The prerequisite is that in the *Type* field a valid value is specified.
  Possible values:
  ▶ `0..255`
- In the *Variation* field, you specify the *variation number*. The prerequisite is that in the *Group no.* field a valid value is specified.
  Possible values:
  ▶ `0..255`

- In the *Function* field, you specify the *function code*. The *function code* identifies the purpose of the message. The prerequisite is that in the *Variation* field a valid value is specified.
  Possible values:
  - `0..128`
    Request messages from *masters*. Specify a single numerical value, for example `1`.
  - `129..255`
    Response messages from *outstations*. Specify a single numerical value, for example `254`.
- In the *Qualifier* field, you specify the *qualifier code* for a pair of each *Group no.*, *Variation*, and *Function* fields. The *qualifier code* is an 8-bit value that defines the *prefix code* and the *range specifier code* for the object in a *DNP3* message. The prerequisite is that in the *Function* field a valid value is specified.
  Possible values:
  - `0x00..0xff`
  You specify multiple individual *qualifier codes* using hexadecimal values separated by a comma for a set of each *Group no.*, *Variation*, and *Function* fields.

When you click the *Ok* button, the device adds the table row. The device assigns the values specified in the *Index*, *Object index*, *Type*, *Group no.*, *Variation*, *Function* and *Qualifier* fields to this table row.

Remove

Removes the selected table row.

Index

Displays the number of the profile to which the table row relates. You specify the index number when you add a table row.

Object index

Displays the number of the object to which the table row relates. You specify the index number when you add a table row.

Type

Specifies the type of the message.

Possible values:

- *request*
  Creates a *request message* object in the object list.
- *response*
  Creates a *response message* object in the object list.

Group no.

Specifies a means of classifying the type or the types of data packets in a message. The prerequisite is that in the *Type* field a valid value is specified.

Possible values:

- `0..255`
  Each group number shares a common *point type* and *method of data packet creation*. The *point type* defines the machine in an *outstation*.

Variation

Specifies the *variation number*. The prerequisite is that in the *Group no.* field a valid value is specified. The device applies the *DNP3 Enforcer* profile only to data packets containing the specified value.

The *DNP3* function provides the choice of encoding formats for the type of data packets known as *variation number*. Every value in the *Group no.* field has a set of *variation numbers*.

Possible values:

- `0..255`
  The field lets you specify the following options:
  - You specify a single *variation number* with a single numerical value, for example `1`.
  - You specify a range with numerical values connected by a dash, for example `0-55`.

Function

The *function code* identifies the purpose of the message. The prerequisite is that in the *Variation* field a valid value is specified. The device applies the *DNP3 Enforcer* profile only to data packets containing the specified value.

Possible values:

- `0..128`
  Request messages from *masters*. Specify a single numerical value, for example `1`.
- `129..255`
  Response messages from *outstations*. Specify a single numerical value, for example `254`.

Qualifier

Specifies the *qualifier code* for a pair of each *Group no.*, *Variation*, and *Function* fields. The *qualifier code* is an 8-bit value that defines the *prefix code* and the *range specifier code* for the object in a *DNP3* message. The prerequisite is that in the *Function* field a valid value is specified. The device applies the *DNP3 Enforcer* profile only to data packets containing the specified value.

Possible values:

- `0x00..0xff`
  You specify multiple individual *qualifier codes* using hexadecimal values separated by a comma for a set of each *Group no.*, *Variation*, and *Function* fields.

Length

Specifies the optional length for the object. The prerequisite is that in the *Function* field a valid value is specified. The device applies the *DNP3 Enforcer* profile only to data packets containing the specified value.

Possible values:

- `0..255`
  Specify a single numerical value, for example `1`.
- `byte_2`
  The second byte of the object data contains the length of the remaining portion of the data.
- `single_bit_packed`
  If the count of bit values is not a multiple of 8, then the device pads the packed single-bit values up to the next byte boundary.

- `double_bit_packed`
  If the count of double bit values is not a multiple of 4, then the device pads the packed double-bit values up to the next byte boundary.
- `variation`
  Encodes the length of the object.

Function name

Specifies the optional name for the *function code*. The prerequisite is that in the *Function* field a valid value is specified.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters
  For example, the device permits data packets with the following *function names*:
  - `READ`
  - `WRITE`
  - `SELECT`

[Index of Default Object List]

Table 1: Request messages

Index	Group no.	Variation	Function	Function name	Length	Qualifier
1	0	209-239	1	READ	-	0x00
2	0	240	1	READ	-	0x00
3	0	240	2	WRITE	byte_2	0x00
4	0	241-243	1	READ	-	0x00
5	0	245-247	1	READ	-	0x00
6	0	245-247	2	WRITE	byte_2	0x00
7	0	248-250	1	READ	-	0x00
8	0	252	1	READ	-	0x00
9	0	254	1	READ	-	0x00 0x06
10	0	255	1	READ	-	0x00 0x06
11	1	0-2	1	READ	-	0x00 0x01 0x06 0x17 0x28
12	1	0	22	ASSIGN CLASS	-	0x00 0x01 0x06 0x17 0x28
13	2	0-3	1	READ	-	0x06 0x07 0x08

Table 1: Request messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
14	3	0-2	1	READ	-	0x00 0x01 0x06 0x17 0x28
15	3	0	22	ASSIGN CLASS	-	0x00 0x01 0x06 0x17 0x28
16	4	0-3	1	READ	-	0x06 0x07 0x08
17	10	0	1	READ	-	0x00 0x01 0x06 0x17 0x28
18	10	0	22	ASSIGN CLASS	-	0x00 0x01 0x06 0x17 0x28
19	10	1	2	WRITE	single_bit_packed	0x00 0x01
20	10	2	1	READ	-	0x00 0x01 0x06 0x17 0x28
21	11	0-2	1	READ	-	0x06 0x07 0x08
22	12	0	22	ASSIGN_CLASS	-	0x00 0x01 0x06 0x17 0x28
23	12	1	3	SELECT	11	0x00 0x01 0x17 0x28
24	12	1	4	OPERATE	11	0x00 0x01 0x17 0x28
25	12	1	5	DIRECT_OPERATE	11	0x00 0x01 0x17 0x28

Table 1: Request messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
26	12	1	6	DIRECT_OPERATE_NR	11	0x00 0x01 0x17 0x28
27	12	2	3	SELECT	11	0x07 0x08
28	12	2	4	OPERATE	11	0x07 0x08
29	12	2	5	DIRECT_OPERATE	11	0x07 0x08
30	12	2	6	DIRECT_OPERATE_NR	11	0x07 0x08
31	12	3	3	SELECT	single_bit_packed	0x00 0x01
32	12	3	4	OPERATE	single_bit_packed	0x00 0x01
33	12	3	5	DIRECT_OPERATE	single_bit_packed	0x00 0x01
34	12	3	6	DIRECT_OPERATE_NR	single_bit_packed	0x00 0x01
35	13	0-2	1	READ	-	0x06 0x07 0x08
36	20	0-2	1	READ	-	0x00 0x01 0x06 0x17 0x28
37	20	5-6	1	READ	-	0x00 0x01 0x06 0x17 0x28
38	20	0	7	IMMEDIATE_FREEZE	-	0x00 0x01 0x06 0x17 0x28
39	20	0	8	IMMEDIATE_FREEZE_NR	-	0x00 0x01 0x06 0x17 0x28
40	20	0	9	FREEZE_CLEAR	-	0x00 0x01 0x06 0x17 0x28

Table 1: Request messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
41	20	0	10	FREEZE_CLEAR_NR	-	0x00 0x01 0x06 0x17 0x28
42	20	0	11	FREEZE_AT_TIME	-	0x00 0x01 0x06 0x17 0x28
43	20	0	12	FREEZE_AT_TIME_NR	-	0x00 0x01 0x06 0x17 0x28
44	20	0	22	ASSIGN_CLASS	-	0x00 0x01 0x06 0x17 0x28
45	21	0-2	1	READ	-	0x00 0x01 0x06 0x17 0x28
46	21	5-6	1	READ	-	0x00 0x01 0x06 0x17 0x28
47	21	9-10	1	READ	-	0x00 0x01 0x06 0x17 0x28
48	21	0	22	ASSIGN_CLASS	-	0x00 0x01 0x06 0x17 0x28
49	22	0-2	1	READ	-	0x06 0x07 0x08
50	22	5-6	1	READ	-	0x06 0x07 0x08
51	23	0-2	1	READ	-	0x06 0x07 0x08

Table 1: Request messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
52	23	5-6	1	READ	-	0x06 0x07 0x08
53	30	0-6	1	READ	-	0x00 0x01 0x06 0x17 0x28
54	30	0	7	IMMEDIATE_FREEZE	-	0x00 0x01 0x06 0x17 0x28
55	30	0	8	IMMEDIATE_FREEZE_NR	-	0x00 0x01 0x06 0x17 0x28
56	30	0	11	FREEZE_AT_TIME	-	0x00 0x01 0x06 0x17 0x28
57	30	0	12	FREEZE_AT_TIME_NR	-	0x00 0x01 0x06 0x17 0x28
58	30	0	22	ASSIGN_CLASS	-	0x00 0x01 0x06 0x17 0x28
59	31	0-8	1	READ	-	0x00 0x01 0x06 0x17 0x28
60	31	0	22	ASSIGN_CLASS	-	0x00 0x01 0x06 0x17 0x28
61	32	0-8	1	READ	-	0x06 0x07 0x08
62	33	0-8	1	READ	-	0x06 0x07 0x08

Table 1: Request messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
63	34	0-3	1	READ	-	0x00 0x01 0x06
64	34	1	2	WRITE	2	0x00 0x01 0x17 0x28
65	34	2	2	WRITE	4	0x00 0x01 0x17 0x28
66	34	3	2	WRITE	4	0x00 0x01 0x17 0x28
67	40	0	1	READ	-	0x00 0x01 0x06
68	40	0	22	ASSIGN_CLASS	-	0x00 0x01 0x06 0x17 0x28
69	40	1-4	1	READ	-	0x00 0x01 0x06 0x17 0x28
70	41	0	22	ASSIGN_CLASS	-	0x00 0x01 0x06 0x17 0x28
71	41	1	3	SELECT	5	0x00 0x01 0x17 0x28
72	41	2	3	SELECT	3	0x00 0x01 0x17 0x28
73	41	3	3	SELECT	5	0x00 0x01 0x17 0x28
74	41	1	4	OPERATE	5	0x00 0x01 0x17 0x28

Table 1: Request messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
75	41	2	4	OPERATE	3	0x00 0x01 0x17 0x28
76	41	3	4	OPERATE	5	0x00 0x01 0x17 0x28
77	41	1	5	DIRECT_OPERATE	5	0x00 0x01 0x17 0x28
78	41	2	5	DIRECT_OPERATE	3	0x00 0x01 0x17 0x28
79	41	3	5	DIRECT_OPERATE	5	0x00 0x01 0x17 0x28
80	41	1	6	DIRECT_OPERATE_NR	5	0x00 0x01 0x17 0x28
81	41	2	6	DIRECT_OPERATE_NR	3	0x00 0x01 0x17 0x28
82	41	3	6	DIRECT_OPERATE_NR	5	0x00 0x01 0x17 0x28
83	42	0-8	1	READ	-	0x06 0x07 0x08
84	43	0-8	1	READ	-	0x06 0x07 0x08
85	50	1	1	READ	-	0x07
86	50	1	2	WRITE	6	0x07
87	50	2	11	FREEZE_AT_TIME	10	0x07
88	50	2	12	FREEZE_AT_TIME_NR	10	0x07
89	50	3	2	WRITE	10	0x07
90	50	4	1	READ	-	0x00 0x01 0x06 0x17 0x28

Table 1: Request messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
91	50	4	2	WRITE	11	0x00 0x01 0x17 0x28
92	60	1	1	READ	-	0x06
93	60	2-4	1	READ	-	0x06 0x07 0x08
94	60	1-4	22	ASSIGN_CLASS	-	0x06
95	60	2-4	20	ENABLE_UNSOLICITED	-	0x06
96	60	2-4	21	DISABLE_UNSOLICITED	-	0x06
97	70	2	29	FILE_AUTHENTICATE	QC_5B_count_1	0x5B
98	70	3	25	OPEN_FILE	QC_5B_count_1	0x5B
99	70	3	27	DELETE_FILE	QC_5B_count_1	0x5B
100	70	4	26	CLOSE_FILE	QC_5B_count_1	0x5B
101	70	4	30	FILE_ABORT	QC_5B_count_1	0x5B
102	70	5-6	1	READ	QC_5B_count_1	0x5B
103	70	5	2	WRITE	QC_5B_count_1	0x5B
104	70	7	28	GET_FILE_INFORMATION	QC_5B_count_1	0x5B
105	70	8	31	ACTIVATE_CONFIGURATION	QC_5B_count_1	0x5B
106	80	1	1	READ	-	0x00 0x01
107	80	1	2	WRITE	single_bit_packed	0x00 0x01
108	81	1	1	READ	-	0x00 0x01
109	82	1	1	READ	-	0x00 0x01
110	83	1	1	READ	-	0x00 0x01
111	85	0	1	READ	-	0x06
112	85	1	1	READ	-	0x00 0x01 0x06 0x17 0x28
113	85	1	2	WRITE	QC_5B	0x5B
114	86	0	22	ASSIGN_CLASS	-	0x00 0x01 0x06 0x17 0x28
115	86	1-3	1	READ	-	0x00 0x01 0x06 0x17 0x28

Table 1: Request messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
116	86	1	2	WRITE	QC_5B	0x5B
117	86	3	2	WRITE	QC_5B	0x5B
118	87	0	1	READ	-	0x06
119	87	1	1	READ	-	0x00 0x01 0x06 0x17 0x28
120	87	1	2	WRITE	QC_5B	0x5B
121	87	1	3	SELECT	QC_5B	0x5B
122	87	1	4	OPERATE	QC_5B	0x5B
123	87	1	5	DIRECT_OPERATE	QC_5B	0x5B
124	87	1	6	DIRECT_OPERATE_NR	QC_5B	0x5B
125	88	0-1	1	READ	-	0x06 0x07 0x08
126	90	1	16	INITIALIZE_APPLICATION	QC_5B	0x5B
127	90	1	17	START_APPLICATION	QC_5B	0x5B
128	90	1	18	STOP_APPLICATION	QC_5B	0x5B
129	101	1-3	1	READ	-	0x00 0x01 0x06 0x17 0x28
130	102	1	1	READ	-	0x00 0x01 0x03 0x04 0x05 0x06 0x17 0x28
131	102	1	2	WRITE	1	0x00 0x01 0x03 0x04 0x05 0x17 0x28
132	110	128	1	READ	-	0x00 0x01 0x03 0x04 0x05 0x06 0x17 0x28

Table 1: Request messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
133	110	128	2	WRITE	variation	0x00 0x01 0x03 0x04 0x05 0x17 0x28
134	110	128	31	ACTIVATE_CONFIGURATION	variation	0x5B
135	111	128	1	READ	-	0x06
136	112	128	2	WRITE	variation	0x00 0x01 0x17 0x28
137	113	0	1	READ	-	0x00 0x01 0x17 0x28
138	113	0	22	ASSIGN_CLASS	-	0x00 0x01 0x06 0x17 0x28

Table 2: Response messages

Index	Group no.	Variation	Function	Function name	Length	Qualifier
139	0	209-239	129	RESPONSE	byte_2	0x00 0x17
140	0	240	129	RESPONSE	byte_2	0x00 0x17
141	0	241-243	129	RESPONSE	byte_2	0x00 0x17
142	0	245-247	129	RESPONSE	byte_2	0x00 0x17
143	0	248-250	129	RESPONSE	byte_2	0x00 0x17
144	0	252	129	RESPONSE	byte_2	0x00 0x17
145	0	255	129	RESPONSE	byte_2	0x00 0x17
146	1	1	129	RESPONSE	single_bit_packed	0x00 0x01 0x17 0x28
147	1	2	129	RESPONSE	1	0x00 0x01 0x17 0x28

Table 2: Response messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
148	2	1	129	RESPONSE	1	0x17 0x28
149	2	2	129	RESPONSE	7	0x17 0x28
150	2	3	129	RESPONSE	3	0x17 0x28
151	2	1	130	UNSOLICITED_RESPONSE	1	0x17 0x28
152	2	2	130	UNSOLICITED_RESPONSE	7	0x17 0x28
153	2	3	130	UNSOLICITED_RESPONSE	3	0x17 0x28
154	3	1	129	RESPONSE	double_bit_packed	0x00 0x01 0x17 0x28
155	3	2	129	RESPONSE	1	0x00 0x01 0x17 0x28
156	4	1	129	RESPONSE	1	0x17 0x28
157	4	2	129	RESPONSE	7	0x17 0x28
158	4	3	129	RESPONSE	3	0x17 0x28
159	4	1	130	UNSOLICITED_RESPONSE	1	0x17 0x28
160	4	2	130	UNSOLICITED_RESPONSE	7	0x17 0x28
161	4	3	130	UNSOLICITED_RESPONSE	3	0x17 0x28
162	10	2	129	RESPONSE	1	0x00 0x01 0x17 0x28
163	11	1	129	RESPONSE	1	0x17 0x28
164	11	2	129	RESPONSE	7	0x17 0x28
165	11	1	130	UNSOLICITED_RESPONSE	1	0x17 0x28
166	11	2	130	UNSOLICITED_RESPONSE	7	0x17 0x28
167	12	1	129	RESPONSE	11	0x00 0x01 0x17 0x28

Table 2: Response messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
168	12	2	129	RESPONSE	11	0x07 0x08
169	12	3	129	RESPONSE	single_bit_packed	0x00 0x01
170	13	1	129	RESPONSE	1	0x17 0x28
171	13	2	129	RESPONSE	7	0x17 0x28
172	13	1	130	UNSOLICITED_RESPONSE	1	0x17 0x28
173	13	2	130	UNSOLICITED_RESPONSE	7	0x17 0x28
174	20	1	129	RESPONSE	5	0x00 0x01 0x17 0x28
175	20	2	129	RESPONSE	3	0x00 0x01 0x17 0x28
176	20	5	129	RESPONSE	4	0x00 0x01 0x17 0x28
177	20	6	129	RESPONSE	2	0x00 0x01 0x17 0x28
178	21	1	129	RESPONSE	5	0x00 0x01 0x17 0x28
179	21	2	129	RESPONSE	3	0x00 0x01 0x17 0x28
180	21	5	129	RESPONSE	4	0x00 0x01 0x17 0x28
181	21	6	129	RESPONSE	2	0x00 0x01 0x17 0x28
182	21	9	129	RESPONSE	4	0x00 0x01 0x17 0x28

Table 2: Response messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
183	21	10	129	RESPONSE	2	0x00 0x01 0x17 0x28
184	22	1	129	RESPONSE	5	0x17 0x28
185	22	2	129	RESPONSE	3	0x17 0x28
186	22	1	130	UNSOLICITED_RESPONSE	5	0x17 0x28
187	22	2	130	UNSOLICITED_RESPONSE	3	0x17 0x28
188	22	5	129	RESPONSE	11	0x17 0x28
189	22	6	129	RESPONSE	9	0x17 0x28
190	22	5	130	UNSOLICITED_RESPONSE	11	0x17 0x28
191	22	6	130	UNSOLICITED_RESPONSE	9	0x17 0x28
192	23	1	129	RESPONSE	5	0x17 0x28
193	23	2	129	RESPONSE	3	0x17 0x28
194	23	1	130	UNSOLICITED_RESPONSE	5	0x17 0x28
195	23	2	130	UNSOLICITED_RESPONSE	3	0x17 0x28
196	23	5	129	RESPONSE	11	0x17 0x28
197	23	6	129	RESPONSE	9	0x17 0x28
198	23	5	130	UNSOLICITED_RESPONSE	11	0x17 0x28
199	23	6	130	UNSOLICITED_RESPONSE	9	0x17 0x28
200	30	1	129	RESPONSE	5	0x00 0x01 0x17 0x28
201	30	2	129	RESPONSE	3	0x00 0x01 0x17 0x28
202	30	3	129	RESPONSE	4	0x00 0x01 0x17 0x28

Table 2: Response messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
203	30	4	129	RESPONSE	2	0x00 0x01 0x17 0x28
204	30	5	129	RESPONSE	5	0x00 0x01 0x17 0x28
205	30	6	129	RESPONSE	9	0x00 0x01 0x17 0x28
206	31	1	129	RESPONSE	5	0x00 0x01 0x17 0x28
207	31	2	129	RESPONSE	3	0x00 0x01 0x17 0x28
208	31	3	129	RESPONSE	11	0x00 0x01 0x17 0x28
209	31	4	129	RESPONSE	9	0x00 0x01 0x17 0x28
210	31	5	129	RESPONSE	4	0x00 0x01 0x17 0x28
211	31	6	129	RESPONSE	2	0x00 0x01 0x17 0x28
212	31	7	129	RESPONSE	5	0x00 0x01 0x17 0x28
213	31	8	129	RESPONSE	9	0x00 0x01 0x17 0x28
214	32	1	129	RESPONSE	5	0x17 0x28
215	32	2	129	RESPONSE	3	0x17 0x28
216	32	3	129	RESPONSE	11	0x17 0x28

Table 2: Response messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
217	32	4	129	RESPONSE	9	0x17 0x28
218	32	5	129	RESPONSE	5	0x17 0x28
219	32	6	129	RESPONSE	9	0x17 0x28
220	32	7	129	RESPONSE	11	0x17 0x28
221	32	8	129	RESPONSE	15	0x17 0x28
222	32	1	130	UNSOLICITED_RESPONSE	5	0x17 0x28
223	32	2	130	UNSOLICITED_RESPONSE	3	0x17 0x28
224	32	3	130	UNSOLICITED_RESPONSE	11	0x17 0x28
225	32	4	130	UNSOLICITED_RESPONSE	9	0x17 0x28
226	32	5	130	UNSOLICITED_RESPONSE	5	0x17 0x28
227	32	6	130	UNSOLICITED_RESPONSE	9	0x17 0x28
228	32	7	130	UNSOLICITED_RESPONSE	11	0x17 0x28
229	32	8	130	UNSOLICITED_RESPONSE	15	0x17 0x28
230	33	1	129	RESPONSE	5	0x17 0x18
231	33	2	129	RESPONSE	3	0x17 0x28
232	33	3	129	RESPONSE	11	0x17 0x28
233	33	4	129	RESPONSE	9	0x17 0x28
234	33	5	129	RESPONSE	5	0x17 0x28
235	33	6	129	RESPONSE	9	0x17 0x28
236	33	7	129	RESPONSE	11	0x17 0x28
237	33	8	129	RESPONSE	15	0x17 0x28
238	33	1	130	UNSOLICITED_RESPONSE	5	0x17 0x28
239	33	2	130	UNSOLICITED_RESPONSE	3	0x17 0x28

Table 2: Response messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
240	33	3	130	UNSOLICITED_RESPONSE	11	0x17 0x28
241	33	4	130	UNSOLICITED_RESPONSE	9	0x17 0x28
242	33	5	130	UNSOLICITED_RESPONSE	5	0x17 0x28
243	33	6	130	UNSOLICITED_RESPONSE	9	0x17 0x28
244	33	7	130	UNSOLICITED_RESPONSE	11	0x17 0x28
245	33	8	130	UNSOLICITED_RESPONSE	15	0x17 0x28
246	34	1	129	RESPONSE	2	0x00 0x01
247	34	2-3	129	RESPONSE	4	0x00 0x01
248	40	1	129	RESPONSE	5	0x00 0x01 0x17 0x28
249	40	2	129	RESPONSE	3	0x00 0x01 0x17 0x28
250	40	3	129	RESPONSE	5	0x00 0x01 0x17 0x28
251	40	4	129	RESPONSE	9	0x00 0x01 0x17 0x28
252	41	1	129	RESPONSE	5	0x00 0x01 0x17 0x28
253	41	2	129	RESPONSE	3	0x00 0x01 0x17 0x28
254	41	3	129	RESPONSE	5	0x00 0x01 0x17 0x28
255	42	1	129	RESPONSE	5	0x17 0x28
256	42	2	129	RESPONSE	3	0x17 0x28

Table 2: Response messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
257	42	3	129	RESPONSE	11	0x17 0x28
258	42	4	129	RESPONSE	9	0x17 0x28
259	42	5	129	RESPONSE	5	0x17 0x28
260	42	6	129	RESPONSE	9	0x17 0x28
261	42	7	129	RESPONSE	11	0x17 0x28
262	42	8	129	RESPONSE	15	0x17 0x28
263	42	1	130	UNSOLICITED_RESPONSE	5	0x17 0x28
264	42	2	130	UNSOLICITED_RESPONSE	3	0x17 0x28
265	42	3	130	UNSOLICITED_RESPONSE	11	0x17 0x28
266	42	4	130	UNSOLICITED_RESPONSE	9	0x17 0x28
267	42	5	130	UNSOLICITED_RESPONSE	5	0x17 0x28
268	42	6	130	UNSOLICITED_RESPONSE	9	0x17 0x28
269	42	7	130	UNSOLICITED_RESPONSE	11	0x17 0x28
270	42	8	130	UNSOLICITED_RESPONSE	15	0x17 0x28
271	43	1	129	RESPONSE	5	0x17 0x28
272	43	2	129	RESPONSE	3	0x17 0x28
273	43	3	129	RESPONSE	11	0x17 0x28
274	43	4	129	RESPONSE	9	0x17 0x28
275	43	5	129	RESPONSE	5	0x17 0x28
276	43	6	129	RESPONSE	9	0x17 0x28
277	43	7	129	RESPONSE	11	0x17 0x28
278	43	8	129	RESPONSE	15	0x17 0x28
279	43	1	130	UNSOLICITED_RESPONSE	5	0x17 0x28

Table 2: Response messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
280	43	2	130	UNSOLICITED_RESPONSE	3	0x17 0x28
281	43	3	130	UNSOLICITED_RESPONSE	11	0x17 0x28
282	43	4	130	UNSOLICITED_RESPONSE	9	0x17 0x28
283	43	5	130	UNSOLICITED_RESPONSE	5	0x17 0x28
284	43	6	130	UNSOLICITED_RESPONSE	9	0x17 0x28
285	43	7	130	UNSOLICITED_RESPONSE	11	0x17 0x28
286	43	8	130	UNSOLICITED_RESPONSE	15	0x17 0x28
287	50	1	129	RESPONSE	6	0x07
288	50	4	129	RESPONSE	11	0x00 0x01 0x17 0x28
289	51	1-2	129	RESPONSE	6	0x07
290	51	1-2	130	UNSOLICITED_RESPONSE	6	0x07
291	52	1-2	129	RESPONSE	2	0x07
292	70	2	129	RESPONSE	QC_5B_count_1	0x5B
293	70	4-7	129	RESPONSE	QC_5B_count_1	0x5B
294	70	4-7	130	UNSOLICITED_RESPONSE	QC_5B_count_1	0x5B
295	80	1	129	RESPONSE	2	0x00 0x01
296	81	1	129	RESPONSE	3	0x07
297	82	1	129	RESPONSE	QC_5B_count_1	0x5B
298	82	1	130	RESPONSE	QC_5B_count_1	0x5B
299	83	1-2	129	RESPONSE	QC_5B	0x5B
300	83	1	130	UNSOLICITED_RESPONSE	QC_5B	0x5B
301	85	1	129	RESPONSE	QC_5B	0x5B
302	86	1	129	RESPONSE	QC_5B	0x5B
303	86	2	129	RESPONSE	1	0x00 0x01 0x17 0x28
304	86	3	129	RESPONSE	QC_5B	0x5B
305	87	1	129	RESPONSE	QC_5B	0x5B
306	88	1	129	RESPONSE	QC_5B	0x5B
307	88	1	130	UNSOLICITED_RESPONSE	QC_5B	0x5B
308	91	1	129	RESPONSE	QC_5B	0x5B

Table 2: Response messages (cont.)

Index	Group no.	Variation	Function	Function name	Length	Qualifier
309	101	1	129	RESPONSE	2	0x00 0x01 0x17 0x28
310	101	2	129	RESPONSE	4	0x00 0x01 0x17 0x28
311	101	3	129	RESPONSE	8	0x00 0x01 0x17 0x28
312	102	1	129	RESPONSE	1	0x00 0x01 0x03 0x04 0x05 0x17 0x28
313	110	128	129	RESPONSE	variation	0x00 0x01 0x03 0x04 0x05 0x17 0x28
314	111	128	129	RESPONSE	variation	0x00 0x01 0x03 0x04 0x05 0x17 0x28
315	111	128	130	UNSOLICITED_RESPONSE	variation	0x00 0x01 0x17 0x28
316	113	128	129	RESPONSE	variation	0x00 0x01 0x17 0x28
317	113	128	130	UNSOLICITED_RESPONSE	variation	0x00 0x01 0x17 0x28

4.6.4 Deep Packet Inspection - IEC104 Enforcer

[Network Security > DPI > IEC104 Enforcer]

This dialog lets you specify the *IEC104 Enforcer* settings and define the *IEC104 Enforcer* specific profiles.

The *IEC104* protocol is a communication protocol used in the automation sector. The *IEC104* protocol helps to transfer the *IEC104* data packets between a *control station* (client) and a *substation* (server) using a TCP/IP network. The *IEC104 Enforcer* function activates the Deep Packet Inspection (DPI) firewall capabilities for the *IEC104* data stream. The *type IDs* in the *IEC104* protocol specify the purpose of the data transfer. The device blocks the data packets that violate the specified profiles.

When the *IEC104 Enforcer* profile is active, the device applies the profile to the data stream.

The device permits only data packets containing the values specified in the following columns:
- *Function type*
- *Advanced type ID list*
- *Originator address list*
- *Common address list*

Operation

Uncommitted changes present

Displays if the *IEC104 Enforcer* profiles applied to the data stream differ from the profiles saved in the device.

Possible values:

▶ `marked`
At least one of the active *IEC104 Enforcer* profiles saved in the device contains modified settings.

To apply the pending profiles to the data stream, click the ⬆ button.

Note:
If there are uncommitted changes on the device, the device commits them during the next system startup.

▶ `unmarked`
The *IEC104 Enforcer* profiles applied to the data stream match the profiles saved in the device.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons


Add

Opens the *Create* window to add a table row.

- In the *Index* field, you specify the number of the profile.
  Possible values:
  ▶ `1..32`

When you click the *Ok* button, the device adds the table row. The device assigns the number specified in the *Index* field to the table row.


Remove

Removes the selected table row.

If you mark the *Profile active* checkbox for the profile, then the device stops you from removing the profile.


Copy

Opens the *Copy* window to copy an existing table row. The prerequisite is that the table row for the profile to be copied is selected.

- In the *Index* field, you specify the new number of the copied profile.
  Possible values:
  ▶ `1..32`

When you click the *Ok* button, the device adds the table row. The device assigns the number specified in the *Index* field to the table row.


Commit changes

The device applies the specified profiles to the data stream.

If you changed the values in the *Function type* field, then the device assigns the specific values to the related profile.

Index

Displays the sequential number of the profile to which the table row relates. You specify the index number when you add a table row.

Description

Specifies a name for the profile.

Possible values:

- Alphanumeric ASCII character string with 0..128 characters
  (default setting: `iec104`)

Function type

Specifies the function type for the *IEC104 Enforcer* profile. After clicking the ✓ button, the device assigns the corresponding *type IDs*.

Possible values:

- *readOnly*
  Assigns the *type IDs* for the *read* function.
  `1,3,5,7,9,11,13,15,20,21,30-40,70,100-102`
- *readWrite*
  Assigns the *type IDs* for the *read/write* functions.
  `1,3,5,7,9,11,13,15,20,21,30-40,45-51,58-64,70,100-102`
- *common*
  Assigns the *type IDs* for the *common* functions.
  `1,3,5,7,9,11,13,15,20,21,30-40,45-51,58-64,70,100-102,110-113,120-127`
- *any* (default setting)
  Assigns the *type IDs* for every function.
  `1,2,..,254,255`
  The device does not permit any subsequent changes in the *Advanced type ID list* column.
- *advanced*
  Lets you specify user-defined values in the *Advanced type ID list* column.

Advanced type ID list

Displays the *advanced type IDs* for the *IEC104 Enforcer* profile. The device permits data packets with the specified properties. The prerequisite is that in the *Function type* column a value other than *any* is specified.

The device lets you specify multiple *Advanced type IDs*. To do this, perform the following steps:

- ☐ For the relevant profile, click into the *Advanced type ID list* column.
  The dialog displays the *Advanced type ID list* window.
- ☐ From the *Advanced type ID list* drop-down list, select the desired *type ID* item.
- ☐ Click the *Add* button.
- ☐ To add multiple *type IDs*, repeat the previously described steps.
- ☐ Click the *Ok* button.

Possible values:

- `0..255`
  You find the meaning of the numbers in section “Meaning of the Advanced type ID list values” on page 194.

Originator address list

Specifies the addresses from which data packets originated. The prerequisite is that in the *Cause of transmission size* column the value `2` is specified.

Possible values:

- `<empty>` (default setting)
  The device permits data packets from any *originator* address.
- `0..255`
  The device permits data packets with the specified *originator* address.

Common address list

Specifies the addresses to which the device forwards the *IEC104* data packets.

Possible values:

- `0..255`
  The device permits data packets with the specified *common* address. The prerequisite is that in the *Common address size* column the value `1` is specified.
- `0..65535 (2¹⁶-1)`
  The device permits data packets with the specified *common* address. The prerequisite is that in the *Common address size* column the value `2` is specified.

Cause of transmission size

Specifies the size in octets that defines the variation of the respective fields in the data packets. The device performs the *DPI* function based on these settings.

Possible values:

- `1`
  The data packets do not contain an *originator* address.
- `2` (default setting)
  The data packets contain an *originator* address.

Common address size

Specifies the size in octets of the *common* address to which the device forwards the *IEC104* data packets. This setting affects the setting in the *Common address list* column.

Possible values:

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

IO address size

Specifies the size in octets of the *information object address*.

Possible values:

- `1`
- `2`
- `3` (default setting)

Allow IEC_60870_5_101

Activates/deactivates the *type IDs* defined in the *IEC101* specification.

Possible values:

- `marked`
  The *type IDs* defined in the *IEC101* specification are active.
  The device permits the *type ID* values `2,4,6,8,10,12,14,16,17,18,19,103,104,105,106` along with the *type IDs* based on the values specified in the *Function type* column or *Advanced type ID list* column.
- `unmarked` (default setting)
  The *type IDs* defined in the *IEC101* specification are inactive.
  The device permits only the *type ID* values based on the values specified in the *Function type* or *Advanced type ID list* column.

Sanity check

Activates/deactivates the plausibility check for the data packets.

Possible values:

- `marked` (default setting)
  The plausibility check is active.
  The device checks the plausibility of the data packets regarding format and specification. The device blocks the data packets that violate the specified profiles.
- `unmarked`
  The plausibility check is inactive.

TCP reset

Activates/deactivates the resetting of the TCP connection in case of a protocol violation or if the plausibility check detects an error.

Possible values:

- `marked` (default setting)
  The resetting of the TCP connection is active.
  If the device identifies a protocol violation or detects a plausibility check error, then the device terminates the TCP connection. The device establishes the TCP connection again on receiving a new request.
- `unmarked`
  The resetting of the TCP connection is inactive.

Debug

Activates/deactivates the debugging of the profiles.

Possible values:

- `marked`
  Debugging is active.
  The device sends the reset packet along with the information related to the termination of TCP connection. The prerequisite is that in the *TCP reset* column the checkbox is marked.
- `unmarked` (default setting)
  Debugging is inactive.

Profile active

Activates/deactivates the profile.

Possible values:

- `marked`
  The profile is active.
  The device applies the *IEC104 Enforcer* profiles specified in this table row to the data stream.
- `unmarked`
  The profile is inactive.

[Advanced type ID list]

Advanced type ID list

Specifies the *Advanced type IDs* for the relevant *IEC104 Enforcer* profile.

You find the meaning of the numbers in section “Meaning of the Advanced type ID list values” on page 194.

Add

Adds the items you selected from the drop-down list to the *Advanced type ID list* field.

Deletes the item from the *Advanced type ID list* field.

Meaning of the Advanced type ID list values

#	Meaning
1	Single point information M_SP_NA_1
2	Single point information with time tag M_SP_TA_1
3	Double point information M_DP_NA_1
4	Double point information with time tag M_DP_TA_1
5	Step position information M_ST_NA_1
6	Step position information with time tag M_ST_TA_1
7	Bit string of 32 bit M_BO_NA_1
8	Bit string of 32 bit with time tag M_BO_TA_1
9	Measured value, normalized value M_ME_NA_1
10	Measured value, normalized value with time tag M_ME_TA_1
11	Measured value, scaled value M_ME_NB_1
12	Measured value, scaled value with time tag M_ME_TB_1
13	Measured value, short floating point value M_ME_NC_1
14	Measured value, short floating point value with time tag M_ME_TC_1
15	Integrated totals M_IT_NA_1
16	Integrated totals with time tag M_IT_TA_1
17	Event of protection equipment with time tag M_EP_TA_1

#	Meaning
18	Packed start events of protection equipment with time tag M_EP_TB_1
19	Packed output circuit information of protection equipment with time tag M_EP_TC_1
20	Packed single-point information with status change detection M_PS_NA_1
21	Measured value, normalized value without quality descriptor M_ME_ND_1
30	Single point information with time tag CP56Time2a M_SP_TB_1
31	Double point information with time tag CP56Time2a M_DP_TB_1
32	Step position information with time tag CP56Time2a M_ST_TB_1
33	Bit string of 32 bit with time tag CP56Time2a M_BO_TB_1
34	Measured value, normalized value with time tag CP56Time2a M_ME_TD_1
35	Measured value, scaled value with time tag CP56Time2a M_ME_TE_1
36	Measured value, short floating point value with time tag CP56Time2a M_ME_TF_1
37	Integrated totals with time tag CP56Time2a M_IT_TB_1
38	Event of protection equipment with time tag CP56Time2a M_EP_TD_1
39	Packed start events of protection equipment with time tag CP56time2a M_EP_TE_1
40	Packed output circuit information of protection equipment with time tag CP56Time2a M_EP_TF_1
45	Single command C_SC_NA_1
46	Double command C_DC_NA_1
47	Regulating step command C_RC_NA_1
48	Setpoint command, normalized value C_SE_NA_1
49	Setpoint command, scaled value C_SE_NB_1
50	Setpoint command, short floating point value C_SE_NC_1e
51	Bit string 32 bit C_BO_NA_1
58	Single command with time tag CP56Time2a C_SC_TA_1
59	Double command with time tag CP56Time2a C_DC_TA_1
60	Regulating step command with time tag CP56Time2a C_RC_TA_1
61	Setpoint command, normalized value with time tag CP56Time2a C_SE_TA_1
62	Setpoint command, scaled value with time tag CP56Time2a C_SE_TB_1
63	Setpoint command, short floating point value with time tag CP56Time2a C_SE_TC_1
64	Bit string 32 bit with time tag CP56Time2a C_BO_TA_1
70	End of initialization M_EI_NA_1
100	(General-) Interrogation command C_IC_NA_1
101	Counter interrogation command C_CI_NA_1
102	Read command C_RD_NA_1
103	Clock synchronization command C_CS_NA_1
104	(IEC 101) Test command C_TS_NB_1
105	Reset process command C_RP_NC_1
106	(IEC 101) Delay acquisition command C_CD_NA_1
107	Test command with time tag CP56Time2a C_TS_TA_1
110	Parameter of measured value, normalized value P_ME_NA_1
111	Parameter of measured value, scaled value P_ME_NB_1
112	Parameter of measured value, short floating point value P_ME_NC_1
113	Parameter activation P_AC_NA_1
120	File ready F_FR_NA_1
121	Section ready F_SR_NA_1
122	Call directory, select file, call file, call section F_SC_NA_1

#	Meaning
123	Last section, last segment F_LS_NA_1
124	Ack file, Ack section F_AF_NA_1
125	Segment F_SG_NA_1
126	F_DR_TA_1
127	QueryLog – Request archive file F_SC_NB_1

4.6.5 Deep Packet Inspection - AMP Enforcer

[Network Security > DPI > AMP Enforcer]

This dialog lets you specify the *AMP Enforcer* (*ASCII Message Protocol Enforcer*) settings and define the *AMP Enforcer* specific profiles.

The ASCII Message Protocol (AMP) is a communication protocol widely used in the automation industry for *Supervisory Control and Data Acquisition* (*SCADA*) and system integration. The ASCII Message Protocol (AMP) is designed to help ensure reliable communication between industrial equipment. The ASCII Message Protocol (AMP) is used to monitor and control industrial automation equipment such as Programmable Logic Controllers (PLCs), sensors, and meters.

The device uses the Deep Packet Inspection (DPI) function to discard data packets that violate one of the specified profiles. The *AMP Enforcer* function supports *Common ASCII Message Protocol* (*CAMP*) and *Non-Intelligent Terminal Protocol* (*NITP*) using *TCP*. The device uses the *AMP Enforcer* function to perform the *DPI* function on the *CAMP* and *NITP* data stream. The device performs the *DPI* function based on the *Program and mode protect* function and the specified profiles.

When the *AMP Enforcer* profile is active, the device applies the profiles to the data stream. The device permits only data packets that contain the values specified in the following columns depending on the status of the *Program and mode protect* function:

- *Protocol*
- *Message type*
- *Address class*
- *Device class*
- *Memory address*
- *Data word*
- *Task code*
- *Task code data*
- *Block check characters*
- *Error check characters*
- *Sanity check*

The menu contains the following dialogs:

- AMP Global
- AMP Profile

4.6.5.1 AMP Global

[Network Security > DPI > AMP Enforcer > Global]

In this dialog, you specify the global settings for the *AMP Enforcer* profile.

Protect mode

Program and mode protect

Activates/deactivates the inspection of the data packets that contain the *Task codes* with the value `config` in the *Mode* column.

Possible values:

- `marked` (default setting)
  The inspection is active. The device forwards only the data packets that match the parameters specified in the profiles. The device discards data packets that contain the value `config` in the *Mode* column for the *Task codes* specified in the profiles.
- `unmarked`
  The inspection is inactive. The device forwards the data packets that match the parameters specified in the profiles, including the data packets that contain *Task codes* with the value `config` in the *Mode* column.

Operation

Uncommitted changes present

Displays if the *AMP Enforcer* profiles applied to the data stream differ from the profiles saved in the device.

Possible values:

- `marked`
  At least one of the active *AMP Enforcer* profiles saved in the device contains modified settings.
  To apply the pending profiles to the data stream, click the ⬆ button.

  Note:
  If there are uncommitted changes on the device, the device commits them during the next system startup.
- `unmarked`
  The *AMP Enforcer* profiles applied to the data stream match the profiles saved in the device.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons


Add

Opens the *Create* window to add a table row.

- In the *Task code* field, you specify the number of the profile.
  Possible values:
  ▶ `00..FF`

When you click the *Ok* button, the device adds the table row. The device assigns the *Task code* specified in the *Task code* field to the table row.


Remove

Removes the selected table row.


Commit changes

The device applies the specified profiles to the data stream.

If you changed the values in the field, then the device assigns the specific values to the related profile.

Task code

Specifies the user-defined *Task code* for the *AMP Enforcer* profile represented by 2 ASCII characters. The *Task codes* are the command or response messages associated with:

- modification of the configuration, application program, or operational mode of the equipment.
- read or write the equipment data.

Possible values:

▶ `00..FF`
You find the meaning of the default *Task codes* in section “Meaning of the Task code values” on page 206.

Description

Specifies a name for the *Task code*.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters

Mode

Specifies the mode applicable for the *Task code*.

Possible values:

- *config*
  Specifies commands associated with the modification of the controller settings, the application program or the operational mode.
- *non-config*
  Specifies read/write commands, excluding the commands associated with modification of the controller settings, application program or operational mode.

4.6.5.2 AMP Profile

[Network Security > DPI > AMP Enforcer > Profile]

This dialog lets you set up profiles for the *AMP Enforcer* function. The profile lets you forward or discard data packets based on the specified values.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the *Create* window to add a table row.

- In the *Index* field, you specify the number of the profile.
  Possible values:
  ▶ `1..32`

When you click the *Ok* button, the device adds the table row. The device assigns the number specified in the *Index* field to the table row.

Remove

Removes the selected table row.

If you mark the *Profile active* checkbox for the profile, then the device stops you from removing the profile.

Copy

Opens the *Copy* window to copy an existing table row. The prerequisite is that the table row for the profile to be copied is selected.

- In the *Index* field, you specify the new number of the copied profile.
  Possible values:
  ▶ `1..32`

When you click the *Ok* button, the device adds the table row. The device assigns the number specified in the *Index* field to the table row.

Index

Displays the sequential number of the profile to which the table row relates. You specify the index number when you add a table row.

Description

Specifies a name for the profile.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters
  (default setting: `amp`)

Protocol

Specifies the TCP payload protocol type of the data packets to which the device applies the profile. The device applies the profile only to data packets that contain the specified value in the *Protocol* field.

Possible values:

- *camp*
  Common ASCII Message Protocol
- *nitp*
  Non-Intelligent Terminal Protocol
- *any* (default setting)
  The device applies the profile to every data packet without evaluating the protocol.

Message type

Specifies if the message is of the type *command* or *response*. The prerequisite is that in the *Protocol* column the value *camp* is specified.

Possible values:

- `any` (default setting)
  The device applies the profile to every data packet without evaluating the message type.
- `00..03` and `FF`
  The device applies the profile only to data packets that contain the specified message type.
  The field lets you specify the following options:
  - You specify a message type with a single hexadecimal value.
    Example: `02`
  - You specify multiple individual message types with comma-separated hexadecimal values.
    Example: `02,03,FF`
- `00..01,04..09` and `FF`
  The device applies the profile only to data packets that contain the specified message type.
  The field lets you specify the following options:
  - You specify a message type with a single hexadecimal value.
    Example: `04`
  - You specify multiple individual message types with comma-separated hexadecimal values.
    Example: `04,05,06,FF`

  You find the meaning of the hexadecimal values in section “Meaning of the Message type values” on page 207.

Address class

Specifies the particular type of the memory to be accessed on the equipment.

Prerequisites:

- In the *Protocol* column, the value *camp* is specified.
- In the *Message type* column, a hexadecimal value in the range `00..01` or `04..09` or the hexadecimal value `FF` is specified.

Possible values:

- `any` (default setting)
  The device applies the profile to every data packet without evaluating the address class.
- `0000..FFFF`
  The device applies the profile only to data packets that contain the specified address class.
  The field lets you specify the following options:
  - You specify an address class with a single hexadecimal value.
    Example: `0000`
  - You specify multiple individual address classes with the hexadecimal values separated by a comma.
    Example: `0000,0003,FFFF`
  - You specify an address class range with hexadecimal values connected by a dash.
    Example: `0004-000A`
  - You can also combine address classes and address class ranges.
    Example: `0000,0003,0004-000A`
    The field lets you specify up to 205 hexadecimal values. When you enter `0000,0003,0004-000A`, for example, you use 4 of 205 hexadecimal values.

Device class

Specifies the type of device class (vendor specific device) to be accessed.

Prerequisites:

- In the *Protocol* column, the value *camp* is specified.
- In the *Message type* column, a hexadecimal value in the range `00..03` or the hexadecimal value `FF` is specified.

Possible values:

- `any` (default setting)
  The device applies the profile to every data packet without evaluating the device class.
- `0000..FFFF`
  The device applies the profile only to data packets that contain the specified device class.
  The field lets you specify the following options:
  - You specify a device class with a single hexadecimal value.
    Example: `0000`
  - You specify multiple individual device classes with hexadecimal values separated by a comma.
    Example: `0000,0003,FFFF`
  - You specify a device class range with hexadecimal values connected by a dash.
    Example: `0004-000A`
  - You can also combine device classes and device class ranges.
    Example: `0000,0003,0004-000A`
    The field lets you specify up to 205 hexadecimal values. When you enter `0000,0003,0004-000A`, for example, you use 4 of 205 hexadecimal values.

Memory address

Specifies the starting address of the memory to be read or written.

Prerequisites:

- In the *Protocol* column, the value *camp* is specified.
- In the *Message type* column, a hexadecimal value in the range `00..01` or `04..09` or the hexadecimal value `FF` is specified.

Possible values:

- `any` (default setting)
  The device applies the profile to every data packet without evaluating the memory address.
- `0000..FFFF`
  The device applies the profile only to data packets that contain the specified memory address.
  The field lets you specify the following options:
  - You specify a memory address with a single hexadecimal value.
    Example: `0000`
  - You specify multiple individual memory addresses with hexadecimal values separated by a comma.
    Example: `0000,0003,FFFF`
  - You specify a memory address range with hexadecimal values connected by a dash.
    Example: `0004-000A`
  - You can also combine memory addresses and memory address ranges.
    Example: `0000,0003,0004-000A`
    The field lets you specify up to 205 hexadecimal values. When you enter `0000,0003,0004-000A`, for example, you use 4 of 205 hexadecimal values.

Data word

Specifies the starting address that the equipment uses to read data from the packet.

Prerequisites:

- In the *Protocol* column, the value *camp* is specified.
- In the *Message type* column, a hexadecimal value in the range `00..01` or `08..09` or the hexadecimal value `FF` is specified.

Possible values:

- `any` (default setting)
  The device applies the profile to every data packet without evaluating the data word.
- `0000..FFFF`
  The device applies the profile only to data packets that contain the specified data word.
  The field lets you specify the following options:
  - You specify a data word with a single hexadecimal value.
    Example: `0000`
  - You specify multiple individual data words with hexadecimal values separated by a comma.
    Example: `0000,0003,FFFF`
  - You specify a data word range with hexadecimal values connected by a dash.
    Example: `0004-000A`
  - You can also combine data words and data word ranges.
    Example: `0000,0003,0004-000A`
    The field lets you specify up to 205 hexadecimal values. When you enter `0000,0003,0004-000A`, for example, you use 4 of 205 hexadecimal values.

Task code

Displays the *Task codes* of the *AMP Enforcer* profile. You can add user-specific *Task codes* in the *Network Security > DPI > AMP Enforcer > Global* dialog.

The prerequisite is that in the *Protocol* column one of the following values is specified:

- *nitp*
- *camp*
  Additionally, in the *Message type* column, a hexadecimal value in the range `00..03` or the hexadecimal value `FF` is specified.
- *any*
  Additionally, in the *Message type* column, the value `any` is specified.

The device lets you specify multiple *Task codes*. To do this, perform the following steps:

- ☐ Click in the *Task code* column of the relevant profile.
  The dialog displays the *Task code* window.
- ☐ Select the desired *Task code* from the *Task code* drop-down list.
- ☐ Click the *Add* button.
- ☐ To add multiple *Task codes*, repeat the previously described steps.
- ☐ Click the *Ok* button.

Possible values:

- `any` (default setting)
  The device applies every *Task code* available in the *Available task codes* field.
- `00..FF`
  The device permits data packets with the specified codes.
  The field lets you specify the following options:
  - A single *Task code* with a single hexadecimal value.
    Example: `00`
  - Multiple *Task codes* with hexadecimal values separated by a comma.
    Example: `00,01,02`

  You find the meaning of the hexadecimal values in section “Meaning of the Task code values” on page 206.

Task code data

Specifies the task code data for the *Task code*.

The prerequisite is that in the *Protocol* column one of the following values is specified:

- *camp*
  Additionally, in the *Message type* column, a hexadecimal value in the range `00..03` or the hexadecimal value `FF`, and in the *Task code* column a single hexadecimal value are specified.
- *nitp*
  Additionally, in the *Task code* column, a single hexadecimal value is specified.

Possible values:

- `0..F`
  The device applies the profile only to data packet that contains the specified task code data. The maximum length is 72 bytes.

Error check characters

Activates/deactivates the error checking of the characters contained in the *CAMP* and *NITP* data packets.

Prerequisite:

- In the *Protocol* column, the value *camp* and in the *Message type* column, a hexadecimal value in the range `00..03` or the hexadecimal value `FF` is specified.
  or
- In the *Protocol* column, the value *nitp* is specified.

Possible values:

- `marked` (default setting)
  The checking is active.
- `unmarked`
  The checking is inactive.

Block check characters

Activates/deactivates the checking of *block check characters* to validate the checksum contained in the *CAMP* data packets.

Prerequisites:

- In the *Protocol* column, the value `camp` is specified.
- In the *Message type* column, a hexadecimal value in the range `00..09` or the hexadecimal value `FF` is specified.

Possible values:

- `marked` (default setting)
  The checking is active.
- `unmarked`
  The checking is inactive.

Debug

Activates/deactivates the debugging of the profiles.

Possible values:

- `marked`
  Debugging is active.
  The device sends the reset packet along with the information related to the termination of TCP connection. The prerequisite is that in the *TCP reset* column the checkbox is marked.
- `unmarked` (default setting)
  Debugging is inactive.

TCP reset

Activates/deactivates the resetting of the TCP connection in case of a protocol violation or if the plausibility check detects an error.

Possible values:

- `marked` (default setting)
  The resetting of the TCP connection is active.
  If the device identifies a protocol violation or detects a plausibility check error, then the device terminates the TCP connection. The device establishes the TCP connection again on receiving a new connection request.
- `unmarked`
  The resetting of the TCP connection is inactive.

Sanity check

Activates/deactivates the plausibility check for the data packets.

Possible values:

- `marked` (default setting)
  The plausibility check is active.
  The device checks the plausibility of the data packets regarding format and specification. The device blocks the data packets that violate the specified profiles.
- `unmarked`
  The plausibility check is inactive.

Profile active

Activates/deactivates the profile.

Possible values:

- `marked`
  The profile is active.
  The device applies the *AMP Enforcer* profiles specified in this table row to the data stream.
- `unmarked`
  The profile is inactive.

[Task code]

Task code

Specifies the *Task codes* for the relevant *AMP Enforcer* profile.

You find the meaning of the hexadecimal values in section “Meaning of the Task code values” on page 206.

Add

Adds the items you selected from the drop-down list to the *AMP Enforcer* field.

Deletes the item from the *AMP Enforcer* field.

Meaning of the Task code values

#	Meaning
01	Read Word Memory Random
02	Write Word Memory Area Random
30	Read Operational Status
32	Program to Run Mode
33	Go to Program Mode
34	Execute Power-up
35	Execute Complete (Warm) Start
36	Execute Partial (Hot) Start
50	Read User Word Area Block
51	Write User Word Area Starting at Address
58	Set Controller Time of Day Clock
59	Write Discrete I/O Status or Force via Data Element Type
5A	Write Block
6B	Read Discrete I/O Status or Force via Data Element Type
71	Read Controller Time of Day Clock
7D	Read SF/Loop Processor Mode
7E	Read Random

#	Meaning
7F	Read Block
88	Select Number of SF Module Task Codes Per Scan
89	Read Number of SF Module Task Codes Per Scan
99	Write VME Memory Area Block/Random
9A	Read VME Memory Area Block/Random

Meaning of the Message type values

#	Meaning
00	Module General Query Command
01	Module General Response Command
02	Packet T/C Command
03	Packed T/C Response
04	Read data Command
05	Read data Response
06	Write data Command
07	Write data Response
08	Mem Exch Command
09	Mem Exch Response
FF	Protocol Error

4.6.6 Deep Packet Inspection - ENIP Enforcer

[Network Security > DPI > ENIP Enforcer]

This dialog lets you specify the *ENIP Enforcer* (*Ethernet Industrial Protocol Enforcer*) settings and define the *ENIP Enforcer* specific profiles.

The Ethernet Industrial Protocol (ENIP) is part of the Common Industrial Protocol (CIP). The Common Industrial Protocol (CIP) defines the object structure and specifies the message transfer. The *ENIP Enforcer* function applies the Deep Packet Inspection (DPI) function to the ENIP and CIP data stream. The Ethernet Industrial Protocol (ENIP) is used to monitor and control industrial automation equipment such as PLCs (Programmable Logic Controllers), sensors, and meters.

The device uses the *ENIP Enforcer* function to perform the DPI function on the data stream. The device performs the DPI function based on the values defined in the specified profiles. The device blocks the data packets that violate the specified profiles.

Note:
The *ENIP Enforcer* function performs the DPI function only on packets that contain an *explicit request*, and drops packets that contain an *implicit request*. An *explicit request* contains *CIP message over TCP*. An *implicit request* contains *CIP message over UDP*.

When the *ENIP Enforcer* profile is active, the device applies the profile to the data stream. The device permits only data packets containing the values specified in the following columns:
- *Function type*
- *Sanity check*

- *Default object list*
- *Wildcard service codes*
- *Allow embedded PCCC* (*Programmable Controller Communication Commands*)

The menu contains the following dialogs:
- ENIP Profile
- ENIP Object

4.6.6.1 ENIP Profile

[Network Security > DPI > ENIP Enforcer > Profile]

In this dialog, you specify the global settings for the *ENIP Enforcer* profile.

Operation

Uncommitted changes present

Displays if the *ENIP Enforcer* profiles applied to the data stream differ from the profiles saved in the device.

Possible values:

- `marked`
  At least one of the active *ENIP Enforcer* profiles saved in the device contains modified settings.
  To apply the pending profiles to the data stream, click the button.

  Note:
  If there are uncommitted changes on the device, the device commits them during the next system startup.

- `unmarked`
  The *ENIP Enforcer* profiles applied to the data stream match the profiles saved in the device.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the *Create* window to add a table row.

- In the *Index* field, you specify the number of the profile.
  Possible values:
  - `1..32`

When you click the *Ok* button, the device adds the table row. The device assigns the number specified in the *Index* field to the table row.

Remove

Removes the selected table row.

If you mark the *Profile active* checkbox for the profile, then the device stops you from removing the profile.

Copy

Opens the *Copy* window to copy an existing table row. The prerequisite is that the table row for the profile to be copied is selected.

- In the *Index* field, you specify the new number of the copied profile.
  Possible values:
  ▶ `1..32`

When you click the *Ok* button, the device adds the table row. The device assigns the number specified in the *Index* field to the table row.

Commit changes

The device applies the specified profiles to the data stream.

If you changed the values in the *Function type* field, then the device assigns the specific values to the related profile.

Index

Displays the sequential number of the profile to which the table row relates. You specify the index number when you add a table row.

Description

Specifies a name for the profile.

Possible values:

▶ Alphanumeric ASCII character string with 0..32 characters
(default setting: `enip`)

Function type

Specifies the function type for the *ENIP Enforcer* profile. After clicking the ✓ button, the device assigns the corresponding *class IDs* and *service codes*.

Possible values:

▶ *readonly*
Assigns the *class IDs* for the *read* function.
You find the list of the readonly *class IDs* in table 4 on page 223.

▶ *readwrite*
Assigns the *class IDs* for the *read/write* functions.
You find the list of the read/write *class IDs* in table 5 on page 228.

▶ *any* (default setting)
Assigns the *class IDs* for every function. You cannot specify user-defined *class IDs* through the *Object* value if the function type is *any*.

▶ *advanced*
Lets you specify user-defined *class IDs*.

Allow embedded PCCC

Activates/deactivates DPI for *PCCC messages* encapsulated in data packets. *PCCC messages* are embedded within the Ethernet Industrial Protocol (ENIP). Activating this setting is useful when securing network traffic to and from PLC-5 and MicroLogix controllers.

Possible values:

- `marked`
  DPI for *PCCC messages* is active. The device assigns the *command codes* and *function codes*, corresponding to the value you specify in the *Function type* column.
  You find the lists of the *command codes* and *function codes* in following tables:
  - See table 6 on page 238.
  - See table 7 on page 238.
  - See table 8 on page 240.
- `unmarked` (default setting)
  DPI for *PCCC messages* is inactive.

Sanity check

Activates/deactivates the plausibility check for the data packets.

Possible values:

- `marked` (default setting)
  The plausibility check is active.
  The device checks the plausibility of the data packets regarding format and specification. The device blocks the data packets that violate the specified profiles.
- `unmarked`
  The plausibility check is inactive.

TCP reset

Activates/deactivates the resetting of the TCP connection in case of a protocol violation or if the plausibility check detects an error.

Possible values:

- `marked` (default setting)
  The resetting of the TCP connection is active.
  If the device identifies a protocol violation or detects a plausibility check error, then the device terminates the TCP connection. The device establishes the TCP connection again on receiving a new connection request.
- `unmarked`
  The resetting of the TCP connection is inactive.

Debug

Activates/deactivates the debugging of the profiles.

Possible values:

- `marked`
  Debugging is active.
  The device sends the reset packet along with the information related to the termination of TCP connection. The prerequisite is that in the *TCP reset* column the checkbox is marked.
- `unmarked` (default setting)
  Debugging is inactive.

Default object list

Specifies the *index numbers* used in the *default object list*.

Possible values:

- `all`
  The device applies the *ENIP Enforcer* profile to every data packet regardless of the *index number*.
- `1..347`
  The device applies the *ENIP Enforcer* profile only to data packets containing *class IDs* and *service codes* in the specified *index number*.
  The field lets you specify the following options:
  - You specify a single *index number* with a single numerical value.
    Example: `1`
  - You specify multiple *index numbers* with numerical values separated by a comma.
    Example: `1,2,3`
  - You specify an *index number* range with numerical values connected by a dash.
    Example: `7-25`
  - You can also combine *index numbers* and *index number* ranges.
    Example: `2,7-25,56`
    The field lets you specify up to 347 numerical values. When you enter `2,7-25,56`, for example, you use 4 of 347 numerical values.

  You find the list of the *class IDs* and corresponding *service codes* in table 3 on page 214.
- `none` (default setting)
  The device does not apply the *index number* to the *ENIP Enforcer* profile.

Wildcard service codes

Specifies the *service codes* which device permits with any valid *class IDs*.

Possible values:

- `0x00..0x7F`
  The device applies the profile only to data packets that contain the specified *service codes*.
  The field lets you specify the following options:
  - You specify a service list with a single hexadecimal value.
    Example: `0x00`
  - You specify multiple individual *service codes* with comma-separated hexadecimal values.
    Example: `0x02,0x03,0x04,0x05`
    The field lets you specify up to 128 hexadecimal values. When you enter `0x02,0x03,0x04,0x05`, for example, you use 4 of 128 hexadecimal values.

Profile active

Activates/deactivates the profile.

Possible values:

- `marked`
  The profile is active.
  The device applies the *ENIP Enforcer* profiles specified in this table row to the data stream.
- `unmarked` (default setting)
  The profile is inactive.

4.6.6.2 ENIP Object

[Network Security > DPI > ENIP Enforcer > Object]

The ENIP function uses objects to transmit values and information between devices. The ENIP function uses *class IDs* and *service codes* to specify how the data within the object is encoded. Each instance of an encoded information element that defines a unique *class ID* and a unique *service code* in a message, is an ENIP object.

This window lets you add custom ENIP objects and also lets you view the previously added custom ENIP objects. To verify that an added ENIP object is valid, check the following parameters:
- *Class ID*
- *Service codes*

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the *Create* window to add a table row.
- From the *Index* drop-down list, you select the profile *index number*.
- In the *Class ID* field, you specify the user-defined *class IDs*.
  Possible values:
  ▶ `0x00..0xFFFFFFFF`
- In the *Service codes* field, you specify the *service codes*.
  Possible values:
  ▶ `0x00..0x7F`

When you click the *Ok* button, the device adds the table row. The device assigns the values specified in the *Index*, *Class ID* and *Service codes* fields to this table row.

Remove

Removes the selected table row.

Index

Displays the number of the profile to which the table row relates. You specify the index number when you add a table row.

Class ID

Specifies the user-defined *class IDs* for the *ENIP Enforcer* profile.

Possible values:

- `0x00..0xFFFFFFFF`

Service codes

Specifies the *service codes*.

Possible values:

- `0x00..0x7F`
  The device applies the profile only to data packets that contain the specified *service codes*.
  The field lets you specify the following options:
  - You specify a service list with a single hexadecimal value.
    Example: `0x00`
  - You specify multiple individual *service codes* with comma-separated hexadecimal values.
    Example: `0x02,0x03,0x04,0x05`
    The field lets you specify up to 128 hexadecimal values. When you enter `0x02,0x03,0x04,0x05`, for example, you use 4 of 128 hexadecimal values.

Description

Displays the name of the object.

[Default object list]

Table 3: Default object list

Index	Class ID	Service codes
1	0x01 = Identity	0x01=Get Attributes All
2		0x05= Reset
3		0x0E= Get Attribute Signal
4		0x10= Set Attribute Signal
5		0x11= Find Next Object Instance
6		0x18= Get Member
7	0x02 = Message Router	0x01= Get Attributes All
8		0x0E = Get Attribute Single
9		0x4B = Write Data Table (Rockwell)
10	0x04 = Assembly	0x08 = Create
11		0x09 = Delete
12		0x0E = Get Attribute Single
13		0x10 = Set Attribute Single
14		0x18 = Get Member
15		0x19 = Set Member
16		0x1A = Insert Member
17		0x1B = Remove Member

Table 3: Default object list (cont.)

Index	Class ID	Service codes
18	0x05 = Connection	0x05 = Reset
19		0x08 = Create
20		0x09 = Delete
21		0x0D = Apply Attributes
22		0x0E = Get Attribute Single
23		0x10 = Set Attribute Single
24		0x11 = Find Next Object Instance
25		0x4B = Connection Bind
26		0x4C = Production Application Lookup
27		0x4E = Safety Close
28		0x54 = Safety Open
29	0x06 = Off-Link Connection Manager[1]	0x01 = Get Attributes All
30		0x02 = Set Attributes All
31		0x0E = Get Attribute Single
32		0x10 = Set Attribute Single
33		0x4E = Forward Close
34		0x52 = Unconnected Send
35		0x54 = Forward Open
36		0x56 = Get Connection Data
37		0x57 = Search Connection Data
38		0x5A = Get Connection Owner
39		0x5B = Large Forward Open
40	0x07 = Register	0x0E = Get Attribute Single
41		0x10 = Set Attribute Single
42	0x08 = Discrete Input Point	0x01 = Get Attributes All
43		0x02 = Set Attributes All
44		0x0E = Get Attribute Single
45		0x10 = Set Attribute Single
46	0x09 = Discrete Output Point	0x01 = Get Attributes All
47		0x02 = Set Attributes All
48		0x0E = Get Attribute Single
49		0x10 = Set Attribute Single
50	0x0A = Analog Input Point	0x01 = Get Attributes All
51		0x02 = Set Attributes All
52		0x0E = Get Attribute Single
53		0x10 = Set Attribute Single
54	0x0B = Analog Output Point	0x01 = Get Attributes All
55		0x02 = Set Attributes All
56		0x0E = Get Attribute Single
57		0x10 = Set Attribute Single
58	0x0E = Presence Sensing	0x0E = Get Attribute Single
59		0x10 = Set Attribute Single

Table 3: Default object list (cont.)

Index	Class ID	Service codes
60	0x0F = Parameter	0x01 = Get Attributes All
61		0x05 = Reset
62		0x0D = Apply Attributes
63		0x0E = Get Attribute Single
64		0x10 = Set Attribute Single
65		0x15 = Restore
66		0x16 = Save
67		0x18 = Get Member
68		0x4B = Get Enum String
69	0x10 = Parameter Group	0x01 = Get Attributes All
70		0x0E = Get Attribute Single
71		0x10 = Set Attribute Single
72	0x12 = Group	0x01 = Get Attributes All
73		0x0E = Get Attribute Single
74	0x1D = Discrete Input Group	0x01 = Get Attributes All
75		0x02 = Set Attributes All
76		0x0E = Get Attribute Single
77		0x10 = Set Attribute Single
78	0x1E = Discrete Output Group	0x01 = Get Attributes All
79		0x02 = Set Attributes All
80		0x0E = Get Attribute Single
81		0x10 = Set Attribute Single
82	0x1F = Discrete Group	0x01 = Get Attributes All
83		0x0E = Get Attribute Single
84	0x20 = Analog Input Group	0x01 = Get Attributes All
85		0x02 = Set Attributes All
86		0x0E = Get Attribute Single
87		0x10 = Set Attribute Single
88	0x21 = Analog Output Group	0x01 = Get Attributes All
89		0x02 = Set Attributes All
90		0x0E = Get Attribute Single
91		0x10 = Set Attribute Single
92	0x22 = Analog Group	0x01 = Get Attributes All
93		0x0E = Get Attribute Single
94		0x10 = Set Attribute Single

Table 3: Default object list (cont.)

Index	Class ID	Service codes
95	0x23 = Position Sensor Object	0x05 = Reset
96		0x0D = Apply Attributes
97		0x0E = Get Attribute Single
98		0x10 = Set Attribute Single
99		0x15 = Restore
100		0x16 = Save
101		0x18 = Get Member
102		0x19 = Set Member
103	0x24 = Position Controller Supervisor Object	0x0E = Get Attribute Single
104		0x10 = Set Attribute Single
105	0x25 = Position Controller Object	0x0E = Get Attribute Single
106		0x10 = Set Attribute Single
107	0x26 = Block Sequencer Object	0x0E = Get Attribute Single
108		0x10 = Set Attribute Single
109	0x27 = Command Block Object	0x0E = Get Attribute Single
110		0x10 = Set Attribute Single
111	0x28 = Motor Data Object	0x0E = Get Attribute Single
112		0x10 = Set Attribute Single
113		0x15 = Restore
114		0x16 = Save
115	0x29 = Control Supervisor Object	0x0E = Get Attribute Single
116		0x10 = Set Attribute Single
117		0x05 = Reset
118	0x2A = AC/DC Drive Object	0x0E = Get Attribute Single
119		0x10 = Set Attribute Single
120		0x15 = Restore
121		0x16 = Save
122	0x2B = Acknowledge Handler Object	0x08 = Create
123		0x09 = Delete
124		0x0E = Get Attribute Single
125		0x10 = Set Attribute Single
126		0x4B = Add AckData Path
127		0x4C = Remove AckData Path
128	0x2C = Overload Object	0x0E = Get Attribute Single
129		0x10 = Set Attribute Single
130		0x15 = Restore
131		0x16 = Save
132	0x2D = Softstart Object	0x0E = Get Attribute Single
133		0x10 = Set Attribute Single
134		0x15 = Restore
135		0x16 = Save

Table 3: Default object list (cont.)

Index	Class ID	Service codes
136	0x2E = Selection Object	0x05 = Reset
137		0x06 = Start
138		0x07 = Stop
139		0x08 = Create
140		0x09 = Delete
141		0x0E = Get Attribute Single
142		0x10 = Set Attribute Single
143		0x18 = Get Member
144		0x19 = Set Member
145		0x1A = Insert Member
146		0x1B = Remove Member
147	0x30 = S-Device Supervisor Object	0x05 = Reset
148		0x06 = Start
149		0x07 = Stop
150		0x0E = Get Attribute Single
151		0x10 = Set Attribute Single
152		0x4B = Abort
153		0x4C = Recover
154		0x4E = Perform Diagnostics
155	0x31 = S-Analog Sensor Object	0x01 = Get Attributes All
156		0x0E = Get Attribute Single
157		0x4B = Zero Adjust
158		0x4C = Gain Adjust
159	0x32 = S-Analog Actuator Object	0x0E = Get Attribute Single
160		0x10 = Set Attribute Single
161	0x33 = S-Single Stage Controller Object	0x0E = Get Attribute Single
162		0x10 = Set Attribute Single
163		0x63 = Calibrate
164	0x34 = S-Gas Calibration Object	0x0E = Get Attribute Single
165		0x10 = Set Attribute Single
166		0x4B = Get All Instances
167	0x35 = Trip Point Object	0x0E = Get Attribute Single
168		0x10 = Set Attribute Single

Table 3: Default object list (cont.)

Index	Class ID	Service codes
169	0x37 = File Object	0x06 = Start
170		0x07 = Stop
171		0x08 = Create
172		0x09 = Delete
173		0x0E = Get Attribute Single
174		0x10 = Set Attribute Single
175		0x15 = Restore
176		0x16 = Save
177		0x18 = Get Member
178		0x4B = Initiate Upload
179		0x4C = Initiate Download
180		0x4D = Initiate Partial Read
181		0x4E = Initiate Partial Write
182		0x4F = Upload Transfer
183		0x50 = Download Transfer
184		0x51 = Clear File
185	0x38 = S-Partial Pressure Object	0x01 = Get Attributes All
186		0x08 = Create
187		0x09 = Delete
188		0x0E = Get Attribute Single
189		0x10 = Set Attribute Single
190		0x4B = Create Range
191		0x4C = Get Instance List
192		0x4D = Get Pressures
193		0x4E = Get All Pressures
194		0x4F = Group Enable
195	0x40 = S-Sensor Calibration Object	0x0E = Get Attribute Single
196		0x10 = Set Attribute Single
197		0x4B = Get all Instances
198	0x41 = Event Log Object	0x05 = Reset
199		0x06 = Start
200		0x07 = Stop
201		0x0E = Get Attribute Single
202		0x10 = Set Attribute Single
203		0x18 = Get Member
204		0x19 = Set Member
205		0x1A = Insert Member
206		0x1B = Remove Member

Table 3: Default object list (cont.)

Index	Class ID	Service codes
207	0x42 = Motion Device Axis Object	0x03 = Get Attribute List
208		0x04 = Set Attribute List
209		0x0E = Get Attribute Single
210		0x10 = Set Attribute Single
211		0x1C = GroupSync
212		0x4B = Get Axis Attributes List
213		0x4C = Set Axis Attributes List
214		0x4D = Set Cyclic Write List
215		0x4E = Set Cyclic Read List
216		0x4F = Run Motor Test
217		0x50 = Get Motor Test Data
218		0x51 = Run Inertia Test
219		0x52 = Get Inertia Test Data
220		0x53 = Run Hookup Test
221		0x54 = Get Hookup Test Data
222	0x43 = Time Sync Object	0x01 = Get Attributes All
223		0x03 = Get Attribute List
224		0x04 = Set Attribute List
225		0x0E = Get Attribute Single
226		0x10 = Set Attribute Single
227	0x44 = Modbus Object	0x0E = Get Attribute Single
228		0x4B = Read Discrete Inputs
229		0x4C = Read Coils
230		0x4D = Read Input Registers
231		0x4E = Read Holding Registers
232		0x4F = Write Coils
233		0x50 = Write Holding Registers
234		0x51 = Modbus Passthrough
235	0x45 = Originator Connection List Object	0x08 = Create
236		0x09 = Delete
237		0x4C = Connection Read
238	0x46 = Modbus Serial Link Object	0x01 = Get Attributes All
239		0x05 = Reset
240		0x0E = Get Attribute Single
241		0x10 = Set Attribute Single
242		0x4B = Get And Clear

Table 3: Default object list (cont.)

Index	Class ID	Service codes
243	0x47 = Device Level Ring (DLR) Object	0x01 = Get Attributes All
244		0x0E = Get Attribute Single
245		0x10 = Set Attribute Single
246		0x18 = Get Member
247		0x4B = Verify Fault Location
248		0x4C = Clear Rapid Faults
249		0x4D = Restart Sign On
250		0x4E = Clear Gateway Partial Fault
251	0x48 = QoS Object	0x01 = Get Attributes All
252		0x0E = Get Attribute Single
253		0x10 = Set Attribute Single
254	0x4D = Target Connection List Object	0x01 = Get Attributes All
255		0x0E = Get Attribute Single
256		0x4C = Connection Read
257	0x4E = Base Energy Object	0x01 = Get Attributes All
258		0x03 = Get Attribute List
259		0x04 = Set Attribute List
260		0x05 = Reset
261		0x08 = Create
262		0x09 = Delete
263		0x0E = Get Attribute Single
264		0x10 = Set Attribute Single
265		0x18 = Get Member
266		0x19 = Set Member
267		0x1A = Insert Member
268		0x1B = Remove Member
269		0x4B = Start Metering
270		0x4C = Stop Metering
271	0x4F = Electrical Energy Object	0x01 = Get Attributes All
272		0x03 = Get Attribute List
273		0x0E = Get Attribute Single
274	0x50 = Non-Electrical Energy Object	0x01 = Get Attributes All
275		0x03 = Get Attribute List
276		0x0E = Get Attribute Single
277	0x51 = Base Switch Object	0x01 = Get Attributes All
278		0x0E = Get Attribute Single
279		0x10 = Set Attribute Single
280	0x52 = SNMP Object	0x01 = Get Attributes All
281		0x0E = Get Attribute Single
282		0x10 = Set Attribute Single

Table 3: Default object list (cont.)

Index	Class ID	Service codes
283	0x53 = Power Management Object	0x01 = Get Attributes All
284		0x03 = Get Attribute List
285		0x04 = Set Attribute List
286		0x0E = Get Attribute Single
287		0x10 = Set Attribute Single
288		0x18 = Get Member
289		0x19 = Set Member
290		0x4D = Power Management
291		0x4E = Set Pass Code
292		0x4F = Clear Pass Code
293	0x54 = RSTP Bridge Object	0x01 = Get Attributes All
294		0x0E = Get Attribute Single
295		0x10 = Set Attribute Single
296	0x55 = RSTP Port Object	0x01 = Get Attributes All
297		0x0E = Get Attribute Single
298		0x10 = Set Attribute Single
299	0xF3 = Connection Configuration Object	0x01 = Get Attributes All
300		0x02 = Set Attributes All
301		0x08 = Create
302		0x09 = Delete
303		0x0E = Get Attribute Single
304		0x10 = Set Attribute Single
305		0x15 = Restore
306		0x4B = Kick Timer
307		0x4C = Open Connection
308		0x4D = Close Connection
309		0x4E = Stop Connection
310		0x4F = Change Start
311		0x50 = Get Status
312		0x51 = Change Complete
313		0x52 = Audit Changes
314	0xF4 = Port Object	0x01 = Get Attributes All
315		0x05 = Reset
316		0x0E = Get Attribute Single
317		0x10 = Set Attribute Single
318	0xF5 = TCP/IP Interface Object	0x01 = Get Attributes All
319		0x02 = Set Attributes All
320		0x0E = Get Attribute Single
321		0x10 = Set Attribute Single

Table 3: Default object list (cont.)

Index	Class ID	Service codes
322	0xF6 = EtherNet Link Object	0x01 = Get Attributes All
323		0x0E = Get Attribute Single
324		0x10 = Set Attribute Single
325		0x4C = Get And Clear
326	0x300 = Module Diagnostics	0x01 = Get Attributes All
327		0x0E = Get Attribute Single
328	0x301 = InputIOCnx	0x01 = Get Attributes All
329		0x0E = Get Attribute Single
330	0x302 = Local Slaves	0x01 = Get Attributes All
331		0x0E = Get Attribute Single
332	0x400 = Service Port Control Object	0x01 = Get Attributes All
333		0x0E = Get Attribute Single
334	0x401 = Dynamic IO Control Object	0x01 = Get Attributes All
335		0x0E = Get Attribute Single
336	0x402 = Router Diagnostics Object	0x01 = Get Attributes All
337		0x0E = Get Attribute Single
338	0x403 = Router Routing Table Object	0x01 = Get Attributes All
339		0x0E = Get Attribute Single
340	0x404 = SMTP	0x01 = Get Attributes All
341		0x0E = Get Attribute Single
342		0x32 = Clear All
343	0x405 = SNTP	0x01 = Get Attributes All
344		0x0E = Get Attribute Single
345		0x32 = Clear All
346	0x406 = HSBY	0x01 = Get Attributes All
347		0x0E = Get Attribute Single

1. A packet with *Class ID*=0x06 contains embedded CIP messages. In this case, the device performs an additional level of DPI on the data packets that contain the *service codes* 0x4E, 0x52, 0x54 and 0x5B. The device blocks a data packet if it contains other than the preceding *service codes* for this *Class ID*.

[List of the class IDs for different function types]

Table 4: Class IDs for function type readonly

Class ID	Service codes
0x01 = Identity	0x01=Get Attributes All
	0x0E= Get Attribute Signal
	0x11= Find Next Object Instance
	0x18= Get Member

Table 4: Class IDs for function type readonly (cont.)

Class ID	Service codes
0x02 = Message Router	0x01= Get Attributes All
	0x0E = Get Attribute Single
	0x4B = Write Data Table (Rockwell)
	0x54
0x04 = Assembly	0x0E = Get Attribute Single
	0x18 = Get Member
0x05 = Connection	0x08 = Create
	0x0E = Get Attribute Single
	0x11 = Find Next Object Instance
	0x4C = Production Application Lookup
0x06 = Off-Link Connection Manager[1]	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x4C
	0x4E = Forward Close
	0x52 = Unconnected Send
	0x54 = Forward Open
	0x56 = Get Connection Data
	0x57 = Search Connection Data
	0x59
	0x5A = Get Connection Owner
	0x5B = Large Forward Open
0x07 = Register	0x0E = Get Attribute Single
0x08 = Discrete Input Point	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x09 = Discrete Output Point	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x0A = Analog Input Point	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x0B = Analog Output Point	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x0E = Presence Sensing	0x0E = Get Attribute Single
0x0F = Parameter	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x18 = Get Member
	0x4B = Get Enum String
0x10 = Parameter Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x12 = Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x1D = Discrete Input Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single

Table 4: Class IDs for function type readonly (cont.)

Class ID	Service codes
0x1E = Discrete Output Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x1F = Discrete Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x20 = Analog Input Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x21 = Analog Output Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x22 = Analog Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x23 = Position Sensor Object	0x0E = Get Attribute Single
	0x18 = Get Member
0x24 = Position Controller Supervisor Object	0x0E = Get Attribute Single
0x25 = Position Controller Object	0x0E = Get Attribute Single
0x26 = Block Sequencer Object	0x0E = Get Attribute Single
0x27 = Command Block Object	0x0E = Get Attribute Single
0x28 = Motor Data Object	0x0E = Get Attribute Single
0x29 = Control Supervisor Object	0x0E = Get Attribute Single
0x2A = AC/DC Drive Object	0x0E = Get Attribute Single
0x2B = Acknowledge Handler Object	0x0E = Get Attribute Single
0x2C = Overload Object	0x0E = Get Attribute Single
0x2D = Softstart Object	0x0E = Get Attribute Single
0x2E = Selection Object	0x0E = Get Attribute Single
	0x18 = Get Member
0x30 = S-Device Supervisor Object	0x0E = Get Attribute Single
0x31 = S-Analog Sensor Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x32 = S-Analog Actuator Object	0x0E = Get Attribute Single
0x33 = S-Single Stage Controller Object	0x0E = Get Attribute Single
0x34 = S-Gas Calibration Object	0x0E = Get Attribute Single
	0x4B = Get All Instances
0x35 = Trip Point Object	0x0E = Get Attribute Single
0x37 = File Object	0x0E = Get Attribute Single
	0x18 = Get Member
	0x4B = Initiate Upload
	0x4D = Initiate Partial Read
	0x4F = Upload Transfer

Table 4: Class IDs for function type readonly (cont.)

Class ID	Service codes
0x38 = S-Partial Pressure Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x4C = Get Instance List
	0x4D = Get Pressures
	0x4E = Get All Pressures
0x40 = S-Sensor Calibration Object	0x0E = Get Attribute Single
	0x4B = Get all Instances
0x41 = Event Log Object	0x0E = Get Attribute Single
	0x18 = Get Member
0x42 = Motion Device Axis Object	0x03 = Get Attribute List
	0x0E = Get Attribute Single
	0x4B = Get Axis Attributes List
	0x50 = Get Motor Test Data
	0x52 = Get Inertia Test Data
	0x54 = Get Hookup Test Data
0x43 = Time Sync Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x0E = Get Attribute Single
0x44 = Modbus Object	0x0E = Get Attribute Single
	0x4B = Read Discrete Inputs
	0x4C = Read Coils
	0x4D = Read Input Registers
	0x4E = Read Holding Registers
0x45 = Originator Connection List Object	0x4C = Connection Read
0x46 = Modbus Serial Link Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x47 = Device Level Ring (DLR) Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x18 = Get Member
0x48 = QoS Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x4D = Target Connection List Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x4E = Base Energy Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x0E = Get Attribute Single
	0x18 = Get Member
0x4F = Electrical Energy Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x0E = Get Attribute Single

Table 4: Class IDs for function type readonly (cont.)

Class ID	Service codes
0x50 = Non-Electrical Energy Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x0E = Get Attribute Single
0x51 = Base Switch Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x52 = SNMP Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x53 = Power Management Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x0E = Get Attribute Single
	0x18 = Get Member
0x54 = RSTP Bridge Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x55 = RSTP Port Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x91 = ANSI Extended Symbol Segment	0x03
	0x55
0x6B	0x55
0x6C	0x01
0xAC	0x01
	0x4C
0xB2	0x08
	0x4E
	0x4F
0xF3 = Connection Configuration Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x4C = Open Connection
	0x4D = Close Connection
	0x4E = Stop Connection
	0x50 = Get Status
0xF4 = Port Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0xF5 = TCP/IP Interface Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0xF6 = EtherNet Link Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x300 = Module Diagnostics	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x301 = InputIOCnx	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x302 = Local Slaves	0x01 = Get Attributes All
	0x0E = Get Attribute Single

Table 4: Class IDs for function type readonly (cont.)

Class ID	Service codes
0x400 = Service Port Control Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x401 = Dynamic IO Control Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x402 = Router Diagnostics Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x403 = Router Routing Table Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x404 = SMTP	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x405 = SNTP	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x406 = HSBY	0x01 = Get Attributes All
	0x0E = Get Attribute Single

1. A packet with *Class ID*=0x06 contains embedded CIP messages. In this case, the device performs an additional level of DPI on the data packets that contain the *service codes* 0x4E, 0x52, 0x54 and 0x5B. The device blocks a data packet if it contains other than the preceding *service codes* for this *Class ID*.

Table 5: Class IDs for function type readwrite

Class ID	Service codes
0x01 = Identity	0x01=Get Attributes All
	0x0E= Get Attribute Signal
	0x10= Set Attribute Signal
	0x11= Find Next Object Instance
	0x18= Get Member
0x02 = Message Router	0x01= Get Attributes All
	0x0E = Get Attribute Single
	0x4B = Write Data Table (Rockwell)
	0x54
0x04 = Assembly	0x08 = Create
	0x09 = Delete
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x18 = Get Member
	0x19 = Set Member
	0x1A = Insert Member
	0x1B = Remove Member
	0x4B
	0x4C

Table 5: Class IDs for function type readwrite (cont.)

Class ID	Service codes
0x05 = Connection	0x05 = Reset
	0x08 = Create
	0x09 = Delete
	0x0D = Apply Attributes
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x11 = Find Next Object Instance
	0x4B = Connection Bind
	0x4C = Production Application Lookup
	0x4E = Safety Close
	0x54 = Safety Open
0x06 = Off-Link Connection Manager[1]	0x01 = Get Attributes All
	0x02 = Set Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x4C
	0x4E = Forward Close
	0x52 = Unconnected Send
	0x54 = Forward Open
	0x56 = Get Connection Data
	0x57 = Search Connection Data
	0x59
	0x5A = Get Connection Owner
	0x5B = Large Forward Open
0x07 = Register	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x08 = Discrete Input Point	0x01 = Get Attributes All
	0x02 = Set Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x09 = Discrete Output Point	0x01 = Get Attributes All
	0x02 = Set Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x0A = Analog Input Point	0x01 = Get Attributes All
	0x02 = Set Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x0B = Analog Output Point	0x01 = Get Attributes All
	0x02 = Set Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single

Table 5: Class IDs for function type readwrite (cont.)

Class ID	Service codes
0x0E = Presence Sensing	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x0F = Parameter	0x01 = Get Attributes All
	0x05 = Reset
	0x0D = Apply Attributes
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x15 = Restore
	0x16 = Save
	0x18 = Get Member
	0x4B = Get Enum String
0x10 = Parameter Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x12 = Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x1D = Discrete Input Group	0x01 = Get Attributes All
	0x02 = Set Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x1E = Discrete Output Group	0x01 = Get Attributes All
	0x02 = Set Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x1F = Discrete Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x20 = Analog Input Group	0x01 = Get Attributes All
	0x02 = Set Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x21 = Analog Output Group	0x01 = Get Attributes All
	0x02 = Set Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x22 = Analog Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single

Table 5: Class IDs for function type readwrite (cont.)

Class ID	Service codes
0x23 = Position Sensor Object	0x05 = Reset
	0x0D = Apply Attributes
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x15 = Restore
	0x16 = Save
	0x18 = Get Member
	0x19 = Set Member
0x24 = Position Controller Supervisor Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x25 = Position Controller Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x26 = Block Sequencer Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x27 = Command Block Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x28 = Motor Data Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x15 = Restore
	0x16 = Save
0x29 = Control Supervisor Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x05 = Reset
0x2A = AC/DC Drive Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x15 = Restore
	0x16 = Save
0x2B = Acknowledge Handler Object	0x08 = Create
	0x09 = Delete
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x4B = Add AckData Path
	0x4C = Remove AckData Path
0x2C = Overload Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x15 = Restore
	0x16 = Save
0x2D = Softstart Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x15 = Restore
	0x16 = Save

Table 5: Class IDs for function type readwrite (cont.)

Class ID	Service codes
0x2E = Selection Object	0x05 = Reset
	0x06 = Start
	0x07 = Stop
	0x08 = Create
	0x09 = Delete
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x18 = Get Member
	0x19 = Set Member
	0x1A = Insert Member
	0x1B = Remove Member
0x30 = S-Device Supervisor Object	0x05 = Reset
	0x06 = Start
	0x07 = Stop
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x4B = Abort
	0x4C = Recover
	0x4E = Perform Diagnostics
0x31 = S-Analog Sensor Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x4B = Zero Adjust
	0x4C = Gain Adjust
0x32 = S-Analog Actuator Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x33 = S-Single Stage Controller Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x63 = Calibrate
0x34 = S-Gas Calibration Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x4B = Get All Instances
0x35 = Trip Point Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single

Table 5: Class IDs for function type readwrite (cont.)

Class ID	Service codes
0x37 = File Object	0x06 = Start
	0x07 = Stop
	0x08 = Create
	0x09 = Delete
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x15 = Restore
	0x16 = Save
	0x18 = Get Member
	0x4B = Initiate Upload
	0x4C = Initiate Download
	0x4D = Initiate Partial Read
	0x4E = Initiate Partial Write
	0x4F = Upload Transfer
	0x50 = Download Transfer
	0x51 = Clear File
0x38 = S-Partial Pressure Object	0x01 = Get Attributes All
	0x08 = Create
	0x09 = Delete
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x4B = Create Range
	0x4C = Get Instance List
	0x4D = Get Pressures
	0x4E = Get All Pressures
	0x4F = Group Enable
0x40 = S-Sensor Calibration Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x4B = Get all Instances
0x41 = Event Log Object	0x05 = Reset
	0x06 = Start
	0x07 = Stop
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x18 = Get Member
	0x19 = Set Member
	0x1A = Insert Member
	0x1B = Remove Member

Table 5: Class IDs for function type readwrite (cont.)

Class ID	Service codes
0x42 = Motion Device Axis Object	0x03 = Get Attribute List
	0x04 = Set Attribute List
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x1C = GroupSync
	0x4B = Get Axis Attributes List
	0x4C = Set Axis Attributes List
	0x4D = Set Cyclic Write List
	0x4E = Set Cyclic Read List
	0x4F = Run Motor Test
	0x50 = Get Motor Test Data
	0x51 = Run Inertia Test
	0x52 = Get Inertia Test Data
	0x53 = Run Hookup Test
	0x54 = Get Hookup Test Data
0x43 = Time Sync Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x04 = Set Attribute List
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x44 = Modbus Object	0x0E = Get Attribute Single
	0x4B = Read Discrete Inputs
	0x4C = Read Coils
	0x4D = Read Input Registers
	0x4E = Read Holding Registers
	0x4F = Write Coils
	0x50 = Write Holding Registers
	0x51 = Modbus Passthrough
0x45 = Originator Connection List Object	0x08 = Create
	0x09 = Delete
	0x4C = Connection Read
0x46 = Modbus Serial Link Object	0x01 = Get Attributes All
	0x05 = Reset
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x4B = Get And Clear

Table 5: Class IDs for function type readwrite (cont.)

Class ID	Service codes
0x47 = Device Level Ring (DLR) Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x18 = Get Member
	0x4B = Verify Fault Location
	0x4C = Clear Rapid Faults
	0x4D = Restart Sign On
	0x4E = Clear Gateway Partial Fault
0x48 = QoS Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x4D = Target Connection List Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x4C = Connection Read
0x4E = Base Energy Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x04 = Set Attribute List
	0x05 = Reset
	0x08 = Create
	0x09 = Delete
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x18 = Get Member
	0x19 = Set Member
	0x1A = Insert Member
	0x1B = Remove Member
	0x4B = Start Metering
	0x4C = Stop Metering
0x4F = Electrical Energy Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x0E = Get Attribute Single
0x50 = Non-Electrical Energy Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x0E = Get Attribute Single
0x51 = Base Switch Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x52 = SNMP Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single

Table 5: Class IDs for function type readwrite (cont.)

Class ID	Service codes
0x53 = Power Management Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x04 = Set Attribute List
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x18 = Get Member
	0x19 = Set Member
	0x4D = Power Management
	0x4E = Set Pass Code
	0x4F = Clear Pass Code
0x54 = RSTP Bridge Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x55 = RSTP Port Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x91 = ANSI Extended Symbol Segment	0x03
	0x55
0x6B	0x55
0x6C	0x01
0xAC	0x01
	0x4C
0xB2	0x08
	0x4E
	0x4F
0xF3 = Connection Configuration Object	0x01 = Get Attributes All
	0x02 = Set Attributes All
	0x08 = Create
	0x09 = Delete
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x15 = Restore
	0x4B = Kick Timer
	0x4C = Open Connection
	0x4D = Close Connection
	0x4E = Stop Connection
	0x4F = Change Start
	0x50 = Get Status
	0x51 = Change Complete
	0x52 = Audit Changes

Table 5: Class IDs for function type readwrite (cont.)

Class ID	Service codes
0xF4 = Port Object	0x01 = Get Attributes All
	0x05 = Reset
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0xF5 = TCP/IP Interface Object	0x01 = Get Attributes All
	0x02 = Set Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0xF6 = EtherNet Link Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x4C = Get And Clear
0x300 = Module Diagnostics	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x301 = InputIOCnx	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x302 = Local Slaves	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x400 = Service Port Control Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x401 = Dynamic IO Control Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x402 = Router Diagnostics Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x403 = Router Routing Table Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x404 = SMTP	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x32 = Clear All
0x405 = SNTP	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x32 = Clear All
0x406 = HSBY	0x01 = Get Attributes All
	0x0E = Get Attribute Single

1. A packet with *Class ID*=0x06 contains embedded CIP messages. In this case, the device performs an additional level of DPI on the data packets that contain the *service codes* 0x4E, 0x52, 0x54 and 0x5B. The device blocks a data packet if it contains other than the preceding *service codes* for this *Class ID*.

[List of the PCCC command codes for different function types]

Table 6: PCCC command codes for function type readonly

Command codes	Function codes
0x0F	0x04
	0x09
	0xA7
	0xA2
	0x17
	0x29
	0x68
	0x01
0x01	None
0x04	None
0x06	0x00
	0x01
	0x03
	0x09

Table 7: PCCC command codes for function type readwrite

Command codes	Function codes
0x00	None

Table 7: PCCC command codes for function type readwrite (cont.)

Command codes	Function codes
0x0F	0x02
	0x04
	0x03
	0x5E
	0x09
	0x08
	0xA7
	0xAF
	0xA2
	0xAA
	0x17
	0x26
	0x79
	0x29
	0x0A
	0x12
	0x68
	0x67
	0x53
	0x55
	0x06
	0x01
	0x00
	0x18
0x01	None
0x02	None
0x03	None
0x04	None
0x05	None
0x06	0x03
	0x00
	0x01
	0x09
	0x07
	0x08
	0x06
	0x0A
	0x05
	0x04
	0x02

Table 7: PCCC command codes for function type readwrite (cont.)

Command codes	Function codes
0x07	0x00
	0x01
	0x03
0x08	None

Table 8: PCCC command codes for function types any and advanced

Command codes	Function codes
0x00	None

Table 8: PCCC command codes for function types any and advanced (cont.)

Command codes	Function codes
0x0F	0x8F
	0x02
	0x3A
	0x82
	0x41
	0x50
	0x52
	0x05
	0x04
	0x03
	0x11
	0x57
	0x5E
	0x81
	0x09
	0x08
	0xA7
	0xAF
	0xA2
	0xAA
	0x17
	0x26
	0x79
	0x29
	0x0A
	0x12
	0x3A
	0x80
	0x07
	0x68
	0x67
	0x53
	0x55
	0x06
	0x01
	0x00
	0x18
0x01	None
0x02	None
0x03	None
0x04	None
0x05	None

Table 8: PCCC command codes for function types any and advanced (cont.)

Command codes	Function codes
0x06	0x03
	0x00
	0x01
	0x09
	0x07
	0x08
	0x06
	0x0A
	0x05
	0x04
	0x02
0x07	0x00
	0x01
	0x03
	0x04
	0x05
	0x06
0x08	None

4.6.7 Deep Packet Inspection - S7 Enforcer

[Network Security > DPI > S7 Enforcer]

This dialog lets you specify the *S7 Enforcer* settings and define *S7 Enforcer* specific templates associated with profiles.

S7comm is a communication protocol based on a master-slave model. Using the S7comm protocol, a master device, such as a Programmable Logic Controller (PLC) or a Human Machine Interface (HMI), initiates communication with one or more slave devices, such as I/O modules, drives, or other PLCs. The S7comm protocol is used for exchanging data, such as reading and writing variables and sending control commands.

The S7comm protocol has an advanced variant called S7comm Plus. In comparison to S7comm, S7comm Plus provides compatibility with modern PLCs and higher flexibility according to various communication requirements. The S7comm Plus protocol offers improved performance and additional features like improved security and scalability.

Using the *S7 Enforcer* function, the device performs Deep Packet Inspection (DPI) on the data stream to monitor and validate conformity with S7comm and S7comm Plus protocol standards. This process involves:

- Creating a template
  You specify specific rules that include the following parameters:
  - *Protocol type*
  - *Function type*
  - *Function group* (only S7comm)
  - *Sub-function group* (only S7comm)

- Creating a profile
  That includes the following additional parameters:
  - *Sanity check*
  - *Debug*
  - *TCP reset*
- Associating the template with the profile
- Applying the profile to the data stream
  The device blocks the data packets that violate the specified profile. The device permits only data packets containing the values specified in the profile.

The device supports up to 40 templates for inspecting the data packets:

- 14 predefined templates
  The device restricts you from deleting predefined templates.
- a maximum of 26 user-defined templates

The menu contains the following dialogs:

- S7 Template
- S7 Profile

4.6.7.1 S7 Template

[Network Security > DPI > S7 Enforcer > Template]

In this dialog, you set up templates for the *S7 Enforcer* function. Each template contains the specified settings. You associate these templates with profiles to forward or discard data packets.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

 Add

Opens the *Create* window to add a table row.

- From the *Index* drop-down list, you select the number of the template or specify a new number.
  To add a new number, enter the value. Then click the + button.
  Possible values:
  ▶ `1..40`
- From the *Protocol type* drop-down list, you select the *protocol type* for the template.
  Possible values:
  ▶ *s7comm*
  ▶ *s7commplus*
- In the *Rule index* field, you specify the number of the rule.
  Possible values:
  ▶ `1..25`

When you click the *Ok* button, the device adds the table row. The device assigns the number specified in the *Index* field to the table row.

 Remove

Removes the selected table row.

 Copy

Opens the *Copy* window to copy an existing table row. The prerequisite is that the table row for the template to be copied is selected.

- In the *Index* field, you specify the new number of the copied profile.
  Possible values:
  ▶ `1..40`

When you click the *Ok* button, the device adds the table row. The device assigns the number specified in the *Index* field to the table row.

Index

Displays the number of the template to which the table row relates. You specify the index number when you add a table row.

Template name

Specifies a name for the template.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters
  (default setting: `template-s7`)

Protocol type

Displays the *protocol type* of the data packets for the template, which you combine with the profile to apply to the data packets. The device applies the profile only to data packets that contain the specified *protocol type*.

Rule index

Displays the number of the rule associated with the template. You specify the rule index number when you add a table row.

Status

Activates/deactivates the rule associated with the template.

Possible values:

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

Function type

Specifies the *Function type* that corresponds to the *protocol type* for the rule associated with the template. The prerequisite is that in the *Protocol type* column a valid value is specified.

You find the list of the *Function types* and corresponding *protocol type* in section "[List of predefined function types for the S7comm and S7comm Plus protocols]" on page 252.

You can select a *Function type* from the drop-down list or specify a user-defined *Function type*. To add a user-defined *Function type*, enter the *Function type* value. Then click the + button.

Possible values:

- `all` (default setting)
  Assigns every *Function type* supported for the corresponding *protocol type*, except for user-defined *Function types*.
- `0x00 (CPU services)`
- `0x01 (Mode transition)`
- `0xf0 (Setup communication)`
- `0x04 (Read Var)`
- `0x05 (Write Var)`
- `0x1a (Request download)`

- `0x1b (Download block)`
- `0x1c (Download ended)`
- `0x1d (Start upload)`
- `0x1e (Upload)`
- `0x1f (End upload)`
- `0x28 (PI-Service)`
- `0x29 (PLC Stop)`
- `0x04b1 (Error)`
- `0x04bb (Explore)`
- `0x04ca (CreateObject)`
- `0x04d4 (DeleteObject)`
- `0x04f2 (SetVariable)`
- `0x04fc (GetVariable)`
- `0x0506 (AddLink)`
- `0x051a (RemoveLink)`
- `0x0524 (GetLink)`
- `0x0542 (SetMultiVariables)`
- `0x054c (GetMultiVariables)`
- `0x0556 (BeginSequence)`
- `0x0560 (EndSequence)`
- `0x056b (Invoke)`
- `0x057c (SetVarSubStreamed)`
- `0x0586 (GetVarSubStreamed)`
- `0x0590 (GetVariablesAddress)`
- `0x059a (Abort)`
- `0x05a9 (Error 2)`
- `0x05b3 (InitSSL)`
- `0x00..0xff` (only S7comm)
  `0x04b1..0xffff` (only S7comm Plus)
  Specifies the user-defined *Function types*.

Function group

Specifies the *Function group* that corresponds to the *Function type* for the rule associated with the template.

Prerequisites:

- In the *Protocol type* column, the value *s7comm* is specified.
- In the *Function type* column, a valid value is specified.
  You find the list of the *Function groups* and corresponding *Function types* in section “[List of predefined Function groups and Sub-function groups for different Function types]” on page 253.

You can select a *Function group* from the drop-down list or specify a user-defined *Function group*.

To add a user-defined *Function group*, enter the value. Then, click the + button.

Possible values:

- `-` (default setting)
  The device does not perform the DPI on the data packets based on the *Function group*.

- `all`
  Assigns every *Function group* supported for the corresponding *Function types*, except for user-defined *Function types*.
- `0x01 (Programmer commands)`
- `0x02 (Cyclic services)`
- `0x03 (Block functions)`
- `0x04 (CPU functions)`
- `0x05 (Security)`
- `0x06 (PBC BSEND)`
- `0x07 (Time functions)`
- `0x3f (NC programming)`
- `0x20 (DR Routing)`
- `0x00 (Stop)`
- `0x01 (Warm Restart)`
- `0x02 (Run)`
- `0x03 (Hot Restart)`
- `0x04 (Hold)`
- `0x06 (Cold Restart)`
- `0x09 (RUN_R (H-System redundant))`
- `0x0b (Link-up)`
- `0x0c (Update)`
- `0x00..0x3f`
  Specifies the user-defined *Function groups*.
  The S7comm protocol supports the following values as *Current mode*. However, the device lets you set up these values as *Function groups*.
  - `0x00 (Stop)`
  - `0x01 (Warm Restart)`
  - `0x02 (Run)`
  - `0x03 (Hot Restart)`
  - `0x04 (Hold)`
  - `0x04 (Hold)`
  - `0x06 (Cold Restart)`
  - `0x09 (RUN_R (H-System redundant))`
  - `0x0b (Link-up)`
  - `0x0c (Update)`

Sub-function group

Specifies the *Sub-function group* that corresponds to the *Function group* for the rule associated with the template.

Prerequisites:

- In the *Protocol type* column, the value *s7comm* is specified.
- In the *Function type* column, a valid value is specified.
  You find the list of the *Function groups* and corresponding *Function types* in section “[List of predefined Function groups and Sub-function groups for different Function types]” on page 253.
- In the *Function group* column, a valid value is specified.
  You find the list of the *Sub-function groups* and corresponding *Function groups* in section “[List of predefined Function groups and Sub-function groups for different Function types]” on page 253.

The device lets you specify multiple *Sub-function groups*. To do this, perform the following steps:

- ☐ Click the *Sub-function group* column of the relevant table row.
  The dialog displays the *Sub-function group* window.
- ☐ Select a *Sub-function group* or specify a user-defined *Sub-function group* from the *Sub-function group* drop-down list. To add a user-defined *Sub-function group*, enter the value. Then, click the

  + button.
- ☐ Click the *Add* button.
- ☐ Repeat the previously described steps to add multiple *Sub-function groups*.
- ☐ Click the *Ok* button.

Possible values:

- `-` (default setting)
  The device does not perform the DPI on the data packets based on the *Sub-function group*.
- `0x00..0xff`
  Specifies the user-defined *Sub-function groups*.

4.6.7.2 S7 Profile

[Network Security > DPI > S7 Enforcer > Profile]

In this dialog, you set up profiles for the *S7 Enforcer* function. A profile lets you forward or discard data packets based on the specified values.

Information

Uncommitted changes present

Displays if the *S7 Enforcer* profiles applied to the data stream differ from the profiles saved in the device.

Possible values:

- `marked`
  At least one of the active *S7 Enforcer* profiles saved in the device contains modified settings.
  To apply the pending profiles to the data stream, click the button.

  Note:
  If there are uncommitted changes on the device, the device commits them during the next system startup.

- `unmarked`
  The *S7 Enforcer* profiles applied to the data stream match the profiles saved in the device.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the *Create* window to add a table row.

- In the *Index* field, you specify the number of the profile.
  Possible values:
  - `1..32`

When you click the *Ok* button, the device adds the table row. The device assigns the number specified in the *Index* field to the table row.

Remove

Removes the selected table row.

If the *Profile active* checkbox is marked for a profile, then the device prevents you from removing it.

Copy

Opens the *Copy* window to copy an existing table row. The prerequisite is that the table row for the profile to be copied is selected.

- In the *Index* field, you specify the new number for the copied profile.
  Possible values:
  ▶ `1..32`

When you click the *Ok* button, the device adds the table row. The device assigns the number specified in the *Index* field to the table row.

Commit changes

The device applies the specified profiles to the data stream.

Index

Displays the number of the profile to which the table row relates. You specify the index number when you add a table row.

Description

Specifies a name for the profile.

Possible values:

▶ Alphanumeric ASCII character string with 0..32 characters
(default setting: `profile-s7`)

Template list

Specifies the number of the template to which the table row relates.

The device lets you specify multiple template numbers. To do this, perform the following steps:

☐ Click the *Template list* column of the relevant table row.
The dialog displays the *Template list* window.
☐ Select the template from the *Template name* drop-down list.
☐ Click the *Add* button.
☐ Repeat the previously described steps to add multiple templates.
☐ Click the *Ok* button.

Possible values:

▶ `1..40`

Sanity check

Activates/deactivates the plausibility check for the data packets.

Possible values:

▶ `marked` (default setting)
The plausibility check is active.
The device checks the plausibility of the data packets regarding format and specification.
▶ `unmarked`
The plausibility check is inactive.

Debug

Activates/deactivates the debugging of the profiles.

Possible values:

- `marked`
  Debugging is active.
  The device sends the reset packet along with the information related to the termination of the TCP connection. The prerequisite is that the checkbox in the *TCP reset* column is marked.
- `unmarked` (default setting)
  Debugging is inactive.

TCP reset

Activates/deactivates the resetting of the TCP connection in case of a protocol violation or if the plausibility check detects an error.

Possible values:

- `marked` (default setting)
  The resetting of the TCP connection is active.
  If the device identifies a protocol violation or detects a plausibility check error, then the device terminates the TCP connection.
- `unmarked`
  The resetting of the TCP connection is inactive. The TCP connection remains established.

Profile active

Activates/deactivates the profile.

Possible values:

- `marked`
  The profile is active.
  The device applies the *S7 Enforcer* profiles specified in this table row to the data stream.
- `unmarked` (default setting)
  The profile is inactive.

[List of predefined function types for the S7comm and S7comm Plus protocols]

Table 9: Function types for S7comm and S7comm Plus protocols

Protocol type	Function type
S7comm	0x00 = CPU services
	0x01 = Mode-transition
	0xf0 = Setup communication
	0x04 = Read Var
	0x05 = Write Var
	0x1a = Request download
	0x1b = Download block
	0x1c = Download ended
	0x1d = Start upload
	0x1e = Upload
	0x1f = End upload
	0x28 = PI-Service
	0x29 = PLC Stop
S7comm Plus	0x04b1 = Error
	0x04bb = Explore
	0x04ca = CreateObject
	0x04d4 = DeleteObject
	0x04f2 = SetVariable
	0x04fc = GetVariable
	0x0506 = AddLink
	0x051a = RemoveLink
	0x0524 = GetLink
	0x0542 = SetMultiVariables
	0x054c = GetMultiVariables
	0x0556 = BeginSequence
	0x0560 = EndSequence
	0x056b = Invoke
	0x057c = SetVarSubStreamed
	0x0586 = GetVarSubStreamedP
	0x0590 = GetVariablesAddress
	0x059a = Abort
	0x05a9 = Error 2
	0x05b3 = InitSSL

[List of predefined Function groups and Sub-function groups for different Function types]

Table 10: Function groups and Sub-function groups for Function types

Function type	Function group	Sub-function group
0x00 = CPU services	0x01 = Programmer commands	0x01 = Block status
		0x02 = Variable status
		0x03 = Output ISTACK
		0x04 = Output BSTACK
		0x05 = Output LSTACK
		0x06 = Time measurement from to
		0x07 = Force selection
		0x09 = Modify variable
		0x09 = Force
		0x0a = Breakpoint
		0x0b = Exit HOLD
		0x0c = Memory reset
		0x0d = Disable job
		0x0e = Enable job
		0x0f = Delete job
		0x10 = Read job list
		0x11 = Read job
		0x12 = Replace job
		0x13 = Block status v2
		0x16 = Flash LED
	0x02 = Cyclic services	0x01 = Cyclic transfer
		0x04 = Unsubscribe
		0x05 = Change driven transfer
		0x07 = Change driven transfer modify
		0x08 = RDREC
	0x03 = Block functions	0x01 = List blocks
		0x02 = List blocks of type
		0x03 = Get block info

Table 10: Function groups and Sub-function groups for Function types (cont.)

Function type	Function group	Sub-function group
	0x04 = CPU functions	0x01 = Read SZL
		0x02 = Message service
		0x03 = Diagnostic message
		0x05 = ALARM_8 indication
		0x06 = NOTIFY indication
		0x07 = ALARM_8 lock
		0x08 = ALARM_8 unlock
		0x09 = SCAN indication
		0x10 = AR SEND indication
		0x0b = ALARM ack
		0x0c = ALARM ack indication
		0x0d = ALARM lock indication
		0x0e = ALARM unlock indication
		0x11 = ALARM_SQ indication
		0x12 = ALARM_S indication
		0x13 = ALARM query
		0x16 = NOTIFY_8 indication
	0x05 = Security	0x01 = PLC password define
	0x06 = PBC BSEND	0x01 = PBC BSEND sub-function
	0x07 = Time functions	0x01 = Read clock
		0x02 = Set clock
		0x03 = Read clock (following)
		0x04 = Set clock
	0x3f = NC programming	0x01 = Request download
		0x02 = Download block
		0x03 = Continue download
		0x04 = Download ended
		0x06 = Start upload
		0x07 = Upload
		0x08 = Continue upload
	0x20 = DR Routing	0x01 = DRR Init
		0x02 = DRR Finish
		0x03 = DRR Data

Table 10: Function groups and Sub-function groups for Function types (cont.)

Function type	Function group	Sub-function group
0x01 = Mode-transition	0x00 = STOP[1]	-
	0x01 = Warm Restart[1]	-
	0x02 = RUN[1]	-
	0x03 = Hot Restart[1]	-
	0x04 = HOLD[1]	-
	0x06 = Cold Restart[1]	-
	0x09 = RUN_R (H-System redundant)[1]	-
	0x0b = LINK-UP[1]	-
	0x0c = UPDATE[1]	-
0xf0 = Setup communication[2]	-	-
0x04 = Read Var[2]	-	-
0x05 = Write Var[2]	-	-
0x1a = Request download[2]	-	-
0x1b = Download block[2]	-	-
0x1c = Download ended[2]	-	-
0x1d = Start upload[2]	-	-
0x1e = Upload[2]	-	-
0x1f = End upload[2]	-	-
0x28 = PI-Service[2]	-	-
0x29 = PLC Stop[2]	-	-

1. The device does not support any predefined *Sub-function groups* for this *Function group*. The device lets you specify only user-defined *Sub-function groups* for this *Function group*.
2. The device does not support any predefined *Function groups* or *Sub-function groups* for this *Function type*. The device lets you specify only user-defined *Function groups* or *Sub-function groups* for this *Function type*.

4.7 DoS

[Network Security > DoS]

Denial of Service (DoS) is a cyberattack that aims to make certain services or devices unusable. 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

4.7.1 DoS Global

[Network Security > DoS > Global]

In this dialog, you specify the DoS settings for the TCP/UDP, IP and ICMP protocols.

Note:
We recommend activating the filters to increase the level of security of the device.

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 compares the TCP header of incoming data packets. If the data offset value multiplied by 4 is smaller than the minimum TCP header size, then the filter discards the data packet.

Possible values:

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

Min. TCP header size

Displays the minimum size of a valid TCP header.

IP

Land Attack filter

Activates/deactivates the *Land Attack* filter. With the *Land Attack* method, the attacking station sends data packets whose source and destination addresses are identical to the IP address of the recipient.

Possible values:

- `marked`
  The filter is active. The device discards data packets whose source and destination addresses are identical.
- `unmarked` (default setting)
  The filter is inactive.

Drop IP Source Route

Activates/deactivates filtering of the received IP data packets with *Strict Source Routing* or *Loose Source Routing*. The *Strict Source Routing* or *Loose Source Routing* is an option in the IP header where the sender specifies the routing path. The data packets follow this routing path to reach the destination.

Possible values:

- `marked` (default setting)
  The filter is active. The device discards IP data packets with a specified routing path in the IP header.
- `unmarked`
  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

Fragmented packets filter

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.

Packet size filter

Activates/deactivates the filter for incoming ICMP packets.

The filter detects ICMP packets whose payload size exceeds the size specified in the *Allowed payload size [byte]* field and discards them.

Possible values:

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

Allowed payload size [byte]

Specifies the maximum allowed payload size of ICMP packets in bytes.

Possible values:

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

Layer 2 frames

802.3 Frames forwarding

Activates/deactivates the forwarding of IEEE 802.3 Ethernet packets.

The *802.3 Frames forwarding* function assists in managing link changes. You can therefore use the function to speed up convergence if a Layer 2 redundancy protocol based on IEEE 802.3 Ethernet packets is active in the network for example, Rapid Spanning Tree Protocol (RSTP). Convergence is the time required to adjust the network to topology changes, for example when the link status on a port changes.

In the default setting, the device discards the IEEE 802.3 Ethernet packets. The device does not support a redundancy protocol and is not part of a redundancy topology. Using the *802.3 Frames forwarding* function, the device forwards the IEEE 802.3 Ethernet packets received on one port to another port. As a result, the device behaves like a hub for IEEE 802.3 Ethernet packets. This helps the neighboring devices to adapt more quickly to topology changes.

To reduce the convergence time, Hirschmann recommends combining the *802.3 Frames forwarding* function with the *Link flap* function. See the *Diagnostics > Ports > Port Monitor* dialog, *Link flap* tab.

Possible values:

- `marked`
  The *802.3 Frames forwarding* function is active. The device forwards IEEE 802.3 Ethernet packets without inspecting or modifying their contents.
  If a hostile network station sends a high volume of IEEE 802.3 Ethernet packets to the device, the device will propagate these packets. This can cause a Denial of Service (Dos) attack.
  If a link on the device becomes inoperable, then the Layer 2 redundancy protocol such as RSTP will find an alternative path by bypassing the device and excluding it from the network path. This scenario poses a potential security risk. Therefore, enable the *802.3 Frames forwarding* function only if you are aware of the effects.
- `unmarked` (default setting)
  The *802.3 Frames forwarding* function is inactive. The device discards IEEE 802.3 Ethernet packets.

5 Virtual Private Network

The menu contains the following dialogs:
- VPN Overview
- VPN Certificates
- VPN Connections

5.1 VPN Overview

[Virtual Private Network > Overview]

Virtual Private Networks (VPN) provide secure communications for remote users or branch offices, allowing them to connect to servers within other branch offices, or even other companies using public networks. Even though the VPN tunnel uses a public network, it has the same behavior as a private network.

VPN tunnels provide secure communications to support the current trend of increased telecommuting and global business operations. In such cases, remote users or branch offices are able to connect to each other and central resources.

To provide secure communications, VPNs use IP Security (IPSec). IPSec has 2 functions for providing confidentiality namely, data encryption and data integrity. To provide authentication and integrity of the source with encryption, the device uses the IPSec Encapsulating Security Payload (ESP). Only the sender and receiver know the security key.

The device also uses the Negotiated Security Association method. The first packet received initiates a negotiation, between the sender and receiver, for which Security Association (SA) parameters the devices are going to use. The devices use the Internet Key Exchange (IKE) for the negotiation process. When negotiating the parameters, the sending and receiving devices agree on the authentication and data-security methods. The devices also perform mutual authentication, and then generate a shared key. The devices use the shared key to encrypt the data contained in each packet.

The VPN LED is green if at least one VPN tunnel is active and established. The LED is a separate LED for VPN and as such is non-configurable for this device. The VPN LED only displays the status of the VPN tunnels.

The dialog contains tabs which display the current VPN tunnels and statuses.

The *Connection errors* tab displays detected errors that are helpful when troubleshooting a VPN tunnel.

The dialog contains the following tabs:
- [Overview]
- [Diagnostics]
- [Connection errors]

Connection

Connections (max.)

Displays the maximum number of VPN tunnels supported. The device limits maximum number of active VPN tunnels to the amount set in *Max. active connections*.

Max. active connections

Displays the maximum number of active VPN tunnels supported.

[Overview]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

VPN index

Displays the table row index for unique identification of a VPN tunnel.

VPN description

Displays the user-defined name for the VPN tunnel.

VPN active

Displays if the VPN tunnel is active/inactive.

The device limits the maximum number of set-up VPN tunnels to the value displayed in the *Connections (max.)* field. The device also limits the maximum number of active VPN tunnels to the value specified in the *Max. active connections* column.

Possible values:

- `marked`
  The VPN tunnel is active.
- `unmarked`
  The VPN tunnel is inactive.

Used IKE version

Displays the version of the IKE protocol that the VPN tunnel uses.

Possible values:

- *`ikev1`*
  The device uses the IKE version `1` (ISAKMP) protocol.
- *`ikev2`*
  The device uses the IKE version `2` protocol.

Startup

Displays the starting role for mediating the key exchange for VPN tunnel.

Possible values:

- *initiator*
  If you specify the role of the device as an *Initiator* for the VPN tunnel, then the device actively initiates the Internet Key Exchange (IKE) and parameter negotiation.
- *responder*
  If you specify the role of the device as a *Responder* for the VPN tunnel, then the device waits for the *Initiator* to begin a key exchange (IKE) and connection parameter negotiation.

Operational status

Displays the current status of the VPN tunnel.

Possible values:

- *up*
  VPN tunnel is established.
- *down*
  VPN tunnel is not established.
- *negotiation*
  If you specify the VPN tunnel for this device as the *Initiator*, then the value indicates that the key exchange and negotiation algorithm is in progress. If the VPN tunnel for this device is the *Responder*, then the value indicates that the VPN tunnel is waiting for the process to begin.
- *constructing*
  The IKE-SA is up. However, the device has detected at least one unestablished IPsec-SA for this instance.
- *dormant*
  The device is waiting for you to complete the configuration before starting the VPN tunnel setup. For example, the device has an unsuccessful hostname resolution.
- *re-keying*
  The key exchange is in progress. The device displays the value after the expiration of either the IKE or the IPSEC lifetime timer.

Connection established [s]

Displays the time, in seconds, since the device established the VPN tunnel for this device. The device updates the value after every IKE re-authentication.

Local host

Displays the name and/or IP address of the local host that the device detected using IKE.

Possible values:

- Alphanumeric ASCII character string with 1..128 characters

Remote host

Displays the name and/or IP address of the remote host that the device detected using IKE.

Possible values:

- Alphanumeric ASCII character string with 1..128 characters

IKE proposal

Displays the algorithms that IKE uses for the key exchange.

The device displays a combination of the *IKE key agreement*, *IKE integrity (MAC)* and *IKE encryption* parameters.

If you set up an IKE algorithm for the device in the *Virtual Private Network > Connections* dialog, and the remote endpoint has a more secure algorithm set up, then it is possible that both the local and remote devices use the remote algorithm.

The device displays the current cipher suite used for the connection.

IPsec proposal

Displays the algorithms that IPsec uses for data communication.

The device displays a combination of the *IPsec key agreement*, *IPsec integrity (MAC)* and *IPsec encryption* parameters.

If you select an IPsec algorithm for the instance in the *Virtual Private Network > Connections* dialog, and the remote endpoint has a better, more secure algorithm set up, then it is possible that both the local and remote devices use the better algorithm.

The device displays the current cipher suite used for the connection.

Tunnels

Displays the number of IPsec tunnels within the VPN network.

[Diagnostics]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

VPN index

Displays the table row index for unique identification of a VPN tunnel.

VPN description

Displays the user-defined name for the VPN tunnel.

VPN active

Displays if the VPN tunnel is active/inactive.

The device limits the maximum number of set-up VPN tunnels to the value displayed in the *Connections (max.)* field. The device also limits the maximum number of active VPN tunnels to the value specified in the *Max. active connections* column.

Possible values:

- `marked`
  The VPN tunnel is active.
- `unmarked`
  The VPN tunnel is inactive.

Tunnel index

Displays the index value that, together with the value in the *VPN index* column, identifies the entry in the connection tunnel info table.

Traffic selector index

Displays the index value that, together with the value in the *VPN index* column, identifies the entry in the traffic selector table which is mapped into the IPsec tunnel.

Possible values:

- `0`
  The traffic selector index is unknown.
- `1..16`

Operational status

Displays the current status of the VPN tunnel.

Possible values:

- *up*
  The Internet Key Exchange-Security Association (IKE-SA) and every Internet Protocol Security-Security Association (IPsec-SA) is up.
- *down*
  The IKE-SA and IPsec-SAs are inactive.

- *negotiation*
  If you specify the VPN tunnel for this instance as the *Initiator*, then the value indicates that the key exchange and negotiation algorithm is in progress. If the VPN tunnel for this instance is the *Responder*, then the value indicates that the VPN tunnel is waiting for the process to begin.
- *constructing*
  The IKE-SA is up. However, the device has detected at least one unestablished IPsec-SA for this instance.
- *dormant*
  The device is waiting for you to complete the configuration before starting the VPN tunnel setup. For example, the device has an unsuccessful hostname resolution.
- *re-keying*
  The key exchange is in progress. The device displays the value after the expiration of either the IKE or the IPSEC lifetime timer.

IKE re-authentication [s]

Displays the remaining time, in seconds, before the next IKE re-authentication. The value 0 indicates that re-authentication is not set up.

Next IKE re-keying [s]

Displays the remaining time, in seconds, before the next IKE re-key. The value 0 indicates that re-keying is not set up.

IKE initiator SPI

Displays the Security Parameter Index (SPI) of the *Initiator*, depending which device you specify as the *Initiator*. For example, when you specify this device as the *Initiator*, then this value is the SPI of the local device.

IKE responder SPI

Displays the SPI of the *Responder*, depending which device you specify as the *Initiator*. For example, when you specify this device as the *Initiator*, then this value is the SPI of the remote device.

Local traffic selector

Displays the local traffic selector for this IPsec tunnel. As a result of the negotiation process between the peers, the local traffic selector can be different from the set-up traffic selector.

Remote traffic selector

Displays the remote traffic selector for this IPsec tunnel. As a result of the negotiation process between the peers, the traffic selector can be different from the set-up traffic selector.

Tunnel status

Displays the current operational status of the IPsec tunnel.

Possible values:

- *unknown*
  The IPsec proposal is in progress. No traffic selectors or security parameters have been negotiated for this IPsec-SA.

- *created*
  The key exchange and the negotiation algorithm is finished for this IPsec-SA, but the tunnel is inactive.
- *routed*
  The encryption policies for the data stream are established, but the negotiation process has not started.
- *installing*
  The peer authentication is established, but the IPsec proposal for this tunnel is still in progress.
- *installed*
  The IPsec-SA is installed.
- *updating*
  The device updates the security associations.
- *re-keying*
  The key exchange is in progress for this IPsec-SA. The device displays the value after the expiration of the IPsec lifetime timer.
- *re-keyed*
  The key exchange for this IPsec-SA is finished and the device sets up a new tunnel. The tunnel will become active after the expiration of the previous IPsec proposal.
- *re-trying*
  The key exchange for this IPsec-SA failed. The device will automatically try to initiate a new key exchange.
- *deleting*
  The device replaces the IPsec tunnel during re-keying. The device keeps the tunnel up for delayed packets. The old and the new tunnel are open simultaneously for 5 seconds in the default setting. After the IPsec lifetime timer has expired, the device deletes the tunnel.
- *destroying*
  The IPsec lifetime timer has expired. The device deletes the tunnel.

IPsec input SPI

Displays IPSec Security Parameter Index (SPI) that the device applies to the data it receives from the VPN tunnel. The SPI lets the device select the Security Association (SA) under which it processes a received packet.

IPsec output SPI

Displays IPSec Security Parameter Index (SPI) that the device applies to the data it transmits to the VPN tunnel.

Next IPsec re-keying [s]

Displays the remaining time, in seconds, before the next re-keying starts for this IPsec tunnel.

IPsec tunnel input [byte]

Displays the number of bytes received into this VPN tunnel.

IPsec-tunnel input [packets]

Displays the number of packets received into this VPN tunnel.

Last IPsec data received [s]

Displays the time, in seconds, since the VPN tunnel has received the last time data.

IPsec tunnel output [byte]

Displays the number of bytes sent into this VPN tunnel.

IPsec tunnel output [packets]

Displays the number of packets sent into this VPN tunnel.

Last IPsec data transmitted [s]

Displays the time, in seconds, since the VPN tunnel has sent the last time data.

[Connection errors]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

VPN index

Displays the table row index for unique identification of a VPN tunnel.

VPN description

Displays the user-defined name for the VPN tunnel.

VPN active

Displays if the VPN tunnel is active/inactive.

The device limits the maximum number of set-up VPN tunnels to the value displayed in the *Connections (max.)* field. The device also limits the maximum number of active VPN tunnels to the value specified in the *Max. active connections* column.

Possible values:

- `marked`
  The VPN tunnel is active.
- `unmarked`
  The VPN tunnel is inactive.

Last connection error

Displays the last error notification that occurred for this VPN tunnel.

When the connection remains inactive, this value is useful to help you isolate detected errors. This value helps you determine if a detected error occurred in the proposal exchange or during tunnel establishment.

Possible values:

- Alphanumeric ASCII character string with 1..512 characters

5.2 VPN Certificates

[Virtual Private Network > Certificates]

A Certification Authority (CA) issues digital certificates to authenticate the identity of devices requesting a VPN tunnel. You set up the devices that form a VPN tunnel to trust the Certification Authority (CA) that signed the digital certificate. When a trusted Certification Authority (CA) signs a digital certificate, the device considers it to be valid. Using a trusted Certification Authority (CA), lets you renew and change the digital certificates transferred onto the device without affecting the VPN. The prerequisite is, that the actual identity information is correct.

Using digital certificates also lets you reduce the required maintenance work. The reason for this is because you change digital certificates less often as you change pre-shared keys. The Certification Authority (CA) generates digital certificates with commence and expiration date. The digital certificate is only valid during this time. When a digital certificate expires, the device requires a new digital certificate.

You generate a self signed certificate using the strongSwan application in conjunction with the Linux Operating System.

Note:
RC2 certificate encryption algorithms are unsupported, for example PKCS12 containers with RC2 encryption or passphrase protection.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Remove

Removes the selected table row.

Upload

Opens the *Upload certificate* window to add a digital certificate to the table.

- In the *Passphrase (private key)* field, you enter the passphrase used with this digital certificate. Possible values:
  - Alphanumeric ASCII character string with 0..128 characters
- In the *URL* field, you specify the path and file name of the digital certificate.

The device gives you the following options for transferring the file onto the device:

- Import from the PC

  When the file is located on your PC or on a network drive, drag and drop it onto the  area.
  As an alternative, click in the area to select the file.
  You can also use SCP or SFTP to transfer the file from your PC to the device. Perform the following steps:
  - ☐ On your PC, open an SCP or SFTP client, for example WinSCP.
  - ☐ Use the SCP or SFTP client to open a connection to the device.
  - ☐ Transfer the file onto the device, into the directory `/upload/vpn-cert`.
    When the file transfer is complete, the device starts installing the digital certificate. If the installation was successful, then the device generates an `ok` file in the directory `/upload/vpn-cert` and deletes the transferred file.

Index

Displays the table row index of the digital certificate entry.

Possible values:

▶ `1..100`

File name

Displays the name of the file uploaded to the device.

Possible values:

▶ Alphanumeric ASCII character string with 1..64 characters

Subject

Displays the subject field of digital certificate.

The subject field of the digital certificate is a combination of the following items the country (C), state (ST), organization (O), organizational unit (OU), common name (CN), and email address of the recipient (emailAddress).

Possible values:

- Alphanumeric ASCII character string with 0..64 characters

Issuer

Displays the issuer of the digital certificate.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters

Valid from

Displays the date and time at which the digital certificate became effective.

Possible values:

- Date and time stamp

Valid until

Displays the digital certificate expiration time and date.

Possible values:

- Date and time stamp

Type

Displays the type of the container file used.

Possible values:

- *ca*
  The transferred file is a digital certificate signed by a Certification Authority (CA).
- *peer*
  The transferred file is a peer certificate.
- *pkcs12*
  The transferred file is a p12 bundle.
- *encryptedkey*
  The transferred file is a key file with password encryption.
- *encryptedpkcs12*
  The transferred file is a p12 bundle with password encryption.

Upload date

Displays the date and time at which the digital certificate was last transferred onto the device.

Possible values:

- Date and time stamp

Private key status

Displays the status of the private key in the peer certificate. Use a peer certificate with a private key.

Possible values:

- *none*
  The peer certificate does not contain a private key.

- *present*
  The device has located and extracted the private key from the peer certificate.
- *notFound*
  The device has located a private key. However, the key is missing the passphrase and the device has suspended the transfer.

Private key file

Displays the name of the private key file.

The device lets you enter alphanumeric characters plus hyphens, underscores and dots.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters

Active connections

Displays the number of active connections that are using this digital certificate.

The device lets you delete the digital certificate only when the value is `0`.

Possible values:

- `0..256`

5.3 VPN Connections

[Virtual Private Network > Connections]

This dialog lets you set up VPN tunnels.

Note:
The device uses software for DES and AES-Galois/Counter Mode (GCM) encryption.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

 Add

Opens the *Create* window to add a table row.

- From the *VPN description* drop-down list, you select an existing description or specify a new description. To enter a new description, click the + button.
  Possible values:
  ▶ Alphanumeric ASCII character string with 0..128 characters
- In the *Traffic selector index* field, you specify the index of the VPN tunnel traffic selector.
  Possible values:
  ▶ `1..16`

 Remove

Removes the selected table row.

 Wizard

Opens the *Wizard* window that helps you associate the ports with the address of one or more desired senders. See “[Wizard: VPN configuration]” on page 285.

VPN description

Specifies the user-defined name for the VPN tunnel.

Possible values:

- Alphanumeric ASCII character string with 1..128 characters

Traffic selector index

Displays the index value that, together with the value in the *VPN index* column, identifies the entry in the traffic selector table.

Possible values:

- `1..16`
  The device lets you specify any available value within the given range.

Status

Displays if the VPN tunnel is active/inactive.

The device limits the maximum number of set-up VPN tunnels to the value displayed in the *Connections (max.)* field. The device also limits the maximum number of active VPN tunnels to the value displayed in *Max. active connections*.

Possible values:

- `marked`
  The VPN tunnel is active.
- `unmarked` (default setting)
  The VPN tunnel is inactive.

Traffic selector description

Specifies the name of the traffic selector.

Possible values:

- Alphanumeric ASCII character string with 1..128 characters

Source address (CIDR)

Specifies the IP address and netmask of the source host. When the device forwards packets containing this source IP address over a VPN tunnel, the device applies the settings specified in this table row. Furthermore, the device applies the associated IPsec and IKE-SA settings, to every IP packet it forwards containing this address.

Possible values:

- Valid IPv4 address and netmask in CIDR notation
- `any` (default setting)
  The device applies the settings in this table row to every packet it forwards.

Source restrictions

Specifies the optional source restrictions using names or numbers entered as `<protocol/port>`. The device sends only the type of data specified through the VPN tunnel.

Examples:

- `tcp/http` is equal to `6/80`
- `udp` is equal to `udp/any`
- `/53` is equal to `any/53`

Possible values:

- Alphanumeric ASCII character string with 1..32 characters
- `<empty>` (default setting)
  The device uses `any/any` as the restriction.

Destination address (CIDR)

Specifies the IP address and netmask of the destination. When the device forwards packets containing this destination IP address over a VPN tunnel, the device applies the settings specified in this table row. Furthermore, for every IP packet the device forwards containing this address, it applies the associated IPsec and IKE-SA settings.

Possible values:

- Valid IPv4 address and netmask in CIDR notation
- `any` (default setting)
  The device applies the settings in this table row to every packet it forwards.

Destination restrictions

Specifies the optional destination restrictions using names or numbers entered as `<protocol/port>`. The device accepts only the type of data specified from the VPN tunnel.

Examples:

- `tcp/http` is equal to `6/80`
- `udp` is equal to `udp/any`
- `/53` is equal to `any/53`

Possible values:

- Alphanumeric ASCII character string with 1..32 characters
- `<empty>` (default setting)
  The device uses `any/any` as the restriction.

Version

Specifies the version of the IKE protocol for the VPN connection.

Possible values:

- *`auto`* (default setting)
  The VPN starts with protocol IKEv2 as the *Initiator* and accepts IKEv1/v2 as the *Responder*.
- *`ikev1`*
  The VPN starts with the IKEv1 protocol.
- *`ikev2`*
  The VPN starts with the IKEv2 protocol.

Startup

Specifies if the device starts this instance as a *Responder* or *Initiator*.

If you specify the local peer as the *Responder*, and the remote peer sends data packets to a specific selector, then the device attempts to establish the connection as the *Responder*. Establishing a connection as a *Responder* depends upon other settings for this connection. For example, if you specify in the *Remote endpoint* field the value `any`, then the device cannot initiate the connection.

Possible values:

- *initiator*
  If you specify that the device starts as an *Initiator*, then the device starts an key exchange with the *Responder*.
- *responder* (default setting)
  If you specify that the device starts as a *Responder*, then the device waits for the *Initiator* to start the key exchange and parameter negotiation.

IKEv1 DPD timeout [s]

Specifies the timeout, in seconds, before the local peer declares the remote peer dead, if the remote peer is unresponsive.

The device supports the *IKEv1 DPD timeout [s]* function using IKEv1.

Possible values:

- `0`
  Deactivates the function.
- `1..86400 (24 h)` (default setting: `120`)

IKE lifetime [s]

Specifies the lifetime, in seconds, of the IKE security association between two network devices to support secure communication. The devices establish a security association after exchanging a set of pre-defined keys.

Possible values:

- `300..86400` (default setting: `28800`)
  The default setting is 8 hours. The maximum setting is 24 hours.

IKE exchange mode

Specifies the use of the phase 1 exchange mode for IKEv1.

The purpose of IKE phase 1 is to establish a secure authenticated communication channel. The device uses the Diffie-Hellman key exchange algorithm to generate a shared secret key. The device then uses the shared secret key to further encrypt IKE communications.

Possible values:

- *main* (default setting)
  The main mode for phase 1 provides identity protection.
- *aggressive*
  You use the aggressive mode to reduce round trips.

Authentication

Specifies the type of authentication that the device uses.

Possible values:

- *psk* (default setting)
  Select this value for the device to use a key that was previously generated and saved on both the remote and local devices.
- *individualx509*
  Select this value for the device to use a digital certificate in X.509 format.
  Use a separate digital certificate for Certification Authority (CA) and local identification.
- *pkcs12*
  Select this value for the device to use a PKCS12 container with the needed digital certificates, which also includes the Certification Authority (CA).

Pre-shared key

Specifies the pre-shared key. The prerequisite is that in the *Authentication* column the value *psk* is specified.

Possible values:

- Alphanumeric ASCII character string with 0..128 characters excluding double-quote and new line characters
  The device also lets you generate pre-shared secrets as hexadecimal or Base64 encoded binary values. The device interprets a character sequence starting with `0x` as a sequence with hexadecimal digits. Similarly, the device also interprets a character sequence starting with multiple zeros as Base64 encoded binary data.

IKE auth. cert. CA

Specifies the name of the Certification Authority (CA) which issued the digital certificate. The device uses this digital certificate for signature verification of the local and remote certificates. The prerequisite is that in the *Authentication* column the value *individualx509* is specified.

Possible values:

- Alphanumeric ASCII character string with 1..128 characters

IKE auth. cert. local

Specifies the file name of the digital certificate the local device uses. The device uses this digital certificate for authentication of the local peer on the remote side.

Possible values:

- Alphanumeric ASCII character string with 1..128 characters
  The behavior depends on the value you specify in the *Authentication* column:
  - *individualx509*
    The digital certificate binds the identity of the local peer to the specified public key signed by the Certification Authority (CA) specified in the *IKE auth. cert. CA* column.
  - *pkcs12*
    The digital certificate in the PKCS bundle binds the identity of the local peer to the specified public key. The device performs this check independently of the digital certificate displayed in the *IKE auth. cert. CA* column.

IKE auth. cert. remote

Specifies the file name of the digital certificate the remote device uses. The device uses this digital certificate for authentication of the remote peer on the local side. This digital certificate binds the identity of the remote peer to the specified public key. The prerequisite is that in the *Authentication* column the value `individualx509` is specified.

Possible values:

- Alphanumeric ASCII character string with 0..128 characters
  The value is optional, because the remote peer typically sends the digital certificate and the device only checks the validity of the digital certificate.

Encrypted private key

Specifies the file name for the private key.

Prerequisites:

- In the *Authentication* column, the value `individualx509` is specified.
- The key saved in the device is encrypted with a passphrase.

The key requires that, in the *Encrypted key/PKCS12 passphrase* column, you specify the passphrase. The device considers the key and the digital certificate unmatched until the key is decrypted.

Possible values:

- Alphanumeric ASCII character string with 0..128 characters

Encrypted key/PKCS12 passphrase

Specifies the passphrase that the device uses for decryption of the private key specified in the *Encrypted private key* column or `pkcs12` certificate container.

Possible values:

- Alphanumeric ASCII character string with 0..128 characters

IKE local identifier type

Specifies the type of local peer identifier that the device uses for the *IKE local ID* parameter.

Possible values:

- `default` (default setting)
  The behavior depends on the value you specify in the *Authentication* column:
  - `psk`
    The device uses the IP address specified in the *Local endpoint* column as the local identifier.
  - `individualx509` or `pkcs12`
    The device uses the distinguished name (DN) contained in the local *IKE auth. cert. local* certificate.
- `address`
  In the *IKE local ID* column, the device uses the IP address or the DNS hostname specified in the *Local endpoint* column.
- `id`
  The device identifies the value specified in the *IKE local ID* column as one of the following types:
  - An IPv4 address or a DNS hostname
  - A key identifier which specifies the data that the device uses to pass vendor-specific information. The device uses the information to identify which pre-shared key it uses for aggressive mode authentication during negotiations.
  - An FQDN web address, for example, `foo.bar.com`

- An email address
- The *ASN.1 X.500 Distinguished Name (DN)* contained within the *IKE auth. cert. remote* column. The local and remote devices exchange their digital certificates to establish the Security Association (SA).

IKE local ID

Specifies the local peer identifier that the device sends to the remote device in the ID payload during phase 1 negotiations. The device uses the ID payload to identify the *Initiator* of the Security Association (SA). The *Responder* uses the identity to determine the correct host system policy requirement for the Security Association (SA).

The formats for this parameter depend on the type specified in the *IKE local identifier type* column.

Possible values:

- `<empty>` (default setting)
  If in the *IKE local identifier type* column, you specify the value `id`, then specify the value using one of the following options:
  - An IPv4 address or a DNS hostname
  - A previously specified key identifier, specifying data that the device uses to pass vendor-specific information.
  - An FQDN web address, for example, `foo.bar.com`
  - An email address
  - An X.500 distinguished name
    Refer to the following syntax as an example when adding the item:
    `CN = XY-D, C = DE,L = NT, ST = BW, O = COMPANY, OU = DEV, E = testuser@company.com`

Remote identifier type

Specifies the type of remote peer identifier that the device uses for the *Remote ID* parameter.

Possible values:

- *any* (default setting)
  The device accepts every received remote identifier without further verification.
- *address*
  In the *Remote ID* column, the device uses the IP address or the DNS hostname specified in the *Remote endpoint* column.
- *id*
  The device identifies the value specified in the *Remote ID* column as one of the following types:
  - An IPv4 address or a DNS hostname
  - A key identifier which specifies the data that the device uses to pass vendor-specific information. The device uses the information to identify which pre-shared key it uses for aggressive mode authentication during phase 1 negotiations.
  - An FQDN web address, for example, `foo.bar.com`
  - An email address
  - The *ASN.1 X.500 Distinguished Name (DN)* contained within the *IKE auth. cert. remote* column. The local and remote devices exchange their digital certificates to establish the Security Association (SA).

Remote ID

Specifies the remote peer identifier which the device compares with the value in the ID payload during phase 1 negotiations. The device uses the ID payload to identify the *Initiator* of the Security Association (SA). The *Responder* uses the identity to determine the correct host system policy requirement for the Security Association (SA).

The formats for this parameter depend on the type specified in the *Remote identifier type* column.

Possible values:

- `<empty>` (default setting)
  If in the *Remote identifier type* column, you specify the value `id`, then specify the value using one of the following options:
  - An IPv4 address or a DNS hostname
  - A previously specified key identifier, specifying data that the device uses to pass vendor-specific information.
  - An FQDN web address, for example, `foo.bar.com`
  - An email address
  - An X.500 distinguished name
    Refer to the following syntax as an example when adding the item:
    `CN = XY-D, C = DE,L = NT, ST = BW, O = COMPANY, OU = DEV, E = testuser@company.com`

IKE key agreement

Specifies which Diffie-Hellman (DH) key agreement algorithm the device uses for establishing the IKE-SA session key.

Possible values:

- `any`
  The device accepts every algorithm when specified as the *Responder*.
- `modp1024` (default setting)
  The value represents an RSA algorithm with 1024 bits modulus which is DH Group 2.
- `modp1536`
  The value represents an RSA algorithm with 1536 bits modulus which is DH Group 5.
- `modp2048`
  The value represents an RSA algorithm with 2048 bits modulus which is DH Group 14.
- `modp3072`
  The value represents an RSA algorithm with 3072 bits modulus which is DH Group 15.
- `modp4096`
  The value represents an RSA algorithm with 4096 bits modulus which is DH Group 16.

IKE integrity (MAC)

Specifies which IKE Integrity Message Authentication Code (MAC) algorithm the device uses. To help keep the information on the VPN secure, the Hash-based Message Authentication Code (HMAC) process in the sending device mixes (hashes) the message data with a shared secret key. The receiving device mixes the results (hash value) with the secret key again, and then applies the hash function a second time.

Possible values:

- `any`
  When you specify the device as the *Responder*, the device accepts any algorithm. When you specify the device as the *Initiator*, the device uses various pre-defined algorithms.
- `hmacmd5`
  The device uses the Message Digest Algorithm 5 (MD5) for the hash function calculation.
- `hmacsha1` (default setting)
  The device uses the Secure Hash Algorithm version 1 (SHA-1) for the hash function calculation.
- `hmacsha256`
  The device uses SHA-256 (part of the version 2 family) for the hash function calculation which the device computes with 32 bit words.

- *hmacsha384*
  The device uses SHA-384 (part of the version 2 family) for hash function calculation which the device computes using a shorter version of SHA-512.
- *hmacsha512*
  The device uses SHA-512 (part of the version 2 family) for hash function calculation which the device computes with 64 bit words.

Note:
We recommend to use the setting *hmacsha256* or higher.

IKE encryption

Specifies the IKE encryption algorithm that the device uses.

Possible values:

- *any*
  When you specify the device as the *Responder*, the device accepts any algorithm. When you specify the device as the *Initiator*, the device uses various pre-defined algorithms.
- *des*
  The device uses the Data Encryption Standard (DES) block cipher for encryption of message data with a 56 bit key.
- *des3*
  The device uses the Triple DES block cipher for encryption of message data which applies the 56 bit key, from DES, 3 times to each block.
- *aes128* (default setting)
  The device uses the Advanced Encryption Standard (AES) with a block size of 128 bits, and a key length of 128 key bits.
- *aes192*
  The device uses the AES with a block size of 128 bits, and a key length of 192 key bits.
- *aes256*
  The device uses the AES with a block size of 128 bits, and a key length of 256 key bits.

Note:
We recommend to use the setting *aes128* or higher.

Local endpoint

Specifies the hostname or IP address of the local IPsec VPN tunnel endpoint.

Possible values:

- any (default setting)
  The device uses the IP address of the interface the device uses to forward data to the remote endpoint.
- Valid IPv4 address and netmask in CIDR notation
- hostname
  Alphanumeric ASCII character string with 1..128 characters

Remote endpoint

Specifies the hostname or IP address of the remote IPsec VPN tunnel endpoint.

Possible values:

- `any` (default setting)
  The device accepts any IP address when establishing an IKE-SA as a VPN *Responder*.
- Valid IPv4 address and netmask in CIDR notation
  If you specify that the device is a *Responder* for this VPN tunnel, then the device accepts a network in CIDR notation, during IKE-SA establishment.
- hostname
  Alphanumeric ASCII character string with 1..128 characters

Re-authentication

Activates/deactivates peer re-authentication after an IKE-SA re-key. If in the *Version* column, you specify the value *ikev1*, then the device constantly re-authenticates the VPN tunnel, even when you unmark the checkbox.

Possible values:

- `marked`
  The device generates a new IKE-SA and attempts to regenerate the IPsec SAs.
- `unmarked` (default setting)
  When you use the IKEv2 protocol, the device re-keys the VPN tunnel and retains the IPsec SAs.

IPsec key agreement

Specifies which Diffie-Hellman key agreement algorithm the device uses for establishing the IPsec-SA session key. If the *Perfect Forward Secrecy (PFS)* function is enabled and a compromise of a single key occurs, then the integrity remains for subsequently generated keys.

Possible values:

- *any*
  When you specify the device as the *Responder*, the device accepts any algorithm. When you specify the device as the *Initiator*, the device uses various pre-defined algorithms.
- *modp1024* (default setting)
  The value represents an Rivest, Shamir, and Adleman (RSA) algorithm with 1024 bits modulus. This value is Diffie-Hellman (DH) Group 2.
- *modp1536*
  The value represents an RSA algorithm with 1536 bits modulus which is DH Group 5.
- *modp2048*
  The value represents an RSA algorithm with 2048 bits modulus which is DH Group 14.
- *modp3072*
  The value represents an RSA algorithm with 3072 bits modulus which is DH Group 15.
- *modp4096*
  The value represents an RSA algorithm with 4096 bits modulus which is DH Group 16.
- *none*
  The device disables the *PFS* function. Disabling the *PFS* function is considered a confidentiality violation and therefore a security risk.

IPsec integrity (MAC)

Specifies which IPsec Integrity MAC algorithm the device uses for the instance. To help keep the information on the VPN secure, the Hash-based Message Authentication Code (HMAC) process in the sending device mixes (hashes) the message data with a shared secret key. The receiving device mixes the results (hash value) with the secret key again, and then applies the hash function a second time.

Possible values:

- *any*
  When you specify the device as the *Responder*, the device accepts any algorithm. When you specify the device as the *Initiator*, the device uses various pre-defined algorithms.
- *hmacmd5*
  The device uses the Message Digest Algorithm 5 (MD5) for the hash function calculation.
- *hmacsha1* (default setting)
  The device uses the Secure Hash Algorithm version 1 (SHA-1) for the hash function calculation.
- *hmacsha256*
  The device uses SHA-256 (part of the version 2 family) for the hash function calculation which the device computes with 32 bit words.
- *hmacsha384*
  The device uses SHA-384 (part of the version 2 family) for hash function calculation which the device computes using a shorter version of SHA-512.
- *hmacsha512*
  The device uses SHA-512 (part of the version 2 family) for hash function calculation which the device computes with 64 bit words.

Note:
We recommend to use the setting *hmacsha256* or higher.

IPsec encryption

Specifies the IPsec encryption algorithm that the device uses.

Possible values:

- *any*
  When you specify the device as the *Responder*, the device accepts any algorithm. When you specify the device as the *Initiator*, the device uses various pre-defined algorithms.
- *des*
  The device uses the Data Encryption Standard (DES) block cipher for encryption of message data with a 56 bit key.
- *des3*
  The device uses the Triple DES block cipher for encryption of message data which applies the 56 bit key, from DES, 3 times to each block.
- *aes128* (default setting)
  The device uses the Advanced Encryption Standard (AES) with a block size of 128 bits, and a key length of 128 key bits.
- *aes192*
  The device uses the AES with a block size of 128 bits, and a key length of 192 key bits.
- *aes256*
  The device uses the AES with a block size of 128 bits, and a key length of 256 key bits.
- *aes128ctr*
  AES-CTR with 128 key bits.
- *aes192ctr*
  AES-CTR with 192 key bits.

- *aes256ctr*
  AES-CTR with 256 key bits.
- *aes128gcm64*
  The device uses the AES-Galois/Counter Mode (GCM) with a 64 bit Integrity Check Value (ICV) and 128 key bits.
- *aes128gcm96*
  AES-GCM with a 96 bit ICV and 128 key bits.
- *aes128gcm128*
  AES-GCM with a 128 bit ICV and 128 key bits.
- *aes192gcm64*
  AES-GCM with a 64 bit ICV and 192 key bits.
- *aes192gcm96*
  AES-GCM with a 96 bit ICV and 192 key bits.
- *aes192gcm128*
  AES-GCM with a 128 bit ICV and 192 key bits.
- *aes256gcm64*
  AES-GCM with a 64 bit ICV and 256 key bits.
- *aes256gcm96*
  AES-GCM with a 96 bit ICV and 256 key bits.
- *aes256gcm128*
  AES-GCM with a 128 bit ICV and 256 key bits.

Note:
We recommend to use the setting *aes128* or higher.

IPsec lifetime [s]

Specifies the lifetime, in seconds, of the IPsec security association between 2 network devices to support secure communication. The devices establish a security association after exchanging a set of pre-defined keys.

Possible values:

- `300..28800` (default setting: `3600`)
  The default setting is one hour. The maximum setting is 8 hours.

Margin time [s]

Specifies the period in seconds, before *IKE lifetime [s]* and *IPsec lifetime [s]* expire, after which the device attempts to negotiate a new key.

Possible values:

- `1..1800` (default setting: `150`)
  The default setting is equal to 2.5 minutes. The maximum value is half an hour.

Log informational entries

Activates/deactivates event log entries for debugging proposes only.

Possible values:

- `marked`
  The device receives and processes the informational messages for this VPN tunnel, and enters the message in the event log.
- `unmarked` (default setting)
  The device receives and processes the informational messages for this connection, without an event log entry.

Log unhandled messages

Activates/deactivates message handling for messages unknown to strongSwan for debugging proposes only.

Possible values:

- `marked`
  The device enters the non-strongSwan messages received for this connection, in the event log.
- `unmarked` (default setting)
  The device ignores the non-strongSwan messages received for this connection.

[Wizard: VPN configuration]

The *Wizard* window lets you set up a VPN tunnel. The device also lets you add or change a VPN tunnel directly in the dialog.

The *Wizard* window guides you through the following steps:
- Create or select entry
- Authentication
- Endpoint and traffic selectors
- Advanced configuration

Create or select entry

VPN

Displays the existing VPN tunnels setup in the device. Select an item to continue. As an alternative, specify a VPN tunnel in the *VPN index* and *VPN description* fields.

VPN index

Specifies the index number of the VPN tunnel.

Possible values:

- `1..256`

VPN description

Specifies the user-defined description for the VPN tunnel.

Possible values:

- Alphanumeric ASCII character string with 1..128 characters

Authentication

For each VPN tunnel you can specify the authentication methods using the following tabs:

- Authentication - Pre-shared key

Authentication - Pre-shared key

Pre-shared key

Specifies the pre-shared key. You can view the specified values by clicking the icon.

Possible values:

- Alphanumeric ASCII character string with 0..128 characters excluding double-quote and new line characters
  The device also lets you generate pre-shared secrets as hexadecimal or Base64 encoded binary values. The device interprets a character sequence starting with `0x` as sequence with hexadecimal digits. Similarly, the device also interprets a character sequence starting with multiple zeros as Base64 encoded binary data.

Authentication - X.509

IKE auth. cert. local

Specifies the name of the local peer identified in the digital certificate. The device uses this digital certificate for authentication of the local peer on the remote side. The digital certificate binds the identity of the local peer to the specified public key signed by the certification authority (CA) specified in the *IKE auth. cert. CA* field.

Possible values:

- Alphanumeric ASCII character string with 1..128 characters

IKE auth. cert. CA

Specifies the name of the Certification Authority (CA) which signed the digital certificate. The device uses this digital certificate for signature verification of the local and remote certificates.

Possible values:

- Alphanumeric ASCII character string with 1..128 characters

Encrypted private key

Specifies the file name for the private key. The prerequisite is that the key saved in the device is encrypted with a passphrase. The key requires that, in the *Encrypted key/PKCS12 passphrase* field, you specify the passphrase. The device considers the key and the digital certificate unmatched until the key is decrypted.

Possible values:

- Alphanumeric ASCII character string with 0..128 characters

Encrypted key/PKCS12 passphrase

Specifies the passphrase that the device uses for decryption of the private key specified in the *Encrypted private key* field. You can view the passphrase by clicking the icon.

Possible values:

- Alphanumeric ASCII character string with 0..128 characters

Authentication - PKCS 12

IKE auth. cert. local

Specifies the name of the local peer identified in the digital certificate. The device uses this digital certificate for authentication of the local peer on the remote side.

Possible values:

- Alphanumeric ASCII character string with 1..128 characters

Encrypted key/PKCS12 passphrase

Specifies the passphrase that the device uses for decryption of the private key specified in the *Encrypted private key* field. You can view the passphrase by clicking the icon.

Possible values:

- Alphanumeric ASCII character string with 0..128 characters

Endpoint and traffic selectors

Local endpoint

Specifies the hostname or IP address of the local IPsec VPN tunnel endpoint.

Possible values:

- `any` (default setting)
  The device uses the IP address of the interface the device uses to forward data to the remote endpoint.
- Valid IPv4 address and netmask in CIDR notation
- hostname
  Alphanumeric ASCII character string with 1..128 characters

Remote endpoint

Specifies the hostname or IP address of the remote IPsec VPN tunnel endpoint.

Possible values:

- `any` (default setting)
  The device accepts any IP address when establishing an IKE-SA as a VPN *Responder*.
- Valid IPv4 address and netmask in CIDR notation
  If you specify that the device is a *Responder* for this VPN tunnel, then the device accepts a network in CIDR notation, during IKE-SA establishment.
- hostname
  Alphanumeric ASCII character string with 1..128 characters

Add traffic selector

Traffic selector description

Specifies the user-defined description for the traffic selector.

Possible values:

- Alphanumeric ASCII character string with 1..128 characters

Source address (CIDR)

Specifies the IP address and netmask of the source host. When the device forwards packets containing this source IP address over a VPN tunnel, the device applies the settings specified in this field. Furthermore, the device applies the associated IPsec and IKE-SA settings, to every IP packet that the device forwards containing the source IP address in the range specified by the source IP and netmask.

Possible values:

- Valid IPv4 address and netmask in CIDR notation
- `any` (default setting)
  The device applies the settings to every packet that the device forwards.

Source restrictions

Specifies the optional source restrictions using names or numbers entered as `<protocol/port>`. The device sends only the type of data specified through the VPN tunnel.

Examples:

- `tcp/http` is equal to `6/80`
- `udp` is equal to `udp/any`
- `/53` is equal to `any/53`

Possible values:

- Alphanumeric ASCII character string with 1..32 characters
- `<empty>` (default setting)
  The device uses `any/any` as the restriction.

Destination address (CIDR)

Specifies the IP address and netmask of the destination. When the device forwards packets containing this destination IP address over a VPN tunnel, the device applies the settings specified in this field. Furthermore, the device applies the associated IPsec and IKE-SA settings to every IP packet that the device forwards containing the destination IP address in the range specified by the destination IP and netmask.

Possible values:

- Valid IPv4 address and netmask in CIDR notation
- `any` (default setting)
  The device applies the settings to every packet that the device forwards.

Destination restrictions

Specifies the optional destination restrictions using names or numbers entered as `<protocol/port>`. The device accepts only the type of data specified from the VPN tunnel.

Examples:

- `tcp/http` is equal to `6/80`
- `udp` is equal to `udp/any`
- `/53` is equal to `any/53`

Possible values:

- Alphanumeric ASCII character string with 1..32 characters
- `<empty>` (default setting)
  The device uses `any/any` as the restriction.

Deletes the corresponding table row.

Add

Adds a table row to the *Add traffic selector* table.

Advanced configuration

For each VPN tunnel you can specify the parameters using the following tabs:
- Advanced configuration - General

Advanced configuration - General

Margin time [s]

Specifies the time in seconds before the connection or the keying channel expires. Afterwards, the device attempts to negotiate a replacement.

Possible values:

- `1..1800` (default setting: `150`)
  The default setting is equal to 2.5 minutes. The maximum value is half an hour.

Advanced configuration - IKE/Key-exchange

Version

Specifies the version of the IKE protocol for the VPN connection.

Possible values:

- *`auto`* (default setting)
  The VPN starts with protocol IKEv2 as the *Initiator* and accepts IKEv1/v2 as the *Responder*.
- *`ikev1`*
  The VPN starts with the IKEv1 (ISAKMP) protocol.
- *`ikev2`*
  The VPN starts with the IKEv2 protocol.

Startup

Specifies if the device starts this instance as a *Responder* or *Initiator*.

Possible values:

- *`initiator`*
  The device starts a key exchange with the *Responder*.
- *`responder`* (default setting)
  The device waits for the *Initiator* to start the key exchange and parameter negotiation.
  If the remote peer sends data packets to a specific selector, then the device attempts to establish the connection as the *Responder*. Establishing a connection as a *Responder* depends upon other settings for this connection. For example, if you specify in the *Remote endpoint* field the value `any`, then the device prevents the remote device from initiating the connection.

IKEv1 DPD timeout [s]

Specifies the timeout, in seconds, before the local peer declares the remote peer dead, if the remote peer is unresponsive.

The device supports the *IKEv1 DPD timeout [s]* function using IKEv1.

Possible values:

- `0`
  Deactivates the function.
- `1..86400 (24 h)` (default setting: `120`)

IKE lifetime [s]

Specifies the lifetime, in seconds, of the IKE security association between two network devices to support secure communication. The devices establish a security association after exchanging a set of pre-defined keys.

Possible values:

- `300..86400` (default setting: `28800`)
  The default setting is 8 hours. The maximum setting is 24 hours.

IKE local identifier type

Specifies the type of local peer identifier that the device uses for the *IKE local ID* parameter.

Possible values:

- *default* (default setting)
  The behavior depends on the value you specify in the following authentication methods:
  - *Pre-shared key*
    The device uses the IP address specified in the *Local endpoint* field as the local identifier. You find the *Local endpoint* field in section “Endpoint and traffic selectors” on page 288.
  - *X.509* or *PKCS 12*
    The device uses the distinguished name (DN) contained in the local *IKE auth. cert. local* certificate.
- *address*
  In the *IKE local ID* field, the device uses the IP address or the DNS hostname specified in the *Local endpoint* field. You find the *Local endpoint* field in section “Endpoint and traffic selectors” on page 288.
- *id*
  The device identifies the value specified in the *IKE local ID* field as one of the following types:
  - An IPv4 address or a DNS hostname
  - A key identifier which specifies the data that the device uses to pass vendor-specific information. The device uses the information to identify which pre-shared key it uses for aggressive mode authentication during negotiations.
  - An FQDN web address, for example, `foo.bar.com`
  - An email address
  - The *ASN.1 X.500 Distinguished Name (DN)* contained within the *IKE auth. cert. remote* field. The local and remote devices exchange their digital certificates to establish the Security Association (SA).

IKE local ID

Specifies the local peer identifier that the device sends to the remote device in the ID payload during phase 1 negotiations. The device uses the ID payload to identify the *Initiator* of the Security Association (SA). The *Responder* uses the identity to determine the correct host system policy requirement for the Security Association (SA).

The formats for this parameter depend on the type specified in the *IKE local identifier type* field.

Possible values:

- `<empty>` (default setting)
- If in the *IKE local identifier type* field, you specify the value `id`, then specify the value using one of the following options:
  - An IPv4 address or a DNS hostname
  - A previously specified key identifier, specifying data that the device uses to pass vendor-specific information.
  - An FQDN web address, for example, `foo.bar.com`
  - An email address
  - An X.500 distinguished name
    Refer to the following syntax as an example when adding the item:
    `CN = XY-D, C = DE,L = NT, ST = BW, O = COMPANY, OU = DEV, E = testuser@example.com`

Remote identifier type

Specifies the type of remote peer identifier that the device uses for the *Remote ID* parameter.

Possible values:

- `any` (default setting)
  The device accepts every received remote identifier without further verification.
- `address`
  In the *Remote ID* field, the device uses the IP address or the DNS hostname specified in the *Remote endpoint* field. You find the *Remote endpoint* field in section "Endpoint and traffic selectors" on page 288.
- `id`
  The device identifies the value specified in the *Remote ID* field as one of the following types:
  - An IPv4 address or a DNS hostname
  - A key identifier which specifies the data that the device uses to pass vendor-specific information. The device uses the information to identify which pre-shared key it uses for aggressive mode authentication during negotiations.
  - An FQDN web address, for example, `foo.bar.com`
  - An email address
  - The *ASN.1 X.500 Distinguished Name (DN)* contained within the *IKE auth. cert. remote* field. The local and remote devices exchange their digital certificates to establish the Security Association (SA).

Remote ID

Specifies the remote peer identifier which the device compares with the value in the ID payload during phase 1 negotiations. The device uses the ID payload to identify the *Initiator* of the Security Association (SA). The *Responder* uses the identity to determine the correct host system policy requirement for the Security Association (SA).

The formats for this parameter depend on the type specified in the *Remote identifier type* field.

Possible values:

- `<empty>` (default setting)
- If in the *Remote identifier type* field, you specify the value `id`, then specify the value using one of the following options:
  - An IPv4 address or a DNS hostname
  - A previously specified key identifier, specifying data that the device uses to pass vendor-specific information.
  - An FQDN web address, for example, `foo.bar.com`

- An email address
- An X.500 distinguished name
  Refer to the following syntax as an example when adding the item:
  `CN = XY-D, C = DE,L = NT, ST = BW, O = COMPANY, OU = DEV, E = testuser@example.com`

IKE exchange mode

Specifies the use of the phase 1 exchange mode for IKEv1.

The purpose of IKE phase 1 is to establish a secure authenticated communication channel. The device uses the Diffie-Hellman (DH) key exchange algorithm to generate a shared secret key. The device then uses the shared secret key to further encrypt IKE communications.

Possible values:

- *main* (default setting)
  The main mode for phase 1 provides identity protection.
- *aggressive*
  You use the aggressive mode to reduce round trips.

IKE key agreement

Specifies which Diffie-Hellman (DH) key agreement algorithm the device uses for establishing the IKE-SA session key.

Possible values:

- *any*
  The device accepts every algorithm when specified as the *Responder*.
- *modp1024* (default setting)
  The value represents an RSA algorithm with 1024 bits modulus which is DH Group 2.
- *modp1536*
  The value represents an RSA algorithm with 1536 bits modulus which is DH Group 5.
- *modp2048*
  The value represents an RSA algorithm with 2048 bits modulus which is DH Group 14.
- *modp3072*
  The value represents an RSA algorithm with 3072 bits modulus which is DH Group 15.
- *modp4096*
  The value represents an RSA algorithm with 4096 bits modulus which is DH Group 16.

IKE integrity (MAC)

Specifies which IKE Integrity Message Authentication Code (MAC) algorithm the device uses. To help keep the information on the VPN secure, the Hash-based Message Authentication Code (HMAC) process in the sending device mixes (hashes) the message data with a shared secret key. The receiving device mixes the results (hash value) with the secret key again, and then applies the hash function a second time.

Possible values:

- *any*
  When you specify the device as the *Responder*, the device accepts any algorithm. When you specify the device as the *Initiator*, the device uses various pre-defined algorithms.
- *hmacmd5*
  The device uses the Message Digest Algorithm 5 (MD5) for the hash function calculation.
- *hmacsha1* (default setting)
  The device uses the Secure Hash Algorithm version 1 (SHA-1) for the hash function calculation.

- *hmacsha256*
  The device uses SHA-256 (part of the version 2 family) for the hash function calculation which the device computes with 32 bit words.
- *hmacsha384*
  The device uses SHA-384 (part of the version 2 family) for hash function calculation which the device computes using a shorter version of SHA-512.
- *hmacsha512*
  The device uses SHA-512 (part of the version 2 family) for hash function calculation which the device computes with 64 bit words.

Note:
We recommend to use the setting *hmacsha256* or higher.

IKE encryption

Specifies the IKE encryption algorithm that the device uses.

Possible values:

- *any*
  When you specify the device as the *Responder*, the device accepts any algorithm. When you specify the device as the *Initiator*, the device uses various pre-defined algorithms.
- *des*
  The device uses the Data Encryption Standard (DES) block cipher for encryption of message data with a 56 bit key.
- *des3*
  The device uses the Triple DES block cipher for encryption of message data which applies the 56 bit key, from DES, 3 times to each block.
- *aes128* (default setting)
  The device uses the Advanced Encryption Standard (AES) with a block size of 128 bits, and a key length of 128 key bits.
- *aes192*
  The device uses the AES with a block size of 128 bits, and a key length of 192 key bits.
- *aes256*
  The device uses the AES with a block size of 128 bits, and a key length of 256 key bits.

Note:
We recommend to use the setting *aes128* or higher.

Advanced configuration - IPSec/Data-exchange

IPsec lifetime [s]

Specifies the lifetime, in seconds, of the IPsec security association between 2 network devices to support secure communication. The devices establish a security association after exchanging a set of pre-defined keys.

Possible values:

- *300..28800* (default setting: *3600*)
  The default setting is one hour. The maximum setting is 8 hours.

IPsec integrity (MAC)

Specifies which IPsec Integrity MAC algorithm the device uses for the instance. To help keep the information on the VPN secure, the Hash-based Message Authentication Code (HMAC) process in the sending device mixes (hashes) the message data with a shared secret key. The receiving device mixes the results (hash value) with the secret key again, and then applies the hash function a second time.

Possible values:

- *any*
  When you specify the device as the *Responder*, the device accepts any algorithm. When you specify the device as the *Initiator*, the device uses various pre-defined algorithms.
- *hmacmd5*
  The device uses the Message Digest Algorithm 5 (MD5) for the hash function calculation.
- *hmacsha1* (default setting)
  The device uses the Secure Hash Algorithm version 1 (SHA-1) for the hash function calculation.
- *hmacsha256*
  The device uses SHA-256 (part of the version 2 family) for the hash function calculation which the device computes with 32 bit words.
- *hmacsha384*
  The device uses SHA-384 (part of the version 2 family) for hash function calculation which the device computes using a shorter version of SHA-512.
- *hmacsha512*
  The device uses SHA-512 (part of the version 2 family) for hash function calculation which the device computes with 64 bit words.

Note:
We recommend to use the setting *hmacsha256* or higher.

IPsec encryption

Specifies the IPsec encryption algorithm that the device uses.

Possible values:

- *any*
  When you specify the device as the *Responder*, the device accepts any algorithm. When you specify the device as the *Initiator*, the device uses various pre-defined algorithms.
- *des*
  The device uses the Data Encryption Standard (DES) block cipher for encryption of message data with a 56 bit key.
- *des3*
  The device uses the Triple DES block cipher for encryption of message data which applies the 56 bit key, from DES, 3 times to each block.
- *aes128* (default setting)
  The device uses the Advanced Encryption Standard (AES) with a block size of 128 bits, and a key length of 128 key bits.
- *aes192*
  The device uses the AES with a block size of 128 bits, and a key length of 192 key bits.
- *aes256*
  The device uses the AES with a block size of 128 bits, and a key length of 256 key bits.
- *aes128ctr*
  AES-CTR with 128 key bits.
- *aes192ctr*
  AES-CTR with 192 key bits.

- *aes256ctr*
  AES-CTR with 256 key bits.
- *aes128gcm64*
  AES-GCM with a 64 bit ICV and 128 key bits.
- *aes128gcm96*
  AES-GCM with a 96 bit ICV and 128 key bits.
- *aes128gcm128*
  AES-GCM with a 128 bit ICV and 128 key bits.
- *aes192gcm64*
  AES-GCM with a 64 bit ICV and 192 key bits.
- *aes192gcm96*
  AES-GCM with a 96 bit ICV and 192 key bits.
- *aes192gcm128*
  AES-GCM with a 128 bit ICV and 192 key bits.
- *aes256gcm64*
  AES-GCM with a 64 bit ICV and 256 key bits.
- *aes256gcm96*
  AES-GCM with a 96 bit ICV and 256 key bits.
- *aes256gcm128*
  AES-GCM with a 128 bit ICV and 256 key bits.

Note:
We recommend to use the setting *aes128* or higher.

IPsec key agreement

Specifies which Diffie-Hellman key agreement algorithm the device uses for establishing the IPsec-SA session key. If the *Perfect Forward Secrecy (PFS)* function is enabled and a compromise of a single key occurs, then the integrity remains for subsequently generated keys.

Possible values:

- *any*
  When you specify the device as the *Responder*, the device accepts any algorithm. When you specify the device as the *Initiator*, the device uses various pre-defined algorithms.
- *modp1024* (default setting)
  The value represents an Rivest-Shamir-Adleman (RSA) algorithm with 1024 bits modulus. This value is Diffie Hellman (DH) Group 2.
- *modp1536*
  The value represents an RSA algorithm with 1536 bits modulus which is DH Group 5.
- *modp2048*
  The value represents an RSA algorithm with 2048 bits modulus which is DH Group 14.
- *modp3072*
  The value represents an RSA algorithm with 3072 bits modulus which is DH Group 15.
- *modp4096*
  The value represents an RSA algorithm with 4096 bits modulus which is DH Group 16.
- *none*
  The device disables the *PFS* function. Disabling the *PFS* function is considered a confidentiality violation and therefore a security risk.

6 Switching

The menu contains the following dialogs:

- Switching Global
- Rate Limiter
- Filter for MAC Addresses
- QoS/Priority
- VLAN

6.1 Switching Global

[Switching > Global]

This dialog lets you specify the following settings:

- Change the Aging time of the MAC address table (forwarding database) entries
- Enable the flow control in the device

If a large number of data packets are received in the priority queue of a port at the same time, then this can cause the port memory to overflow. This happens, for example, when the device receives data on a Gigabit port and forwards it to a port with a lower bandwidth. The device discards superfluous data packets.

The flow control mechanism defined in IEEE 802.3 helps ensure that no data packets are lost due to a buffer overflow on a port. Shortly before the buffer memory of a port 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 connected devices then stop sending data packets for the duration of the signaling. On an uplink port, this can possibly cause undesired sending interruptions in the higher-level network segment (“wandering backpressure”). The flow control mechanism thus lowers the network to the bandwidth that the slowest device in the network can process.

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 MAC address table (forwarding database).

You find the MAC address table (forwarding database) 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.

6.2 Rate Limiter

[Switching > Rate Limiter]

The device lets you limit the amount of data packets on the ports to help provide stable operation even with a large data volume. If the amount of data packets on a port exceed the threshold value, then the device discards the excess data packets on this port.

The rate limiter function operates only on Layer 2, and is used to limit the effects of storms of data packets that flood the device (typically Broadcasts).

The rate limiter function ignores protocol information on higher layers, such as IP or TCP.

The dialog contains the following tabs:
- [Ingress]

[Ingress]

In this tab you enable the *Rate Limiter* function. The threshold value specifies the maximum amount of data packets the port receives. If the amount of data packets on a port exceed the specified threshold value, then the device discards the excess data packets on this port.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.

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 *Unit* column, then enter a percentage value from `1` to `100`.
  - If you select the value *`pps`* in the *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 *Unit* column, then enter a percentage value from `0` to `100`.
  - If you select the value *`pps`* in the *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 *Unit* column, then enter a percentage value from `0` to `100`.
  - If you select the value *`pps`* in the *Unit* column, then enter an absolute value for the data rate.

6.3 Filter for MAC Addresses

[Switching > Filter for MAC Addresses]

This dialog lets you display and edit address filters for the MAC address table (forwarding database). Address filters specify the way the data packets are forwarded in the device based on the destination MAC address.

Each table row represents one filter. The device automatically sets up the filters. The device lets you set up additional filters manually.

The device forwards the data packets as follows:

- When the table contains the destination address of a data packet, the device forwards the data packet from the receiving port to the port specified in the table row.
- When there is no table row for the destination address, the device forwards the data packet from the receiving port to every other port.

Table

To delete the learned MAC addresses from the MAC address table (forwarding database), click in the *Basic Settings > Restart* dialog the *Clear FDB* button.

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the *Create* window to add a table row.

- In the *MAC address* field, you specify the destination MAC address.
- In the *VLAN ID* field, you specify the VLAN ID.
- In the list field, you select the ports.
  - If the destination MAC address is a unicast address, select exactly one port.
  - If the destination MAC address is a multicast or broadcast address, select one or more ports.
  - Do not select a port to add a *Discard* filter. The device discards data packets with the destination MAC address specified in the table row.

Remove

Removes the selected table row.

Clear FDB

Deletes the MAC addresses from the forwarding table that have the value *Learned* in the *Status* column.

Address

Displays the destination MAC address to which the table row relates.

VLAN ID

Displays the ID of the VLAN to which the table row relates.

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.
- *Mgmt*
  MAC address of the device. The address filter is protected against changes.
- *Permanent*
  Address filter set up manually. The address filter stays set up permanently.

<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 has automatically set up the filter based on received data packets.
- `unicast static`
  The port transmits data packets to the destination address. A user has set up the filter.
- `multicast static`
  The port transmits data packets to the destination address. A user has set up the filter.

6.4 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

6.4.1 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.

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).

6.4.2 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

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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 forwards the data packet depending on the value specified in the *Trust mode* column.

Possible values:

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

6.4.3 802.1D/p Mapping

[Switching > QoS/Priority > 802.1D/p Mapping]

The device forwards data packets with a VLAN tag according to the contained QoS/priority information with a higher or lower priority.

In this dialog, you see which VLAN priority is assigned to which *traffic class*. You assign the *traffic classes* to the priority queues of the ports.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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.

Default assignment of the VLAN priority to traffic classes

VLAN Priority	Traffic class	Content description according to IEEE 802.1D
`0`	2	`Best Effort` Normal data without prioritizing
`1`	0	`Background` Non-time-sensitive data and background services
`2`	1	`Standard` Normal data
`3`	3	`Excellent Effort` Crucial data
`4`	4	`Controlled Load` Time-sensitive data with a high priority

VLAN Priority	Traffic class	Content description according to IEEE 802.1D
5	5	Video Video transmission with delays and jitter <100 ms
6	6	Voice Voice transmission with delays and jitter <10 ms
7	7	Network Control Data for network management and redundancy mechanisms

6.5 VLAN

[Switching > VLAN]

With VLAN (Virtual Local Area Network) you distribute the data packets in the physical network to logical subnets. This provides you with the following advantages:

- High flexibility
  - With VLAN you distribute the data packets 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 packets 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 IEEE 802.1Q. The VLAN tagging in the data packet indicates the VLAN to which the data packet belongs.

The device forwards the tagged data packets of a VLAN only on ports that are assigned to the same VLAN. This reduces the network load.

The device learns the MAC addresses for every VLAN separately (independent VLAN learning).

The menu contains the following dialogs:

- VLAN Global
- VLAN Configuration
- VLAN Port

6.5.1 VLAN Global

[Switching > VLAN > Global]

This dialog lets you view general VLAN parameters for the device.

Configuration

Buttons

Reset VLAN settings

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 for the device management in the *Basic Settings > Network > Global* dialog.

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 set up in the device.

See the *Switching > VLAN > Configuration* dialog.

The VLAN 1 is permanently set up in the device.

6.5.2 VLAN Configuration

[Switching > VLAN > Configuration]

In this dialog, you manage the VLANs. To set up a VLAN, add a further table row. 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 sets up dynamic VLANs:
  – *Routing*: The device sets up a VLAN for every router interface.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons


Add

Opens the *Create* window to add a table row.

In the *VLAN ID* field, you specify the VLAN ID.


Remove

Removes the selected table row.

VLAN ID

ID of the VLAN.

The device supports up to 64 VLANs simultaneously set up.

Possible values:

▶ `1..4042`

Status

Displays how the VLAN is set up.

Possible values:

▶ *other*
VLAN 1

▶ *permanent*
VLAN set up by the user.
If you save the settings in the non-volatile memory, then the VLANs with this setting remain set up after a restart.

Name

Specifies the name of the VLAN.

Possible values:

- Alphanumeric ASCII character string with 0..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 has automatically set up the entry based on the *GVRP* or *MVRP* function.
- `F` = Forbidden
  The port is not a member of the VLAN and does not transmit data packets of this VLAN.
- `U` = Untagged (default setting for VLAN 1)
  The port is a member of the VLAN and transmits the data packets without a VLAN tag. Use this setting if the connected device does not evaluate any VLAN tags, for example on end ports.
- `LU` = Untagged Learned
  The port is a member of the VLAN and transmits the data packets without a VLAN tag.
  The device has automatically set up the entry 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, connections to the device management interrupt when you apply the changes. Then, access to the device management is only possible using the Command Line Interface through the serial connection.

6.5.3 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 forwards data packets and one of the following situations occurs:
- The port receives data packets without a VLAN tagging.
- The port receives data packets with VLAN priority information (VLAN ID `0`, priority tagged).
- The VLAN ID in the tag of the data packet differs from the VLAN ID of the port.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.

Port-VLAN ID

Specifies the VLAN ID which the device assigns to data packets received without a VLAN tag.

Prerequisites:
- In the *Acceptable packet types* column, the value *admitAll* is specified.

Possible values:

▶ `1..4042` (default setting: `1`)
A VLAN you set up.

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` (default setting)
  The ingress filtering is active.
  The device compares the VLAN ID in the data packet with the VLANs of which the port is a member. See the *Switching > VLAN > Configuration* dialog. If the VLAN ID in the data packet matches one of these VLANs, then the device forwards the data packet. Otherwise, the device discards the data packet.
- `unmarked`
  The ingress filtering is inactive.
  The device forwards received data packets without comparing the VLAN ID. Thus, the device also forwards data packets in VLANs in which the port is not a member.

7 Routing

The menu contains the following dialogs:

- Routing Global
- Routing Interfaces
- ARP
- Open Shortest Path First
- Routing Table
- L3 Relay
- Loopback Interface
- L3-Redundancy
- NAT

7.1 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:

- *Source Routing*
  With source routing, the data packet contains the routing information and overwrites the settings in the router with it.
- *ICMP Redirects*
  ICMP redirect data packets are able to modify the routing table. The device generally ignores received ICMP redirect data packets. The settings in the *Routing > Interfaces > Configuration* dialog, column *ICMP redirects*, have an effect only on the sending of ICMP redirect data packets.

In accordance with RFC 2644, the device does not exchange any broadcast data packets from external networks in a local network. This behavior supports you in protecting the devices in the local network against overloading, for example due to so-called smurf attacks.

This dialog lets you enable the routing function in the device and to specify further settings.

Operation

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.

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).
- An *ICMP echo reply* packet is the response to an *ICMP echo request* packet 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 responds to a received *ICMP echo request* packet with an *ICMP echo reply* packet.
- `unmarked`
  Responding to pings is inactive.

Send redirects

Activates/deactivates the sending of *ICMP Redirect* messages on the router interfaces.

Possible values:

- `marked` (default setting)
  The sending of *ICMP Redirect* messages is active.
  In the *Routing > Interfaces > Configuration* dialog, you have the option of individually activating the sending on every router interface. See the *ICMP redirects* function.
- `unmarked`
  The sending of *ICMP Redirect* messages is inactive.
  This setting helps prevent the multiplication of data packets, if both hardware and software functions of the device forward a copy of the same data packet.

Rate limit interval [ms]

Specifies the average minimum period in milliseconds between each *ICMP echo request* packet sent by the device. The device limits its *ICMP echo reply* packets to a number determined by a *Token bucket* algorithm.

Possible values:

- `0..2147483647 (2³¹-1)` (default setting: `1000`)
  The *Rate limit* is disabled.
- `10..2147483647 (2³¹-1)` (default setting: `1000`)
  - In periods without sending an ICMP packet, the device accumulates tokens to send bursts when necessary.
  - In the case of a burst, the interval is shorter than specified here.
  - The maximum allowed value of the transmission *Rate limit* is 100 data packets per 1000 ms.

Rate limit burst size

Displays the maximum number of ICMP packets, the device sends during a burst to each receiver.

Possible values:

▶ 6

Information

Default TTL

Displays the fixed TTL value 64 which the device adds to IP packets that the device management sends.

TTL (Time To Live, also known as “Hop Count”) identifies the maximum number of routing steps, which the sent *ICMP echo request* packet may traverse on its 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.

7.2 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

7.2.1 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 rows. To set up a VLAN-based router interface, use the *Wizard* window.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

 Add

Opens the *Create* window to add a table row. In the *VLAN ID* field, you specify the VLAN ID.

 Remove

Removes the selected table row.

 Wizard

Opens the *Wizard* window that helps you associate the ports with the address of one or more desired senders. See “[Wizard: Configure VLAN router interface]” on page 319.

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 device accepts the following characters:
  - `<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:

- *up*
  The port is enabled.
- *down*
  The port is disabled.

IP address

Specifies the IP address for the router interface.

The prerequisite is that the checkbox in the *DHCP client* column is unmarked.

Possible values:

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

Verify that the IP subnet of the router interface does not overlap with any subnet connected to another interface of the device:

- management port
- router interface
- loopback interface

Netmask

Specifies the netmask for the router interface.

The prerequisite is that the checkbox in the *DHCP client* column is unmarked.

Possible values:

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

Routing

Activates/deactivates the *Routing* function on the router interface.

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

Possible values:

- `marked`
  The *Routing* function is active.
  - With port-based routing, the device transforms the port into a router interface.
    Enabling the *Routing* function removes the port from the VLANs in which it was previously a member. Disabling the *Routing* function does not re-establish 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 are specified for the router interface.

DHCP client

Activates/deactivates the *DHCP client* function on the router interface.

Possible values:

- `marked` (default setting)
  The *DHCP client* function is active.
  The device requests the IP address for the particular router interface using DHCP.
  The device does not support the *DHCP* function on VLAN-based router interfaces.
- `unmarked`
  The *DHCP client* function is inactive.

Remaining lease time [s]

Displays the remaining time in seconds for which the IP address assigned by the DHCP server to the router interface is valid.

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.

MTU value

Specifies the maximum allowed size of IP packets on the router interface in bytes.

Possible values:

- `0`
  Restores the default value (`1500`).
- `68..1500` (default setting: `1500`)

ICMP unreachables

Displays if the sending of *ICMP Destination Unreachable* messages is active on the router interface.

Possible values:

- `marked`
  The router interface sends *ICMP Destination Unreachable* messages.

ICMP redirects

Displays if the sending of *ICMP Redirect* messages is active on the router interface.

Possible values:

- `marked`
  The router interface sends *ICMP Redirect* messages.
- `unmarked` (default setting)
  The router interface does not send *ICMP Redirect* messages.

[Wizard: Configure VLAN router interface]

This *Wizard* window lets you set up VLAN-based router interfaces.

The *Wizard* window guides you through the following steps:
- Create or select VLAN
- Setup VLAN

Create or select VLAN

VLAN ID

Displays the VLANs set up in the device. To continue, select an item from the list. As an alternative, specify a value in the *VLAN ID* field below.

VLAN ID

Specifies the ID of a VLAN. As an alternative, select an item in the *VLAN ID* overview above. You can also set up a VLAN in the *Switching > VLAN > Configuration* dialog.

Possible values:

- `1..4042`

Setup VLAN

VLAN ID

Displays the ID of the VLAN that you have specified in the preceding *Wizard* step.

Name

Specifies the name of the VLAN. This setting overwrites the setting specified for the port in the *Switching > VLAN > Configuration* dialog.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters (hexadecimal ASCII code `0x20..0x7E`) including space characters

<Port number>

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 sending the 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 sends the data packets without a VLAN tag.
  Use this setting if the connected device does not evaluate any VLAN tags, for example on ports to which an end device is directly connected.
- `unmarked`
  The port sends the data packets with a VLAN tag.

Port-VLAN ID

Specifies the VLAN ID which the device assigns to data packets received 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:

- A VLAN you set up (default setting: `1`)

Setup virtual router port

The device lets you specify up to 2 IP addresses (1 primary, 1 secondary) for a router interface and a total of up to 64 IP addresses.

When you assign a port to the router interface that already sends data packets to another VLAN, the device displays a message upon closing the *Wizard* window:

- If you click the *Yes* button, then the related ports send the data packets from now on only in the router VLAN.
  In the *Switching > VLAN > Configuration* dialog, the related ports in the table row of the router VLAN have the value `U` or `T`, in the table rows of other VLANs the value `-`.
- If you click the *No* button, then the related ports send the data packets in the router VLAN and other VLANs. This setting can cause undesired behavior and may also pose a security risk. Do not use this setting if you transmit data over untrusted networks.

Primary address

Address

Specifies the primary IP address for the router interface.

Possible values:

- Valid IPv4 address

Netmask

Specifies the primary netmask for the router interface.

Possible values:

- Valid IPv4 netmask

Secondary addresses

Address

Specifies a further IP address for the router interface (Multinetting).

Possible values:

- Valid IPv4 address

Note:
Specify an IP address which is different from the primary IP address of the router interface.

Netmask

Specifies the netmask for the secondary IP address.

Possible values:

- Valid IPv4 netmask

Add

Adds a VLAN-based router interface.

7.2.2 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 2 IP addresses (1 primary, 1 secondary) for a router interface and a total of up to 64 IP addresses.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the *Create* window to add another IP address to the router interface selected in the table.

- From the *Port* drop-down list, you select the port or VLAN to be assigned 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 does not overlap with any subnet connected to another interface of the device:

- management port
- router interface
- loopback interface

Remove

Removes the selected table row.

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.

7.3 ARP

[Routing > ARP]

Using the Address Resolution Protocol (ARP), the device learns the MAC address that belongs to an IP address.

The menu contains the following dialogs:

- ARP Global
- ARP Current
- ARP Static

7.3.1 ARP Global

[Routing > ARP > Global]

This dialog lets you set the ARP parameters and view statistical values.

Configuration

Aging time [s]

Specifies the average time in seconds, after which the device removes an entry from the ARP table. The device actually removes an entry after a randomly determined time in the range (0.5 to 1.5)× of the value defined here.

When there is data exchange with the associated device within this time period, the time measuring begins from the start again.

Possible values:

- `15..21600` (default setting: `1200`)

Response timeout [s]

Specifies the time in seconds, that the device waits for a response before the query is seen as a failure.

Possible values:

- `1..10` (default setting: `1`)

Retries

Specifies how many times the device repeats a failed query before it discards the query to this address.

Possible values:

- `0..10` (default setting: `4`)

Information

Current entries total

Displays the number of entries that the ARP table currently contains.

This includes:

- Addresses of the devices which are connected to the router interfaces. See the *Routing > ARP > Current* dialog.
- Addresses of the devices which are connected to the device management. See the *Diagnostics > System > ARP* dialog.

Entries (max.)

Displays how many entries the ARP table can contain at a maximum.

Total entry peaks

Displays how many entries the ARP table has already contained at a maximum.

To reset the counter to the value `0`, in the *Routing > ARP > Current* dialog, click the button.

Current static entries

Displays the current number of statically set-up entries in the ARP table. See the *Routing > ARP > Static* dialog.

Static entries (max.)

Displays the number of statically set-up entries the ARP table can contain at a maximum.

7.3.2 ARP Current

[Routing > ARP > Current]

This dialog lets you view the ARP table and delete the dynamically set-up entries.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

 Remove

Removes the selected table row.

 Clear ARP table

Deletes the dynamically set up addresses from the ARP 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 set-up entry.
  When no data packet was sent to or received from the associated device 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 set-up entry.

  When you remove the dynamically set-up addresses from the ARP table using the button, the entry remains.
- *local*
  Identifies the IP/MAC address assignment of the router interface.
- *invalid*
  Invalid entry.

7.3.3 ARP Static

[Routing > ARP > Static]

This dialog lets you add to the ARP table IP/MAC address assignments that you have specified yourself.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons


Remove

Removes the selected table row.


Wizard

Opens the *Wizard* window that helps you associate the ports with the address of one or more desired senders. See “[Wizard: ARP]” on page 330.

IP address

Displays the IP address of the static ARP entry.

MAC address

Displays the MAC address that the device assigns to the IP address when answering an ARP request.

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.

[Wizard: ARP]

The *Wizard* window lets you add the IP/MAC address assignments in the ARP table. The prerequisite is that at least one router interface is set up.

Edit ARP table

Perform the following steps:

- ☐ Specify the IP address and the associated MAC address.

  Note:
  Verify the MAC address carefully. Doing so can help protect the network against unauthorized devices that might perform a Man-in-the-Middle (MITM) attack.

- ☐ Insert the IP/MAC address assignment in the *Static entries* field. To do this, click the *Add* button.
- ☐ Close the *Wizard* window. To do this, click the *Finish* button.
- ☐ Specify the router interface in the *Port* column.
- ☐ Enable the IP/MAC address assignment. To do this, mark the checkbox in the *Active* column.

Static entries

Displays the static entries set-up. You can remove a static entry by clicking the ✕ icon.

IP address

Specifies the IP address of the static ARP entry.

Possible values:

- ▶ Valid IPv4 address

MAC address

Specifies the MAC address that the device assigns to the IP address when answering an ARP request.

Possible values:

- ▶ Valid MAC address

7.4 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) send 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

7.4.1 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 the *OSPF* function 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 (2³¹-1)`
  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 the *OSPF* function 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 the *OSPF* function.

Possible values:

- `0` (default setting)
  The *OSPF* function automatically assigns a cost of 20 for routes learned from external sources (static or directly connected).
- `1..16777214 (2²⁴-2)`

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. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
  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.

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`
  The router immediately begins the SPF calculation after receiving the *Topology Change* packet.
- `1..65535 (2¹⁶-1)` (default setting: `5`)

Hold time [s]

Specifies the minimum time, in seconds, between consecutive SPF calculations.

Possible values:

- `0..65535 (2¹⁶-1)` (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 time in seconds after entering the overflow state that a router attempts to leave the overflow state. When the router leaves the overflow state, the router sends new non-default AS-external-LSAs.

Possible values:

- `0..2147483647 (2³¹-1)` (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.

[Configuration]

This dialog lets you specify the following settings:
- the manner in which the device calculates the path costs
- how the *OSPF* function handles *default routes*
- the type of route the *OSPF* function 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.

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.

The *OSPF* function 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 set up 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 the *OSPF* function advertises when learned from other protocols.

Possible values:

- `0`
  The device uses the value specified in the *Default metric* field.
- `1..16777214 (2²⁴-2)`

Metric type

Displays the metric type of the *default route* which the *OSPF* function 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.

[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*.

The number of routes that the device learns through the *OSPF* function is limited to the size of the routing table.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Source

Displays the source protocol, from which the *OSPF* function redistributes routes. This object also acts as the identifier for the table row.

Activating a table row lets the device redistribute routes from the specific source protocol into OSPF.

Possible values:

- *connected*
  The router is directly connected to the route.
- *static*
  A network administrator has specified the route in the router.

Active

Activates/deactivates route redistribution from the source protocol into OSPF.

Possible values:

- `marked`
  Redistribution of routes learned from the source protocol is active.
- `unmarked` (default setting)
  OSPF route redistribution is inactive.

Metric

Specifies the metric value for routes redistributed from this protocol.

Possible values:

- `0` (default setting)
  The device uses the value specified in the *Default metric* field.
- `1..16777214 (2²⁴-2)`

Metric type

Specifies the route metric type which the *OSPF* function 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 the *OSPF* function.

When you set a route tag, the *OSPF* function 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 (2³²-1)` (default setting: `0`)

Subnets

Activates/deactivates subnet route redistribution into the *OSPF* function.

The *OSPF* function only redistributes classful routes into the OSPF domain. 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.

7.4.2 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 64 OSPF Areas.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the *Create* window to add a table row.

- In the *Area ID* field you specify the area ID for the new table row.
  Possible values:
  - Octet value displayed like an IPv4 address

Remove

Removes the selected table row.

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 7 AS 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. The *OSPF* function 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. The *OSPF* function 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.

7.4.3 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 adding 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 Stub Area. To do this, perform the following steps:
  - ☐ In the *Routing > OSPF > Areas* dialog, add a table row.
  - ☐ Change the value in the *Area type* column to *`stub area`*.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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 (2²⁴-1)` (default setting: `1`)
  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`
  The router does not import area summaries. The stub area relies entirely on the *default route*. This makes the *default route* a Totally Stub Area.
- `unmarked` (default setting)
  The router both summarizes and propagates summary LSAs into the stub area.

7.4.4 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 stream, 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 adding 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 an NSSA. To do this, perform the following steps:
  - ☐ In the *Routing > OSPF > Areas* dialog, add a table row.
  - ☐ Change the value in the *Area type* column to `nssa`.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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 generating *Type 7 external* LSAs for external routes.
- `unmarked`
  The NSSA ASBRs redistribute external routes into the NSSA.

Originate default info

Activates/deactivates generating *Type 7 default* LSAs.

The prerequisite is that the router is an NSSA ABR or ASBR.

Possible values:

- `marked`
  The router generates *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 (2²⁴-2)` (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, the *OSPF* function performs a translator election. When multiple candidates exist, the *OSPF* function 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* LSAs.
- *disabled*
  Another NSSA border router is translating *Type 7* LSAs into *Type 5* LSAs.

Translator stability interval [s]

Specifies the time in seconds after the router loses a translation election that it continues to translate *Type 7* LSAs into *Type 5* LSAs.

Possible values:

- `0..65535 (2¹⁶-1)` (default setting: `40`)

Translator events

Displays the number of translator status changes that have occurred since the last system startup.

Discontinuities in the value of this counter occur while the *OSPF* function is disabled and can occur during re-initialization of the management system.

Totally NSSA

Activates/deactivates importation of summary routes into the NSSA as *Type 3 summary* LSAs.

Possible values:

- `marked`
  The router suppresses summary route importation making the area a Totally NSSA.
- `unmarked` (default setting)
  The router imports summary routes into the NSSA as *Type 3 summary* LSAs.

7.4.5 OSPF Interfaces

[Routing > OSPF > Interfaces]

This dialog lets you specify, activate, and display OSPF parameters on the router interfaces.

The device lets you activate up to 64 OSPF router interfaces.

The device uses the OSPF routing protocol to exchange reachability information between the routers. The device uses routing information learned from peers to determine the next hop towards the destination. To route the data packets correctly, the router authenticates OSPF protocol exchanges to help prevent malicious or incorrect routing information from getting introduced into the routing table.

The *OSPF* function supports multiple types of authentication. You set up the type of authentication in use on a per interface basis. The cryptographic authentication option `md5`, helps protect the 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

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the interface to which the table row relates.

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 the *OSPF* function.

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 (DR)* 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 (DR)* 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 time in 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 time in 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 (2¹⁶-1)` (default setting: `10`)

Dead interval [s]

Specifies the time in seconds that the device waits for the *Hello* packets before it declares the neighboring router to be unavailable.

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 (2¹⁶-1)` (default setting: `40`)
  Specify a lower value to get a faster detection of a neighbor that is unavailable.

  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 data packets.
- *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. The *OSPF* function 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. The *OSPF* function 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 sends *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 the 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, the router sends the passwords as clear text.
- *MD5*
  The router uses the message-digest algorithm MD5 authentication. This type of authentication helps make the network more secure.

Auth key

Specifies the authentication key.

After entering the field displays ***** (asterisk) instead of the authentication key.

Possible values:

- Alphanumeric ASCII character string with 16 characters
  - with 8 characters if from the *Auth type* drop-down list the *simple* item is selected
  - with 16 characters if from 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 the network against passive attacks and helps provide significant protection against active attacks.

The prerequisite is that for changing the value in the *Auth type* column the value `MD5` is specified.

Possible values:

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

Cost

Specifies the internal metric.

The *OSPF* function uses link cost as the metric. The *OSPF* function also uses the cost of a link to calculate the SPF routes. The *OSPF* function 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)
  The device calculates the metric and automatically adjusts the value when the interface bandwidth changes.
- `1..65535 (2¹⁶-1)`
  The *OSPF* function uses the value specified here as metric.

Calculated cost

Displays the metric value which the *OSPF* function 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.

7.4.6 OSPF Virtual Links

[Routing > OSPF > Virtual Links]

The *OSPF* function 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.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the *Create* window to add a table row.

- From the *Area ID* drop-down list you select the area ID for the new table row.
- In the *Neighbor ID* field you specify the router ID of the virtual neighbor.

Remove

Removes the selected table row.

Area ID

Displays the area ID of the transit area through which the virtual link connects the separated areas.

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 time in seconds between *Link State 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 time in seconds that the device waits for the *Hello* packets before it declares the neighboring router to be unavailable.

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 (2¹⁶-1)` (default setting: `40`)
  Specify a lower value to get a faster detection of a neighbor that is unavailable.

Note:
Lower values are prone to interoperability issues.

Hello interval [s]

Specifies the time in 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 (2¹⁶-1)` (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 data packets.
- *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 the 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, the router sends the passwords as clear text.
- *MD5*
  The router uses the message-digest algorithm MD5 authentication. This type of authentication helps make the network more secure.

Auth key

Specifies the authentication key.

After entering the field displays ***** (asterisk) instead of the authentication key.

Possible values:

- Alphanumeric ASCII character string with 16 characters
  - with 8 characters if from the *Auth type* drop-down list the *simple* item is selected
  - with 16 characters if from 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 the network against passive attacks and helps provide significant protection against active attacks.

The prerequisite is that for specifying this value, in the *Auth type* column the value *MD5* is specified.

Possible values:

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

7.4.7 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, the *OSPF* function lets you split a large area into smaller subnets.

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.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons


Add

Opens the *Create* window to add a table row.

- From the *Area ID* drop-down list you select the area ID of the address range.
- From 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.


Remove

Removes the selected table row.

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.

7.4.8 OSPF Diagnostics

[Routing > OSPF > Diagnostics]

To function properly, the *OSPF* function 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]

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 data packets transmitted 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* packets 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* packets to exchange information about the OSPF settings 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 sends 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 generates 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)* generates a single network summary LSA from the information contained in the *Type 1* and *Type 2* LSAs received from the DRs. The ABR sends network summary LSAs describing inter-area destinations. The router floods *Type 3* LSAs across every area connected to it, except that 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 generates a single ASBR summary LSA from the information contained in the *Type 1* and *Type 2* LSAs received from the DRs. The ABR sends *Type 4* LSAs to areas different from 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 that this is the area for which it generated the *Type 4* LSA.
- *Type 5* LSAs are *AS external* LSAs. The AS boundary routers generate the *AS external* LSAs describing destinations external to the AS. The *Type 5* LSAs contain information redistributed into the *OSPF* function 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 sends the same LSA to multiple neighbors, the router increments the count for each neighbor.

Hello received

Displays the total number of OSPFv2 *Hello* packets received since resetting the counters.

Hello transmitted

Displays the total number of OSPFv2 *Hello* packets transmitted since resetting the counters.

DB descriptions received

Displays the total number of OSPFv2 Database Description packets received since resetting the counters.

DB descriptions transmitted

Displays the total number of OSPFv2 Database Description packets transmitted since resetting the counters.

LS requests received

Displays the total number of OSPFv2 Link State Request packets received since resetting the counters.

LS requests transmitted

Displays the total number of OSPFv2 Link State Request packets transmitted since resetting the counters.

LS updates received

Displays the total number of OSPFv2 LS Update packets received since resetting the counters.

LS updates transmitted

Displays the total number of OSPFv2 LS Update packets transmitted since resetting the counters.

LS ACK updates received

Displays the total number of OSPFv2 LS Acknowledgement packets received since resetting the counters.

LS ACK updates 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.

[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

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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 generates 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 accepts LSA with MaxAge.
- Otherwise, the router accepts 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 value of the advertisement increases with each router that transmits the message. Excluding the age field lets the router send the message without updating the checksum field.

[Neighbors]

The *Hello* packet is responsible for neighbor acquisition, maintenance, and bidirectional communication between neighbors.

During the acquisition process, the routers on a segment compare their settings 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

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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 table row relates.

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 the *Hello interval [s]* column.
- *init*
  The router has recently received 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 bidirectional state.
- *exchangeStart*
  The first step in setting up 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 DD packets (Database Description) 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 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 to be unavailable. The timer initiates the count down after the router receives a *Hello* packet.

[Virtual neighbors]

The *OSPF* function requires a continuous connection of the Autonomous System backbone area. The *OSPF* function 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* function lets you specify virtual links through every type of area except for stub areas.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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 data 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 lets a router identify and share its optional capabilities with 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 the *Hello interval [s]* column.
- *init*
  The router has recently received 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 bidirectional state.
- *exchangeStart*
  The first step in setting up 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 DD packets (Database Description) 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 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. For example, if the device has received a *Hello* packet or the device has established bidirectional communication.

Length of retransmission queue

Displays the length of the retransmission list.

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 specify 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.

[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

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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 generates 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 router transmits the message across the network. Excluding the age field lets the router send the message without updating the checksum field.

[Route]

The dialog displays the OSPF route information learned from the Link State Advertisements (LSA).

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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 OSPF within an area.
- *inter*
  Entry for routes from OSPF 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.

7.5 Routing Table

[Routing > Routing Table]

This dialog displays the routing table with the routes set up 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 set-up 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

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons


Add

Opens the *Create* window to add a static route.

- In the *Network address* field, you specify the address of the destination network.
  Possible values:
  - Valid IPv4 address

  If you specify a *default route* (`0.0.0.0`), then you specify a *default gateway* in the *Next hop IP address* field. This setting takes precedence over the setting in the following dialog:
  - *Basic Settings > Network > IPv4* 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 numerically lowest value. The default setting is the value specified in the *Configuration* frame, field *Preference*.
- From the *Track name* drop-down list, you select 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*.

Remove

Removes the selected table row.

Port

Displays the router interface through which the device currently sends 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 added this route when setting up the router interface. See the *Routing > Interfaces >* Configuration dialog.
- *netmgmt*
  A user added 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 added this route. See the *Routing > OSPF* dialog.

Preference

Specifies the "administrative distance" of the route.

The device uses this value instead of the metric, when the metric of the routes is incomparable.

Possible values:

- *0*
  Reserved for routes that the device added 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 numerically lowest value.
- *255*
  In routing decisions, the device ignores the route.

The *Administrative Distance* can be set for static routes added using the button.

Metric

Displays the metric of the route.

The device sends the data packets using the route with the numerically lowest 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 *Advanced > 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.

7.6 L3 Relay

[Routing > L3 Relay]

In a Layer 3 subnet, clients send Bootstrap Protocol (BOOTP)/Dynamic Host Configuration Protocol (DHCP) broadcast messages to the DHCP server to request information for the network settings, such as IP addresses. Routers help provide a boundary for broadcast messages so that BOOTP/DHCP requests are confined within the local subnet. The *L3 Relay* function acts as a proxy for clients that require information from a BOOTP/DHCP server located in a different Layer 3 network segment.

When you set up the client device to retrieve its network settings from a Dynamic Host Configuration Protocol (DHCP) server located in a different subnet, the *L3 Relay* function lets the network device relay requests to a BOOTP/DHCP server located in a different network.

Using *IP helper addresses* and *UDP helper ports*, the L3 Relay function relays Dynamic Host Configuration Protocol (DHCP) packets between the clients and the servers. The *IP helper address* is the IP address of the DHCP server.

Clients use the *UDP helper port* to send broadcast requests to DHCP servers on UDP port 67.

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 network device sends circuit ID suboption information, which identifies the local agent, to the DHCP server. When the DCHP server responds, the network device then recognizes its role as the L3 Relay agent. With the help of the suboption information, the network device helps ensure that the responses are directed back to the appropriate agent.

Possible values:

- `marked`
  The device adds the circuit ID of the DHCP L3 Relay agent to the suboptions for client requests.
- `unmarked` (default setting)
  The device does not add the circuit ID of its L3 Relay agent to the suboptions for client requests.

BOOTP/DHCP wait time (min.)

Specifies the minimum amount of time in seconds that the device waits before relaying the BOOTP/DHCP request.

The end devices send broadcast requests on the local network. This setting lets a local BOOTP/DHCP server respond to the client request before the router relays the client request.

Possible values:

- `0..100` (default setting: `0`)
  If there is no local BOOTP/DHCP server in the network, then set the value to `0`.

BOOTP/DHCP hops (max.)

Specifies the maximum number of cascaded relay agent devices allowed to relay the BOOTP/DHCP request. Each relay agent device that relays a message, increments the hop count value by `1`.

If the hop count of a received BOOTP/DHCP packet exceeds the maximum number of hops specified here, then the device drops the BOOTP/DHCP request. This keeps the message from repeating indefinitely within the network.

Possible values:

- `1..16` (default setting: `4`)

Information

The following fields display the values since the last device restart. The device resets the values to `0` after a restart.

DHCP client messages received

Displays the number of DHCP requests received from the clients.

DHCP client messages relayed

Displays the number of DHCP requests relayed 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 relayed 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 relayed 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 the device discarded.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

 Add

Opens the *Create* window to add a table row.

- In the *Port* field, you specify the port-based router interface.

  Note:
  The device does not support the *L3 Relay* function on VLAN-based router interfaces.

  Possible values:
  - `All` (default setting)
    The device processes the data packets received on all the interfaces. Relay entries with this value specify a global setting.
  - `<available interfaces>`
    The device processes the data packets received on the specified interfaces.
    Interface configurations take priority over global configurations. If the destination UDP port for a data packet matches an entry on an ingress interface, then the device processes the data packet according to the interface configuration. If none of the interface entries match the data packet, then the device processes the data packet according to the global configuration.
- In the *UDP port* field, you specify the *UDP helper port* values for data packets received on this interface. When active, the device relays data packets received with this destination *UDP port* value to the IP address specified in the *IP address* field.
  Possible values:
  - `dhcp`
    Equal to UDP port `67`.
    The device relays Dynamic Host Configuration Protocol (DHCP) requests for IP address assignment and networking parameters.
- In the *IP address* field, you specify the *IP helper address* for the data packets received on the interface.
  Possible values:
  - Valid IP address
    The IP address `0.0.0.0` specifies the entry as a discard entry. The device drops data packets that match a discard entry. You specify discard entries only on the interfaces.

  Prerequisites:
  - To enter the IP address `0.0.0.0`, verify that in the *Port* field, a value other than `All` is specified.
  - To enter an IP address other than `0.0.0.0`, verify that in the *Port* field, the value `All` is specified.

Remove

Removes the selected table row.

Reset statistics

Resets the table statistics.

Port

Displays the port-based router interface to which the table row relates.

Note:
The device does not support the *L3 Relay* function on VLAN-based router interfaces.

UDP port

Displays the destination UDP port for client messages received on the interface. The device relays DHCP requests that match the UDP port criteria to the specified *IP helper address*.

IP address

Displays the *IP helper address* for the data packets received on the interface.

Status

Displays if the *IP helper address* and the *UDP port* items added to the respective port are active.

7.7 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 set up 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

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

 Add

Opens the *Create* window to add a loopback interface.

- In the *Index* field, you specify the number that uniquely identifies the loopback interface.
  Possible values:
  ▶ `1..8`

 Remove

Removes the selected table row.

Index

Displays the number that uniquely identifies the loopback interface. You specify the index number when you add a table row.

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.

7.8 L3-Redundancy

[Routing > L3-Redundancy]

The menu contains the following dialogs:
- VRRP

7.8.1 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.

Note:
For further information on the *VRRP* function, see the “Configuration” user manual.

The menu contains the following dialogs:
- VRRP Configuration
- VRRP Statistics
- VRRP Tracking

7.8.1.1 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 2 addresses per virtual router

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.

Configuration

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. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
  If the device is the VRRP master, then the device sends an SNMP trap.
- `unmarked` (default setting)
  The sending of SNMP traps is inactive.

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. To operate the device 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. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
  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.

Information

Version

Specifies the VRRP version.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

 Add

Opens the *Create* window to add a table row.

- From the *Port* drop-down list, you select the port number.
- In the *VRID* field, you specify the Virtual Router Identifier (VRID).

 Remove

Removes the selected table row.

 Wizard

Opens the *Wizard* window that helps you associate the ports with the address of one or more desired senders. See “[Wizard: VRRP configuration]” on page 384.

Port

Displays the port number to which the table row relates.

VRID

Displays the Virtual Router Identifier.

Active

Activates/deactivates the VRRP instance specified in this table row.

Possible values:

- `marked`
  The *VRRP* instance is active.
- `unmarked` (default setting)
  The *VRRP* instance is inactive.

Oper status

Displays the table row status. The operational state of the related virtual router controls the row status of a currently active table row.

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. If the value differs from the value in the *Priority* field, then the tracked object is unavailable or the virtual router is the IP address owner.

Possible values:

- `1..254` (default setting: `100`)
  The higher the number, the higher the priority. When you set up 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. This distribution simplifies adding another router later with a priority between the existing values, for example with the value `75`.

Priority

Displays the *VRRP* priority value. You specify the priority in the *Routing > OSPF > Interfaces* dialog. The router with the higher priority value takes over the master router role. If the virtual router IP address is the same as the IP address of a router interface, then the router is the IP address owner. If an IP address owner exists, then the *VRRP* function lets the device assign the IP address owner the priority value `255` and declares the router as the master router.

Possible values:

- `0`
  The higher the number, the higher the priority. When you disable or remove a *VRRP* router, which is in the master role, you force the instance to send an advertisement with priority value `0`. This lets the other backup routers know that the master does not participate. Sending a priority value `0` forces a new election.
- `1..255`
  The value `255` means that the virtual router is the IP address owner.

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 set up, then the device returns `0.0.0.0`.

Possible values:

- Valid IPv4 address

Preempt mode

Activates/deactivates the preempt mode. This setting specifies if this router, as a backup router, takes over the master router role when the master router has a lower VRRP priority.

Possible values:

- `marked` (default setting)
  The *Preempt mode* is active. The router takes the master router role from a router with a lower VRRP priority without an election.
- `unmarked`
  The *Preempt mode* is inactive. The router assumes the role of a backup router and listens for master router advertisements. After the *Master Down* interval expires, and no advertisements received from the master router, the router participates in the master router election process.

Proxy ARP

Activates/deactivates the *Proxy ARP* function on the virtual router interface. The function lets you reach devices in other networks as if these devices were located in the local network. The *Proxy ARP* function is required when the device uses the VRRP instance with *1:1 NAT* rules. The prerequisite is that in the *Routing > Interfaces > Configuration* dialog for the relevant interface in use by the VRRP instance, the *Proxy ARP* checkbox is unmarked.

Possible values:

- `marked`
  The *Proxy ARP* function is active.
  The device responds to ARP requests received from end devices that are located in other networks.
- `unmarked` (default setting)
  The *Proxy ARP* function is inactive.

VRRP master candidate

Specifies the IP address for the primary virtual router. Physical routers within a virtual router instance use the VRRP IP address for the communication. If the virtual router IP address is the same as the IP address of a router interface, then the router is the IP address owner and the master router.

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*.
  You can select the IP address of a router interface set up in the *Routing > Interfaces > Configuration* dialog.

Master IP address

Displays the current master router interface IP address.

Possible values:

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

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* page.
  - Select a router interface from the *Port* drop-down list.
  - Specify the Virtual Router Identifier in the *VRID* column.
- ☐ In the *Wizard* window, open the *Edit entry* page.
  - In *VRRP* tab 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 from the drop-down list.
- ☐ 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, select a table row and click the button to edit it.
  Or

- ☐ Double-click a field in the table and edit the value 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, select a table row and click the button.

[Wizard: VRRP configuration]

The *Wizard* window helps you set up a VRRP router instance.

Prerequisites:
- Network routing is functioning correctly.
- On the router interfaces used in the VRRP instance the IP addresses are specified.

The *Wizard* window guides you through the following steps:
- Create or select entry
- Edit entry
- Tracking
- Virtual IP addresses

Create or select entry

VRRP instances

Displays the existing instances available in the device. Select an item to continue. As an alternative, select a port and specify a value in the *VRID* field below.

Port

Specifies the port-based or VLAN-based router interface. You verify in the *Routing > Interfaces > Configuration* dialog if a router interface is set up on the port.

Possible values:

- `<Port number>`
  Port-based router interface
- `VLAN/ <VLAN ID>`
  VLAN-based router interface

VRID

Specifies the Virtual Router Identifier.

Possible values:

- `1..255`
  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.

Edit entry

For each instance you can specify the parameters using the following tabs:

- Edit entry - VRRP

Edit entry - VRRP

Operation

Enables/disables the *VRRP* redundancy for the current instance.

Possible values:

- *On*
  The *VRRP* function is enabled for the current instance.
- *Off* (default setting)
  The *VRRP* function is disabled for the current instance.

Configuration

Base priority

Specifies the priority of the virtual router. If the value differs from the value in the *Priority* field, then the tracked object is unavailable or the virtual router is the IP address owner.

Possible values:

- `1..254` (default setting: `100`)
  The higher the number, the higher the priority. When you set up 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. This distribution simplifies adding another router later with a priority between the existing values, for example with the value `75`.

Priority

Displays the *VRRP* priority value. You specify the priority in the *Routing > OSPF > Interfaces* dialog. The router with the higher priority value takes over the master router role. If the virtual router IP address is the same as the IP address of a router interface, then the router is the IP address owner. If an IP address owner exists, then the *VRRP* function lets the device assign the IP address owner the priority value `255` and declares the router as the master router.

Possible values:

- `0`
  The higher the number, the higher the priority. When you disable or remove a *VRRP* router, which is in the master role, you force the instance to send an advertisement with priority value `0`. This lets the other backup routers know that the master does not participate. Sending a priority value `0` forces a new election.
- `1..255`
  The value `255` means that the virtual router is the IP address owner.

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)
  The *Preempt mode* is active. The router takes the master router role from a router with a lower VRRP priority without an election.
- `unmarked`
  The *Preempt mode* is inactive. The router assumes the role of a backup router and listens for master router advertisements. After the *Master Down* interval expires, and no advertisements received from the master router, the 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.

Proxy ARP

Activates/deactivates the *Proxy ARP* function on the virtual router interface. The function lets you reach devices in other networks as if these devices were located in the local network. The *Proxy ARP* function is required when the device uses the VRRP instance with *1:1 NAT* rules. The prerequisite is that in the *Routing > Interfaces > Configuration* dialog for the relevant interface in use by the VRRP instance, the *Proxy ARP* checkbox is unmarked.

Possible values:

- `marked`
  The *Proxy ARP* function is active.
  The device responds to ARP requests received from end devices that are located in other networks.
- `unmarked` (default setting)
  The *Proxy ARP* function is inactive.

VRRP master candidate

Specifies the IP address for the primary virtual router. Physical routers within a virtual router instance use the VRRP IP address for the communication. If the virtual router IP address is the same as the IP address of a router interface, then the router is the IP address owner and the master router.

Possible values:

- Valid IP address (default setting: `0.0.0.0`)
  You can select the IP address of a router interface set up in the *Routing > Interfaces > Configuration* dialog.

Tracking

Current track entries

Displays the existing tracking objects available in the device. You set up tracking objects in the *Advanced > Tracking > Configuration* dialog. Select an item to continue. As an alternative, select a tracking object in the *Track name* field below.

Each tracking object contains the following parameters separated by a dash:

- Type of the tracking object
- Identification number of the tracking object
- Name of the tracking object

There are the following types of tracking objects:

- *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 sending periodic *ICMP echo request* packets.
- *Logical*
  The device monitors tracking objects logically linked to each other and thus enables complex monitoring tasks.

Assigned track entries

Displays the tracking objects assigned with a *Decrement* value. You can remove an item clicking the ✕ icon.

Track name

Specifies the name of the tracking object to which the virtual router is linked. Select an item from the drop-down list to continue. You set up tracking objects in the *Advanced > Tracking > Configuration* dialog.

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*.

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`

Note:
If in the *Routing > L3-Redundancy > VRRP > Configuration* dialog the value in the *Priority* column is `255`, then the virtual router is the IP address owner. In this case, the priority of the virtual router remains unchanged.

Add

Adds an item in the *Assigned track entries* field based on the values specified in the *Track name* and *Decrement* fields.

Virtual IP addresses

IP address

Displays the primary IP address of the router interface.

Possible values:

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

Multinetting

Displays the secondary IP address for the router interface and the subnet mask of the secondary IP addresses. You specify the secondary IP address and subnet mask in the *Routing > Interfaces > Configuration* dialog.

Virtual IP addresses

Displays the virtual IP address that you specified in the *IP address* field. You can remove an item clicking the ✕ icon.

IP address

Specifies the assigned IP address of the master router within a virtual router.

Possible values:

- Valid IPv4 address

Add

Adds an item in the *Virtual IP addresses* field based on the value specified in the *IP address* field.

7.8.1.2 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

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the router interface number to which the table row relates.

VRID

Displays the Virtual Router IDentifier.

Become master

Displays the number of times that the device has taken the master role. A high number can be an indication of an unstable network.

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 set up 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.

7.8.1.3 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*.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the *Create* window to add a table row.

- From the *Port VRID* drop-down list, you select the interface and router ID of a virtual router that has been set up.
- From the *Track name* drop-down list, you select the tracking object with which the device links the virtual router.

Remove

Removes the selected table row.

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 *Advanced* > *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:

- `-` (default setting)
- `1..253`

Note:
If in the *Routing > L3-Redundancy > VRRP > Configuration* dialog the value in the *Priority* column is `255`, then the virtual router is the IP address owner. 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:

- `marked`
  The monitoring of the tracking object is active.
- `unmarked`
  The monitoring of the tracking object is inactive. You activate the monitoring in the *Advanced* > Tracking > *Configuration* dialog, *Active* column.

7.9 NAT

[Routing > NAT]

The menu contains the following dialogs:

- NAT Global
- 1:1 NAT
- Destination NAT

- Masquerading NAT
- Double NAT

7.9.1 NAT Global

[Routing > NAT > NAT Global]

Network Address Translation (*NAT*) contains several procedures which automatically change the IP address information in the data packet. When set up in the device, the *NAT* function enables communication links between devices in different networks.

This dialog displays how many *NAT* rules can be set up for the individual *NAT* processes and indicates changes to the active *NAT* rules.

The device provides a multi-step approach to set up and apply the *NAT* rules:

- You add a rule.
- You assign the rule to a router interface.
  Up to this step, changes have no effect on the behavior of the device and the data stream.
- You apply the rule to the data stream. To do this, click the button in the respective frame.

1:1 NAT

Buttons

Commit

Applies the *1:1 NAT* rules saved in the device to the data stream.

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

Note:
While the device is activating the saved rules, you cannot establish any new communication connections.

1:1 NAT rules (max.)

Displays the maximum number of *1:1 NAT* rules that the device lets you set up.

Configured 1:1 NAT rules

Displays the number of *1:1 NAT* rules set up in the device.

1:1 NAT pending actions

Displays if the *1:1 NAT* rules applied to the data stream differ from the saved *1:1 NAT* rules.

Possible values:

- `marked`
  At least one saved *1:1 NAT* rule contains modified settings. To apply the pending rules to the data stream, click the button.
- `unmarked`
  The device applies the saved *1:1 NAT* rules to the data stream.

Destination NAT

Buttons

Commit

Applies the *Destination NAT* rules saved in the device to the data stream.

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

Note:
While the device is activating the saved rules, you cannot establish any new communication connections.

Destination NAT rules (max.)

Displays the maximum number of *Destination NAT* rules that the device lets you set up.

Configured Destination NAT rules

Displays the number of *Destination NAT* rules set up in the device.

Configured Destination NAT interfaces

Displays the number of *Destination NAT* router interfaces set up in the device.

Destination NAT pending actions

Displays if the *Destination NAT* rules applied to the data stream differ from the saved *Destination NAT* rules.

Possible values:

- `marked`
  At least one saved *Destination NAT* rule contains modified settings. To apply the pending rules to the data stream, click the button.
- `unmarked`
  The device applies the saved *Destination NAT* rules to the data stream.

Masquerading NAT

Buttons

Commit

Applies the *Masquerading NAT* rules saved in the device to the data stream.

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

Note:
While the device is activating the saved rules, you cannot establish any new communication connections.

Masquerading NAT rules (max.)

Displays the maximum number of *Masquerading NAT* rules that the device lets you set up.

Configured Masquerading NAT rules

Displays the number of *Masquerading NAT* rules set up in the device.

Configured Masquerading NAT interfaces

Displays the number of *Masquerading NAT* router interfaces set up in the device.

Masquerading NAT pending actions

Displays if the *Masquerading NAT* rules applied to the data stream differ from the saved *Masquerading NAT* rules.

Possible values:

- `marked`
  At least one saved *Masquerading NAT* rule contains modified settings. To apply the pending rules to the data stream, click the button.
- `unmarked`
  The device applies the saved *Masquerading NAT* rules to the data stream.

Double NAT

Buttons

Commit

Applies the *Double NAT* rules saved in the device to the data stream.

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

Note:
While the device is activating the saved rules, you cannot establish any new communication connections.

Double NAT rules (max.)

Displays the maximum number of *Double NAT* rules that the device lets you set up.

Configured Double NAT rules

Displays the number of *Double NAT* rules set up in the device.

Configured Double NAT interfaces

Displays the number of *Double NAT* router interfaces set up in the device.

Double NAT pending actions

Displays if the *Double NAT* rules applied to the data stream differ from the saved *Double NAT* rules.

Possible values:

- `marked`
  At least one saved *Double NAT* rule contains modified settings. To apply the pending rules to the data stream, click the button.
- `unmarked`
  The device applies the saved *Double NAT* rules to the data stream.

7.9.2 1:1 NAT

[Routing > NAT > 1:1 NAT]

The *1:1 NAT* function lets you establish communication links within a local network to devices that are located in other networks. The *NAT* router virtually “shifts” the devices into the public network. To do this, the *NAT* router replaces the virtual with the actual IP address in the data packet while sending it. A typical application is connecting some identically structured production cells with the same IP address to a server farm.

The prerequisite for the *1:1 NAT* process is that the *NAT* router itself responds to ARP requests. To do this, activate the *Proxy ARP* function for the relevant interface in the *Routing > Interfaces >* Configuration dialog or in the *Routing > L3-Redundancy > VRRP > Configuration* dialog.

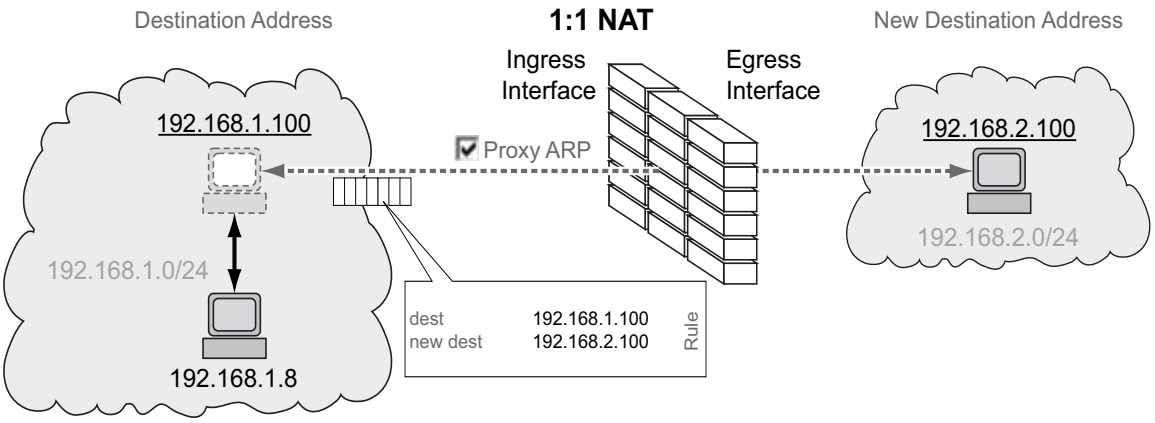


Figure 3: How the 1:1 NAT function works

To use the *NAT* function, set up a router interface for each network and turn on the routing function in the device.

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

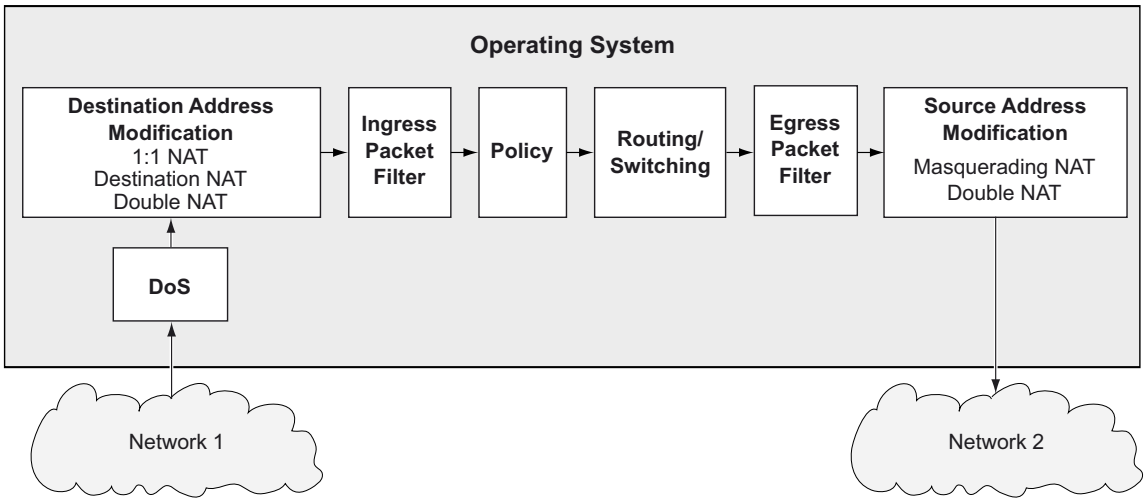


Figure 4: Processing sequence of the data packets in the device

The menu contains the following dialogs:

- 1:1 NAT Rule

7.9.2.1 1:1 NAT Rule

[Routing > NAT > 1:1 NAT > Rule]

In this dialog, you set up the *1:1 NAT* rules and assign router interfaces to which the device applies the *1:1 NAT* rules. The device lets you set up to 255 *1:1 NAT* rules.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the *Create* window to add a table row.

- In the *Destination address* field, you specify the destination address of the data packets to which the device applies the rule. The device sends data packets with this destination address to the destination address specified in the *New destination address* column.
  Possible values:
  - Valid IPv4 address
    The device applies the *1:1 NAT* rule only to data packets which contain the destination address specified here.
  - Valid IPv4 address and netmask in CIDR notation
    The device applies the *1:1 NAT* rule only to data packets which contain a destination address in the subnet specified here.
- In the *New destination address* field, you specify the actual IP address of the destination device. The device sends data packets to the destination address specified here.
  Possible values:
  - Valid IPv4 address
    The device replaces the destination address in the data packet with this new destination address.
  - Valid IPv4 address and netmask in CIDR notation
    The device replaces the destination address in the data packet with a destination address in the subnet specified here.

  When you click the *Ok* button, the device adds the table row. The device assigns the values specified in the *Destination address* and *New destination address* fields to this table row.

Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.

Rule name

Displays the name of the *1:1 NAT* rule. To change the name, click the relevant field.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters

Priority

Specifies the priority of the *1:1 NAT* rule.

Using the priority, you specify the order in which the device applies several rules to the data stream. The device applies the rules in ascending order starting with priority `0`.

Possible values:

- `0..6500` (default setting: `0`)

Ingress interface

Assigns the *1:1 NAT* rule to the router interface on which the device receives data packets. The *1:1 NAT* rule makes the destination device virtually accessible in the network connected here.

Possible values:

- `<Interface number>`
  The device applies the *1:1 NAT* rule to this router interface, and only to data packets addressed to the IP address specified in the *Destination address* column.
- `no Port`
  No router interface is assigned to the *1:1 NAT* rule. Someone removed the router interface after the last edit of the *1:1 NAT* rule.

You enable on the ARP proxy function on this router interface in the *Routing > Interfaces >* Configuration dialog.

Destination address

Specifies the destination address of the data packets to which the device applies the *1:1 NAT* rule. The device sends data packets with this destination address to the destination address specified in the *New destination address* column.

Possible values:

- Valid IPv4 address
  The device applies the *1:1 NAT* rule only to data packets which contain the destination address specified here.
- Valid IPv4 address and netmask in CIDR notation
  The device applies the *1:1 NAT* rule only to data packets which contain a destination address in the subnet specified here.

Egress interface

Assigns the *1:1 NAT* rule to the router interface on which the device forwards the modified data packets. The destination device can actually be reached in the network connected here.

Possible values:

- `<Interface number>`
  The device forwards the modified data packets on this router interface.
- `no Port`
  No router interface is assigned to the *1:1 NAT* rule. Someone removed the router interface after the last edit of the *1:1 NAT* rule.

New destination address

Specifies the actual IP address of the destination device. The device sends data packets to the destination address specified here.

Possible values:

- Valid IPv4 address
  The device replaces the destination address in the data packet with this new destination address.
- Valid IPv4 address and netmask in CIDR notation
  The device replaces the destination address in the data packet with a destination address in the subnet specified here.

Trap

Activates/deactivates the sending of SNMP traps when the device applies a *1:1 NAT* rule to a data packet.

Possible values:

- `marked`
  The sending of SNMP traps is active. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
  If the device applies the *1:1 NAT* rule to a data packet, then the device sends an SNMP trap.
- `unmarked` (default setting)
  The sending of SNMP traps is inactive.

Log

Activates/deactivates the logging in the log file. See the *Diagnostics > Report > System Log* dialog.

Possible values:

- `marked`
  Logging is activated.
  When the device applies the *1:1 NAT* rule to a data packet, the device places an entry in the log file.
- `unmarked` (default setting)
  Logging is deactivated.

Active

Activates/deactivates the *1:1 NAT* rule.

Possible values:

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

7.9.3 Destination NAT

[Routing > NAT > Destination NAT]

The *Destination NAT* function lets you divert the data stream of outgoing communication links to or through a server in a local network.

A special form of the *Destination NAT* function is *port forwarding*. You use *port forwarding* to hide the structure of a network from the outside while still allowing communication links from the outside into the network. A typical application is remote control of a PC in a production cell. The maintenance station establishes the communication link to the *NAT* router, and the *Destination NAT* function takes care of the routing to the production cell.

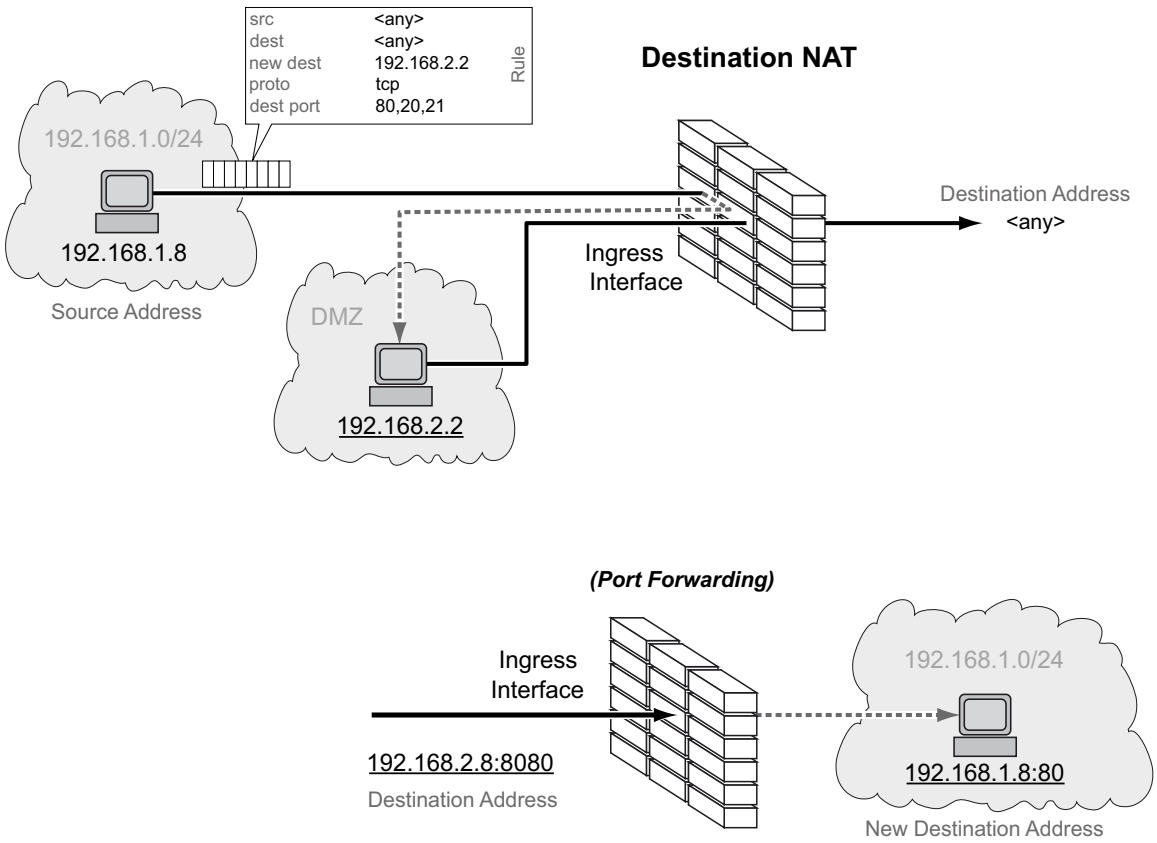


Figure 5: How the Destination NAT function works

To use the *NAT* function, set up a router interface for each network and turn on the routing function in the device.

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

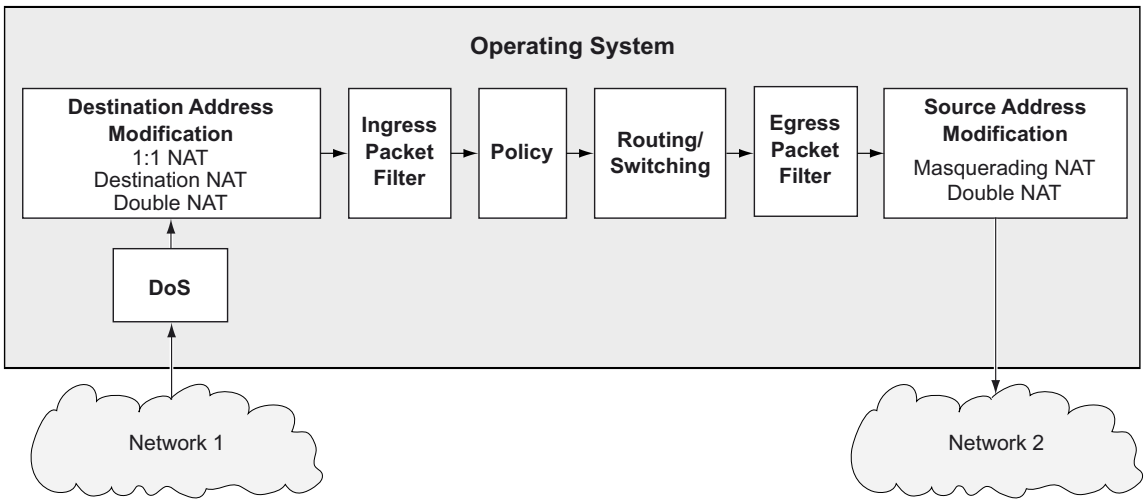


Figure 6: Processing sequence of the data packets in the device

The menu contains the following dialogs:

- Destination NAT Rule
- Destination NAT Mapping
- Destination NAT Overview

7.9.3.1 Destination NAT Rule

[Routing > NAT > Destination NAT > Rule]

In this dialog, you set up the *Destination NAT* rules.

You assign a router interface to the affected *Destination NAT* rule in the *Routing > NAT > Destination NAT > Mapping* dialog.

An overview of which *Destination NAT* rule is to be assigned to which router interface can be found in the *Routing > NAT > Destination NAT > Overview* dialog.

The device lets you set up to 255 *Destination NAT* rules.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the *Create* window to add a table row.

- In the *New destination address* field, you specify the actual IP address of the destination device. The device sends data packets to the destination address specified here.
  Possible values:
  - Valid IPv4 address
    The device replaces the destination address in the data packet with this new destination address.

  When you click the *Ok* button, the device adds the table row. The device assigns the value specified in the *New destination address* field to this table row.

Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.

Rule name

Displays the name of the *Destination NAT* rule. To change the name, click the relevant field.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters

Source address

Specifies the source address of the data packets to which the device applies the *Destination NAT* rule.

Possible values:

- `any` (default setting)
  The device applies the *Destination NAT* rule to data packets with any source address.
- Valid IPv4 address
  The device applies the *Destination NAT* rule only to data packets containing the source address specified here.
- Valid IPv4 address and netmask in CIDR notation
  The device applies the *Destination NAT* rule only to data packets containing a source address in the subnet specified here.
- An exclamation mark (`!`) preceding the IP address reverses the expression into its opposite. The device applies the *Destination NAT* rule to data packets NOT containing the source address specified here.

Source port

Specifies the source port of the data packets to which the device applies the *Destination NAT* rule. The prerequisite is that in the *Protocol* field the value `TCP` or `UDP` is specified.

Possible values:

- `any` (default setting)
  The device applies the *Destination NAT* rule to every data packet without evaluating the source port.
- `1..65535 (2¹⁶-1)`
  The device applies the *Destination NAT* rule only to data packets containing the specified source port.
  The field lets you specify the following options:
  - You specify a port with a single numerical value, for example `21`.
  - You specify multiple individual ports with numerical values separated by commas, for example `21,80,110`.
  - You specify a port range with numerical values connected by dashes, for example `2000-3000`.
  - You can also combine ports and port ranges, for example `21,2000-3000,65535`.
    The column lets you specify up to 15 numerical values. When you enter `21,2000-3000,65535`, for example, you use 4 of 15 numerical values.

Destination address

Specifies the destination address of the data packets to which the device applies the *Destination NAT* rule. The device sends data packets with this destination address to the destination address specified in the *New destination address* column.

Possible values:

- `any`
  The device applies the *Destination NAT* rule to data packets with any destination address.

- Valid IPv4 address
  The device applies the *Destination NAT* rule only to data packets which contain the destination address specified here.
- Valid IPv4 address and netmask in CIDR notation
  The device applies the *Destination NAT* rule only to data packets which contain a destination address in the subnet specified here.
- An exclamation mark (`!`) preceding the IP address reverses the expression into its opposite. The device applies the *Destination NAT* rule to data packets NOT containing the destination address specified here.

Destination port

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

Possible values:

- `any` (default setting)
  The device applies the *Destination NAT* rule to every data packet without evaluating the destination port.
- `1..65535 (2¹⁶-1)`
  The device applies the *Destination NAT* rule only to data packets containing the specified destination port.
  The field lets you specify the following options:
  - You specify a port with a single numerical value, for example `21`.
  - You specify multiple individual ports with numerical values separated by commas, for example `21,80,110`.
  - You specify a port range with numerical values connected by dashes, for example `2000-3000`.
  - You can also combine ports and port ranges, for example `21,2000-3000,65535`.
    The column lets you specify up to 15 numerical values. When you enter `21,2000-3000,65535`, for example, you use 4 of 15 numerical values.

New destination address

Specifies the actual IP address of the destination device. The device sends data packets to the destination address specified here.

Possible values:

- Valid IPv4 address
  The device replaces the destination address in the data packet with this new destination address.

New destination port

Specifies the port of the destination device. The device forwards data packets to the destination port specified here.

Possible values:

- `any`
  The device retains the original destination port in the data packet.
- `1..65535 (2¹⁶-1)`
  The device replaces the destination port in the packet with this new destination port.

Protocol

Restricts the *Destination NAT* rule to an IP protocol. The device applies the *Destination NAT* rule only to data packets of the specified IP protocol.

Possible values:

- `icmp`
  Internet Control Message Protocol (RFC 792)
- `igmp`
  Internet Group Management Protocol
- `ipip`
  IP in IP tunneling (RFC 1853)
- `tcp`
  Transmission Control Protocol (RFC 793)
- `udp`
  User Datagram Protocol (RFC 768)
- `esp`
  IPsec Encapsulated Security Payload (RFC 2406)
- `ah`
  IPsec Authentication Header (RFC 2402)
- `icmpv6`
  Internet Control Message Protocol for IPv6
- `any` (default setting)
  The device applies the *Destination NAT* rule to every data packet without evaluating the IP protocol.

Log

Activates/deactivates the logging in the log file. See the *Diagnostics > Report > System Log* dialog.

Possible values:

- `marked`
  Logging is activated.
  When the device applies the *Destination NAT* rule to a data packet, the device places an entry in the log file.
- `unmarked` (default setting)
  Logging is deactivated.

Trap

Activates/deactivates the sending of SNMP traps when the device applies a *Destination NAT* rule to a data packet.

Possible values:

- `marked`
  The sending of SNMP traps is active. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
  If the device applies the *Destination NAT* rule to a data packet, then the device sends an SNMP trap.
- `unmarked` (default setting)
  The sending of SNMP traps is inactive.

Active

Activates/deactivates the *Destination NAT* rule.

Possible values:

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

7.9.3.2 Destination NAT Mapping

[Routing > NAT > Destination NAT > Mapping]

In this dialog, you assign the *Destination NAT* rules to a router interface. To do this, click the button.

You add and edit the *Destination NAT* rules in the *Routing > NAT > Destination NAT > Rule*.

An overview of which *Destination NAT* rule is to be assigned to which router interface can be found in the *Routing > NAT > Destination NAT > Overview* dialog.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Remove

Removes the selected table row.

Assign

Opens the *Assign* window. In this window, you assign a set-up router interface to an existing *Destination NAT* rule.

Port

Displays the number of the router interface on which the device applies the *Destination NAT* rule.

Rule index

Displays the sequential number of the *Destination NAT* rule. See the *Index* column in the *Routing > NAT > Destination NAT > Rule* dialog. You specify the index number when you add a table row.

Rule name

Displays the name of the *Destination NAT* rule. See the *Rule name* column in the *Routing > NAT > Destination NAT > Rule* dialog.

Direction

Displays if the device applies the *Destination NAT* rule to data packets received or sent.

Possible values:

- *ingress*
  The device applies the *Destination NAT* rule to data packets received on the router interface.

Priority

Specifies the priority of the *Destination NAT* rule.

Using the priority, you specify the order in which the device applies several rules to the data stream. The device applies the rules in ascending order starting with priority `1`.

Possible values:

- `1..6500` (default setting: `1`)

Active

Activates/deactivates the *Destination NAT* rule.

Possible values:

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

7.9.3.3 Destination NAT Overview

[Routing > NAT > Destination NAT > Overview]

In this dialog, you will find an overview of which *Destination NAT* rule is assigned to which router interface.

You add and edit the *Destination NAT* rules in the *Routing > NAT > Destination NAT > Rule*.

You assign a router interface to the affected *Destination NAT* rule in the *Routing > NAT > Destination NAT > Mapping* dialog.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the number of the router interface on which the device applies the *Destination NAT* rule.

Rule index

Displays the sequential number of the *Destination NAT* rule. See the *Index* column in the *Routing > NAT > Destination NAT > Rule* dialog.

Rule name

Displays the name of the *Destination NAT* rule. See the *Rule name* column in the *Routing > NAT > Destination NAT > Rule* dialog.

Destination address

Displays the destination address of the data packets to which the device applies the *Destination NAT* rule. The device sends data packets with this destination address to the destination address specified in the *New destination address* column.

New destination address

Displays the actual IP address of the destination device. The device sends data packets to the destination address specified here.

Trap

Displays if the device sends an SNTP trap when it applies the *Destination NAT* rule to a data packet.

Possible values:

- `marked`
  The device sends an SNMP trap. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
- `unmarked`
  The device does not send an SNMP trap.

Log

Displays if the device places an entry in the log file when it applies the *Destination NAT* rule to a data packet.

Possible values:

- `marked`
  When the device applies the *Destination NAT* rule to a data packet, the device places an entry in the log file. See the *Diagnostics > Report > System Log* dialog.
- `unmarked`
  Logging is disabled.

Direction

Displays if the device applies the *Destination NAT* rule to data packets received or sent.

Possible values:

- *`ingress`*
  The device applies the *Destination NAT* rule to data packets received on the router interface.

Priority

Displays the priority of the *Destination NAT* rule.

The device applies rules to the data stream in ascending order starting with priority `1`.

7.9.4 Masquerading NAT

[Routing > NAT > Masquerading NAT]

The *Masquerading NAT* function hides any number of devices behind the IP address of the *NAT* router and thus hides the structure of a network from other networks. To do this, the *NAT* router replaces the sender address in the data packet with its own IP address. Also, the *NAT* router replaces the source port in the data packet with its own value to send the response data packets back to the original sender later on.

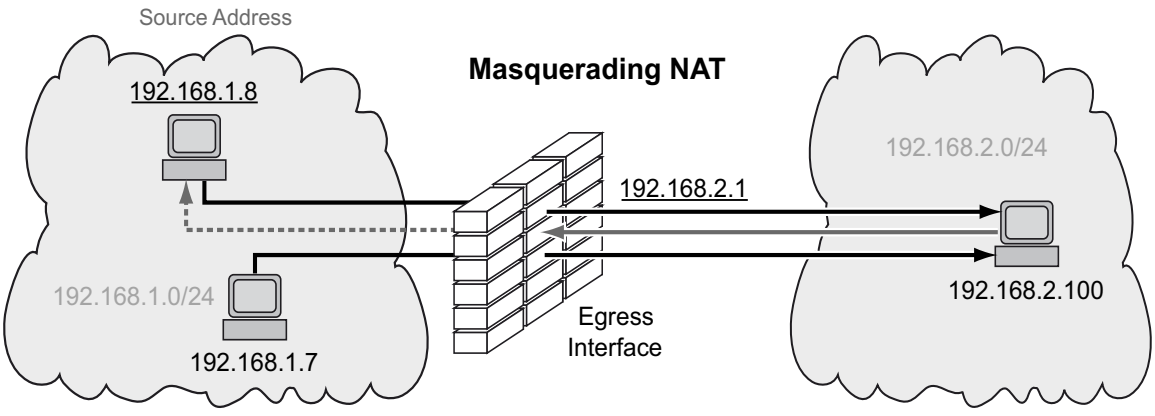


Figure 7: How the Masquerading NAT function works

To use the *NAT* function, set up a router interface for each network and turn on the routing function in the device.

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

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

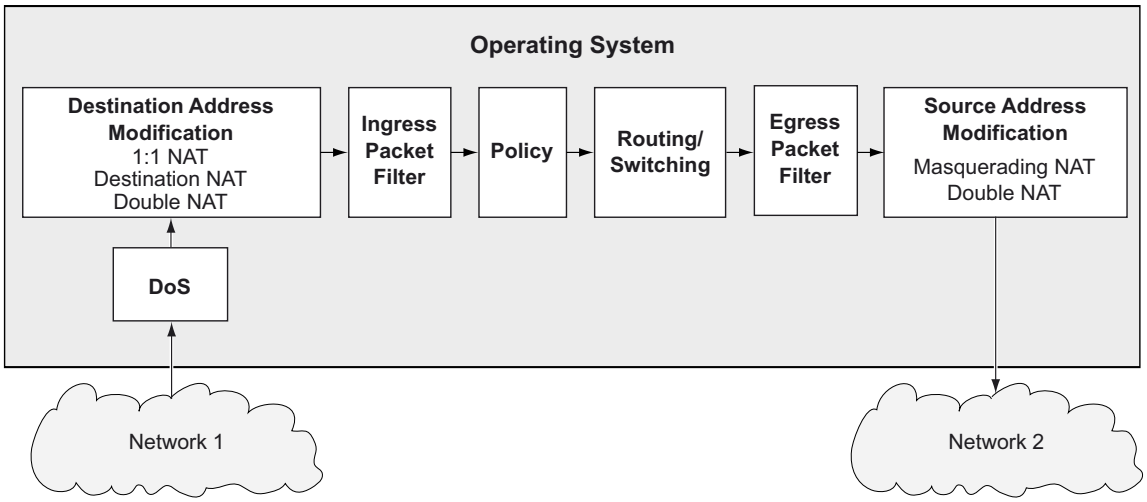


Figure 8: Processing sequence of the data packets in the device

The menu contains the following dialogs:

- Masquerading NAT Rule
- Masquerading NAT Mapping
- Masquerading NAT Overview

7.9.4.1 Masquerading NAT Rule

[Routing > NAT > Masquerading NAT > Rule]

In this dialog, you set up the *Masquerading NAT* rules.

You assign a router interface to the affected *Masquerading NAT* rule in the *Routing* > *NAT* > Masquerading NAT > *Mapping* dialog.

An overview of which *Masquerading NAT* rule is to be assigned to which router interface can be found in the *Routing* > *NAT* > *Masquerading NAT* > *Overview* dialog.

The device lets you set up to 128 *Masquerading NAT* rules.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Adds a table row.

Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.

Rule name

Displays the name of the *Masquerading NAT* rule. To change the name, click the relevant field.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters

Source address

Specifies the source address of the data packets to which the device applies the *Masquerading NAT* rule.

Possible values:

- any
  The device applies the *Masquerading NAT* rule to data packets with any source address.
- Valid IPv4 address
  The device applies the *Masquerading NAT* rule only to data packets containing the source address specified here.

- Valid IPv4 address and netmask in CIDR notation
  The device applies the *Masquerading NAT* rule only to data packets containing a source address in the subnet specified here.
- An exclamation mark (`!`) preceding the IP address reverses the expression into its opposite. The device applies the *Masquerading NAT* rule to data packets NOT containing the source address specified here.

Source port

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

Possible values:

- `any` (default setting)
  The device applies the *Masquerading NAT* rule to every data packet without evaluating the source port.
- `1..65535 (2¹⁶-1)`
  The device applies the *Masquerading NAT* rule only to data packets containing the specified source port.
  The field lets you specify the following options:
  - You specify a port with a single numerical value, for example `21`.
  - You specify multiple individual ports with numerical values separated by commas, for example `21,80,110`.
  - You specify a port range with numerical values connected by dashes, for example `2000-3000`.
  - You can also combine ports and port ranges, for example `21,2000-3000,65535`.
    The column lets you specify up to 15 numerical values. When you enter `21,2000-3000,65535`, for example, you use 4 of 15 numerical values.

Protocol

Restricts the *Masquerading NAT* rule to an IP protocol. The device applies the *Masquerading NAT* rule only to data packets of the specified IP protocol.

Possible values:

- *tcp*
  Transmission Control Protocol (RFC 793)
- *udp*
  User Datagram Protocol (RFC 768)
- *any* (default setting)
  The device applies the *Masquerading NAT* rule to every data packet without evaluating the IP protocol.

Log

Activates/deactivates the logging in the log file. See the *Diagnostics > Report > System Log* dialog.

Possible values:

- `marked`
  Logging is activated.
  When the device applies the *Masquerading NAT* rule to a data packet, the device places an entry in the log file.
- `unmarked` (default setting)
  Logging is deactivated.

Trap

Activates/deactivates the sending of SNMP traps when the device applies a *Masquerading NAT* rule to a data packet.

Possible values:

- `marked`
  The sending of SNMP traps is active. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
  If the device applies the *Masquerading NAT* rule to a data packet, then the device sends an SNMP trap.
- `unmarked` (default setting)
  The sending of SNMP traps is inactive.

IPsec exempt

Activates/deactivates applying the *Masquerading NAT* rule to IPsec data packets.

Possible values:

- `marked`
  The device does not apply the *Masquerading NAT* rule to the IPsec data packets. The device sends IPsec data packets through the VPN tunnel without any modification.
- `unmarked` (default setting)
  The device applies the *Masquerading NAT* rule to the IPsec data packets. The device sends IPsec data packets through the VPN tunnel depending on the settings of the Traffic Selector in the *Source address (CIDR)* and *Source restrictions* columns. See the *Virtual Private Network > Connections* dialog.

Active

Activates/deactivates the *Masquerading NAT* rule.

Possible values:

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

7.9.4.2 Masquerading NAT Mapping

[Routing > NAT > Masquerading NAT > Mapping]

In this dialog, you assign the *Masquerading NAT* rules to a router interface. To do this, click the button.

You add and edit the *Masquerading NAT* rules in the *Routing > NAT > Masquerading NAT > Rule*.

An overview of which *Masquerading NAT* rule is to be assigned to which router interface can be found in the *Routing > NAT > Masquerading NAT > Overview* dialog.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Remove

Removes the selected table row.

Assign

Opens the *Assign* window. In this window, you assign a set-up router interface to an existing *Masquerading NAT* rule.

Port

Displays the number of the router interface on which the device applies the *Masquerading NAT* rule.

Rule index

Displays the sequential number of the *Masquerading NAT* rule. See the *Index* column in the *Routing > NAT > Masquerading NAT > Rule* dialog. You specify the index number when you add a table row.

Rule name

Displays the name of the *Masquerading NAT* rule. See the *Rule name* column in the *Routing > NAT > Masquerading NAT > Rule* dialog.

Direction

Displays if the device applies the *Masquerading NAT* rule to data packets received or sent.

Possible values:

- *egress*
  The device applies the *Masquerading NAT* rule to data packets sent on the router interface.

Priority

Specifies the priority of the *Masquerading NAT* rule.

Using the priority, you specify the order in which the device applies several rules to the data stream. The device applies the rules in ascending order starting with priority `1`.

Possible values:

- `1..6500` (default setting: `1`)

Active

Activates/deactivates the *Masquerading NAT* rule.

Possible values:

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

7.9.4.3 Masquerading NAT Overview

[Routing > NAT > Masquerading NAT > Overview]

In this dialog, you will find an overview of which *Masquerading NAT* rule is assigned to which router interface.

You add and edit the *Masquerading NAT* rules in the *Routing* > *NAT* > *Masquerading NAT* > *Rule*.

You assign a router interface to the affected *Masquerading NAT* rule in the *Routing* > *NAT* > Masquerading NAT > *Mapping* dialog.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the number of the router interface on which the device applies the *Masquerading NAT* rule.

Rule index

Displays the sequential number of the *Masquerading NAT* rule. See the *Index* column in the *Routing* > NAT > *Masquerading NAT* > *Rule* dialog.

Rule name

Displays the name of the *Masquerading NAT* rule. See the *Rule name* column in the *Routing* > *NAT* > Masquerading NAT > *Rule* dialog.

Trap

Displays if the device sends an SNTP trap when it applies the *Masquerading NAT* rule to a data packet.

Possible values:

- `marked`
  The device sends an SNMP trap. The prerequisite is that in the *Diagnostics* > *Status Configuration* > *Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
- `unmarked`
  The device does not send an SNMP trap.

Log

Displays if the device places an entry in the log file when it applies the *Masquerading NAT* rule to a data packet.

Possible values:

- `marked`
  When the device applies the *Masquerading NAT* rule to a data packet, the device places an entry in the log file. See the *Diagnostics > Report > System Log* dialog.
- `unmarked`
  Logging is disabled.

Direction

Displays if the device applies the *Masquerading NAT* rule to data packets received or sent.

Possible values:

- *egress*
  The device applies the *Masquerading NAT* rule to data packets sent on the router interface.

Priority

Displays the priority of the *Masquerading NAT* rule.

The device applies rules to the data stream in ascending order starting with priority 1.

7.9.5 Double NAT

[Routing > NAT > Double NAT]

The *Double NAT* function lets you establish communication links between end devices located in different IP networks, which have no way to specify a *default gateway* or *default route*. The *NAT* router virtually “shifts” the devices into the other network. To do this, the *NAT* router replaces the source address and the destination address in the data packet during sending. A typical application is the linking of controllers located in different networks.

The prerequisite for the *Double NAT* function is that the *NAT* router itself responds to ARP requests from the respective network. To make this happen, turn on the ARP proxy function on the ingress interface and on the egress interface.

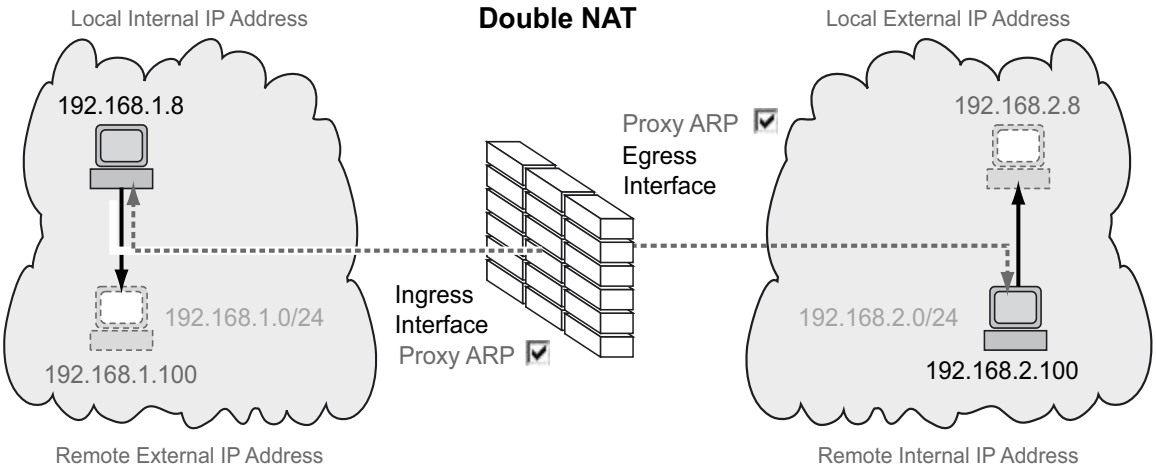


Figure 9: How the Double NAT function works

To use the *NAT* function, set up a router interface for each network and turn on the routing function in the device.

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

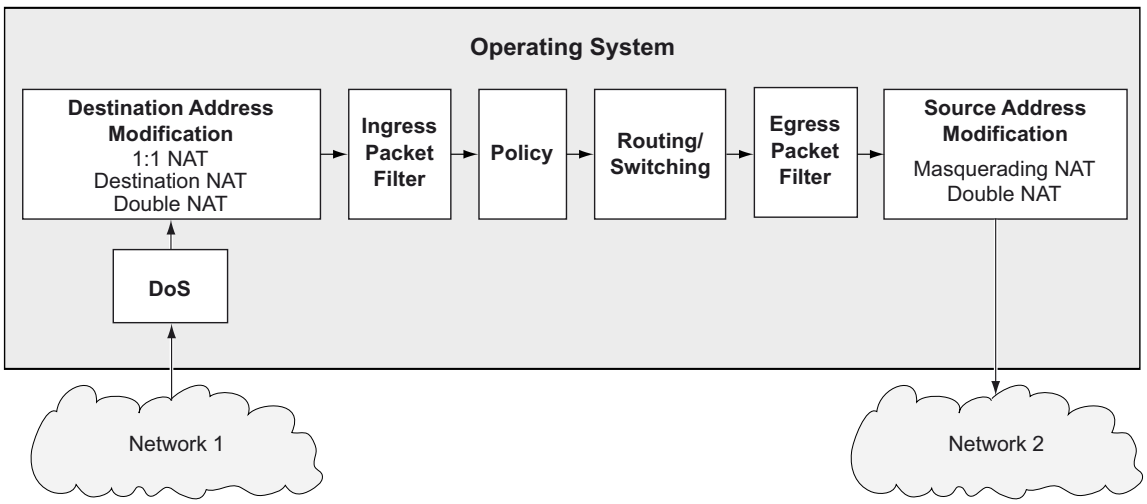


Figure 10: Processing sequence of the data packets in the device

The menu contains the following dialogs:

- Double NAT Rule
- Double NAT Mapping
- Double NAT Overview

7.9.5.1 Double NAT Rule

[Routing > NAT > Double NAT > Rule]

In this dialog, you set up the *Double NAT* rules.

You assign the router interfaces to the related *Double NAT* rule in the *Routing* > *NAT* > *Double NAT* > Mapping dialog.

An overview of which *Double NAT* rule is assigned to which router interfaces you find in the *Routing* > NAT > *Double NAT* > *Overview* dialog.

The device lets you set up to 255 *Double NAT* rules.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the *Create* window to add a table row.

- In the *Local internal IP address* field, you specify the actual IP address for the device placed in the first network.
  Possible values:
  - Valid IPv4 address
    The device applies the *Double NAT* rule only to data packets containing the source address specified here.
- In the *Local external IP address* field, you specify the virtual IP address in the second network for the device placed in the first network.
  Possible values:
  - Valid IPv4 address
    The device applies the *Double NAT* rule only to data packets containing the source address specified here.

- In the *Remote internal IP address* field, you specify the actual IP address for the device placed in the second network.
  Possible values:
  ▶ Valid IPv4 address
  The device applies the *Double NAT* rule only to data packets containing the source address specified here.
- In the *Remote external IP address* field, you specify the virtual IP address in the first network for the device placed in the second network.
  Possible values:
  ▶ Valid IPv4 address
  The device applies the *Double NAT* rule only to data packets containing the source address specified here.

  When you click the *Ok* button, the device adds the table row. The device assigns the values specified in the *Local internal IP address*, *Local external IP address*, *Remote internal IP address* and *Remote external IP address* fields to this table row.

Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.

Rule name

Displays the name of the *Double NAT* rule. To change the name, click the relevant field.

Possible values:

▶ Alphanumeric ASCII character string with 0..32 characters

Local internal IP address

Specifies the actual IP address for the device placed in the first network.

Possible values:

▶ Valid IPv4 address
The device applies the *Double NAT* rule only to data packets containing the source address specified here.

Local external IP address

Specifies the virtual IP address in the second network for the device placed in the first network.

Possible values:

▶ Valid IPv4 address
The device applies the *Double NAT* rule only to data packets containing the source address specified here.

Remote internal IP address

Specifies the actual IP address for the device placed in the second network.

Possible values:

- Valid IPv4 address
  The device applies the *Double NAT* rule only to data packets containing the source address specified here.

Remote external IP address

Specifies the virtual IP address in the first network for the device placed in the second network.

Possible values:

- Valid IPv4 address
  The device applies the *Double NAT* rule only to data packets containing the source address specified here.

Log

Activates/deactivates the logging in the log file. See the *Diagnostics > Report > System Log* dialog.

Possible values:

- `marked`
  Logging is activated.
  The device places an entry in the log file when it applies the *Double NAT* rule to a data packet.
- `unmarked` (default setting)
  Logging is deactivated.

Trap

Activates/deactivates the sending of SNMP traps when the device applies a *Double NAT* rule to a data packet.

Possible values:

- `marked`
  The sending of SNMP traps is active. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
  If the device applies the *Double NAT* rule to a data packet, then the device sends an SNMP trap.
- `unmarked` (default setting)
  The sending of SNMP traps is inactive.

Active

Activates/deactivates the *Double NAT* rule.

Possible values:

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

7.9.5.2 Double NAT Mapping

[Routing > NAT > Double NAT > Mapping]

In this dialog, you assign the *Double NAT* rules to a router interface. To do this, click the button.

You add and edit the *Double NAT* rules in the *Routing > NAT > Double NAT > Rule*.

An overview of which *Double NAT* rule is assigned to which router interfaces you find in the *Routing > NAT > Double NAT > Overview* dialog.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Remove

Removes the selected table row.

Assign

Opens the *Assign* window. In this window, you assign a set-up router interface to an existing *Double NAT* rule.

Port

Displays the number of the router interface on which the device applies the *Double NAT* rule.

Rule index

Displays the sequential number of the *Double NAT* rule. See the *Index* column in the *Routing > NAT > Double NAT > Rule* dialog. You specify the index number when you add a table row.

Rule name

Displays the name of the *Double NAT* rule. See the *Rule name* column in the *Routing > NAT > Double NAT > Rule* dialog.

Direction

Displays if the device applies the *Double NAT* rule to data packets received or sent.

Possible values:

- *ingress*
  The device applies the *Double NAT* rule to data packets received on the router interface.

- *egress*
  The device applies the *Double NAT* rule to data packets sent on the router interface.
- *both*
  The device applies the *Double NAT* rule to data packets received or sent on the router interface.

You can change the value when you click the button.

Priority

Specifies the priority of the *Double NAT* rule.

Using the priority, you specify the order in which the device applies several rules to the data stream. The device applies the rules in ascending order starting with priority `1`.

Possible values:

- `1..6500` (default setting: `1`)

Active

Activates/deactivates the *Double NAT* rule.

Possible values:

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

7.9.5.3 Double NAT Overview

[Routing > NAT > Double NAT > Overview]

In this dialog, you will find an overview of which *Double NAT* rule is assigned to which router interface.

You add and edit the *Double NAT* rules in the *Routing* > *NAT* > *Double NAT* > *Rule*.

You assign the router interfaces to the related *Double NAT* rule in the *Routing* > *NAT* > *Double NAT* > Mapping dialog.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the number of the router interface on which the device applies the *Double NAT* rule.

Rule index

Displays the sequential number of the *Double NAT* rule. See the *Index* column in the *Routing* > *NAT* > Double NAT > *Rule* dialog.

Rule name

Displays the name of the *Double NAT* rule. See the *Rule name* column in the *Routing* > *NAT* > *Double NAT* > *Rule* dialog.

Local internal IP address

Displays the actual IP address for the device placed in the first network.

Local external IP address

Displays the virtual IP address in the second network for the device placed in the first network.

Remote internal IP address

Displays the actual IP address for the device placed in the second network.

Remote external IP address

Displays the virtual IP address in the first network for the device placed in the second network.

Trap

Displays if the device sends an SNTP trap when it applies the *Double NAT* rule to a data packet.

Possible values:

- `marked`
  The device sends an SNMP trap. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
- `unmarked`
  The device does not send an SNMP trap.

Log

Displays if the device places an entry in the log file when it applies the *Double NAT* rule to a data packet.

Possible values:

- `marked`
  When the device applies the *Double NAT* rule to a data packet, the device places an entry in the log file. See the *Diagnostics > Report > System Log* dialog.
- `unmarked`
  Logging is disabled.

Direction

Displays if the device applies the *Double NAT* rule to data packets received or sent.

Possible values:

- *ingress*
  The device applies the *Double NAT* rule to data packets received on the router interface.
- *egress*
  The device applies the *Double NAT* rule to data packets sent on the router interface.
- *both*
  The device applies the *Double NAT* rule to data packets received or sent on the router interface.

Priority

Displays the priority of the *Double NAT* rule.

The device applies rules to the data stream in ascending order starting with priority 1.

8 Diagnostics

The menu contains the following dialogs:

- Status Configuration
- System
- Syslog
- Ports
- LLDP
- Report

8.1 Status Configuration

[Diagnostics > Status Configuration]

The menu contains the following dialogs:

- Device Status
- Security Status
- Signal Contact
- Alarms (Traps)

8.1.1 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 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:

- *ok*
- *error*
  The device displays this value to indicate a detected error in one of the monitored parameters.

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. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
  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.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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.

Temperature

Activates/deactivates the monitoring of the temperature in the device.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If the temperature exceeds the specified upper threshold value or falls below the specified lower threshold value, then in the *Device status* frame, the value changes to `error`.
- `unmarked`
  Monitoring is inactive.

You specify the temperature threshold values in the *Basic Settings > System* dialog, *Upper temp. limit [°C]* field and *Lower temp. limit [°C]* field.

External memory removal

Activates/deactivates the monitoring of the active external memory.

Possible values:

- `marked`
  Monitoring is active.
  If you remove the active external memory from the device, then in the *Device status* frame, the value changes to `error`.
- `unmarked` (default setting)
  Monitoring is inactive.

External memory not in sync

Activates/deactivates the monitoring of the configuration profile in the device and in the external memory.

Possible values:

- `marked`
  Monitoring is active.
  In the *Device status* frame, the value changes to `error` in the following situations:
  - The configuration profile only exists in the device.
  - The configuration profile in the device differs from the configuration profile in the external memory.
- `unmarked` (default setting)
  Monitoring is inactive.

Power status

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.

[Port]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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.

[Status]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Timestamp

Displays the date and time of the event.

Cause

Displays the event which caused the SNMP trap.

8.1.2 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:

- *ok*
- *error*
  The device displays this value to indicate a detected error in one of the monitored parameters.

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. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
  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.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Password default settings unchanged

Activates/deactivates the monitoring of the password for the locally set up user account `admin`.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If the password is set to the default setting for the `admin` user account, 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 shorter than 8

Activates/deactivates the monitoring of the *Min. password length* policy.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If the value for the *Min. password length* policy is less than `8`, then in the *Security status* frame, the value changes to *`error`*.
- `unmarked`
  Monitoring is inactive.

You specify the *Min. password length* policy in the *Device Security > User Management* dialog in the *Configuration* frame.

Password policy settings deactivated

Activates/deactivates the monitoring of the Password policies settings.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If the value for at least one of the following policies is less than `1`, then in the *Security status* frame, the value changes to *`error`*.
  - *Upper-case characters (min.)*
  - *Lower-case characters (min.)*
  - *Digits (min.)*
  - *Special characters (min.)*
- `unmarked`
  Monitoring is inactive.

You specify the policy settings in the *Device Security > User Management* dialog in the *Password policy* frame.

User account password policy check deactivated

Activates/deactivates the monitoring of the *Policy check* function.

Possible values:

- `marked`
  Monitoring is active.
  If the *Policy check* function is inactive for at least one user account, then in the *Security status* frame, the value changes to `error`.
- `unmarked` (default setting)
  Monitoring is inactive.

You activate the *Policy check* function in the *Device Security > User Management* dialog.

HTTP server active

Activates/deactivates the monitoring of the HTTP server.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If you enable the HTTP server, then in the *Security status* frame, the value changes to `error`.
- `unmarked`
  Monitoring is inactive.

You enable/disable the HTTP server in the *Device Security > Management Access > Server* dialog, *HTTP* tab.

SNMP unencrypted

Activates/deactivates the monitoring of the SNMP server.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If at least one of the following conditions applies, then in the *Security status* frame, the value changes to `error`:
  - The *SNMPv1* function is enabled.
  - The *SNMPv2* function is enabled.
  - The encryption for SNMPv3 is disabled.
    You enable the encryption in the *Device Security > User Management* dialog, in the *SNMP encryption type* column.
- `unmarked`
  Monitoring is inactive.

You specify the settings for the SNMP agent in the *Device Security > Management Access > Server* dialog, *SNMP* tab.

Access to System Monitor 1 through the serial interface possible

Activates/deactivates monitoring the System Monitor 1 status.

When System Monitor 1 is active, you can change to System Monitor 1 through the serial connection during system startup.

Possible values:

- `marked`
  Monitoring is active.
  If you activate System Monitor 1, then in the *Security status* frame, the value changes to *error*.
- `unmarked` (default setting)
  Monitoring is inactive.

You activate/deactivate System Monitor 1 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 > Global* 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`*.
- `unmarked`
  Monitoring is inactive.

Self-signed HTTPS certificate present

Activates/deactivates the monitoring of the digital certificate of the HTTPS server.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If the HTTPS server uses a self-generated digital certificate, then in the *Security status* frame, the value changes to *`error`*.
- `unmarked`
  Monitoring is inactive.

[Port]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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.

[Status]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Timestamp

Displays the date and time of the event.

Cause

Displays the event which caused the SNMP trap.

8.1.3 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

8.1.3.1 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 from the *Mode* drop-down list the *Manual setting* item is selected.

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. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
  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.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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 the specified upper threshold value or falls below the specified lower threshold value, then the signal contact opens.
- `unmarked`
  Monitoring is inactive.

You specify the temperature threshold values in the *Basic Settings > System* dialog, *Upper temp. limit [°C]* field and *Lower temp. limit [°C]* field.

External memory removed

Activates/deactivates the monitoring of the active external memory.

Possible values:

- `marked`
  Monitoring is active.
  If you remove the active external memory from the device, then the signal contact opens.
- `unmarked` (default setting)
  Monitoring is inactive.

External memory not in sync with NVM

Activates/deactivates the monitoring of the configuration profile in the device and in the external memory.

Possible values:

- `marked`
  Monitoring is active.
  The signal contact opens in the following situations:
  - The configuration profile only exists in the device.
  - The configuration profile in the device differs from the configuration profile in the external memory.
- `unmarked` (default setting)
  Monitoring is inactive.

Power status

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.

[Port]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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.

[Status]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Timestamp

Displays the date and time of the event.

Cause

Displays the event which caused the SNMP trap.

8.1.4 Alarms (Traps)

[Diagnostics > Status Configuration > Alarms (Traps)]

The device lets you send an SNMP trap in response to specific events.

You specify the events for which the device triggers an SNMP trap in the following dialogs:
- *Diagnostics > Status Configuration > Device Status*
- *Diagnostics > Status Configuration > Security Status*

When setting up loopback interfaces, the device uses the IP address of the first loopback interface as the source for the SNMP traps. Otherwise, the device uses the address of the device management.

The menu contains the following dialogs:
- Trap Destinations

8.1.4.1 Trap Destinations

[Diagnostics > Status Configuration > Alarms (Traps) > Trap Destinations]

In this dialog, you specify the trap destinations to which the device sends SNMP traps.

Operation

Operation

Enables/disables sending SNMP traps.

Possible values:

- *On* (default setting)
  Sending SNMP traps is enabled.
- *Off*
  Sending SNMP traps is disabled.

SNMPv1/v2 trap community

Name

Specifies the community string that the device sends in each SNMPv1/v2 trap for authentication to the trap destination.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters
  `trap` (default setting)

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons


Add

Opens the *Create* window to add a table row. Thus, you set up a trap destination on the device.

- In the *Name* field, you specify a name for the trap destination.
  Possible values:
  - Alphanumeric ASCII character string with 1..32 characters
- In the *Address* field, you specify the IP address and the port of the trap destination.
  Possible values:
  - `<IPv4 address>:<port>`
    If you do not specify a port, then the device automatically adds port `162` to the trap destination.


Remove

Removes the selected table row.

Name

Displays the name you specified for the trap destination (trap host).

Address

Specifies the IP address and the port of the trap destination (trap host).

Possible values:

- `<IPv4 address>:<port>`
  If you do not specify a port, then the device automatically adds port `162` to the trap destination.

Active

Activates/deactivates the sending of SNMP traps to the 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.

8.2 System

[Diagnostics > System]

The menu contains the following dialogs:

- System Information
- Configuration Check
- ARP
- Selftest

8.2.1 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

Save system information

Saves the HTML page on your PC using the web browser dialog.

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

Note:
The dialog displays the devices detected as connected to the neighboring device as if they were directly connected to the device itself.

Configuration

Start configuration check...

Starts the check and updates the content of the table.

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.

Information

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.

If you have set up more than 39 VLANs in the device, then the dialog continuously 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.

Information

Displays the number of `INFORMATION` level deviations that the device detected during the configuration check.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Displays detailed information about the detected deviations in the area below the table row. To hide the detailed information again, click the  button. If you click the icon in the table header, you display or hide the detailed information for each table row.

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 a summary of the detected deviations.

8.2.3 ARP

[Diagnostics > System > ARP]

This dialog displays the MAC and IP addresses of the neighboring devices connected to the device management.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Clear ARP table

Deletes the dynamically set up addresses from the ARP 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.

Active

Displays that the ARP table contains the IP/MAC address assignment as an active entry.

8.2.4 Selftest

[Diagnostics > System > Selftest]

This dialog lets you do the following:
- Activate/deactivate the option of accessing System Monitor 1 during system startup.
- Specify how the device behaves in the case of a detected error.

Configuration

If the device does not detect any readable configuration profile when restarting, then the following settings block your access to the device permanently.
- *SysMon1 is available* checkbox is `unmarked`.
- *Load default config on error* checkbox is `unmarked`.

This is the case, for example, if the password of the configuration profile that you are loading differs from the password set in the device. To have the device unlocked again, contact your sales partner.

SysMon1 is available

Activates/deactivates the option of accessing System Monitor 1 during system startup.

Possible values:

- `marked` (default setting)
  The device lets you change to System Monitor 1 during system startup.
- `unmarked`
  The device starts without the option of accessing System Monitor 1.

Among other things, System Monitor 1 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. Access to the device management is only possible using the Command Line Interface through the serial connection.
  To regain the access to the device through the network, change to System Monitor 1 and reset the settings. After the system startup, the device uses the default settings.

Table

In this table you specify how the device behaves in the case of a detected error.

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Cause

Detected 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:

- *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 is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
- *reboot* (default setting)
  The device triggers a restart.

8.3 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.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Adds a table row.

Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.

When you delete a table row, this leaves a gap in the numbering. When you add a table row, 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`)
- DNS name in the format `<domain>.<tld>` or `<host>.<domain>.<tld>`
  The prerequisite is that you also enable the *Client* function in the *Advanced > DNS > Client > Global* dialog.
  To establish an encrypted connection using a digital certificate, verify that the `Common Name` or `Subject Alternative Name` information in the digital certificate that you have transferred onto the device matches the value you specify here. Otherwise, the device will not be able to verify the identity of the server.

Destination UDP port

Specifies the UDP port on which the syslog server expects the log entries.

Possible values:

- `1..65535 (2¹⁶-1)` (default setting: `514`)

Min. severity

Specifies the minimum severity of the events. The device sends a log entry for events with this severity and with more urgent severities to the syslog server.

Possible values:

- *emergency*
- *alert*
- *critical*
- *error*
- *warning* (default setting)
- *notice*
- *informational*
- *debug*

Type

Specifies the type of the log entry transmitted by the device.

Possible values:

- *systemlog* (default setting)
- *audittrail*

Active

Activates/deactivates the transmission of events to the syslog server.

Possible values:

- `marked`
  The device sends events to the syslog server.
- `unmarked` (default setting)
  The transmission of events to the syslog server is deactivated.

8.4 Ports

[Diagnostics > Ports]

The menu contains the following dialogs:

- SFP

8.4.1 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.

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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.

8.4.2 Port Monitor

[Diagnostics > Ports > Port Monitor]

In this dialog, you specify the settings for the *Link flap* function.

The dialog contains the following tabs:
- [Link flap]

[Link flap]

The *Link flap* function assists in managing link changes. You can therefore use the function to speed up convergence if a Layer 2 redundancy protocol based on IEEE 802.3 Ethernet packets is active in the network for example, Rapid Spanning Tree Protocol (RSTP). Convergence is the time required to adjust the network to topology changes, for example when the link status on a port changes.

The *Link flap* function is intended for use in networks with an active Layer 2 redundancy protocol such as RSTP. However, the device itself does not support a redundancy protocol and is not part of the redundant topology.

Using the *Link flap* function, the device replicates detected link changes that occur on one port to another port. This behavior helps a switch device connected to the other port as a direct neighbor to shorten the convergence time. The prerequisite is that both ports are connected to the same Layer 2 network.

The *Link flap* function exclusively affects the physical ports 1/1 and 1/3.

If the *Link flap* function is enabled, then the device disables the following port in case of the condition mentioned:
- Port 1/1, if the link on port 1/3 becomes inoperable
- Port 1/3, if the link on port 1/1 becomes inoperable

As soon as the condition no longer exists and the link is operational again, the device re-enables the port that it had previously deactivated. During this period, the device management remains accessible through the management port.

Operation

Operation

Enables/disables the *Link flap* function. The prerequisite is that in the *Basic Settings > Port* dialog, *Configuration* tab, the *Port on* checkbox is marked for ports 1/1 and 1/3. If one of the ports is deactivated for any reason, then after a reboot the device will not re-enable the *Link flap* function.

To use the *Link flap* function, also activate the *802.3 Frames forwarding* function. To do this, in the *Network Security > DoS > Global* dialog, *Layer 2 frames* frame, mark the *802.3 Frames forwarding* checkbox. With this setting, the device replicates link status information between ports 1/1 and 1/3.

Possible values:

- *On*
  The *Link flap* function is enabled.

  Note:
  If a link on the device becomes inoperable, RSTP or another Layer 2 redundancy protocol will find an alternative path by bypassing the device and excluding it from the network path. This scenario poses a potential security risk. Therefore, enable the *Link flap* function only if you are aware of the effects.

- *Off* (default setting)
  The *Link flap* function is disabled.

8.5 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 lets a network management station map the structure of the network.

This menu lets you set up the topology discovery and to display the information received in tabular form.

The menu contains the following dialogs:
- LLDP Configuration
- LLDP Topology Discovery

8.5.1 LLDP Configuration

[Diagnostics > LLDP > Configuration]

This dialog lets you set up 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 sends LLDP data packets.

Possible values:

- `5..32768 (2¹⁵)` (default setting: `30`)

Transmit interval multiplier

Specifies the factor for determining the time-to-live value for the LLDP data packets.

Possible values:

- `2..10` (default setting: `4`)

The time-to-live value coded in the LLDP header results from multiplying this value with the value in the *Transmit interval [s]* field.

Reinit delay [s]

Displays the delay in seconds for the reinitialization of a port.

If in the *Operation* column the value *Off* is specified, then the device tries to reinitialize the port after the time specified here has elapsed.

Transmit delay [s]

Displays the delay in seconds for transmitting successive LLDP data packets after the device settings change.

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

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.

Operation

Specifies if the port transmits LLDP data packets.

Possible values:

- *`transmit`*
  The port sends LLDP data packets but does not save any information about neighboring devices.
- *`receive`*
  The port receives LLDP data packets but does not send 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 send 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 sends the TLV with the port description.
- `unmarked`
  The transmitting of the TLV is inactive.
  The device does not send 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 sends the TLV with the device name.
- `unmarked`
  The transmitting of the TLV is inactive.
  The device does not send 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 sends the TLV with the system description.
- `unmarked`
  The transmitting of the TLV is inactive.
  The device does not send 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 sends the TLV with the system capabilities.
- `unmarked`
  The transmitting of the TLV is inactive.
  The device does not send 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 MAC address table (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.

8.5.2 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 through LLDPDUs is useful for many reasons. Thus the device detects which devices in the network are neighbors and through which ports they are connected.

The dialog lets you display the network and to detect the connected devices along with their specific features.

This dialog displays the collected LLDP information for the neighboring devices. This information lets a network management station map the structure of the 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 MAC address table (forwarding database) 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 through a hub, the table shows one line for each connected device.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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 MAC address table (forwarding database)
- `unmarked`
  The connected device has active LLDP support.

Neighbor address

Displays the IPv4 address or hostname with which the access to the neighboring device management is possible.

Neighbor IPv6 address

Displays the IPv6 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 auto-negotiation.

Autonegotiation

Displays if auto-negotiation is active 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 active on the port of the neighboring device.

8.6 Report

[Diagnostics > Report]

The menu contains the following dialogs:

- Report Global
- Persistent Logging
- System Log
- Audit Trail

8.6.1 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

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 detailed device information for support purposes on your PC.

Console logging

Buttons

Download support information

Generates a ZIP archive which the web browser lets you download from the device.

The ZIP archive contains files with detailed device information for support purposes. For further information, see “Support Information: Files in ZIP archive” on page 472.

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. For further information, see “Meaning of the event severities” on page 472.

The device outputs the messages on the serial interface.

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 generates 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 adding 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 for the reception of *SNMP Get requests*.

Possible values:

- *On*
  The logging is enabled.
  The device logs each received *SNMP Get request* as an event in the syslog.
  From 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 for the reception of *SNMP Set requests*.

Possible values:

- *On*
  The logging is enabled.
  The device logs each received *SNMP Set request* as an event in the syslog.
  From 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 logs for received *SNMP Get requests*. For further information, see “Meaning of the event severities” on page 472.

Possible values:

- *emergency*
- *alert*
- *critical*

- *error*
- *warning*
- *notice* (default setting)
- *informational*
- *debug*

Severity set request

Specifies the severity of the event that the device logs for received *SNMP Set requests*. For further information, see “Meaning of the event severities” on page 472.

Possible values:

- *emergency*
- *alert*
- *critical*
- *error*
- *warning*
- *notice* (default setting)
- *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. For further information, see “Meaning of the event severities” on page 472.

Possible values:

- *emergency*
- *alert*
- *critical*
- *error*
- *warning* (default setting)
- *notice*
- *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.

Support Information: Files 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* protocol.
config.xml	XML	Contains the settings of the device saved in the "Selected" configuration profile. The file name is the same as the name of the current "Selected" configuration profile.
defaultconfig.xml	XML	Contains the default settings of the device.
runningconfig.xml	XML	Contains the current operating settings of the device.
script	TEXT	Contains the output of the command `show running-config script`.
supportinfo.html	HTML	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
error	Error status
warning	Warning
notice	Significant, normal status
informational	Information message
debug	Debug message

8.6.2 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 generated 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 generated file.

Possible values:

- `0..4096` (default setting: `1024`)

The value `0` deactivates saving of log entries in the log file.

Files (max.)

Specifies the number of log files that the device keeps in the external memory.

As soon as the specified maximum number of files has been attained, the device deletes the oldest file and renames the remaining files.

Possible values:

- `0..25` (default setting: `4`)

The value `0` deactivates saving of log entries in the log file.

Severity

Specifies the minimum severity of the events. The device saves the log entry for events with this severity and with more urgent severities in the log file in the external memory.

Possible values:

- *emergency*
- *alert*
- *critical*
- *error*
- *warning* (default setting)
- *notice*
- *informational*
- *debug*

Log file target

Specifies the external memory device for logging.

Possible values:

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

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Clear persistent log file

Deletes the log files from the external memory.

Index

Displays the index number to which the table row 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.

8.6.3 System Log

[Diagnostics > Report > System Log]

This dialog displays the System Log file. The device logs device-internal events in the System Log file. The device keeps the logged events even after a restart.

To search the System Log file, use the search function of your web browser.

The dialog lets you download a copy of the System Log file onto your computer. The device provides the file to be downloaded in HTML or CSV format.

Buttons

 Save log file

Downloads a copy of the System Log file onto your computer, based on the web browser settings.

Possible values:

- *CSV*
  The device provides the file in CSV format.
- *HTML*
  The device provides the file in HTML format.

 Clear log file

Clears the System Log file on the device.

8.6.4 Audit Trail

[Diagnostics > Report > Audit Trail]

This dialog displays the Audit Trail. The dialog lets you save the log file as an HTML file on your PC.

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 to the device. This lets you keep track of WHO changes WHAT in the device and WHEN. The prerequisite is that the access role `auditor` or `administrator` is assigned to your user account.

The device logs the following user actions, among others:
- A user logging into the device management 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 consecutive 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 device software updates
- Configuration changes using HiDiscovery
- Device software updates and automatic configuration of the device through the external memory
- Opening and closing of SNMP through 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 system startup, access to System Monitor 1 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 System Monitor 1. 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 System Monitor 1. See the *Diagnostics > System > Selftest* dialog, *SysMon1 is available* checkbox.

Buttons

Save audit trail file

Saves the HTML page on your PC using the web browser dialog.

9 Advanced

The menu contains the following dialogs:
- DHCP
- DNS
- Tracking
- Command Line Interface

9.1 DHCP

[Advanced > DHCP]

The menu contains the following dialogs:
- DHCP Server

9.1.1 DHCP Server

[Advanced > DHCP > DHCP Server]

The Dynamic Host Configuration Protocol (DHCP) lets a server assign the IP settings to the devices on the network (clients). The DHCP server stores and assigns the available IP addresses and further settings, if specified.

The DHCP server in the device listens for requests on UDP port 67 and responds to the client devices on UDP port 68. When the device receives a DHCP request, it validates the IP address to be assigned before leasing the IP address and other IP settings to the requesting client device.

The menu contains the following dialogs:
- DHCP Server Global
- DHCP Server Pool
- DHCP Server Lease Table

9.1.1.1 DHCP Server Global

[Advanced > DHCP > DHCP Server > Global]

This dialog lets you activate the *DHCP Server* function per port.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the number of the physical port on which the device listens for DHCP requests and reponds to the client devices.

The device does not support the *DHCP* function on VLAN-based router interfaces.

DHCP server active

Activates/deactivates the *DHCP Server* function on this port.

Possible values:

- `marked` (default setting)
  The *DHCP Server* function is active.
- `unmarked`
  The *DHCP Server* function is inactive.

9.1.1.2 DHCP Server Pool

[Advanced > DHCP > DHCP Server > Pool]

In this dialog, you specify the settings for assigning a certain IP address to client devices from which the device receives a DHCP request.

The device assigns an IP address from a specific pool (address range) depending on which physical port the requesting client device is connected to. The MAC address of the requesting client device is a further criterion for the pool from which the device assigns an IP address.

The device provides a maximum of 128 pools. Up to 1000 client devices can receive their IP settings from the device.

The device manages the IP settings in two types of pools.

- Static pools
  To assign the same IP address to a specific device each time, the device manages the relevant IP settings in a pool whose address range is exactly one IP address.
  Static pools are useful, for example, to assign a fixed IP address to a server, NAS, or printer.
- Dynamic pools
  To assign IP addresses from a certain address range, the device manages the relevant IP settings in a pool whose address range includes multiple IP addresses.

When you enable the *Routing* function, the settings for a specific DHCP server pool take effect only if one of the following prerequisites matches:

- The device has a router interface in the subnet of the respective DHCP pool.
- The device management is accessible in the subnet of the respective DHCP pool.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Adds a table row.

Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.

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 range start

Specifies the fixed IP address for a static pool or the start IP address of an address range.

Possible values:

- Valid IPv4 address (default setting: `0.0.0.0`)
  Verify that the value is within the range of IP addresses specified in the *IP address* and *Netmask* fields for the corresponding port. See the *Routing > Interfaces > Configuration* dialog.

IP range end

Specifies the end IP address of an address range. For a static pool, keep the default setting or add the same value as specified in the *IP range start* column.

Possible values:

- Valid IPv4 address (default setting: `0.0.0.0`)
  Verify that the value is within the range of IP addresses specified in the *IP address* and *Netmask* fields for the corresponding port. See the *Routing > Interfaces > Configuration* dialog.

Port

Specifies the number of the physical port on which the requesting client device is connected.

Possible values:

- `<Port number>` (default setting: `1/1`)
  The device assigns an IP address to the requesting client device only if the local device receives the DHCP request on the specified port.
  The device does not support the *DHCP* function on VLAN-based router interfaces.

MAC address

Specifies the MAC address of the requesting client device.

Possible values:

- `-` (default setting)
  For the IP address assignment, the server ignores this variable.
- Valid Unicast MAC address
  Specify the value with a colon separator, for example `00:11:22:33:44:55`.

Lease time [s]

Specifies the limited period in seconds for which the device leases each IP address.

The client device is responsible for renewing the IP address before the period expires. If the client device does not renew its IP address in time, then the IP address returns to the address pool.

Possible values:

- `60..220752000 (2555 d)` (default setting: `86400`)
- `4294967295 (2³²-1)`
  Use this value for assignments unlimited in time, and for assignments using 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 (default setting: `0.0.0.0`)

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 (default setting: `255.255.255.0`)

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 (default setting: `0.0.0.0`)

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

9.1.1.3 DHCP Server Lease Table

[Advanced > DHCP > DHCP Server > Lease Table]

This dialog displays the currently assigned IP addresses for each port.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the number of the port through which the device to which the IP address is assigned is connected.

IP address

Displays the IP address to which the table row relates.

Status

Displays the lease phase.

According to the standard for DHCP operations, there are 4 phases when assigning 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*
  The 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 how long the assigned IP address is still valid.

Leased MAC address

Displays the MAC address of the device to which the IP address is assigned.

Hostname

Displays the hostname of the device to which the IP address is assigned.

9.2 DNS

[Advanced > DNS]

The menu contains the following dialogs:
- DNS Client
- DNS Cache

9.2.1 DNS Client

[Advanced > DNS > Client]

DNS (Domain Name System) is a service in the network that translates hostnames into IP addresses. This name resolution lets you contact other devices using their hostnames instead of their IP addresses.

Using the *Client* function the device sends requests for resolving hostnames in IP addresses to a DNS server.

The menu contains the following dialogs:
- DNS Client Global
- DNS Client Current
- DNS Client Static

9.2.1.1 DNS Client Global

[Advanced > DNS > Client > Global]

In this dialog, you enable the *Client* 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.

9.2.1.2 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

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Index

Displays the sequential number of the DNS server.

Address

Displays the IP address of the DNS server. The device forwards requests for resolving hostnames in IP addresses to the DNS server with this IP address.

9.2.1.3 DNS Client Static

[Advanced > DNS > Client > Static]

In this dialog, you specify the DNS servers to which the device forwards requests for resolving hostnames 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

Source

Specifies the source from which the device obtains the IP address of DNS servers to which the device addresses requests.

Possible values:

- *user*
  The device uses the IP addresses specified in the table.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

 Add

Opens the *Create* window to add a table row.

- In the *Index* field, you specify the index number.
  Possible values:
  - `1..4`
    The device lets you specify up to 4 external DNS servers.
- In the *IP address* field, you specify the IP address of the DNS server.
  Possible values:
  - Valid IPv4 address

 Remove

Removes the selected table row.

Index

Displays the sequential number of the DNS server. You specify the index number when you add a table row.

IP address

Specifies the IP address of the DNS server.

Possible values:

- Valid IPv4 address

Active

Activates/deactivates the table row.

Prerequisites:

- In the *Advanced > DNS > Client > Global* dialog the *DNS client* function is enabled.
- In the *Configuration* frame, the item `user` is selected from the *Source* drop-down list.

Possible values:

- `marked` (default setting)
  The table row is active.
  The device sends requests to the DNS server specified in the first active table row. When the device does not receive a response from this server, it sends the requests to the DNS server specified in the next active table row. The relevant timeout is specified in the *Configuration* frame, *Request timeout [s]* field.
- `unmarked`
  The table row is inactive.
  The device does not send requests to this DNS server.

9.2.2 DNS Cache

[Advanced > DNS > Cache]

The *Cache* function lets the device respond to requests for resolving hostnames in IP addresses.

The menu contains the following dialogs:

- DNS Cache Global

9.2.2.1 DNS Cache Global

[Advanced > DNS > Cache > Global]

In this dialog, you enable the *Cache* function. When the *Cache* function is enabled, the device operates as a Caching DNS server.

When a downstream device requests the IP address of an unknown hostname and the Caching DNS server finds a matching entry in its cache, the Caching DNS server returns the IP address.

The cache provides memory space for up to 128 hostnames with associated IP address.

Operation

Buttons

Flush cache

Deletes every entry from the DNS cache.

Operation

Enables/disables the *Cache* function.

Possible values:

- *On* (default setting)
  The *Cache* function is enabled.
- *Off*
  The *Cache* function is disabled.

9.3 Tracking

[Advanced > 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 *Advanced > 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 from the *Track name* drop-down list.

The menu contains the following dialogs:

- Tracking Configuration
- Tracking Applications

9.3.1 Tracking Configuration

[Advanced > Tracking > Configuration]

In this dialog, you set up the tracking objects.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons


Add

Opens the *Create* window to add a table row.

- From the *Type* drop-down list, you select 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 sending periodic *ICMP echo request* packets.
  - *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..256


Remove

Removes the selected table row.

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 sending periodic *ICMP echo request* packets.
- *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 the values displayed in the *Type* and *Track ID* columns.

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 *ICMP echo 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 *ICMP echo 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 *ICMP echo request* packets for the number of times specified here, 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 *ICMP echo request* packets for the number of times specified here, 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 *ICMP echo request* packets.

TTL (Time To Live, also known as “Hop Count”) identifies the maximum number of routing steps, which the sent *ICMP echo request* packet may traverse on its 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.

9.3.2 Tracking Applications

[Advanced > 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 to open the *Create* window and select the tracking object from the *Track name* drop-down list.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

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 the values displayed in the *Type* and *Track ID* columns.

9.4 Command Line Interface

[Advanced > CLI]

This dialog lets you access the device using the Command Line Interface.

Prerequisites:
- In the *Device Security > Management Access > Server* dialog, *SSH* tab the SSH server is enabled.
- On your workstation, install a SSH-capable client application which registers a handler for URLs starting with `ssh://` in your operating system.

Buttons

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 an SSH-capable client application, then the SSH-capable client establishes a connection to the device management using the SSH protocol.

A Index

P

Q

R

S

B Technical 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.belden.com.

For technical support, visit 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 decide against any compromise in any case. 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 IRD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen
  Germany

HIRSCHMANN

A BELDEN BRAND

HIRSCHMANN
A BELDEN BRAND

User Manual

Configuration
Industrial Firewall
EAGLE40-03

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

You find the latest user documentation for your device at: doc.hirschmann.com

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

Contents

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 item
–	List item – second level
▶	Parameter value
☐	Task 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 device

The device provides the following plug-and-play solutions for replacing a device with a device of the same type, for instance, if a failure was detected or for preventive maintenance:

- 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 91.

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 transfer your own digital certificate onto the device.
  See “HTTPS certificate management” on page 310.
- 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 “Transferring your own key onto the device” on page 301.

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) Serial interface (Out-of-Band)	Terminal emulation software
System Monitor 1	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:
Web browsers and other third-party software routinely validate digital certificates.

If your web browser displays a message indicating a conflict in validating the digital certificate of the device, perform the following steps:
- ☐ Verify if the digital certificate has expired.
- ☐ Verify if your web browser no longer regards the algorithm used for generating the digital certificate as trustworthy.

To solve the conflict in validation, regenerate the digital certificate on the device using the latest device software. As an alternative, generate a digital certificate externally, using up-to-date signature algorithms. Transfer the new digital certificate onto the device.

Starting the Graphical User Interface

The prerequisite for starting the Graphical User Interface is that the IP parameters are set up in the device. See “Specifying the IP parameters” on page 39.

Perform the following steps:
- ☐ Start your web browser.
- ☐ Type the IP address of the device in the address field of the web browser.
  Use the following form: `https://xxx.xxx.xxx.xxx`
  The web browser sets up the connection to the device and displays the login dialog.
- ☐ When you want to change the language of the Graphical User Interface, click the appropriate link in the top right corner of the login dialog.
- ☐ Enter the user name.

- ☐ Enter the password.
  The default password is `private`.
  After you enter the default password for the first time, the device will prompt you to assign a new password.
- ☐ Click the *Login* button.
  The web browser displays the Graphical User Interface.

1.2 Command Line Interface

The Command Line Interface lets you 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*. You can download the software from www.chiark.greenend.org.uk/~sgtatham/putty/.

- ☐ Install the *PuTTY* program on your computer.

1.2.2 Access to the Command Line Interface using the Secure Shell (SSH)

In the following example, you use the *PuTTY* program. Another option to access your device using SSH is the OpenSSH Suite.

Perform the following steps:

- ☐ Start the *PuTTY* program on your computer.

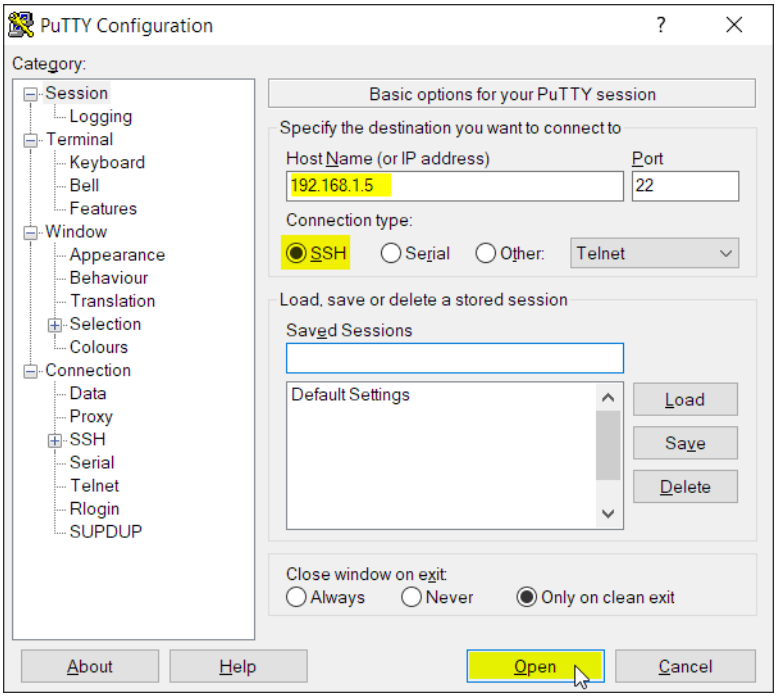


Figure 1:PuTTY input screen

- In the *Host Name (or IP address)* field you enter the IP address of your device.
  The IP address consists of 4 decimal numbers with values from `0` to `255`. The 4 decimal numbers are separated by points.
- Specify the connection type.
  Select the *SSH* radio button in the *Connection type* option list.
  After selecting and setting the required parameters, the device lets you 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 set up, establishing the connection takes up to a minute.
  When you first log into the device management, towards the end of the connection setup, the *PuTTY* program displays a security alert message and lets you check the fingerprint of the key.

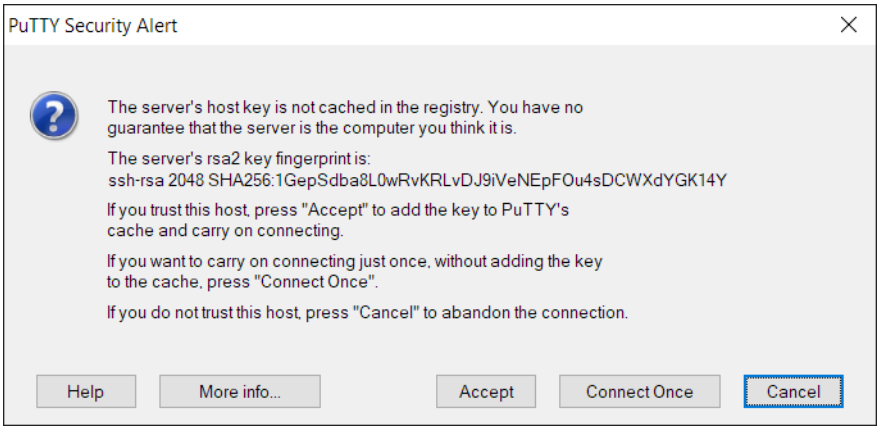


Figure 2:Security alert prompt for the fingerprint

- Check the fingerprint.
  This helps protect yourself from unwelcome guests.
- When the fingerprint matches the fingerprint of the device key, click the *Yes* button.
  The device lets you display the finger prints of the device keys with the command `show ssh` or in the *Device Security > Management Access > Server* dialog, *SSH* tab.
  The Command Line Interface appears on the screen with a window for entering the user name.
  The device enables up to 5 users to have access to the Command Line Interface at the same time.
- Enter the user name.
  The default user name is `admin`.
- Press the <Enter> key.

- ☐ Enter the password.
  The default password is `private`.
  After you enter the default password for the first time, the device will prompt you to assign a new password.
- ☐ Press the <Enter> key.

```
login as: admin
admin@192.168.1.5's password:


                    Copyright (c) 2011-2025 Hirschmann Automation and Control GmbH

                                  All rights reserved

                              EAGLE40 Release HiSecOS-05.2.00

                               (Build date 2025-04-08 08:49)


                    System Name   :  EAGLE40-ECE555d6e545
                    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
                    System Time   :  2025-04-10 12:00:33


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.

EAGLE>
```

Figure 3: Start screen of the Command Line Interface

1.2.3 Access to the device management using the Command Line Interface through the serial connection

You can connect an external management station (VT100 terminal or PC with terminal emulation) to the serial interface. The device lets you set up the serial connection to access the device management using System Monitor 1 or the Command Line Interface.

VT 100 terminal settings	
Speed	`115200 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. As an alternative, connect the device to a COM port of your PC using terminal emulation based on VT100 and press any key.
- ☐ As an alternative, you set up the serial data connection to the device with the serial interface using the *PuTTY* program. Press the <Enter> key.

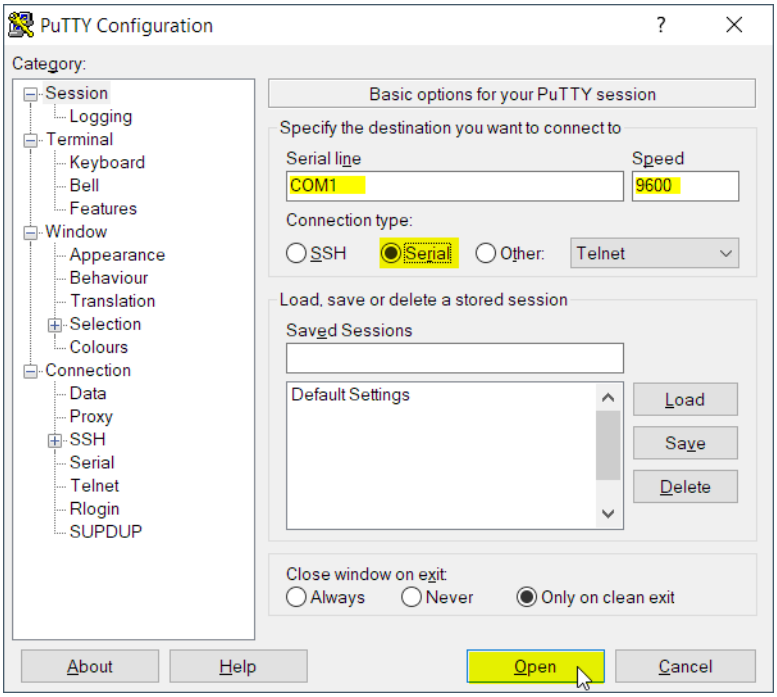


Figure 4:Serial data connection with the serial interface using the PuTTY program

- ☐ 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`.
  After you enter the default password for the first time, the device will prompt you to assign a new password.
- ☐ Press the <Enter> key.

```
                Copyright (c) 2011-2025 Hirschmann Automation and Control GmbH

                                All rights reserved

                            EAGLE40 Release HiSecOS-05.2.00

                             (Build date 2025-04-08 08:49)


                System Name   :  EAGLE40-ECE555d6e545
                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
                System Time   :  2025-04-10 12:00:33


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.

EAGLE>
```

Figure 5: Start screen of the Command Line Interface

1.2.4 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 lets you execute these commands in the *Privileged Exec* mode.

The following figure displays the modes of the Command Line Interface.

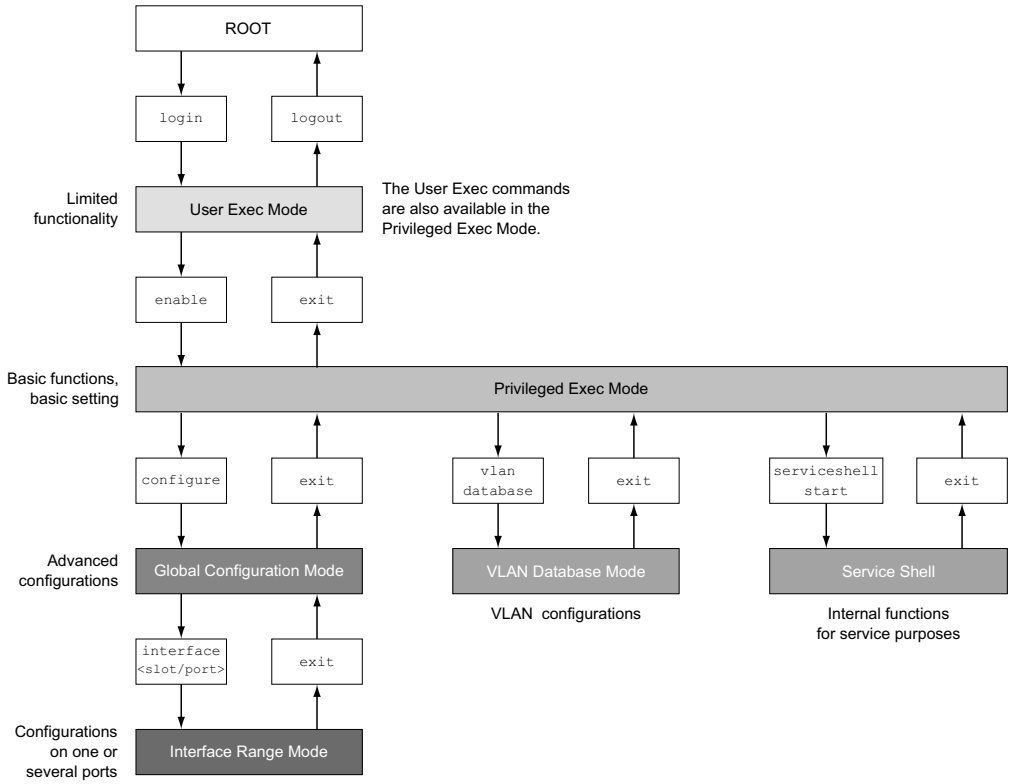


Figure 6: Structure of the Command Line Interface

The Command Line Interface supports, depending on the user level, the following modes:

- *User Exec* mode
  When you log into the device management with the Command Line Interface, you are in the *User Exec* mode. The *User Exec* mode contains a limited range of commands.
  Command prompt: `(EAGLE) >`
- *Privileged Exec* mode
  To access the entire range of commands, you change to the *Privileged Exec* mode. The prerequisite for changing to the *Privileged Exec* mode is that you log into the device management as a privileged user. In the *Privileged Exec* mode, you are able to execute the *User Exec* mode commands, too.
  Command prompt:`(EAGLE) #`
- VLAN mode
  The VLAN mode contains VLAN-related commands.
  Command prompt: `(EAGLE) (VLAN)#`
- Service Shell
  The Service Shell is for service purposes only.
  Command prompt: `/mnt/fastpath #`

- *Global Config* mode
  The *Global Config* mode lets you perform modifications to the current configuration. This mode groups general setup commands.
  Command prompt: `(EAGLE) (config)#`
- *Interface Range* mode
  The commands in the *Interface Range* mode affect a specific port, a selected group of multiple ports or all port of the device. The commands modify a value or switch a function on/off on one or more specific ports.
  - All physical ports in the device
    Command prompt: `(EAGLE) ((interface) all)#`
    Example: When you switch from the *Global Config* mode to the *Interface Range* mode, the command prompt changes as follows:
    ```
    (EAGLE) (config)#interface all
    (EAGLE) ((Interface)all)#
    ```
  - A single port on one interface
    Command prompt: `(EAGLE) (interface <slot/port>)#`
    Example: When you switch from the *Global Config* mode to the *Interface Range* mode, the command prompt changes as follows:
    ```
    (EAGLE) (config)#interface 2/1
    (EAGLE) (interface 2/1)#
    ```
  - A range of ports on one interface
    Command prompt: `(EAGLE) (interface <interface range> )#`
    Example: When you switch from the *Global Config* mode to the *Interface Range* mode, the command prompt changes as follows:
    ```
    (EAGLE) (config)#interface 1/2-1/4
    (EAGLE) ((Interface)1/2-1/4)#
    ```
  - A list of single ports
    Command prompt: `(EAGLE) (interface <interface list>)#`
    Example: When you switch from the *Global Config* mode to the *Interface Range* mode, the command prompt changes as follows:
    ```
    (EAGLE) (config)#interface 1/2,1/4,1/5
    (EAGLE) ((Interface)1/2,1/4,1/5)#
    ```
  - A list of port ranges and single ports
    Command prompt: `(EAGLE) (interface <complex range>)#`
    Example: When you switch from the *Global Config* mode to the *Interface Range* mode, the command prompt changes as follows:
    ```
    (EAGLE) (config)#interface 1/2-1/4,1/6-1/9
    (EAGLE) ((Interface)1/2-1/4,1/6-1/9)
    ```

The following table displays the command modes, the command prompts (input request characters) visible in the corresponding mode, and the option with which you quit this mode.

Table 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`:
		`(EAGLE) >logout`
		`Are you sure (Y/N) ?y`

Privileged Exec mode	From the *User Exec* mode, you enter the command `enable`:
	`(EAGLE) >enable`
	`(EAGLE) #`
		To quit the *Privileged Exec* mode and return to the *User Exec* mode, you enter `exit`:
		`(EAGLE) #exit`
		`(EAGLE) >`

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`:
	`(EAGLE) #vlan database`
	`(EAGLE) (Vlan)#`
		To end the VLAN mode and return to the *Privileged Exec* mode, you enter `exit` or press <CTRL>+<Z>.
		`(EAGLE) (Vlan)#exit`
		`(EAGLE) #`

Global Config mode	From the *Privileged Exec* mode, you enter the command `configure`:
	`(EAGLE) #configure`
	`(EAGLE) (config)#`
	From the *User Exec* mode, you enter the command `enable`, and then in *Privileged Exec* mode, enter the command `Configure`:
	`(EAGLE) >enable`
	`(EAGLE) #configure`
	`(EAGLE) (config)#`
		To quit the *Global Config* mode and return to the *Privileged Exec* mode, you enter `exit`:
		`(EAGLE) (config)#exit`
		`(EAGLE) #`
		To then quit the *Privileged Exec* mode and return to the *User Exec* mode, you enter `exit` again:
		`(EAGLE) #exit`
		`(EAGLE) >`

Interface Range mode	From the *Global Config* mode you enter the command `interface {all|<slot/port>|<interface range> |<interface list>|<complex range>}`.
	`(EAGLE) (config)#interface <slot/port>`
	`(EAGLE) (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>.
		`(EAGLE) (interface slot/port)#exit`
		`(EAGLE) #`

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.

```
(EAGLE)>
  cli              Set the CLI preferences.
  enable           Turn on privileged commands.
  help             Display help for various special keys.
  history          Show a list of previously run commands.
  logout           Exit this session.
  ping             Send ICMP echo packets to a specified IP address.
  show             Display device options and settings.

(EAGLE)>
```

Figure 7: Commands in the User Exec mode

1.2.5 Executing the commands

Syntax analysis

When you log into the device management with the Command Line Interface, you are in the *User Exec* mode. The Command Line Interface displays the prompt `(EAGLE)>` on the screen.

When you enter a command and press the <Enter> key, the Command Line Interface starts the syntax analysis. The Command Line Interface searches the command tree for the desired command.

When the command is outside the Command Line Interface command range, a message informs you of the detected error.

Example:

You want to execute the `show system info` command, but enter `info` without `f` and press the <Enter> key.

The Command Line Interface then displays a message:

```
(EAGLE)>show system 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.

1.2.6 Structure of a command

This section describes the syntax, conventions and terminology, and uses examples to represent them.

Format of commands

Most of the commands include parameters.

When the command parameter is missing, the Command Line Interface informs you about the detection of an incorrect command syntax.

This manual displays the commands and parameters in the `Courier` font.

Parameters

The sequence of the parameters is relevant for the correct syntax of a command.

Parameters are required values, optional values, selections, or a combination of these things. The representation indicates the type of the parameter.

Table 3: Parameter and command syntax

`<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. 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 insert 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:

```
*(EAGLE)#cli prompt Device name
Error: Invalid command 'name'

*(EAGLE)#cli prompt 'Device name'

*(Device name)#
```

1.2.7 Examples of commands

Example 1: clear arp-table-switch

Command for clearing the ARP table of the management agent (cache).

`clear arp-table-switch` is the command name. The command is executable without any other parameters by pressing the <Enter> key.

Example 2: radius server timeout

Command to specify the RADIUS server timeout value.

```
(EAGLE) (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.

```
(EAGLE) (config)#radius server auth modify 1
 [name]               RADIUS authentication server name.
 [port]               RADIUS authentication server port.
                      (default: 1812).
 [msgauth]            Enable or disable the message authenticator
                      attribute for this server.
 [primary]            Configure the primary RADIUS server.
 [status]             Enable or disable a RADIUS authentication
                      server entry.
 [secret]             Configure the shared secret for the RADIUS
                      authentication server.
 [encrypted]          Configure the encrypted shared secret.
  <cr>                Press Enter to execute the command.
```

`radius server auth modify` is the command name.

The parameter `<1..8>` (RADIUS server index) is required. The value range is `1..8` (integer).

The parameters `[name]`, `[port]`, `[msgauth]`, `[primary]`, `[status]`, `[secret]` and `[encrypted]` are optional.

1.2.8 Input prompt

Command mode

With the input prompt, the Command Line Interface displays which of the three modes you are in:

- `(EAGLE) >`
  User Exec mode
- `(EAGLE) #`
  Privileged Exec mode
- `(EAGLE) (config)#`
  Global Config mode
- `(EAGLE) (Vlan)#`
  VLAN Database mode
- `(EAGLE) ((Interface)all)#`
  Interface Range mode / All ports of the device
- `(EAGLE) ((Interface)2/1)#`
  Interface Range mode / A single port on one interface
- `(EAGLE) ((Interface)1/2-1/4)#`
  Interface Range mode / A range of ports on one interface
- `(EAGLE) ((Interface)1/2,1/4,1/5)#`
  Interface Range mode / A list of single ports
- `(EAGLE) ((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.
  `*(EAGLE)>`
- Pound sign `#`
  A pound sign `#` at the beginning of the input prompt displays you that the boot parameters and the parameters during the boot phase are different.
  `*#(EAGLE)>`
- Exclamation point `!`
  An exclamation point `!` at the beginning of the input prompt displays: the password for the `admin` user account corresponds with the default setting.
  `!(EAGLE)>`

Wildcards

The device lets you change the command line prompt.

The Command Line Interface supports the following wildcards:

Table 6: Using wildcards within the Command Line Interface input prompt

Wildcard	Description
`%d`	System date
`%t`	System time
`%i`	IP address of the device
`%m`	MAC address of the device
`%p`	Product name of the device

```
!(EAGLE)>enable

!(EAGLE)#cli prompt %i

!192.168.1.5#cli prompt (EAGLE)%d

!*(EAGLE)2025-04-10#cli prompt (EAGLE)%d%t

!*(EAGLE)2025-04-10 12:00:33#cli prompt %m

!*AA:BB:CC:DD:EE:FF#
```

1.2.9 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:

```
(EAGLE) #help

HELP:
Special keys:

  Ctrl-H, BkSp delete previous character
  Ctrl-A  .... go to beginning of line
  Ctrl-E  .... go to end of line
  Ctrl-F  .... go forward one character
  Ctrl-B  .... go backward one character
  Ctrl-D  .... delete current character
  Ctrl-U, X .. delete to beginning of line
  Ctrl-K  .... delete to end of line
  Ctrl-W  .... delete previous word
  Ctrl-P  .... go to previous line in history buffer
  Ctrl-R  .... rewrites or pastes the line
  Ctrl-N  .... go to next line in history buffer
  Ctrl-Z  .... return to root command prompt
  Ctrl-G  .... aborts running tcpdump session
  Tab, <SPACE> command-line completion
  Exit    .... go to next lower command prompt
  ?       .... list choices

(EAGLE) #
```

Figure 8: Listing the key combinations with the Help command

1.2.10 Data entry elements

Command completion

To simplify typing commands, the Command Line Interface lets you use command completion (Tab Completion). Thus you are able to abbreviate key words.

- Type in the beginning of a keyword. When the characters entered identify a keyword, the Command Line Interface completes the keyword after you press the tab key or the space key. When there is more than one option for completion, enter the letter or the letters necessary for uniquely identifying the keyword. Press the tab key or the space key again. After that, the system completes the command or parameter.
- When you make a non-unique entry and press <Tab> or <Space> twice, the Command Line Interface provides you with a list of options.
- On a non-unique entry and pressing <Tab> or <Space>, the Command Line Interface completes the command up to the end of the uniqueness. When several commands exist and you press <Tab> or <Space> again, the Command Line Interface provides you with a list of options.
  Example:
  ```
  (EAGLE) (Config)#lo
  (EAGLE) (Config)#log
  logging logout
  ```
  When you enter `lo` and <Tab> or <Space>, the Command Line Interface completes the command up to the end of the uniqueness to `log`.
  When you press <Tab> or <Space> again, the Command Line Interface provides you with a list of options (`logging logout`).

Possible commands/parameters

You can obtain a list of the commands or the possible parameters by entering `help` or `?`, for example by entering `(EAGLE) >show ?`

When you enter the command displayed, you get a list of the parameters available for the command `show`.

When you enter the command without space character in front of the question mark, the device displays the help text for the command itself:

```
!*#(EAGLE)(Config)#show?

   show          Display device options and settings.
```

1.2.11 Use cases

Saving the Configuration

To help ensure that your password settings and your other configuration changes are kept after the device is reset or after an interruption of the voltage supply, you save the configuration. To do this, perform the following steps:

- ☐ Enter `enable` to change 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:

- Prerequisites for executing the command:
  - You are in the *Global Config* mode.
    See “Mode-based command hierarchy” on page 21.
  - You have the access role *administrator*.

Syntax of commands and parameters: See “Structure of a command” on page 25.

Examples for executable commands:

- `radius server auth add 1 ip 192.168.30.40`
- `radius server auth add 2 ip 192.168.40.50 name radiusserver2`
- `radius server auth add 3 ip 192.168.50.60 port 1813`
- `radius server auth add 4 ip 192.168.60.70 name radiusserver4 port 1814`

1.2.12 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 an inoperable device**.

Start the Service Shell

The prerequisite is that you are in *User Exec* mode: `(EAGLE) >`

Perform the following steps:

- ☐ Enter `enable` and press the <Enter> key.
  To reduce the effort when typing:
  - ☐ Enter `e` and press the <Tab> key.
- ☐ Enter `serviceshell start` and press the <Enter> key.
  To reduce the effort when typing:
  - ☐ Enter `ser` and press the <Tab> key.
  - ☐ Enter `s` and press the <Tab> key.

```
!EAGLE >enable

!*EAGLE #serviceshell start
 WARNING! The service shell offers advanced diagnostics and functions.
 Proceed only when instructed by a service technician.

 You can return to the previous mode using the 'exit' command.

 BusyBox v1.31.0 (2025-04-10 12:00:33 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 possibilities of service personnel 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. **To reactivate the Service Shell, the device requires disassembly by the manufacturer.**

The prerequisites are:
- The Service Shell is not started.
- You are in *User Exec* mode: `(EAGLE) >`

Perform the following steps:
☐ Enter `enable` and press the <Enter> key.
To reduce the effort when typing:
☐ Enter `e` and press the <Tab> key.

- ☐ Enter `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.

```
!EAGLE >enable

!*EAGLE #serviceshell deactivate
Notice: If you continue, then the Service Shell is permanently deactivated.
This step is irreversible!
For details, refer to the Configuration Manual.
Are you sure (Y/N) ?
```

1.3 System Monitor 1

The System Monitor 1 lets you set basic operating parameters before starting the operating system.

1.3.1 Functional scope

In System Monitor 1, you carry out the following tasks, for example:
- Managing the operating system and verifying the device software image
- Updating the operating system
- Starting the operating system
- Deleting configuration profiles, resetting the device to the factory settings
- Checking boot code information

1.3.2 Accessing System Monitor 1

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	115200 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 change to System Monitor 1.
  ```
- ☐ Press the <1> key within 3 seconds.
  The device starts the System Monitor 1. The screen displays the following view:

```
System Monitor 1
(Selected OS: ...-5.2 (2025-04-08 08:49))

1  Manage operating system
2  Update operating system
3  Start selected operating system
4  Manage configurations
5  Show boot code information
q  End (reset and reboot)




sysMon1>
```

Figure 9: System Monitor 1 view

- ☐ Select a menu item by entering the number.
- ☐ To leave a submenu and return to the main menu, press the <ESC> key.

2 Specifying the IP parameters

When you install the device for the first time, specify the IP parameters.

The device provides the following options for entering the IP parameters during the first installation:

- Entry using the Command Line Interface.
  When you preconfigure your device outside its operating environment, or restore the network access (“In-Band”) to the device, choose this “Out-of-Band” method.
- Entry using the HiDiscovery protocol.
  When you have a previously installed network device or you have another Ethernet connection between your PC and the device, you choose this “In-Band” method.
- Configuration using the external memory.
  When you are replacing a device with a device of the same type and have already saved the configuration in the external memory, you choose this method.
- Configuration using the Graphical User Interface.
  When the device already has an IP address and is reachable using the network, the Graphical User Interface provides you with another option for configuring the IP parameters.

2.1 IP parameter basics

2.1.1 IPv4

IP address

The IP addresses consist of 4 bytes. Write these 4 bytes in decimal notation, separated by a decimal point.

RFC 1340 written in 1992, defines 5 IP address classes.

Table 8: IP address classes

Class	Network address	Host address	Address range
A	1 Byte	3 Bytes	0.0.0.0..127.255.255.255
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

The first byte of an IP address is the network address. The worldwide leading regulatory board for assigning network addresses is the Internet Assigned Numbers Authority (IANA). 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

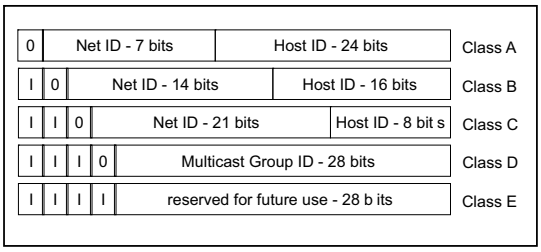


Figure 10: Bit representation of the IP address

When the first bit of an IP address is 0, it belongs to class A. The first octet is less than 128.

When the first bit of an IP address is 1 and the second bit is 0, it belongs to class B. The first octet is between 128 and 191.

When the first 2 bits of an IP address are 1, it belongs to class C. The first octet is higher than 191.

Assigning the address of the host (*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 subnets. The netmask assigns the IP addresses of the individual devices to a particular subnet.

You perform subnet 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 subnet 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

How to use the netmask

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?

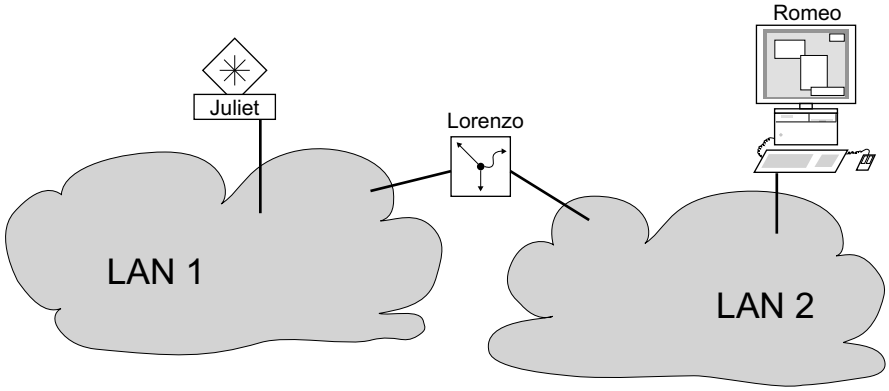


Figure 11: The management agent is separated from its network management station by a router

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 through Lorenzo, the same way the first letter traveled from Romeo to Juliet.

Classless Inter-Domain Routing

Class C with a maximum of 254 (2^8-2) addresses was too small, and class B with a maximum of 65534 $(2^{16}-2)$ 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 specify 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 combining a number of class C address ranges. Supernetting lets you 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 through the serial connection.

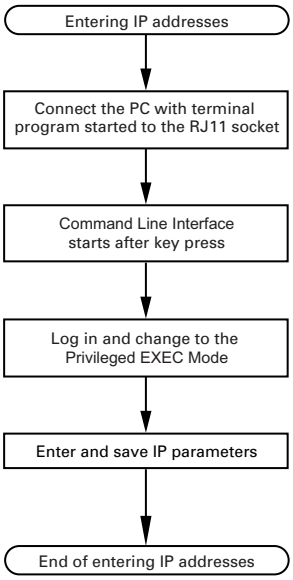
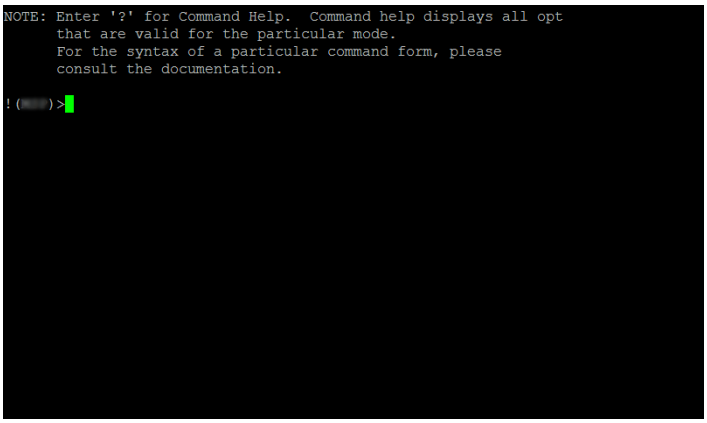


Figure 12: Flow chart for entering IP addresses

Note:
If a terminal or PC with terminal emulation is unavailable in the vicinity of the installation location, you can set up 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.



- ☐ Enter the IP parameters.
  - Local IP address
    In the default setting, the local IP address is `0.0.0.0`.
  - Netmask
    When you divided the network into subnets, and these are identified with a netmask, enter the netmask here. In the default setting, the local netmask is `0.0.0.0`.
  - IP address of the gateway.
    This entry is only required in cases where the device and the network management station are located in different subnets (see on page 41 “How to use the netmask”).
    Specify the IP address of the gateway between the subnet 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`	To change to the Privileged EXEC mode.
`network parms 10.0.1.23 255.255.255.0`	To 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`	To save the current settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

After entering the IP parameters, you easily set up the device using the Graphical User Interface.

2.3 Specifying the IP parameters using HiDiscovery

The HiDiscovery protocol lets you assign IP parameters to the device using the Ethernet.

You easily set up other parameters using the Graphical User Interface.

Perform the following steps:
- ☐ Install the HiDiscovery program on your computer.
- ☐ Start the HiDiscovery program.

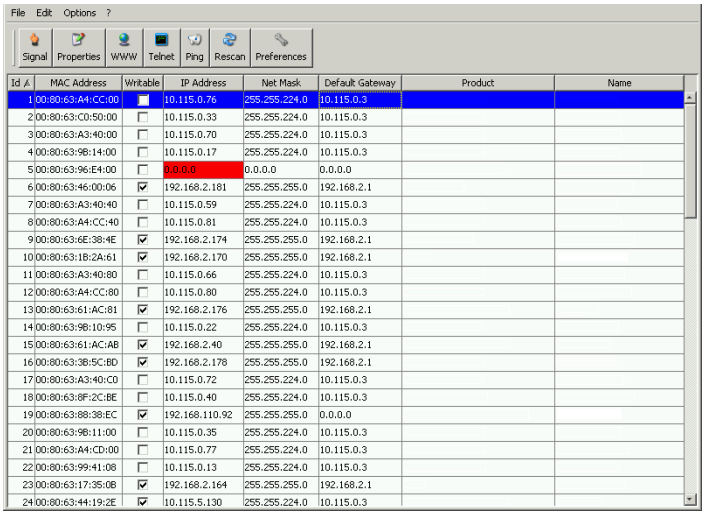


Figure 13: HiDiscovery

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 interfaces, you can select the desired network interface in the HiDiscovery toolbar.

HiDiscovery displays a line for every device that responds to a HiDiscovery protocol inquiry.

HiDiscovery lets you 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.

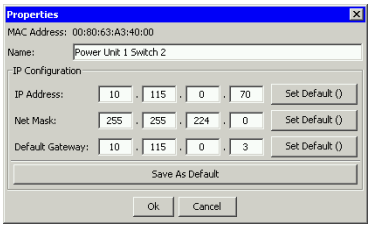


Figure 14: HiDiscovery – assigning IP parameters

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.

2.4 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 set up the HiDiscovery access.

- ☐ In the *VLAN ID* column you specify the VLAN in which the device management can be accessed over the network.

Note here that you can only access the device management using ports that are members of the relevant VLAN.

The *MAC address* field displays the MAC address of the device with which you access the device over the network.

- ☐ In the *HiDiscovery protocol v1/v2* frame you specify the settings for accessing the device using the HiDiscovery software.
- ☐ The HiDiscovery protocol lets you allocate an IP address to the device on the basis of its MAC address. Activate the HiDiscovery protocol if you want to allocate an IP address to the device from your PC with the HiDiscovery software.
- ☐ Open the *Basic Settings > Network > IPv4* dialog.

In this dialog, you specify the source from which the device gets its IP parameters after starting.

- ☐ In the *Management interface* frame you first specify where the device gets its IP parameters from:
  - In the `Local` mode, the device uses the network parameters from the internal device memory.

Note:
When you change the allocation mode of the IP address, the device activates the new mode immediately after you click the ✓ button.

- ☐ If required, you enter the IP address, the netmask and the *Gateway* in the *IP parameter* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

3 Access to the device

3.1 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 into the device management.
- ☐ Log into the device management 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 into the device management through the Command Line Interface, the device prompts you to confirm your new password.
- ☐ Log into the device management 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.

3.2 Authentication lists

When a user accesses the device management using a specific connection, the device verifies the login credentials of the user through an authentication list which contains the policies that the device applies for authentication.

The prerequisite for a user to access the device management is that at least one policy is assigned to the authentication list of the application through which access is performed.

3.2.1 Applications

The device provides an application for each type of connection through which someone accesses the device:

- Access to the Command Line Interface using the serial connection: `Console(V.24)`
- Access to the Command Line Interface using SSH: `SSH`
- Access to the Graphical User Interface: `WebInterface`

3.2.2 Policies

When a user logs in with valid login data, the device lets the user have access to its device management. The device authenticates the users using the following policies:

- User management of the device
- LDAP
- RADIUS

The device gives you the option of a fall-back solution. For this, you specify more than one policy in the authentication list. When authentication is unsuccessful using the current policy, the device applies the next specified policy.

3.2.3 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` To display 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.

☐ In the *Active* column of the desired authentication list, unmark the checkbox.

☐ Apply the settings temporarily. To do this, click the ✓ button.

`authlists disable <AuthList>`	To deactivate the authentication list `<AuthList>`.

3.2.4 Adjusting 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 passes authentication requests to a RADIUS or TACACS+ 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 table row.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`authlists add loginGUI`	To add 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.

☐ Apply the settings temporarily. To do this, click the ✓ button.

`authlists set-policy loginGUI radius local reject reject reject`	To assign the policies *`radius`*, *`local`* and *`reject`* to the authentication list `loginGUI`.
`show authlists`	To display the authentication lists that are set up.

☐ Assign an application to the authentication list `loginGUI`.

☐ Open the *Device Security > Authentication List* dialog.

☐ In the table, select the authentication list `loginGUI`.

☐ Click the button.
The dialog displays the *Allocate applications* window.

- ☐ Click the application `WebInterface` to highlight it.
- ☐ 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`show applists`	To display the applications and the allocated lists.
`applists set-authlist WebInterface loginGUI`	To assign the `loginGUI` application to the authentication list `WebInterface`.

3.3 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 or TACACS+ 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.

3.3.1 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.

Note:
The following applies to the Command Line Interface: Users to whom a specific authorization profile is assigned are allowed to use commands and functions from this authorization profile or a lower level role. The commands available to a user also depend on the Command Line Interface mode in which the user is currently working. See “Mode-based command hierarchy” on page 21.

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.

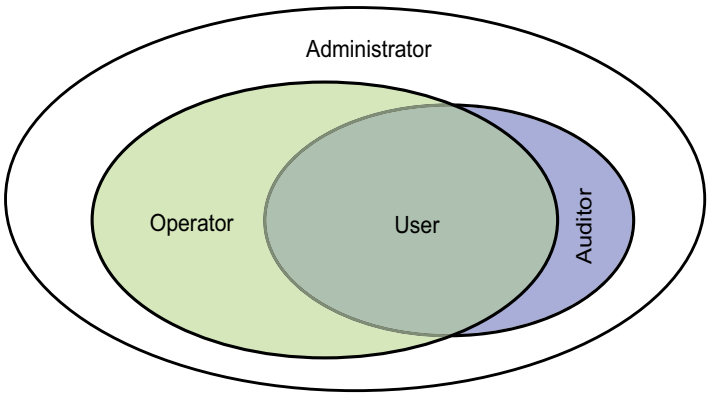


Figure 15: Access roles for user accounts

Table 9: 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: • Add, modify or delete user accounts • Activate, deactivate or unlock user accounts • Change every password • Set up the password management • Set or change system time • Load files to the device, for example, device settings, certificates, or device software images • Reset settings and security-related settings to the state on delivery • Set up the RADIUS or TACACS+ server and the authentication lists • Apply scripts using the Command Line Interface • Enable/disable CLI logging and SNMP logging • External memory activation and deactivation • Activate or deactivate System Monitor 1 • Enable/disable the services for the access to the device management (for example SNMP). • Set up 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 set up 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. • As an administrator you assign this access role to temporarily lock a user account. • If an administrator assigns a different access role to the user account and an error is detected, then the device assigns this access role to the user account.	No activities allowed.

3.3.2 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` — To display the user accounts that are set up.

3.3.3 Default user accounts

In the default setting, the user account `admin` is set up in the device.

Table 10: Settings of the default user account

Parameter	Default setting
User name	`admin`
Password	`private`
Role	*`administrator`*
User locked	`unmarked`
Policy check	`unmarked`
SNMP auth type	*`hmacmd5`*
SNMP encryption type	*`des`*

Change the password for the `admin` user account before making the device available in the network.

3.3.4 Changing default passwords

To help prevent undesired access, change the password of the default user account. To do this, perform the following steps:

☐ Change the password for the `admin` user account.

- ☐ Open the *Device Security > User Management* dialog.
  The dialog displays the user accounts that are set up.
- ☐ To require a specified minimum complexity for the passwords, 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 table 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`users password-policy-check <user> enable`	To activate the checking of the password for the `<user>` user account based on the specified policy. In this way, you require a specified minimum complexity for the passwords.

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`	To specify the password `SECRET` for the user account `USER`. Enter at least 6 characters.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

3.3.5 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, you set up the user account for a user `USER` with the access role *`operator`*. Users with the access role *`operator`* are authorized to monitor and set up the device, with the exception of security-related settings. To do this, perform the following steps:

☐ Create a 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, you give the user account the name `USER`.
- ☐ Click the *Ok* button.
- ☐ To require a specified minimum complexity for the passwords, 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 access role.
  In this example, you select the value *operator*.
- ☐ To activate the user account, mark the checkbox in the *Active* column.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
  The dialog displays the user accounts that are set up.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`users add USER`	To add the `USER` user account.
`users password-policy-check USER enable`	To activate the checking of the password for the `USER` user account based on the specified policy. In this way, you require a specified minimum complexity for the passwords.
`users password USER SECRET`	To specify the password `SECRET` for the user account `USER`. Enter at least 6 characters.
`users access-role USER operator`	To assign the access role *operator* to the user account `USER`.
`users enable USER`	To activate the user account `USER`.
`show users`	To display the user accounts that are set up.
`save`	To 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.

3.3.6 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 table row for the relevant user account, unmark the checkbox in the *Active* column.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`users disable <user>`	To disable user account.
`show users`	To display the user accounts that are set up.
`save`	To 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.

☐ Select the table row of the relevant user account.

☐ Click the button.

`users delete <user>`	To delete the user account `<user>`.
`show users`	To display the user accounts that are set up.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

3.3.7 Adjusting policies for passwords

The device lets you check if the passwords for the user accounts match the specified policy. When the passwords match the policy, you obtain a higher 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 of consecutive unsuccessful 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 consecutive unsuccessful login attempts as well as the possible lockout of the user apply only when accessing the device management through:

- the Graphical User Interface
- the SSH protocol

Note:
When accessing the device management using the Command Line Interface through the serial connection, the number of unsuccessful 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 can attempt to log into the device management. 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.

☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`passwords min-length 6`	To specify the policy for the minimum length of the password.
`passwords min-lowercase-chars 1`	To specify the policy for the minimum number of lower-case letters in the password.
`passwords min-numeric-chars 1`	To specify the policy for the minimum number of digits in the password.
`passwords min-special-chars 1`	To specify the policy for the minimum number of special characters in the password.
`passwords min-uppercase-chars 1`	To specify the policy for the minimum number of upper-case letters in the password.
`show passwords`	To display the policies that are set up.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

3.4 LDAP function

Server administrators manage *Active Directories* which contain user login credentials for applications used in the office environment. The *Active Directory* is hierarchical in nature, containing user names, passwords, and the authorized read/write permission levels for each user.

This device uses the Lightweight Directory Access Protocol (LDAP) to retrieve user login information and permission levels from a *Active Directory*. This provides a “single sign on“ for network devices. Retrieving the login credentials from an *Active Directory* lets the user log in with the same login credentials used in the office environment.

An LDAP session starts with the device contacting the Directory System Agent (DSA) to search the *Active Directory* of an LDAP server. If the server finds multiple entries in the *Active Directory* for a user, then the server sends the higher permission level found. The DSA listens for information requests and sends responses on TCP port `389` for LDAP, or on TCP port `636` for LDAP over SSL (LDAPS). Clients and servers encode LDAPS requests and responses using the Basic Encoding Rules (BER). The device opens a new connection for every request and closes the connection after receiving a response from the server.

The device lets you transfer a digital certificate to the device. The certificate helps the device to verify the server for Secure Socket Layer (SSL) and Transport Layer Security (TLS) connections. For security reasons, Hirschmann recommends using only digital certificates signed by a Certification Authority (CA).

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

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.

3.4.1 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 digital 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.

3.4.2 Setting up LDAP

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, you specify which attributes in the *Active Directory* contain the user login credentials and the permission level. The device then compares the user login credentials with the permission levels specified in the device and lets the user log into the device management at the assigned permission level.

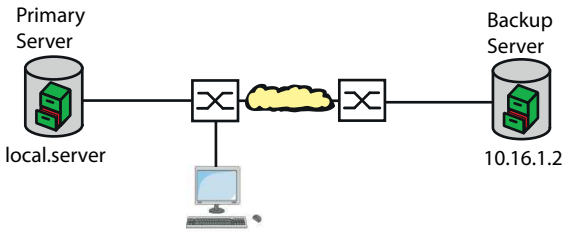


Figure 16: Application example of an LDAP setup

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 digital certificate)	`SSL`
The server administrator sent the digital certificate in an email.	Digital certificate for primary server saved locally	Digital 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` `ADMINISTRATOR`	`OPERATOR` `ADMINISTRATOR`

Perform the following steps:

- ☐ Open the *Device Security > Authentication List* dialog.
- ☐ To set up the device to retrieve the user login credentials from the first *Active Directory*, 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, specify 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, specify 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 digital certificate to verify the identity of the server.

- ☐ When the file is located on your PC or on a network drive, drag and drop it onto the area. As an alternative, click in the area to select the file.
- ☐ To transfer the file to the device, click the *Start* button.
- ☐ To add a table row, 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 digital certificate for server validation. In the *Connection security* column, specify the value `startTLS`.
- ☐ To activate the table row, mark the checkbox in the *Active* column.
- ☐ Using the information received from the Backup server administrator, add and activate another table row, then specify the settings in the corresponding columns.

- ☐ Open the *Device Security > LDAP > Role Mapping* dialog.
- ☐ To add a table row, click the button.

When a user logs into the device management, with LDAP set up 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 into the device management 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 access role.
- ☐ To activate the table row, 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 access role *administrator*.
  To activate the table row, mark the checkbox in the *Active* column.
- ☐ Open the *Device Security > LDAP > Configuration* dialog.
- ☐ Enable the *LDAP* function.
  Select the *On* radio button in the *Operation* frame.

The following table describes how to set up the *LDAP* function in the device using the Command Line Interface. The table displays the commands for *Index*=1. To set up other indexes, use the same commands and substitute the appropriate information.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ldap cache-timeout 1440`	To specify the device to flush the non-volatile memory after a day.
`ldap client server add 1 local.server port 389`	To add a connection to the remote authentication client server with the hostname `local.server` and the UDP port `389`.
`ldap client server modify 1 security startTLS`	To specify the type of security used for the connection.
`ldap client server modify 1 description Primary_AD_Server`	To specify the configuration name of the entry.
`ldap basedn ou=Users,ou=City,ou=Country,dc=server,dc=local`	To specify the Base Domain Name used to find the *Active Directory* on the server.
`ldap search-attr userPrincipalName`	To specify the attribute to search for in the *Active Directory* which contains the login credential of the users.
`ldap bind-user user@company.com`	To specify the name and domain of the service user.
`ldap bind-passwd Ur-123456`	To specify the password of the service user.
`ldap client server enable 1`	To enable the remote authentication client server connection.
`ldap mapping add 1 access-role operator mapping-type attribute mapping-parameter OPERATOR`	To add a remote authentication role mapping entry for the access role *`operator`*. Map the access role *`operator`* to the attribute containing the word `OPERATOR`.
`ldap mapping enable 1`	To enable the remote authentication role mapping entry.
`ldap operation`	To enable the remote authentication function.

3.5 SNMP access

The Simple Network Management Protocol (SNMP) lets you work with a network management system to monitor the device over the network and change its settings.

3.5.1 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-only* access and `private` for *read and write* access 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 and write* access than for *read-only* 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.

3.5.2 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 the 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 table row of the relevant user account in the *SNMP auth type* field. Select the desired setting.
- ☐ Click the table row of the relevant user account in the *SNMP encryption type* field. Select the desired setting.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`users snmpv3 authentication <user> md5 | sha1`	To assign the HMAC-MD5 or HMACSHA protocol for authentication requests to the user account `<user>`.
`users snmpv3 encryption <user> des | aescfb128 | none`	To assign 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`	To display the user accounts that have been set up.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

4 VPN – Virtual Private Network

A virtual private network (VPN) refers to the part of a public network that someone uses for their private purposes.

The special feature of a VPN, as the name “private” suggests, is that the VPN tunnels the private data through a public network. Different measures help protect the data of the virtual private network from spying, data falsification and other attacks from external subscribers.

In the industrial environment, for example, a VPN serves to connect 2 plant sections with each other using the public Internet.

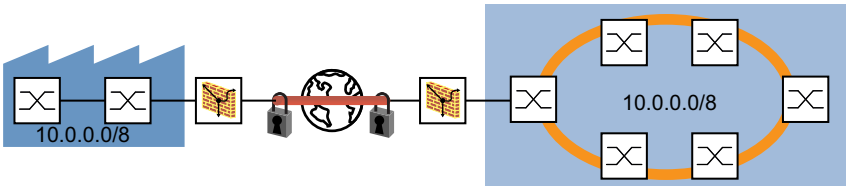


Figure 17: VPN for connecting 2 plant sections

4.1 Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec) is a protocol suite that authenticates and encrypts data packets sent over public networks.

Data transmission in a VPN involves:

- Integrity protection
  Integrity protection helps verify that the data transmitted is genuine, for example, that the data source is a trustworthy sender (is authentic) and that the recipient receives the data in its true form.
- Encryption
  Encryption helps protect the data prohibiting unauthorized persons from viewing the data. Encryption procedures code the data being transmitted using a code (key) that is only available to the authorized communication subscribers.
- Traffic flow confidentiality
  The traffic flow confidentiality helps protect the identification of the recipient and sender of the data packet from unauthorized person.
  IPsec performs this in the tunnel mode by encrypting the complete IP packet.

The 2 endpoints negotiate which security parameters to use on the VPN connection. IPsec provides 2 modes for the negotiations

- Transport mode
  In the transport mode, the 2 endpoints authenticate themselves to each other, then they set up the parameters required for signatures and encryption. As the communication is taking place between the 2 specific endpoints, the recipient and sender addresses remain visible.
- Tunnel mode
  In the tunnel mode, the 2 Routers/Gateways authenticate themselves to each other, then they set up the parameters required for signatures and encryption.
  With the 2 Routers/Gateways specific, the VPN connection has 2 addressable endpoints. But the communication takes place between the subscribers of the network connected to the Routers/Gateways. This permits the transmission of encryption communication data, including the recipient and sender addresses. The endpoints of the VPN connection use the addresses of the Routers/Gateways to send data.
  The device also lets you use the tunnel mode for the VPN connection between an endpoint and a Router/Gateway. Thus, the address data within the network connected to the Router/Gateway remains hidden.

4.2 Internet Key Exchange (IKE)

IPsec uses the Internet Key Exchange (IKE) protocol for authentication, for exchanging keys and for agreeing on further parameters for the security arrangement of a VPN connection.

4.2.1 Authentication

Use authentication as part of the security arrangement. During authentication, the connection peers display each other their ID cards, so to speak.

This ID card consists of the following parts:

- A pre-shared key, which is a character string previously exchanged using a different communication channel.
- A digital certificate signed by a Certification Authority (CA).
  Digital certificates in X.509 format contain the following data:
  - Information about the Certification Authority (CA)
  - Validity period of the digital certificate
  - Information about the permitted usage
  - The Designated Name (X.500 DN) that identifies the person who assigned the digital certificate to the Certification Authority (CA)
  - The public key belonging to this identity
  - A digital signature for verifying the connection between this identity and its related public key

  Larger companies and authorities usually have their own Certification Authority (CA).
  A commonly used file extension for a digital certificate based on the PKCS#12 standard is `.p12`.
  You can also find the information contained in a PKCS#12 file separately in individual files with the file extension `.pem`.

4.2.2 Encryption

To help protect the data, IKE uses various cryptographic algorithms for data encryption. The endpoints of the VPN connection require the key to code and decode the data.

The following list contains the initial steps in setting up the IKE security arrangement between the VPN connection endpoints:

- The endpoints agree on a cryptographic algorithm which subsequently uses the key for coding and decoding the IKE protocol messages.
- The endpoints specify the time periods during which the key exchange takes place.
- The endpoints identify the devices on which the coding and decoding takes place. The administrator specifies the endpoints beforehand in the settings of each endpoint.

After the endpoints complete the steps listed above, the devices agree on the key to code and decode the data.

4.2.3 Generating a digital certificate using OpenSSL

Using OpenSSL lets you generate and sign a digital certificate to use for VPN authentication.

Prerequisite: On a Windows system, you need a text editor that correctly handles Unix line breaks, for example the *Notepad++* application.

Generate a digital certificate. To do this, perform the following steps:

- ☐ Download OpenSSL from https://openssl-library.org and install the application.
- ☐ Specify the install directory `c:\openssl` and accept the other installation defaults.
- ☐ Start the *Command Prompt* program on your computer.
- ☐ To add the appropriate directories and files, enter the following commands in the Administrator window in the *Command Prompt* window:

```
C:\Users\username> cd \
C:\> cd openssl
C:\OpenSSL> md certs
C:\OpenSSL> cd certs
C:\OpenSSL\certs> md nameCA
C:\OpenSSL\certs> md nameCA\newcerts
C:\OpenSSL\certs> notepad++ nameCA\index.txt
```

- ☐ Save the `index.txt` file and exit the *Notepad++* program.
- ☐ In the *Command Prompt* window, add a file named `serial.txt`, with the following command:

```
C:\OpenSSL\certs> notepad++ nameCA\serial.txt
```

- ☐ Open the `serial.txt` file using the *Notepad++* program.
- ☐ In the *Notepad++* window, enter the value `01` on the first line.
- ☐ Save the `serial.txt` file and exit the *Notepad++* program.
- ☐ To set the path to the OpenSSL application, enter the following command in the *Command Prompt* window:

```
C:\> set path=c:\openssl\bin;%path%
```

- ☐ To set the path to the OpenSSL configuration file, enter the following command in the *Command Prompt* window:

```
C:\OpenSSL\certs> set OPENSSL_CONF=c:\openssl\bin\openssl.cfg
```

- ☐ Using a text editor, edit the configuration file `openssl.cfg` located in the `c:\openssl\bin` directory. The `countryName` and `stateOrProvinceName` values are optional. Therefore change the value `match` to `optional`. Save the settings. The resulting configuration is as follows:

```
# For the CA policy
[ policy_match ]
countryName = optional
stateOrProvinceName = optional
organizationName = match
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
```

- ☐ To generate a private RSA key named `priv.key`, enter the following command in a *Command Prompt* window:

```
C:\OpenSSL\certs> openssl genrsa -out priv.key 1024
```

The window displays the following text while generating the private RSA key:

```
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.................++++++
.....................................................++++++
e is 65537 (0x10001)
```

The OpenSSL application also lets you generate digital certificates. To display the possible certificate types, enter the following command in a *Command Prompt* window:

```
C:\OpenSSL\bin\openssl.exe help
```

- ☐ To generate a Certificate Signing Request (CSR) with a validity of 365 days, for example, and to self-sign it, enter the following command in a *Command Prompt* window:

```
C:\OpenSSL\certs> openssl req -new -x509 -days 365 -key priv.key -out nameCA/mycert.pem
```

- ☐ When requested, enter the appropriate distinguished name (DN) `information` for the digital certificate. When you press the <Enter> key, you can leave the optional fields blank.
  - ☐ For example, enter the following values:

```
Country Name: de
State or Province Name: BW
Locality Name: Neckartenzlingen
Organization Name: Hirschmann Automation and Control
Org. Unit Name: INET
Common Name: EAGLE40-ECE555d6e545
```

4.3 Application example for connecting 2 subnets

In a large company network, a transfer network connects the subnets to each other. A VPN connects 2 of these subnets for example, the production control and the production hall. To hide the internal IP addresses, set up the VPN to function in the tunnel mode.

The following information about the VPN is available:

Parameter	Router 1	Router 2
IP address of internal port	10.0.1.201	10.0.3.201
IP address of external port	10.0.2.1	10.0.2.2
Pre-shared key	123456abcdef	123456abcdef
Start IKE mode as	Initiator	Responder
IP parameters of the connecting networks	10.0.1.0/24	10.0.3.0/24

Prerequisite for further configuration:
- Both device 1 and 2 are in the router mode.
- Specify the IP parameters on the router interfaces.
- The devices in the 10.0.1.0/24 subnet have the IP address of the internal interface on Router 1, as their gateway.

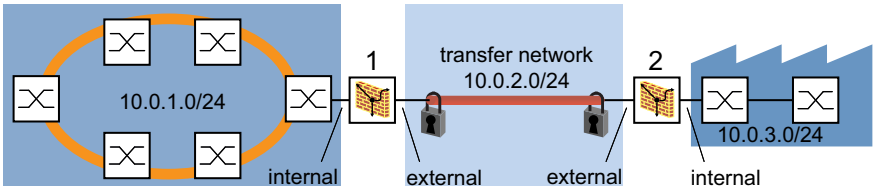


Figure 18: Connecting 2 subnets using a transfer network

Perform the following steps:

☐ Create a VPN connection.

☐ Open the *Virtual Private Network > Connections* dialog.

☐ Click the button.

The *Create or select entry* table displays the VPN connections already available in the device.

☐ In the *VPN index* field, enter an available index number.

☐ In the *VPN description* column, specify a connection name for example, `Production Control - Production Hall 1`.

☐ Click the *Next* button.

☐ Specify the authentication parameters.

The device uses the values specified in the *Wizard* window, *Authentication* page to validate its identity. In this example, the device authenticates itself using a pre-shared key.

☐ Select in the *Authentication* frame, *Authentication* field the value *Pre-shared key (PSK)*.

☐ In the *Pre-shared key (PSK)* frame, specify the following settings:

- The value `123456abcdef` in the *Pre-shared key* column
- The value `123456abcdef` in the *Confirm* column

The default setting of the *Change* checkbox lets you enter and confirm the pre-shared key for new VPN connections. For existing VPN connections the *Pre-shared key* and the *Confirm* fields are inactive. To activate the fields, mark the checkbox in the *Change* column.

☐ Click the *Next* button.

☐ Specify the Endpoint and Traffic Selector parameters.

The device uses the values specified in the *Endpoint and traffic selectors* dialog to identify the data source and destination. The table displays the type of data to send through the VPN tunnel.

☐ In the *Endpoints* frame, specify the following settings:

- The value `10.0.2.1` in the *Local endpoint* column
- The value `10.0.2.2` in the *Remote endpoint* column

In the current example, the external ports of the 2 device are the endpoints for of the VPN connection.

☐ To identify data that the device sends through the VPN tunnel, click the *Add traffic selector* button in the *Add traffic selector* frame.

- ☐ In the *Add traffic selector* dialog, specify the following settings:
  - The value `1` in the *Traffic selector index* column
    The device enters the index number, but also lets you change it.
  - The value `Any Traffic` in the *Traffic selector description* column
  - The value `10.0.1.0/24` in the *Source address (CIDR)* column
  - The value in the *Source restrictions* column is optional.
    The default setting is `any/any`. The device sends only the type of data specified through the VPN tunnel.
  - The value `10.0.3.0/24` in the *Destination address (CIDR)* column
  - The value in the *Destination restrictions* column is optional.
    The default setting is `any/any`. The device excepts only the specified type of data from the VPN tunnel.
- ☐ Click the *Ok* button.
- ☐ Click the *Next* button.

☐ Enter the IKE key exchange IPSec parameters.

The device uses the values specified in the *Advanced configuration* dialog. In this example, the device is the initiator and selects the protocol automatically.

☐ In the *General* frame, *Margin time [s]* field, the default setting is 540 s. This is equal to 9 minutes.

☐ In the *IKE/Key-exchange* frame, specify the following settings:

- The value `auto` in the *Version* column
  With this, the device selects the protocol version automatically, depending on the VPN remote terminal.
- The value `initiator` in the *Startup* column
  The device initiates the VPN connection to the remote terminal.
- The value `email` in the *IKE local identifier type* column
- For example, the value `user1@company.com` in the *IKE local ID* column
- The value `email` in the *Remote identifier type* column
- For example, the value `user2@company.com` in the *Remote ID* column
- The value `main` in the *IKE exchange mode* column
- The value `modp1024` in the *IKE key agreement* column
- The value `hmacsha1` in the *IKE integrity (MAC)* column
- The value `aes128` in the *IKE encryption* column
- The value `120` in the *IKEv1 DPD timeout [s]* column
  If the device does not receive a sign of life from the remote terminal within 120 seconds, then it terminates the VPN connection.
- The value `28800` in the *IKE lifetime [s]* column
  After the lifetime elapses, the 2 participating devices agree on new keys for the IKE security arrangement (IKE SA). The lifetime provides a periodic key change for the IKE SA.

☐ In the *IPSec/Data-exchange* frame, specify the following settings:

- The value `modp1024` in the *IPsec key agreement* column
- The value `hmacsha1` in the *IPsec integrity (MAC)* column
- The value `aes128` in the *IPsec encryption* column
- The value `3600` in the *IPsec lifetime [s]* column

☐ To apply the settings, click the *Finish* button.

☐ Activate the connection.

☐ To activate the connection, mark the checkbox in the *VPN active* column.

☐ Save the settings.

☐ Apply the settings temporarily. To do this, click the ✓ button.

☐ Make exactly the same settings on both devices.
On the second device, replace the IP address and specify the value `responder` in the *Startup* column.

5 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 in the network using the following options:
- The Network Time Protocol (NTP) is accurate to the order of sub-milliseconds.

5.1 Setting the time

When there is no reference time source available to you, you can manually set the system time in the device.

When you start the device after it has been powered down, it initializes the clock with January 1 2025, 01:00 UTC+1.
- Network Time Protocol

Perform the following steps:

☐ Open the *Time > Basic Settings* dialog.

- The *System time (UTC)* field displays the date and time of the device system clock with reference to Universal Time Coordinated (UTC). 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.

☐ To make the device apply the time of your computer to the *System time* field, click the *Set time from PC* button.
Based on the value in the *Local offset [min]* field, the device calculates the time in the *System time (UTC)* field: The *System time (UTC)* comes from the *System time* minus the *Local offset [min]* value and a possible shift due to daylight saving time.

- The *Time source* field displays the origin of the time data. The device automatically selects the source with the greatest accuracy.
The source is initially `Local`.
When NTP is active and the device receives a valid NTP packet, the device sets its time source to `ntp`.
- The *Local offset [min]* value specifies the difference in minutes between Universal Time Coordinated (UTC) and local time.

- ☐ To cause the device to determine the time zone on your PC, click the *Set time from PC* button. The device calculates the difference between local time and Universal Time Coordinated (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.

- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`clock set <YYYY-MM-DD> <HH:MM:SS>`	To set the system time of the device.
`clock timezone offset <-780..840>`	To enter the difference in minutes between the local time and the received Universal Time Coordinated (UTC).
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

5.2 Automatic daylight saving time changeover

When you operate the device in a time zone with a summer time change, the device lets you set up the automatic daylight saving time changeover.

If the *Daylight saving time* mode is enabled, the device advances the local system time by one hour during the summer time. At the end of summer time, the device sets the local system time back again by one hour.

5.2.1 Setting daylight saving time using pre-defined profiles

The device lets you specify the start and end of daylight saving time using pre-defined profiles.

The device includes the following pre-defined profiles:

- *EU*
  Daylight saving time settings as applicable in the European Union.
- *USA*
  Daylight saving time settings as applicable in the United States of America.

To select the *EU* profile for the daylight saving time settings, perform the following steps:

- ☐ Open the *Time > Basic Settings* dialog, *Daylight saving time* tab.
- ☐ In the *Operation* frame, click the *Profile...* button.
- ☐ Select the *EU* item from the *Profile...* list.
  Selecting a profile overwrites the settings specified in the *Summertime begin* and *Summertime end* frames.
- ☐ Click the *Ok* button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`clock summer-time mode eu`	To enable the *Daylight saving time* mode with the profile `eu`.

5.2.2 Setting daylight saving time manually

The network administrator wants to specify the following daylight saving time settings:

Summertime begin
- *Week* = *Last*
- *Day* = *Sunday*
- *Month* = *March*
- *System time* = `02:00`

Summertime end
- *Week* = *Last*
- *Day* = *Sunday*

- *Month* = *October*
- *System time* = 03:00

For the purpose described above, perform the following steps:

- ☐ Open the *Time > Basic Settings* dialog, *Daylight saving time* tab.
- ☐ Enable the *Daylight saving time* mode.
  Select the *On* radio button in the *Operation* frame.
- ☐ In the *Summertime begin* frame, specify the following settings:
  - *Week* = *Last*
  - *Day* = *Sunday*
  - *Month* = *March*
  - *System time* = 02:00
- ☐ In the *Summertime end* frame, specify the following settings:
  - *Week* = *Last*
  - *Day* = *Sunday*
  - *Month* = *October*
  - *System time* = 03:00
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`clock summer-time mode recurring`	To enable the *Daylight saving time* mode.
`clock summer-time recurring start last sun mar 02:00`	To specify the time at which the device sets the clock forward from standard time to summer time. • `last` To specify the *Last* week in the month. • `sun` To specify the day *Sunday*. • `mar` To specify the month *March*. • `02:00` To specify the time 02:00.
`clock summer-time recurring end last sun oct 03:00`	To specify the time at which the device resets the clock from summer time to standard time. • `last` To specify the *Last* week in the month. • `sun` To specify the day *Sunday*. • `oct` To specify the month *October*. • `03:00` To specify the time 03:00.

5.3 Synchronizing time in the network with NTP

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

NTP uses levels, or hierarchies, of clock sources called *stratum* layers. *Stratum* layers define the distance from the reference clock. *Stratum 0* represents the top layer. The *stratum 0* layer consists of radio clocks, atomic clocks, or GPS clocks. The device operates at layers *stratum 1* through *stratum 16*.

Furthermore, an NTP device operates as a primary server, secondary server, or client. Synchronize the primary NTP-Server directly to the *stratum 0* layer.

A secondary NTP-Server synchronizes to one or more servers and provides a synchronization signal for one or more servers or clients. When you use the device in `client` mode, the device sends requests to the active NTP-Servers listed in the *Time > NTP > Server* dialog. In the `client-server` mode, the device also answers requests sent from dependent servers and clients.

An NTP-Client synchronizes to one or more upstream NTP-Servers. To synchronize to the NTP-Server, set up the client devices to send Unicast requests or listen for broadcasts.

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

5.3.1 Preparing the NTP configuration

Perform the following steps:

- ☐ To get an overview of how the time is passed on, draw a network plan with the devices participating in NTP. When planning, bear in mind that the accuracy of the time depends on the signal runtime.

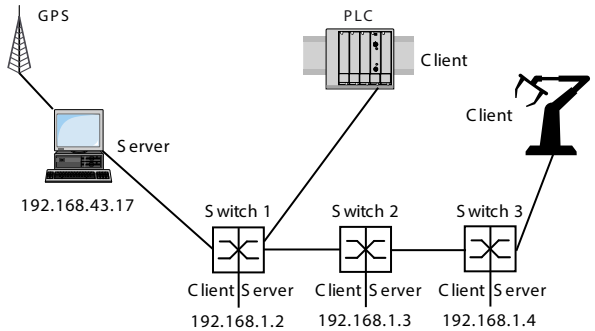


Figure 19: NTP cascading

Table 11: Settings for the example

Device	192.168.1.2	192.168.1.3	192.168.1.4
Client only frame			
Client	`Off`	`Off`	`Off`
Mode		`unicast`	

Table 11: Settings for the example (cont.)

Device	192.168.1.2	192.168.1.3	192.168.1.4
Client and server frame			
Server	*On*	*Off*	*On*
Mode	*client-server*		*client-server*
ServerIP address	192.168.43.17	192.168.1.2	192.168.43.17

- ☐ Enable the *NTP* function in the devices whose time you want to set using NTP. The NTP server of the device responds to received Unicast requests and sends Broadcast packets as soon as it is set up and enabled.
- ☐ If no reference clock is available, then specify a device as the reference clock and set its system time as accurately as possible.

5.3.2 NTP configuration

In the *Client only* frame:
- *Client* – Enable/disable the function
- *Mode* – In the *unicast* mode the device sends a request to a designated Unicast server and expects a reply from that server. In the *broadcast* mode, the device sends no request and waits for a Broadcast from one or more Broadcast servers.

In the *Client and server* frame:
- *Server* – Enable/disable the function
- *Mode* – Set the connection parameters
- *Stratum* – This setting helps prevent other clients from using the device as a reference time source (default setting: 12).

Set up an NTP client, using the example for switch 2. To do this, perform the following steps:

- ☐ Open the *Time > NTP > Global* dialog.
- ☐ Before you enable the *Client* function, disable the *Server* function. Select the *Off* radio button in the *Client and server* frame.
  Enable the *Client* function.
  Select the *On* radio button in the *Client only* frame.
- ☐ In the *Mode* field, specify the value *unicast*.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Time > NTP > Server* dialog.
- ☐ To add a table row, click the button.
- ☐ For switch 2:
  In the *IP address* column, specify the value 192.168.1.2.
- ☐ To activate the table row, mark the checkbox in the *Active* column.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ntp server operation disable`	To disable the NTP server.

`ntp client operation enable`	To enable the NTP client.
`ntp client operating-mode unicast`	To activate the NTP client in Unicast operating mode.
`ntp peers add 1 ip 192.168.1.2`	To add index `1` with an ip address of `192.168.1.2` as a NTP server to which the device sends requests.

Set up an NTP client server, using the example for switch 1 and 3. To do this, perform the following steps:

- ☐ Open the *Time > NTP > Global* dialog.
- ☐ Before you enable the *Server* function, disable the *Client* function. Select the *Off* radio button in the *Client only* frame.
  Enable the *Server* function.
  Select the *On* radio button in the *Client and server* frame.
- ☐ In the *Mode* field, specify the value *client-server*.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Time > NTP > Server* dialog.
- ☐ To add a table row, click the button.
- ☐ For switch 1 and switch 3:
  In the *IP address* column, specify the value `192.168.43.17`.
- ☐ To activate the table row, mark the checkbox in the *Active* column.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

Set up both switch 1 and 3 with the following commands.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ntp client operation enable`	To enable the NTP client.
`ntp server operation enable`	To enable the NTP server.
`ntp server operating-mode client-server`	To activate the client-server operating mode.
`ntp peers add 1 ip 192.168.43.17`	To add index `1` with an ip address of `192.168.43.17` as a NTP server to which the device sends requests.

6 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.

To keep the changes after a reboot, the device lets you save the settings in a configuration profile in the non-volatile memory (*NVM*). 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.

6.1 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.

6.1.1 Volatile memory (RAM) and non-volatile memory (NVM)

You can recognize if the settings in the volatile memory (*RAM*) differ from the settings of the "selected" configuration profile in the non-volatile memory (*NVM*). To do this, perform the following steps:

- ☐ Check the banner of the Graphical User Interface:
  - – When the icon is visible, the settings differ.
  - – When no icon is visible, the settings match.

Or:

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ Check the status of the checkbox in the *Information* frame:
  - – When the checkbox is marked, the settings match.
  - – When the checkbox is unmarked, the settings differ.

```
show config status

Configuration Storage sync State
--------------------------------
running-config to NV.....................out of sync
...
```

6.1.2 External memory (ACA) and non-volatile memory (NVM)

You can recognize if the settings copied to the external memory (ACA) differ from the settings of 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 marked, the settings match.
  - When the checkbox is unmarked, the settings differ.

```
show config status

Configuration Storage sync State
--------------------------------
...
NV to ACA.................................out of sync
...
```

6.2 Saving the settings

6.2.1 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). 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`	To display the configuration profiles contained in the non-volatile memory (`nvm`).
`enable`	To change to the Privileged EXEC mode.
`save`	To 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 the device adds a configuration profile in the non-volatile memory (*NVM*) or overwrites 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`	To display the configuration profiles contained in the non-volatile memory (`nvm`).
`enable`	To change to the Privileged EXEC mode.
`copy config running-config nvm profile <string>`	To 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. During the system startup, 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.

- ☐ Select the table row of the desired 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`	To change to the Privileged EXEC mode.
`show config profiles nvm`	To display the configuration profiles contained in the non-volatile memory (`nvm`).
`configure`	To change to the Configuration mode.
`config profile select nvm 1`	To select the configuration profile. Take note of the adjacent name of the configuration profile.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

6.2.2 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 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`config envm config-save usb`	To enable the function. When you save a configuration profile, the device saves a copy in the external memory. `usb` = External USB memory
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

6.2.3 Exporting a configuration profile

The device lets you save a configuration profile to a server as an XML file. If you use the Graphical User Interface, then you have the option to save the XML file directly to your PC.

Prerequisites:
- To save the file on a server, you need a server available 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.
- ☐ Select the table row of the desired configuration profile.

Export the configuration profile to your PC. To do this, perform the following steps:

- ☐ Click the link in the *Profile name* column.
  The configuration profile is downloaded and saved as an XML file on your PC.

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 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>`
    Remember to make the SCP or SFTP server known to the device before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog. When you click the *Ok* button, the device displays the *Credentials* window. There you enter *User name* and *Password* to log into the server.
- ☐ Click the *Ok* button.
  The configuration profile is now saved as an XML file in the specified location.

`show config profiles nvm`	To display the configuration profiles contained in the non-volatile memory (`nvm`).
`enable`	To change to the Privileged EXEC mode.
`copy config nvm remote sftp://<user_name>:<password>@<IP_address>/<path>/<file_name>`	To save the “Selected” configuration profile in the non-volatile memory (`nvm`) on a SFTP server.

6.3 Loading settings

If you save multiple configuration profiles in the memory, then you have the option to load a different configuration profile.

6.3.1 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.
- ☐ Select the table row of the desired 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`	To display the configuration profiles contained in the non-volatile memory (nvm).
`enable`	To change to the Privileged EXEC mode.
`copy config nvm profile config3 running-config`	To 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.

6.3.2 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 during the system startup 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 during the system startup.
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*.

☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`config envm load-priority usb  first`	To enable the function. During the system startup, the device loads a configuration profile from the external memory. *usb* = External USB memory
`show config envm settings`	To display the settings of the external memory (`envm`).

```
Type   Status      Auto Update Save Config Config Load Prio
------ ----------- ----------- ----------- ---------------
usb    ok          [x]         [x]         first
```

`save`	To 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`	To display the configuration profiles contained in the non-volatile memory (`nvm`).
`enable`	To change to the Privileged EXEC mode.
`copy config envm profile  config3 nvm`	To copy the configuration profile `config3` from the external memory (`envm`) to the non-volatile memory (`nvm`).

6.3.3 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 import a file from a server, you need a server available on the network.
- To import a file from 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.
- ☐ From the *Select source* drop-down list, select the location from where the device imports the configuration profile.
  - ▶ *PC/URL*
    The device imports the configuration profile from the local PC or from a remote server.
  - ▶ *External memory*
    The device imports the configuration profile from the external memory.

Import the configuration profile from the local PC or from a remote server. To do this, perform the following steps:

- ☐ Import the configuration profile:
  - ☐ If the file is on your PC or on a network drive, then drag and drop the file into the  area. As an alternative, click in the area to select the file.
    You can also use SCP or SFTP to transfer the file from your PC to the device. To do this, perform the following steps:
    On your PC, open an SCP or SFTP client, for example WinSCP.
    Use the SCP or SFTP client to open a connection to the device.
    Transfer the file onto the device, into the directory `/nv/cfg`.
  - ☐ If the file is on an SCP or SFTP server, then specify the URL 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 into the server.
    `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`
    Remember to make the SCP or SFTP server known to the device before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog.
- ☐ 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* 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, select the name of the configuration profile to be imported from the *Profile name* drop-down list.
  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
```

To change to the Privileged EXEC mode.

```
copy config remote  sftp://
<user name>:<password>@<IP_address>/
<path>/<file_name> running-config
```

To import and activate the settings of a configuration profile saved on a SFTP server. The device copies the settings into the volatile memory and disconnects the connection to the Command Line Interface. The device immediately uses the settings of the imported configuration profile.

6.4 Resetting the device to the default setting

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.

6.4.1 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`	To change to the Privileged EXEC mode.
`clear factory`	To delete 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.

6.4.2 Using System Monitor 1

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 System Monitor 1, press the <1> key within 3 seconds when prompted during reboot.
  The device displays System Monitor 1.
- ☐ 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.

7 Updating the device software

Hirschmann is continually working on improving and developing their software. Check regularly if there is an updated version of the device software that provides you with additional benefits. You find information and software downloads on the Hirschmann product pages on the Internet at catalog.belden.com.

The device gives you the following options to update the device software:
- Loading a previous device software version
- Software update from the PC
- Software update from a server
- Software update from the external memory

Note:
The device settings are kept after you update 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 device software when you are already logged into the device management, perform the following steps:

☐ Open the *Basic Settings > Software* dialog.
The *Running version* field displays the version number and creation date of the currently running device software that the device loaded during the last system startup.

`enable`	To change to the Privileged EXEC mode.
`show system info`	To display the system information such as the version number and creation date of the currently running device software that the device loaded during the last system startup.

7.1 Loading a previous device 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.

7.2 Software update from the PC

The device lets you update the device software, if a suitable device software image is saved on a storage medium which is accessible from your PC.

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

Perform the following steps:

- ☐ Navigate to the folder where the device software image is saved.
- ☐ Open the *Basic Settings > Software* dialog.
- ☐ Drag and drop the file into the  area. As an alternative, click in the area to select the file.
- ☐ Start the software update. To do this, click the *Start* button.
  - The device transfers the previously used device software to the backup memory.
  - The device transfers the selected file to the flash memory, replacing the previously used device software.
    As soon as the update procedure is completed successfully, the device displays a success notification.
    During the next startup, the device boots with the device software that you have transferred.

You can also use SCP or SFTP to transfer the file from your PC to the device. To do this, perform the following steps:

- ☐ On your PC, open an SCP or SFTP client, for example WinSCP.
- ☐ Use the SCP or SFTP client to open a connection to the device.
- ☐ Transfer the file onto the device, into the directory `/upload/firmware`.
  When the file transfer is complete, the device starts updating the device software. If the update was successful, then the device generates an `ok` file in the directory `/upload/firmware` and deletes the transferred file.
  The device loads the device software during the next system startup.

7.3 Software update from a server

The device lets you update its software if you have access to a server where a suitable device software image is saved.

The device gives you the following options to update the device software:
- Software update from an SFTP server
- Software update from an SCP server

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

7.3.1 Software update from an SFTP server

This option lets you update the device software image from an SFTP server.

Prerequisites:
- The access role `administrator` is assigned to the user account you use to perform the actions on the device.

Perform the following steps:

- ☐ Open the *Basic Settings > Software* dialog.
- ☐ In the *Software update* frame, *URL* field, specify the URL for the device software image using the following format:
  `sftp://user:password@IP_address/path/to/software_image.bin`
  You can also specify the URL without the user name and password. In this case, enter them in the *Credentials* window after clicking the *Start* button.
- ☐ Click the *Start* button.
  - The device transfers the previously used device software to the backup memory.
  - The device transfers the selected file to the flash memory, replacing the previously used device software.
    As soon as the update procedure is completed successfully, the device displays an information that the device software was successfully updated.
    During the next startup, the device boots with the device software that you have transferred.

```
enable

copy firmware remote sftp://
user:password@10.0.1.159:21/path/to/
software_image.bin system
```

To change to the Privileged EXEC mode.

To transfer the device software image from an SFTP server to the flash memory of the device.

- `copy firmware remote`
  To copy the device software image from a remote location.
- `sftp://user:password@10.0.1.159:21/path/to/software_image.bin`
  URL of the SFTP server where the device software image is saved.
  You can also specify the URL without the user name and password. In this case, the device will prompt you to enter the missing information afterwards.
  - `sftp://`
    Protocol for the file transfer
  - `user`
    User account name of the SFTP server
  - `password`
    User account password
  - `10.0.1.159`
    IP address of the SFTP server
  - `/path/to/`
    The path to the device software image on the SFTP server
  - `software_image.bin`
    Name of the device software image
- `system`
  To transfer the copied device software image to the flash memory.

7.3.2 Software update from an SCP server

This option lets you update the device software image from an SCP server.

Prerequisites:
- The access role `administrator` is assigned to the user account you use to perform the actions on the device.

Perform the following steps:

- ☐ Open the *Basic Settings* > *Software* dialog.
- ☐ In the *Software update* frame, *URL* field, specify the URL for the device software image using the following format:
  `scp://user:password@IP_address/path/to/software_image.bin`
  You can also specify the URL without the user name and password. In this case, enter them in the *Credentials* window after clicking the *Start* button.
- ☐ Click the *Start* button.
  - The device transfers the previously used device software to the backup memory.
  - The device transfers the selected file to the flash memory, replacing the previously used device software.
    As soon as the update procedure is completed successfully, the device displays an information that the device software was successfully updated.
    During the next startup, the device boots with the device software that you have transferred.

```
enable

copy firmware remote scp://
user:password@10.0.1.159:21/path/to/
software_image.bin system
```

To change to the Privileged EXEC mode.

To transfer the device software image from an SCP server to the flash memory of the device.

- `copy firmware remote`
  To copy the device software image from a remote location.
- `user:password@10.0.1.159:21/path/to/software_image.bin`
  URL of the SCP server where the device software image is saved.
  You can also specify the URL without the user name and password. In this case, the device will prompt you to enter the missing information afterwards.
  - `scp://`
    Protocol for the file transfer
  - `user`
    User account name of the SCP server
  - `password`
    User account password
  - `10.0.1.159`
    IP address of the SCP server
  - `/path/to/`
    The path to the device software image on the SCP server
  - `software_image.bin`
    Name of the device software image
- `system`
  To transfer the copied device software image to the flash memory.

7.4 Software update from the external memory

7.4.1 Manually—initiated by the administrator

The device lets you update the device software with a few mouse clicks, if a suitable device software image is saved on the external memory.

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

Perform the following steps:

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ In the *External memory* frame, verify that the relevant external memory is selected from the *Selected external memory* drop-down list.
- ☐ Open the *Basic Settings > Software* dialog.
- ☐ Mark the table row for which the *File location* column displays the value `usb`.
- ☐ Start the software update. To do this, click the ⬆ button.
  - The device transfers the previously used device software to the backup memory.
  - The device transfers the selected file to the flash memory, replacing the previously used device software.
    As soon as the update procedure is completed successfully, the device displays a success notification.
    During the next startup, the device boots with the device software that you have transferred.

7.4.2 Automatically—initiated by the device

When the following files are located in the external memory during the system startup, the device updates the device software automatically:

- the device software image
- a text file `startup.txt` with the content `autoUpdate=<software_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:

- ☐ Transfer the new device software image into the main directory of the external memory. Use only a device software image 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=<software_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 device software image exist which is specified in the `startup.txt` file?
- Is the version of the device software image more recent than the device software that the device is currently using?

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 device 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 a wrong device software image
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE`
  Software update aborted because the device did not save the device software image.

8 Configuring the ports

The following port configuration functions are available.

- Enabling/Disabling the port
- Selecting the operating mode
- Hardware LAN bypass

8.1 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`no shutdown`	To enable the interface.

8.2 Selecting the operating mode

In the default setting, the ports are set to *Autoneg* 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 *Autoneg* column.
  - ☐ In the *Manual configuration* column, specify the desired operating mode (transmission rate, duplex mode).
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`no auto-negotiate`	To disable the automatic configuration mode.
`speed 100 full`	To set port speed 100 Mbit/s and full-duplex.

8.3 Hardware LAN bypass

The Hardware LAN bypass is used to maintain the data communication in case of a power loss or a detected failure.

- When the Hardware LAN bypass is inactive, the ports *1/1* and *1/2* are connected to the internal ports of the device. The device normally forwards the data packets from and to port *1/1* and port *1/2*.
- When the Hardware LAN bypass is active, the device disconnects the ports *1/1* and *1/2* from the internal ports. The device instead connects port *1/1* and port *1/2* physically to each other. Data packets directly pass from port *1/1* to port *1/2* and vice versa.

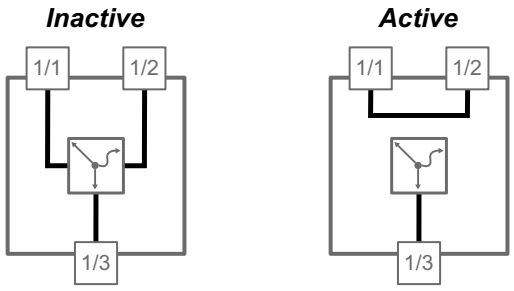


Figure 20: States of the Hardware LAN bypass

The device supports the following modes of Hardware LAN bypass:

- System-off bypass
  The device maintains data communication between the ports *1/1* and *1/2* when the device is inoperable.
- Run-time bypass
  The device maintains the data communication between the ports *1/1* and *1/2* when the device is under maintenance or configuration.

8.3.1 System-off bypass

In the default setting, the System-off bypass is disabled. When the System-off bypass is enabled, the device maintains data communication between port *1/1* and port *1/2* in case the device powers down or detects an application failure.

Enabling the System-off bypass

You enable the System-off bypass using the Command Line Interface.

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`hardware systemoff-bypass`	To enable the System-off bypass.

```
show hardware systemoff-bypass                To display the status of the System-off bypass.
Systemoff hardware LAN By-Pass Information
---------------------
Operation State.............................enabled
save                                          To save the settings in the non-volatile memory
                                              (NVM) in the “Selected” configuration profile.
```

Disabling the System-off bypass

You disable the System-off bypass using the Command Line Interface.

Perform the following steps:

```
enable                                        To change to the Privileged EXEC mode.
configure                                     To change to the Configuration mode.
no hardware systemoff-bypass                  To disable the System-off bypass.
show hardware systemoff-bypass                To display the status of the System-off bypass.
Systemoff hardware LAN By-Pass Information
---------------------
Operation State.............................disabled
save                                          To save the settings in the non-volatile memory
                                              (NVM) in the “Selected” configuration profile.
```

8.3.2 Run-time bypass

In the default setting, the Run-time bypass is disabled. When the Run-time bypass is enabled, the device maintains data communication between port *1/1* and port *1/2* in case the device is under maintenance or configuration. The device functions that forward data packets from and to port *1/1* and port *1/2* are disabled.

The following characteristics indicate that the Run-time bypass is enabled:

- On the device, the port LED for port *1/1* and port *1/2* extinguishes.
- In the *Basic Settings > Port* dialog, *Configuration* tab, the checkbox for ports *1/1* and *1/2* in the *State* column is unmarked.

Enabling the Run-time bypass

You enable the Run-time bypass using the Command Line Interface. Use the serial connection or a port apart from *1/1* and *1/2* to access the management of the device.

Perform the following steps:

```
enable                                        To change to the Privileged EXEC mode.
configure                                     To change to the Configuration mode.
hardware runtime-bypass                       To enable the Run-time bypass.
```

```
show hardware runtime-bypass                To display the status of the Run-time bypass.
Run-time hardware LAN By-Pass Information
---------------------
Operation State.............................enabled
save                                        To save the settings in the non-volatile memory
                                            (NVM) in the “Selected” configuration profile.
```

Disabling the Run-time bypass

You disable the Run-time bypass using the Command Line Interface. Use the serial connection or a port apart from *1/1* and *1/2* to access the management of the device.

Perform the following steps:

```
enable                                      To change to the Privileged EXEC mode.
configure                                   To change to the Configuration mode.
no hardware runtime-bypass                  To disable the Run-time bypass.
show hardware runtime-bypass                To display the status of the Run-time bypass.
Run-time hardware LAN By-Pass Information
---------------------
Operation State.............................disabled
save                                        To save the settings in the non-volatile memory
                                            (NVM) in the “Selected” configuration profile.
```

9 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 to reduce possible unauthorized access to the device.

- Changing the SNMPv1/v2 community
- Disabling SNMPv1/v2
- Disabling HTTP
- Using your own HTTPS certificate
- Using your own SSH key
- Disabling HiDiscovery
- Restricting access to device management
- Adjusting the session timeouts

9.1 Changing the SNMPv1/v2 community

SNMPv1 and SNMPv2 work unencrypted. Every SNMP packet contains the IP address of the sender and the plaintext *community name* with which the sender accesses the device. If the *SNMPv1* and/or *SNMPv2* function is active, then the device lets anyone who knows the *community name* access the device. Treat the *community names* with discretion.

The *community names* `public` for *read-only* access and `private` for *read and write* access are preset. If you are using SNMPv1 or SNMPv2, then change the default *community name*. 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 64 alphanumeric characters are allowed.
  - The device differentiates between upper and lower case.
  - Specify a different *community name* than for *read-only* access.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`snmp community rw <community name>`	To specify the community for *read and write* access.
`show snmp community`	To display the communities that have been set up.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

9.2 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`no snmp access version v1`	To deactivate the SNMPv1 protocol.
`no snmp access version v2`	To deactivate the SNMPv2 protocol.
`show snmp access`	To display the SNMP server settings.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

9.3 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.
- ☐ Disable the *HTTP* protocol.
  Select the *Off* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`no http server`	To 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`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`https server`	To enable the HTTPS protocol.

9.4 Disabling the HiDiscovery access

HiDiscovery lets you assign IP parameters to the device over the network during commissioning. HiDiscovery communicates in the device management VLAN without encryption and authentication.

After the device is commissioned, we recommend to set HiDiscovery to read-only or to disable HiDiscovery access completely. To do this, perform the following steps:

- ☐ Open the *Basic Settings > Network > Global* 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.
- ☐ Disable HiDiscovery access completely.
  Select the `Off` radio button in the *HiDiscovery protocol v1/v2* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`network hidiscovery mode read-only`	To disable write permission of the HiDiscovery software.
`no network hidiscovery operation`	To disable HiDiscovery access.

9.5 Restricting access to device management

In the default setting, everyone can access the device management from any IP address using any protocol. The device lets you restrict access to device management for selected protocols from a specific IP address range or through a specific physical port.

9.5.1 Restricting access through a specific physical port

In the following example, you set up the device so that access to device management with any supported IP-based protocol is possible only through the physical port *1/1*.

Perform the following steps:

- ☐ Open the *Device Security > Management Access > IP Access Restriction* dialog.
- ☐ To add a rule with default settings, click the button.
- ☐ Specify the following settings for the rule:
  - *Address* column = `0.0.0.0`
  - *Netmask* column = `0.0.0.0`
  - *Interface* column = `1/1`
- ☐ To activate the rule, mark the checkbox in the *Active* column.

Note:
Before you enable the access restriction, verify that the table contains at least one active rule that grants you access to the device management. Otherwise, access to the device management is only possible using the Command Line Interface through the serial connection.

- ☐ Enable the access restriction.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`show network management access global`	To display if the access restriction is enabled or disabled.
`show network management access rules`	To display the entries that have been configured.
`network management access add 2`	To add a rule with index `2`.
`network management access modify 2 interface 1/1`	To assign rule `2` to port `1/1`.
`no network management access status 1`	To deactivate the default rule which lets everyone access the device management through any physical port.
`network management access status 2`	To activate the rule with index `2`.
`network management access operation`	To enable the access restriction.

9.5.2 Restricting access from a specific IP address range

In the following 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 12: 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 table row.
  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 row, 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 row, 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.

Note:
Before you enable the access restriction, verify that the table contains at least one active rule that grants you access to the device management. Otherwise, access to the device management is only possible using the Command Line Interface through the serial connection.

- ☐ Enable the access restriction.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`show network management access global`	To display if the access restriction is enabled or disabled.
`show network management access rules`	To display the entries that have been configured.
`no network management access operation`	To disable the IP access restriction.

`network management access add 2`	To add a rule with index 2 for the address range of the company network.
`network management access modify 2 ip 192.168.1.0`	To specify the IP address of the company network.
`network management access modify 2 mask 24`	To specify the netmask of the company network.
`network management access modify 2 ssh disable`	To deactivate SSH for the address range of the company network. Repeat the operation for every unwanted protocol.
`network management access add 3`	To add a rule with index 3 for the address range of the mobile phone network.
`network management access modify 3 ip 109.237.176.0`	To specify the IP address of the mobile phone network.
`network management access modify 3 mask 24`	To specify the netmask of the mobile phone network.
`network management access modify 3 snmp disable`	To deactivate SNMP for the address range of the mobile phone network. Repeat the operation for every unwanted protocol.
`no network management access status 1`	To deactivate the default entry. This entry lets users have access to the device from any IP address and the supported protocols.
`network management access status 2`	To activate the rule with index 2 for the address range of the company network.
`network management access status 3`	To activate the rule with index 3 for the address range of the mobile phone network.
`show network management access rules`	To display the entries that have been configured.
`network management access operation`	To enable the access restriction.

9.6 Adjusting the session timeouts

The device lets you automatically terminate the session upon inactivity of the user that is logged in. 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 the 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ssh timeout <0..160>`	To specify the timeout period in minutes for Command Line Interface sessions using an SSH connection.

Timeout for Command Line Interface sessions using the 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`cli serial-timeout <0..160>`	To specify the timeout period in minutes for Command Line Interface sessions using the 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`network management access web timeout <0..160>`	To specify the timeout period in minutes for Graphical User Interface sessions

10 Controlling the data traffic

The device checks the data packets to be forwarded in accordance with defined rules. Data packets to which the rules apply are either forwarded by the device or blocked. If data packets do not correspond to any of the rules, then the device blocks the packets.

Routing ports to which no rules are assigned allow packets to pass. As soon as a rule is assigned, the assigned rules are processed first. After that, the specified standard action of the device takes effect.

The device provides the following functions for controlling the data stream:
- Checking the contents and states of data packets (packet filter)
- Service request control (Denial of Service (DoS))

The device observes and monitors the data stream. The device takes the results of the observation and the monitoring and combines them with the rules for the network security to generate what is known as a status table. Based on this status table, the device decides whether to accept, drop or reject data.

The device processes data packets in the following sequence:

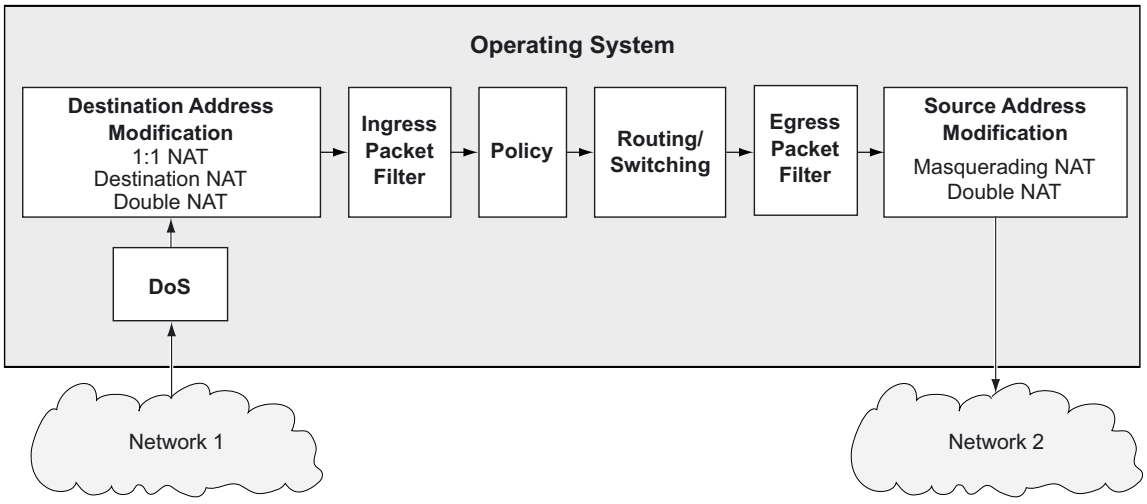


Figure 21: Processing sequence of the data packets in the device

Note:
The device uses hardware to filter the data stream through the packet filters. This causes the device to process the data stream at a slow rate. For this reason, when you expect high volumes, use ACLs. To track the “connection state“, use packet filters.

10.1 Asset

An asset represents a physical device, for example a PLC (Programmable Logic Controller), a computer, or a network device. An asset can also represent a virtual object, for example a multicast address range, or a multicast address. Assets help provide flexibility while adding and maintaining *Packet Filter* rules.

An asset contains the following parameters:
- *Type*
- *Manufacturer*
- *Model*
- *General location*
- *Specific location*
- *Asset tag*
- *IP address*
- *MAC address*

You combine assets with the *Packet Filter* rules. When you apply the *Packet Filter* rules to the data packet, the device filters undesired data packets received on the router interface. See the *Network Security > Packet Filter > Routed Firewall Mode > Rule* and *Network Security > Packet Filter > Routed Firewall Mode > Assignment* dialogs to set up the *Packet Filter* rules.

The device lets you set up to 50 assets.

10.1.1 Adding an asset

The network administrator wants to add an asset with the following characteristics:
- *Type* = `controller`
- *Model* = `unity-pro`
- *Asset tag* = `corporate`
- *IP address* = `192.168.112.5`

For the purpose described above, add the asset with the above values and name `corporate-unity-pro`.

Perform the following steps:

- ☐ Open the *Network Security > Asset* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
  - ☐ In the *Name* field, specify the value `corporate-unity-pro`.
  - ☐ Click the *Ok* button.
    The device adds a table row with the default settings.
- ☐ Specify the following settings for the table row:
  - *Type* column = `controller`
  - *Model* column = `unity-pro`
  - *Asset tag* column = `corporate`
  - *IP address* column = `192.168.112.5`
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
enable

configure

asset add 1 name corporate-unity-pro type
controller model unity-pro tag corporate
ip-address 192.168.112.5
```

To change to the Privileged EXEC mode.

To change to the Configuration mode.

To add an asset.

- `asset add 1`
  To add an asset with index = `1`.
- `name corporate-unity-pro`
  To specify the name `corporate-unity-pro`.
- `type controller`
  To specify the asset type `controller`.
- `model unity-pro`
  To specify the asset model `unity-pro`.
- `tag corporate`
  To specify the asset tag `corporate`.
- `ip-address 192.168.112.5`
  To specify the asset IP address `192.168.112.5`.

10.2 Protocol

Protocols define the particular services that communicate between devices in the network. The device has several predefined protocols that are common to many industrial systems. However, in special cases, you may want to add new protocols for specific types of equipment or situations.

A protocol contains the following parameters:
- *Protocol type*
- *Ethertype*
- *Ethertype custom value*
- *Protocol number*
- *Port*

You combine protocols with the *Packet Filter* rules. When you apply the *Packet Filter* rules to the data packet, the device filters undesired data packets received on the router interface. See the *Network Security > Packet Filter > Routed Firewall Mode > Rule* and *Network Security > Packet Filter > Routed Firewall Mode > Assignment* dialogs to set up the *Packet Filter* rules.

The device lets you set up to 50 user-defined protocols.

10.2.1 Adding a protocol

The network administrator wants to add a user-defined protocol with the following characteristics:
- *Protocol type* = `tcp`
- *Port* = `200`

For the purpose described above, add the protocol with the above values and name `my-protocol`.

Perform the following steps:

- ☐ Open the *Network Security > Protocol* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
  - ☐ In the *Protocol name* field, specify the value `my-protocol`.
  - ☐ Click the *Ok* button.
    The device adds a table row with the default settings.
- ☐ Specify the following settings for the table row:
  - *Protocol type* column = `tcp`
  - *Port* column = `200`
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
enable
configure
protocol add 1 name my-protocol protocol-
type tcp port 200
```

To change to the Privileged EXEC mode.

To change to the Configuration mode.

To add a user-defined protocol.

- `protocol add 1`
  To add a protocol with index = `1`.
- `name my-protocol`
  To specify the name `my-protocol`.
- `protocol-type tcp`
  To specify the protocol type `tcp`.
- `port 200`
  To specify the L4 destination port `200`.

10.3 Packet Filter – Routed Firewall Mode

10.3.1 Description

The *Routed Firewall Mode* (*Layer 3*) packet filter contains rules which the device applies successively to the data stream on its routing ports. The filtering naturally includes checking and evaluation of the data stream. The device contains a stateful firewall. A stateful firewall tracks the state of the connections transversing it.

The firewall filters both the contents and the status of the conveyed data packets. For each type, you have different criteria that you compile into individual rules as required.

The device also lets you specify the rules based on assets and user-defined protocols. See sections “Asset” on page 122 and “Protocol” on page 124.

In case of filtering for the content of a packet, the device checks the following criteria:
- IP header (source address, target address, protocol)
- TCP/UDP header (source port, target port)

You can set up the corresponding values in the table of the *Network Security > Packet Filter > Routed Firewall Mode > Rule* dialog.

When filtering according to the status of a packet, the firewall checks the criteria, which you can optionally set up in the *Network Security > Packet Filter > Routed Firewall Mode > Rule* dialog, *Parameters* field.

When you add a rule in this dialog, the value in the *Parameters* column is `none` initially. This default value causes filtering according to the status or the Ethernet header of a packet.

To activate optional, status or content filter criteria, you can enter different parameters, which each have the form `key=<value>`. Which keys are valid depends in part on the protocol of the rule. The keys `mac=<value>` and `state=<value>` apply everywhere and are independent of the protocol. The keys `type=<value>` and `code=<value>` are permitted only for the Internet Control Message Protocol (ICMP); the key `flags=<value>` is only permitted for the Transmission Control Protocol (TCP).

In the table below, you will find several examples for entries in the *Parameters* column and their effect on filtering. You have the option to enter several keys separated by commas. You can also enter several values separated by dashes. In addition, you can also enter different keys with several values in each case.

Table 13: Possible entries in the Parameters column

Entry	Meaning
`mac=de:ad:de:ad:be:ef`	This rule only applies to packets with the source MAC address de:ad:de:ad:be:ef.
`state=new`	This rule only applies to packets coming from a new connection.
`state=est`	This rule only applies to packets coming from a connection that already exists.
`state=new|est`	This rule applies to every packet coming from a new connection or a connection that already exists.
`type=5`	This rule only applies to packets with ICMP type 5.
`flags=syn`	This rule only applies to packets for which the SYN flag is set.
`state=new|rel,flags=rst`	This rule applies to every packet coming from a new or relative connections and that has the `RST` flag set.

For further information on valid entries in the *Parameters* column, see the "Graphical User Interface" reference manual.

The device enables simultaneous filtering according to content and status of data packets. You can compile any combinations of both types of filtering into individual rules. The device lets you set up to 2048 individual rules.

Upon receipt of a data packet to be routed, the device generally applies the packet filer rules to the data packet. The device executes one rule after the other, until the data packet reaches the first rule that applies to it. The rules that follow are ignored.

To remove a rule, select the affected table row and click the button.

When none of the rules you set up applies to a data packet or you have not set up individual rules, the *Routed Firewall Mode* packet filter applies a default rule. Three possible default rules are available here:

Table 14: Handling filtered data packets

Rule	Operation
`accept`	The device forwards the data packet in accordance with the address information.
`drop`	The device deletes the data packet without informing the sender.
`reject`	The device deletes the data packet and informs the sender.

Note:
In the default setting, the device applies the `accept` action. You can change this setting in the *Network Security > Packet Filter > Routed Firewall Mode > Global* dialog, *Default policy* field.

The *Routed Firewall Mode* packet filter follows a two-stage concept to activate newly added or modified rules. If you click the button, then the device caches the rules listed in the table. To apply the rules to the data stream, in the *Network Security > Packet Filter > Routed Firewall Mode > Global* dialog, click the button.

When you have set up and activated the status-dependent filter criteria, you can have the corresponding effects displayed in the status table. You can find this table with the name *Firewall state (connection tracking) table* on the bottom of the *Diagnostics > System > System Information* dialog. Based on the entries listed there, you can check which connections are currently established. Verify that the data packets permitted by you actually pass through the firewall, for example.

Note:
To delete the information from the firewall state table, click in the *Basic Settings > Restart* dialog the *Clear firewall table* button.

10.3.2 Setting up packet filter rules

The figure displays a typical application case:

A production controller wants to request data from a production robot.

The production robot is located in a production cell which a firewall keeps separate from the company network. The firewall is to help prevent data stream between the production cell and the rest of the company network. Only the data stream between the robot and the production control PC is allowed to flow freely.

The following is known:

Parameter	Robot	Firewall	PC
IP address interface `1/1`		10.0.1.201	
IP address interface `1/4`		10.0.2.1	
IP address	10.0.1.5		10.0.2.17
Gateway	10.0.1.201		10.0.2.1

Prerequisite for further configuration:
- The firewall is in Router mode.
- The IP parameters of the firewall router interface are set up.
- The devices in the internal network have the IP address of port 1 of the firewall as their *Gateway*.
- The *Gateway* and the IP address of the PC and the robot are set up.

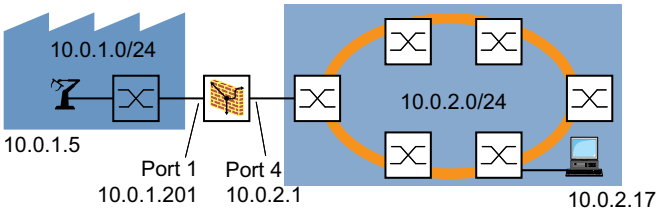


Figure 22: Application example of a Packet Filter setup

Create a rule for incoming IP packets. To do this, perform the following steps:

☐ Open the *Network Security > Packet Filter > Routed Firewall Mode > Rule* dialog.

By default, no interface is assigned an explicit rule. In the *Default policy* field, the value `accept` is specified. Consequently, the data stream passes through the device without restriction. Adding a rule and assigning it to the relevant interface changes this condition.

☐ Add a rule.

☐ Specify the following settings for the rule:
- The value `10.0.2.17` or `10.0.2.17/32` in the *Source address* column
- The value `any` in the *Source port* column
- The value `10.0.1.5` or `10.0.1.5/32` in the *Destination address* column
- The value `any` in the *Destination port* column
- The value `any` in the *Protocol* column
- The value `accept` in the *Action* column

The device lets you limit the rule to IP packets that fulfill certain ICMP criteria. Additionally, specify the following settings for the rule:
- The value `icmp` in the *Protocol* column
- The value `type=3,code=1` in the *Parameters* column
  `type=3` = Destination Unreachable
  `code=1` = Host Unreachable
  The values behind `type` and `code` are 1- to 3-digit decimal values. For the possible values, see the "Graphical User Interface" reference manual. Entering an ICMP code is optional.

☐ To activate the rule, mark the checkbox in the *Active* column.

☐ Apply the settings temporarily. To do this, click the ✓ button.

- ☐ Apply the rule to an interface. To do this, perform the following steps:
  - ☐ Open the *Network Security > Packet Filter > Routed Firewall Mode > Assignment* dialog.
  - ☐ Click the button.
    The dialog displays the *Create* window.
  - ☐ In the *Interface* field, specify the value `1/4`.
  - ☐ In the *Direction* field, specify the value `ingress` to activate this rule for the incoming data stream.
  - ☐ In the *Rule index* column, specify the index number of the rule.
  - ☐ Click the *Ok* button.
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Open the *Network Security > Packet Filter > Routed Firewall Mode > Global* dialog.
- ☐ Apply the rule to the data stream. To do this, click the button.

Create rules for sending IP packets. To do this, perform the following steps:

- ☐ Open the *Network Security > Packet Filter > Routed Firewall Mode > Rule* dialog.
- ☐ Create a rule `drop everything` that drops every IP packet.
  Specify the following settings for the rule:
  - The value `drop everything` in the *Description* column
  - The value `any` in the *Source address* column
  - The value `any` in the *Source port* column
  - The value `any` in the *Destination address* column
  - The value `any` in the *Destination port* column
  - The value `any` in the *Protocol* column
  - The value *drop* in the *Action* column
  - Unmarking the checkbox in the *Log* column
- ☐ Create a rule `filter data` that explicitly allows to send selected IP packets.
  Specify the following settings for the rule:
  - The value `filter data` in the *Description* column
  - The value `10.0.1.5/32` in the *Source address* column
  - The value `any` in the *Source port* column
  - The value `10.0.2.17/32` in the *Destination address* column
  - The value `any` in the *Destination port* column
  - The value `any` in the *Protocol* column
  - The value *accept* in the *Action* column
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Apply the rule to an interface. To do this, perform the following steps:
  - ☐ Open the *Network Security > Packet Filter > Routed Firewall Mode > Assignment* dialog.
  - ☐ Click the button.
    The dialog displays the *Create* window.
  - ☐ In the *Interface* field, specify the interface to which you want the rule assigned.
  - ☐ In the *Direction* field, specify the value *egress* to activate this rule for the outbound data stream.
  - ☐ In the *Rule index* column, specify the index number of the `filter data` rule.
  - ☐ Click the *Ok* button.
  - ☐ Repeat these steps to allocate the rule `drop everything` to the interface.
- ☐ Specify the priority of the rules in the *Priority* column:
  - The value `1` for the `filter data` rule
  - The value `2` for the `drop everything` rule
- ☐ To activate the rules, mark the checkbox in the *Active* column.

- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Network Security > Packet Filter > Routed Firewall Mode > Global* dialog.
- ☐ To apply the rules to the data stream, click the ⬆ button.

10.4 Packet Filter – Transparent Firewall Mode

10.4.1 Description

The *Transparent Firewall Mode* packet filter contains rules which the device applies successively to the data stream on its non-routing ports or VLAN interfaces. The *Transparent Firewall Mode* packet filter evaluates every data packet that passes through the firewall based on the connection status as mentioned below:

- For IPv4, evaluation is *stateful*.
- For other Layer 2 and Layer 3 protocols, evaluation is *stateless*.

The device also lets you specify the rules based on assets and user-defined protocols. See sections “Asset” on page 122 and “Protocol” on page 124.

The device filters the undesired data packets selectively while the connection is unknown.

The rules contain specific match criteria and actions. The device lets you specify the following criteria in the rules to filter the data packets:

- Ethernet header
  - *Source MAC address*
  - *Destination MAC address*
  - *Ethertype*
- IP header
  - *Source IP address*
  - *Destination IP address*
  - *Protocol*
- TCP/UDP header
  - *Source port*
  - *Destination port*

The available actions are as follows:

- `accept`
- `drop`

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

If no rule matches, then the device applies the default rule. In the default setting, the default rule has the value `accept`. As a result, the device accepts the received data packets. The device lets you change the default rule in the *Network Security > Packet Filter > Transparent Firewall Mode > Global* dialog, *Default policy* field.

You add, modify or delete rules and specify the filtering criteria in the *Network Security > Packet Filter > Transparent Firewall Mode > Rule* dialog. The device lets you set up to 999 individual rules. You can assign a single rule to any number of ports or VLANs.

The *Transparent Firewall Mode* packet filter follows a two-stage concept to activate newly added or modified rules. If you click the ✓ button, then the device caches the rules listed in the table. To apply the rules to the data stream, in the *Network Security > Packet Filter > Routed Firewall Mode > Global* dialog, click the ⬆ button.

The prerequisite to accept IP data packets is that the device accepts ARP data packets. In the default setting, the device accepts ARP data packets.

10.4.2 Setting up packet filter rules

Setting up rules based on IP addresses

In the following example, the network administrator wants to accept the data packets from computers B and C to computer A based on the IP address of the devices. The firewall keeps computer A separate from the company network. The firewall helps prevent access between computer A and the rest of the company network. The firewall only permits access from computers B and C to computer A.

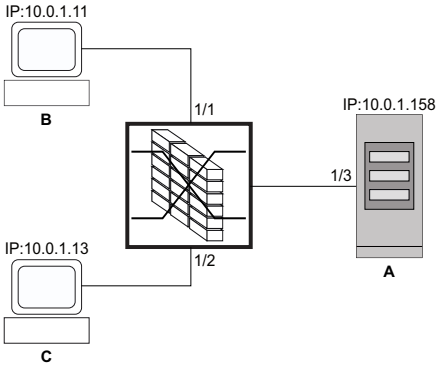


Figure 23: Application example of a packet filter based on IP addresses

Prerequisites:
- Firewall is in Bridge mode
- In the *Default policy* field, the value `drop` is specified.

Perform the following steps:
☐ Create an IP rule for end device B.

☐ Open the *Network Security > Packet Filter > Transparent Firewall Mode > Rule* dialog.

☐ Click the button.
The device adds a rule.

☐ Specify the following settings for the rule:
- *Description* column = `accept ipv4 dev b to dev a`
- *Ethertype* column = `ipv4`
- *Source IP address* column = `10.0.1.11`
- *Destination IP address* column = `10.0.1.158`

☐ Activate the rule. To do this, mark the checkbox in the *Active* column.

☐ Apply the settings temporarily. To do this, click the ✓ button.

☐ Open the *Network Security > Packet Filter > Transparent Firewall Mode > Assignment* dialog.

- ☐ Click the button.
  The dialog displays the *Create* window.
  - ☐ From the *Port/VLAN* drop-down list, select the port *1/1*.
  - ☐ From the *Direction* drop-down list, select the item `ingress` to activate the rule for incoming data packets.
  - ☐ From the *Index* drop-down list, select the item `accept ipv4 dev b to dev a: 1`.
- ☐ Click the *Ok* button.
- ☐ Apply the rule to the data stream. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`packet-filter l2 rule add 1 action accept src-ip 10.0.1.11 dest-ip 10.0.1.158 ethertype ipv4 description accept ipv4 dev b to dev a`	To add a *Transparent Firewall Mode* packet filter rule. • `packet-filter l2 rule add 1` To add a *Transparent Firewall Mode* packet filter rule with index = `1`. • `action accept` • `src-ip 10.0.1.11` • `dest-ip 10.0.1.158` • `ethertype ipv4` • `description accept ipv4 dev b to dev a` To specify the user-specific name `accept ipv4 dev b to dev a`.
`packet-filter l2 rule enable 1`	To activate the *Transparent Firewall Mode* packet filter rule `1`.
`packet-filter l2 if add port 1 ingress 1 1`	To apply the *Transparent Firewall Mode* packet filter rule `1` on port *1/1*. • `packet-filter l2 if add port 1` To add a *Transparent Firewall Mode* packet filter rule for port *1/1*. • `ingress` To apply the *Transparent Firewall Mode* packet filter rule to the data packets received. • `1` To select the *Transparent Firewall Mode* packet filter rule `1`. • `1` To specify priority = `1`

- ☐ Create an IP rule for end device C.

- ☐ Open the *Network Security > Packet Filter > Transparent Firewall Mode > Rule* dialog.
- ☐ Click the button.
  The device adds a rule.
- ☐ Specify the following settings for the rule:
  - *Description* column = `accept ipv4 dev c to dev a`
  - *Ethertype* column = `ipv4`
  - *Source IP address* column = `10.0.1.13`
  - *Destination IP address* column = `10.0.1.158`
- ☐ Activate the rule. To do this, mark the checkbox in the *Active* column.

- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Network Security > Packet Filter > Transparent Firewall Mode > Assignment* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
  - ☐ From the *Port/VLAN* drop-down list, select the port *1/2*.
  - ☐ From the *Direction* drop-down list, select the item `ingress` to activate the rule for incoming data packets.
  - ☐ From the *Index* drop-down list, select the item `accept ipv4 dev c to dev a: 2`.
- ☐ Click the *Ok* button.
- ☐ Apply the rule to the data stream. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`packet-filter l2 rule add 2 action accept src-ip 10.0.1.13 dest-ip 10.0.1.158 ethertype ipv4 description accept ipv4 dev c to dev a`	To add a *Transparent Firewall Mode* packet filter rule. • `packet-filter l2 rule add 2` To add a *Transparent Firewall Mode* packet filter rule with index = `2`. • `action accept` • `src-ip 10.0.1.11` • `dest-ip 10.0.1.158` • `ethertype ipv4` • `description accept ipv4 dev c to dev a` To specify the user-specific name `accept ipv4 dev c to dev a`.
`packet-filter l2 rule enable 2`	To activate the *Transparent Firewall Mode* packet filter rule `2`.
`packet-filter l2 if add port 2 ingress 2 1`	To apply the *Transparent Firewall Mode* packet filter rule `2` on port *1/2*. • `packet-filter l2 if add port 2` To add a *Transparent Firewall Mode* packet filter rule for port *1/2*. • `ingress` To apply the *Transparent Firewall Mode* packet filter rule to the data packets received. • `2` To select the *Transparent Firewall Mode* packet filter rule `2`. • `1` To specify priority = `1`

Setting up rules based on MAC addresses

In the following example, the network administrator wants to accept the data packets from computers B and C to computer A based on the MAC address of the devices. The firewall keeps computer A separate from the company network. The firewall helps prevent access between computer A and the rest of the company network. The firewall only permits access from computers B and C to computer A. The computers B and C are part of VLAN `10`.

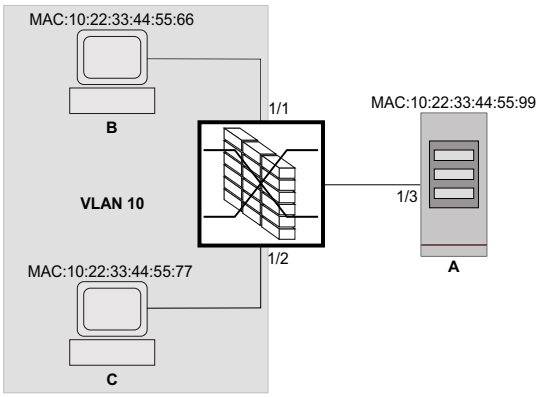


Figure 24: Application example of a packet filter based on MAC addresses

Prerequisites:
- Firewall is in Bridge mode
- In the *Default policy* field, the value `drop` is specified.

Perform the following steps:
☐ Create a MAC rule for end device B.

☐ Open the *Network Security > Packet Filter > Transparent Firewall Mode > Rule* dialog.

☐ Click the button.
The device adds a rule.

☐ Specify the following settings for the rule:
- *Description* column = `accept mac dev b to dev a`
- *Source MAC address* column = `10:22:33:44:55:66`
- *Destination MAC address* column = `10:22:33:44:55:99`
- *Ethertype* column = `vlan8021q`
- *VLAN ID* column = `10`

The prerequisite to change the value in the *VLAN ID* column is:
- In the *Ethertype* column, the value `vlan8021q` is specified.
  or
- In the *Ethertype* column, the value `custom` is specified and in the *Ethertype custom value* column, a valid value is specified.

☐ Activate the rule. To do this, mark the checkbox in the *Active* column.

☐ Apply the settings temporarily. To do this, click the ✓ button.

- ☐ Open the *Network Security > Packet Filter > Routed Firewall Mode > Assignment* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
  - ☐ From the *Port/VLAN* drop-down list, select the port *1/1*.
  - ☐ From the *Direction* drop-down list, select the item `ingress` to activate the rule for incoming data packets.
  - ☐ From the *Index* drop-down list, select the item `accept mac dev b to dev a: 1`.
- ☐ Apply this rule to the data stream. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`packet-filter l2 rule add 1 action accept src-mac 10:22:33:44:55:66 dest-mac 10:22:33:44:55:99 ethertype vlan8021q vlan 10 description accept mac dev b to dev a`	To add a *Transparent Firewall Mode* packet filter rule. • `packet-filter l2 rule add 1` To add a *Transparent Firewall Mode* packet filter rule with index = `1`. • `action accept` • `src-mac 10:22:33:44:55:66` • `dest-mac 10:22:33:44:55:99` • `ethertype vlan8021q` • `vlan 10` • `description accept mac dev b to dev a` To specify the user-specific name `accept mac dev b to dev a`.
`packet-filter l2 rule enable 1`	To activate the *Transparent Firewall Mode* packet filter rule `1`.
`packet-filter l2 if add port 1 ingress 1 1`	To apply the *Transparent Firewall Mode* packet filter rule `1` on port *1/1*. • `packet-filter l2 if add port 1` To add a *Transparent Firewall Mode* packet filter rule for port *1/1*. • `ingress` To apply the *Transparent Firewall Mode* packet filter rule to the data packets received. • `1` To select the *Transparent Firewall Mode* packet filter rule `1`. • `1` To specify priority = `1`

☐ Create a MAC rule for end device C.

☐ Open the *Network Security > Packet Filter > Transparent Firewall Mode > Rule* dialog.

☐ Click the button.
The device adds a rule.

☐ Specify the following settings for the rule:
- *Description* column = `accept mac dev c to dev a`
- *Source MAC address* column = `10:22:33:44:55:77`
- *Destination MAC address* column = `10:22:33:44:55:99`
- *Ethertype* column = *vlan8021q*
- *VLAN ID* column = `10`

The prerequisite to change the value in the *VLAN ID* column is:
- In the *Ethertype* column, the value *vlan8021q* is specified.
  or
- In the *Ethertype* column, the value *custom* is specified and in the *Ethertype custom value* column, a valid value is specified.

☐ Activate the rule. To do this, mark the checkbox in the *Active* column.

☐ Apply the settings temporarily. To do this, click the ✓ button.

☐ Open the *Network Security > Packet Filter > Transparent Firewall Mode > Assignment* dialog.

- ☐ Click the button.
  The dialog displays the *Create* window.
  - ☐ From the *Port/VLAN* drop-down list, select the port *1/2*.
  - ☐ From the *Direction* drop-down list, select the item `ingress` to activate the rule for incoming data packets.
  - ☐ From the *Index* drop-down list, select the item `accept mac dev c to dev a: 2`.
- ☐ Click the *Ok* button.
- ☐ Apply the rule to the data stream. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`packet-filter l2 rule add 2 action accept src-mac 10:22:33:44:55:77 dest-mac 10:22:33:44:55:99 ethertype vlan8021q vlan 10 description accept mac dev c to dev a`	To add a *Transparent Firewall Mode* packet filter rule. • `packet-filter l2 rule add 2` To add a *Transparent Firewall Mode* packet filter rule with index = `2`. • `action accept` • `src-mac 10:22:33:44:55:77` • `dest-mac 10:22:33:44:55:99` • `ethertype vlan8021q` • `vlan 10` • `description accept mac dev c to dev a` To specify the user-specific name `accept mac dev c to dev a`.
`packet-filter l2 rule enable 2`	To activate the *Transparent Firewall Mode* packet filter rule `2`.
`packet-filter l2 if add port 2 ingress 2 1`	To apply the *Transparent Firewall Mode* packet filter rule `2` on port *1/2*. • `packet-filter l2 if add port 2` To add a *Transparent Firewall Mode* packet filter rule for port *1/2*. • `ingress` To apply the *Transparent Firewall Mode* packet filter rule to the data packets received. • `2` To select the *Transparent Firewall Mode* packet filter rule `2`. • `1` To specify priority = `1`.

10.5 Helping protect against DoS attacks

Denial of Service (DoS) is a cyberattack that aims to make certain services or devices unusable. Attackers as well as network administrators can use the port scan method to discover open ports in a network to find vulnerable devices. The function helps you protect the network against invalid or falsified data packets targeted at certain services or devices. You have the option of specifying filters to restrict the data stream for protection against DoS attacks. The filters check the received data packets. The device discards a data packet if it matches the filter criteria.

To help protect the device itself and other devices in the network from DoS attacks, the device lets you specify the following options:
- Filters for TCP and UDP packets
- Filters for IP packets
- Filters for ICMP packets
- 802.3 Frames forwarding

The filters help prevent an attacking station from:
- Detecting services and applications that use the open ports
- Detecting active devices in a network
- Accessing sensitive data in a network
- Detecting active security devices like a firewall used in a network

Note:
You can combine the filters in any way. When you activate several filters, the device applies the filters in the order in which they are specified in the IP table. If an incoming data packet matches a filter, the device discards the respective data packet and then stops further processing.

10.5.1 Filters for TCP and UDP packets

To selectively process *TCP* and *UDP* packets, the device offers you the following filters:
- Activating the Null Scan filter function
- Activating the Xmas filter function
- Activating the SYN/FIN filter function
- Activating the TCP Offset protection function
- Activating the TCP SYN protection function
- Activating the L4 Port protection function
- Activating the Min. Header Size filter function

Activating the Null Scan filter function

With the *Null Scan* method, the attacking station sends data packets with the following properties:
- No *TCP* flags are set.
- The *TCP* sequence number is 0.

The device uses the *Null Scan filter* function to discard incoming *TCP* packets that contain malicious properties.

In the default setting, the *Null Scan filter* function is disabled. To activate the *Null Scan filter* function, perform the following steps:

- ☐ Open the *Network Security > DoS > Global* dialog.
- ☐ Activate the *Null Scan filter* function. To do this, in the *TCP/UDP* frame, mark the *Null Scan filter* checkbox.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos tcp-null`	To activate the *Null Scan filter* function.
`no dos tcp-null`	To deactivate the *Null Scan filter* function.

Activating the Xmas filter function

With the *Xmas* method, the attacking station sends data packets with the following properties:
- The *TCP* flags *FIN*, *URG*, and *PSH* are simultaneously set.
- The *TCP* sequence number is 0.

The device uses the *Xmas filter* function to discard incoming *TCP* packets that contain malicious properties.

In the default setting, the *Xmas filter* function is disabled. To activate the *Xmas filter* function, perform the following steps:

- ☐ Open the *Network Security > DoS > Global* dialog.
- ☐ Activate the *Xmas filter* function. To do this, in the *TCP/UDP* frame, mark the *Xmas filter* checkbox.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos tcp-xmas`	To activate the *Xmas filter* function.
`no dos tcp-xmas`	To deactivate the *Xmas filter* function.

Activating the SYN/FIN filter function

With the *SYN/FIN* method, the attacking station sends data packets with the *TCP* flags *SYN* and *FIN* set simultaneously. The device uses the *SYN/FIN filter* function to discard incoming packets with the *TCP* flags *SYN* and *FIN* set simultaneously.

In the default setting, the *SYN/FIN filter* function is disabled. To activate the *SYN/FIN filter* function, perform the following steps:

- ☐ Open the *Network Security > DoS > Global* dialog.
- ☐ Activate the *SYN/FIN filter* function. To do this, in the *TCP/UDP* frame, mark the *SYN/FIN filter* checkbox.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos tcp-syn-fin`	To activate the *SYN/FIN filter* function.
`no dos tcp-syn-fin`	To deactivate the *SYN/FIN filter* function.

Activating the TCP Offset protection function

With the *TCP Offset* method, the attacking station sends data packets whose fragment offset is equal to 1. The fragment offset is a field in the *IP* header which helps to identify the sequence of fragments in received data packets. The device uses the *TCP Offset protection* function to discard incoming *TCP* data packets whose fragment offset field in the *IP* header is equal to 1.

Note:
The device accepts *UDP* and *ICMP* packets whose fragment offset field of the *IP* header is equal to 1.

In the default setting, the *TCP Offset protection* function is disabled. To activate the *TCP Offset protection* function, perform the following steps:

- ☐ Open the *Network Security > DoS > Global* dialog.
- ☐ Activate the *TCP Offset protection* function. To do this, in the *TCP/UDP* frame, mark the *TCP Offset protection* checkbox.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos tcp-offset`	To activate the *TCP Offset protection* function.
`no dos tcp-offset`	To deactivate the *TCP Offset protection* function.

Activating the TCP SYN protection function

With the *TCP SYN* method, the attacking station sends data packets with the *TCP* flag *SYN* set and an L4 (layer 4) source port <1024. The device uses the *TCP SYN protection* function to discard incoming packets with the *TCP* flag *SYN* set and an L4 (layer 4) source port <1024.

In the default setting, the *TCP SYN protection* function is disabled. To activate the *TCP SYN protection* function, perform the following steps:

- ☐ Open the *Network Security > DoS > Global* dialog.
- ☐ Activate the *TCP SYN protection* function. To do this, in the *TCP/UDP* frame, mark the *TCP SYN protection* checkbox.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos tcp-syn`	To activate the *TCP SYN protection* function.
`no dos tcp-syn`	To deactivate the *TCP SYN protection* function.

Activating the L4 Port protection function

An attacking station can send *TCP* or *UDP* data packets whose source port number and destination port number are identical. The device uses the *L4 Port protection* function to discard incoming *TCP* and *UDP* packets whose L4 source port and destination port number are identical.

In the default setting, the *L4 Port protection* function is disabled. To activate the *L4 Port protection* function, perform the following steps:

- ☐ Open the *Network Security > DoS > Global* dialog.
- ☐ Activate the *L4 Port protection* function. To do this, in the *TCP/UDP* frame, mark the *L4 Port protection* checkbox.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos l4-port`	To activate the *L4 Port protection* function.
`no dos l4-port`	To deactivate the *L4 Port protection* function.

Activating the Min. Header Size filter function

The device uses the *Min. Header Size filter* function to check the *TCP* header of received data packets. The device discards the data packet when (data offset value × 4) < minimum *TCP* header size.

The *Min. Header Size filter* function detects received data packets with the following properties:

(*IP* payload length in the *IP* header - *IP* header outer size) < minimum *TCP* header size.

In the default setting, the *Min. Header Size filter* function is disabled. To activate the *Min. Header Size filter* function, perform the following steps:

- ☐ Open the *Network Security > DoS > Global* dialog.
- ☐ Activate the *Min. Header Size filter* function. To do this, in the *TCP/UDP* frame, mark the *Min. Header Size filter* checkbox.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos tcp-min-header`	To activate the *Min. Header Size filter* function.
`no dos tcp-min-header`	To deactivate the *Min. Header Size filter* function.

10.5.2 Filters for IP packets

To selectively process *IP* packets, the device offers you the following filters:
- Activating the Land Attack filter function
- Deactivating the Drop IP Source Route function

Activating the Land Attack filter function

With the *Land Attack* method, the attacking station sends data packets whose source and destination addresses are identical to the *IP* address of the recipient. The device uses the *Land Attack filter* function to discard received packets whose source and destination addresses are identical.

In the default setting, the *Land Attack filter* function is disabled. To activate the *Land Attack filter* function, perform the following steps:

- ☐ Open the *Network Security > DoS > Global* dialog.
- ☐ Activate the *Land Attack filter* function. To do this, in the *IP* frame, mark the *Land Attack filter* checkbox.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos ip-land enable`	To activate the *Land Attack filter* function.
`no dos ip-land disable`	To deactivate the *Land Attack filter* function.

Deactivating the Drop IP Source Route function

The device uses the *Drop IP Source Route* function to filter the received *IP* data packets with the *Strict Source Routing* or *Loose Source Routing* option set. The device discards *IP* data packets with a specified source routing path in the *IP* header.

Strict Source Routing or *Loose Source Routing* is an option in the *IP* header where the sender specifies the routing path. A router that respects these options sends the respective data packets to the next destination controlled by this option. An attacking station can use the *IP Source Route* method to find the route that the data packets take to reach their destination. For this, the attacking station sends an *IP* packet with the *Strict Source Routing* or *Loose Source Routing* option set and uses the response from the router to get information about the route of the data packet.

In the default setting, the *Drop IP Source Route* function is enabled. To deactivate the *Drop IP Source Route* function, perform the following steps:

- ☐ Open the *Network Security > DoS > Global* dialog.
- ☐ Deactivate the *Drop IP Source Route* function. To do this, in the *IP* frame, unmark the *Drop IP Source Route* checkbox.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`no dos ip-src-route`	To deactivate the *Drop IP Source Route*function.
`dos ip-src-route`	To activate the *Drop IP Source Route*function.

10.5.3 Filters for ICMP packets

To selectively process *ICMP* packets, the device offers you the following filters:
- Activating the Fragmented packets filter function
- Activating the Packet size filter function

Activating the Fragmented packets filter function

The device uses the *Fragmented packets filter* function to protect the network from attacking stations that send fragmented *ICMP* packets. Fragmented *ICMP* packets can cause the destination device to fail if the destination device processes fragmented *ICMP* packets incorrectly. The device uses the *Fragmented packets filter* function to discard fragmented *ICMP* packets.

In the default setting, the *Fragmented packets filter* function is disabled. To activate the *Fragmented packets filter* function, perform the following steps:

- ☐ Open the *Network Security > DoS > Global* dialog.
- ☐ Activate the *Fragmented packets filter* function. To do this, in the *ICMP* frame, mark the *Fragmented packets filter* checkbox.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos icmp-fragmented`	To activate the *Fragmented packets filter* function.
`no dos icmp-fragmented`	To deactivate the *Fragmented packets filter* function.

Activating the Packet size filter function

The device uses the *Packet size filter* to discard data packets whose payload size exceeds the size specified in the *Allowed payload size [byte]* field.

The *Packet size filter* function helps protect the network from attacking stations that send *ICMP* packets whose payload size exceeds the size specified in the *Allowed payload size [byte]* field.

In the default setting, the *Packet size filter* function is disabled. To activate the *Packet size filter* function, perform the following steps:

- ☐ Open the *Network Security > DoS > Global* dialog.
- ☐ Activate the *Packet size filter* function. To do this, in the *ICMP* frame, mark the *Packet size filter* checkbox.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos icmp payload-check`	To activate the *Packet size filter* function.
`no dos icmp payload-check`	To deactivate the *Packet size filter* function.

10.5.4 802.3 Frames forwarding

The *802.3 Frames forwarding* function assists in managing link changes. You can therefore use the function to speed up convergence if a Layer 2 redundancy protocol based on IEEE 802.3 Ethernet packets is active in the network, for example, Rapid Spanning Tree Protocol (RSTP). Convergence is the time required to adjust the network to topology changes, for example when the link status on a port changes.

In the default setting, the device discards the IEEE 802.3 Ethernet packets. The device does not support a redundancy protocol and is not part of a redundancy topology. Using the *802.3 Frames forwarding* function, the device forwards the IEEE 802.3 Ethernet packets received on one port to another port. As a result, the device behaves like a hub for IEEE 802.3 Ethernet packets. This helps the neighboring devices to adapt more quickly to topology changes.

To reduce the convergence time, Hirschmann recommends combining the *802.3 Frames forwarding* function with the *Link flap* function. See the *Diagnostics > Ports > Port Monitor* dialog, *Link flap* tab.

Note:
If a hostile network station sends a high volume of IEEE 802.3 Ethernet packets to the device, the device will propagate these packets. This can cause a Denial of Service (Dos) attack.

Activating the 802.3 Frames forwarding function

In the default setting, the *802.3 Frames forwarding* function is inactive. To activate the *802.3 Frames forwarding* function, perform the following steps:

- ☐ Open the *Network Security > DoS > Global* dialog.
- ☐ Activate the *802.3 Frames forwarding* function. To do this, in the *Layer 2 frames* frame, mark the *802.3 Frames forwarding* checkbox.

  Note:
  If a link on the device becomes inoperable, then the Layer 2 redundancy protocol such as RSTP will find an alternative path by bypassing the device and excluding it from the network path. This scenario poses a potential security risk. Therefore, enable the *802.3 Frames forwarding* function only if you are aware of the effects.

- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos l2-frame-forwarding`	To activate the *802.3 Frames forwarding* function.

10.6 Deep Packet Inspection function

The *DPI* function (*DPI*) lets you monitor and filter data packets. The function supports you in protecting the network from undesirable content, such as spam or viruses.

The *DPI* function inspects data packets for undesirable characteristics and protocol violations. The protocol inspects the header and the payload of the data packets.

10.7 Deep Packet Inspection - Modbus Enforcer function

The *Modbus* protocol is widely used in the automation sector.
- The protocol is based on *Function code*, the commands.
- Some of the *Function code* let you specify register or coil address ranges.

The device uses the *Modbus Enforcer* function to perform Deep Packet Inspection (DPI) on the data stream to inspects data packets for undesirable characteristics and protocol violations. The device performs DPI based on the values defined in the specified profiles. The device discards the data packets that violate the specified profiles.

When the checkbox in the *TCP reset* column is marked, the device terminates the Modbus or TCP connection if it detects any of the following conditions:
- Violation of the Modbus protocol standard as specified in the *Sanity check* column.
- Violation of the possible *function codes* as specified in the *Function code* column.
- Violation of the *unit identifiers* as specified in the *Unit identifier* column.

10.7.1 Application example for the Modbus Enforcer function

The device uses the *DPI* function to monitor the data stream between the *Modbus master* and the *Modbus client (outstation)*. The *DPI* function inspects the data packets for the specified characteristics.

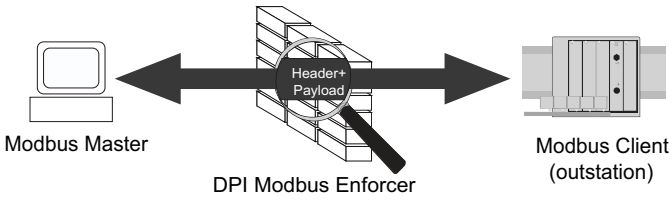


Figure 25: Inspection of data packets

The network administrator wants the device to forward data packets from the *Modbus master* to the *Modbus client (outstation)* with the following characteristics, while performing a *Sanity check*:
- *Function code*:
  - `1 (Read Coils)`
  - `2 (Read Discrete Inputs)`
  - `3 (Read Holding Registers)`
  - `23|128-255|512-1023 (Read/Write Multiple Registers)`, read address range `128..255`, write address range `512..1023`.
- *Unit identifier* = `254,255`

Creating a Modbus Enforcer profile

For the purpose described in the application example, add the *Modbus Enforcer* profile in the device with the above values and name `my-modbus`.

Perform the following steps:

- ☐ Open the *Network Security > DPI > Modbus Enforcer* dialog.
- ☐ Click the ⊞ button.
  The dialog displays the *Create* window.
- ☐ In the *Index* field, specify the value `1`.
- ☐ Click the *Ok* button.
  The device adds a profile.
- ☐ Specify the following settings for the profile:
  - *Description* column = `my-modbus`
  - *Function type* column = *advanced*
  - *Function code* column = `1,2,3,23|128-255|512-1023`
    Separate the address ranges with a vertical bar (pipe).
  - *Unit identifier* column = `254,255`
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dpi modbus addprofile 1 description my-modbus function-type advanced function-code-list 1,2,3,23|128-255|512-1023 unit-identifier-list 254,255`	To add the *Modbus Enforcer* profile. • `dpi modbus addprofile 1` To add the *Modbus Enforcer* profile with index = `1`. • `description my-modbus` To specify the user-specific name `my-modbus`. • `function-type advanced` To specify the *function type* `advanced`. • `function-code-list 1,2,3,23|128-255|512-1023` To assign the *function codes* `1,2,23` and address ranges `|128-255|512-1023`. • `unit-identifier-list 254,255` To specify the unit identifiers `254,255`.

Activating the Modbus Enforcer profile

Perform the following steps:

- ☐ Open the *Network Security > DPI > Modbus Enforcer* dialog.
- ☐ Mark the checkbox in the *Profile active* column.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`dpi modbus enableprofile 1`	To activate the *Modbus Enforcer* profile `1`. After activating the profile, the device helps prevent profile modifications.

Applying the Modbus Enforcer profile to the data stream

Perform the following steps:

- ☐ Open the *Network Security > DPI > Modbus Enforcer* dialog.
- ☐ Click the ⬆ button.

`dpi modbus commit` — To apply the *Modbus Enforcer* profiles.

10.8 Deep Packet Inspection - OPC Enforcer function

OLE for Process Control (OPC) is an integration protocol for industrial environments. The *OPC Enforcer* function supports the network security. The device blocks the data packets that violate the specified profiles. Upon user request, the device verifies the data packets for their plausibility and their fragment characteristics. The device verifies and observes *OPC* data connections and helps protect against invalid or fake data packets. The function dynamically activates TCP ports for each data connection. When requested by an *OPC* server, the device sets up the data connection exclusively between the *OPC* server and the related *OPC* client.

The prerequisite is that *authentication level 5* or lower is set up in your end device to perform the Deep Packet Inspection (DPI). The end device can be a computer or any other equipment capable of sending *OPC* data packets. The *authentication level* defines the type of authentication required for an *OPC* client to connect with an *OPC* server.

The device removes the state information from the packet filter on the following events only:
- When applying the profiles saved in the device to the data stream.
- When activating/deactivating the *Routing* function on a router interface.

The removed state information includes potential *DCE RPC* information for the *OPC Enforcer* function. Consequently, the device interrupts open communication connections.

10.8.1 Application example for the OPC Enforcer function

The device uses the *DPI* function to monitor the data stream between the *OPC master* and *OPC client* (*outstation*). The device inspects the data packets for the specified characteristics.

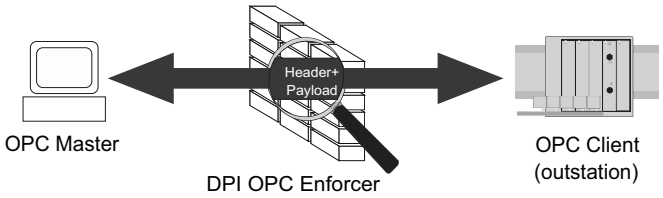


Figure 26: Inspection of data packets

The network administrator wants the device to forward data packets from the *OPC master* to the *OPC client* (*outstation*). The data packets contain the following characteristics:
- *Sanity check* = marked
- *Fragment check* = marked
- *Timeout at connect* = 4

Creating a OPC Enforcer profile

For the purpose described in the application example, add the *OPC Enforcer* profile with the above values and name `my-opc`.

Perform the following steps:

- ☐ Open the *Network Security > DPI > OPC Enforcer* dialog.
- ☐ Click the  button.
  The dialog displays the *Create* window.
- ☐ In the *Index* field, specify the value `1`.
- ☐ Click the *Ok* button.
  The device adds a profile.
- ☐ Specify the following settings for the profile:
  - *Description* column = `my-opc`
  - *Timeout at connect* column = `4`
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dpi opc addprofile 1 description my-opc timeout-connect 4`	To add the *OPC Enforcer* profile. • `dpi opc addprofile 1` To add the *OPC Enforcer* profile with index = `1`. • `description my-opc` To specify the user-specific name `my-opc`. • `timeout-connect 4` To specify the period `4` seconds after which the device terminates the OPC data connection.

Activating the OPC Enforcer profile

Perform the following steps:

- ☐ Mark the checkbox in the *Profile active* column.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`dpi opc enableprofile 1`	To activate the *OPC Enforcer* profile `1`. After activating the profile, the device helps prevent profile modifications.

Applying the OPC Enforcer profile to the data stream

Perform the following step:

☐ Click the ⬆ button.

`dpi opc commit` To apply the *OPC Enforcer* profiles.

10.9 Deep Packet Inspection - DNP3 Enforcer function

The *DNP3* protocol (*Distributed Network Protocol v3*) provides multiplexing, error checking, link control, prioritization, and Layer 2 addressing services for user data.

- The protocol is based on the profile that contains *function code* list, *objects*, and commands. The *DNP3* function uses *objects* to transmit values and information between devices. The *DNP3* function uses *group numbers* to categorize the data type and *variation numbers* to specify how the data within the group is encoded. Each instance of an encoded information element that defines a valid group and variation in the message, is an *object*.
- To control how the device processes the data packets during inspection, you specify the value of each *object* in the following fields in the Graphical User Interface:
  - *Index of Default Object List*
  - *Type*
  - *Group no.*
  - *Variation*
  - *Function*
  - *Function name*
  - *Length*
  - *Qualifier*

The device uses the *DPI* function to discard data packets that violate the specified profiles. When the checkbox in the *TCP reset* column is marked, then the device terminates the *TCP* connection if it detects any of the following conditions:

- Violation of the DNP3 standard as specified in the *Sanity check* and *CRC check* columns.
- Violation of the allowed *function codes* as specified in the *Function code list* column.
- Violation of the allowed *objects* as specified in the following fields in the Graphical User Interface:
  - *Index of Default Object List*
  - *Type*
  - *Group no.*
  - *Variation*
  - *Function*
  - *Function name*
  - *Length*
  - *Qualifier*

10.9.1 Application example for the DNP3 Enforcer function

The device uses the *DPI* function to monitor the data stream between the *DNP3 master* and *DNP3 client* (*outstation*). The *DPI* function inspects the data packets for the specified characteristics.

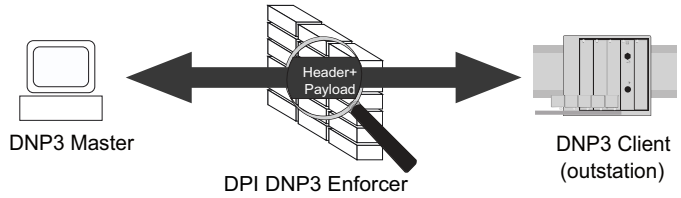


Figure 27: Inspection of data packets

The network administrator wants the device to forward data packets from the *DNP3 master* to *DNP3 client* (*outstation*). The data packets contain the following *function codes* and *objects*:

- *Function code list*:
  - `1 (Read)`
  - `2 (Write)`
  - `3 (Select)`
  - `23 (Delay Measurement)`
- *Index of Default Object List* column = `6`
- *Sanity check* column = marked
- *Objects*:
  - *Index* = `1 - dnp3`
  - *Object index* = `1`
  - *Type* = `request`
  - *Group no.* = `5`
  - *Variation* = `1`
  - *Function* = `2`
  - *Function name* = `WRITE`
  - *Length* = `1`
  - *Qualifier* = `0x17,0x28`

Creating a DNP3 Enforcer profile

For the purpose described in the application example, add the *DNP3 Enforcer* profile with the above values and name `my-dnp3`.

Perform the following steps:

- ☐ Open the *Network Security > DPI > DNP3 Enforcer > Profile* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
  - ☐ In the *Index* field, specify the value `1`.
  - ☐ Click the *Ok* button.
    The device adds a profile.
- ☐ Specify the following settings for the profile:
  - *Description* column = `my-dnp3`
  - *Function code list* column = `1,2,3,23`
  - *Index of Default Object List* column = `6`
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

- ☐ Create and apply the *Objects* to the *DNP3 Enforcer* profile. To do this, perform the following steps:
  - ☐ Open the *Network Security > DPI > DNP3 Enforcer > Object* dialog.
  - ☐ Click the button.
    The dialog displays the *Create* window.
  - ☐ From the *Index* drop-down list, select the item `1 - dnp3`.
  - ☐ In the *Object index* field, specify the value `1`.
  - ☐ From the *Type* drop-down list, select the item *`request`*.
  - ☐ In the *Group no.* field, specify the value `5`.
  - ☐ In the *Variation* field, specify the value `1`.
  - ☐ In the *Function* field, specify the value `2`.
  - ☐ In the *Qualifier* field, specify the value `0x17,0x28`.
  - ☐ Click the *Ok* button.
    The device adds a new object.
- ☐ Specify the following settings for the object:
  - *Function name* column = `WRITE`
  - *Length* column = `1`
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`

To change to the Privileged EXEC mode.

`configure`

To change to the Configuration mode.

```
dpi dnp3 profile add 1 description my-dnp3
function-code-list 1,2,3,23 default-
object-list 6
```

To add the *DNP3 Enforcer* profile.

- `dpi dnp3 profile add 1`
  To add the *DNP3 Enforcer* profile with index = `1`.
- `description my-dnp3`
  To specify the user-specific name `my-dnp3`.
- `function-code-list 1,2,3,23`
  To specify the *function codes* `1,2,3,23`.
- `default-object-list 6`
  To specify the index of *default object list* `6`.

```
dpi dnp3 object 1 add 1 object-type request
group-number 5 variation-number 1 function-
code 2 function-name write function-length
1 qualifier-code-list 0x17,0x28
```

To add the user-specific *objects* to the *DNP3 Enforcer* profile `1`.

- `dpi dnp3 object 1`
  To select the *DNP3 Enforcer* profile `1`.
- `add 1`
  To add *object* with index = `1`.
- `object-type request`
  To specify the object type `request`.
- `group-number 5`
  To specify the group number type `5`.
- `variation-number 1`
  To specify the variation number `1`.
- `function-code 2`
  To specify the function code `2`.
- `function-name write`
  To specify the function name `write`.
- `function-length 1`
  To specify the function length `1`.
- `qualifier-code-list 0x17,0x28`
  To specify the qualifier code `0x17,0x28`.

Activating the DNP3 Enforcer profile

Perform the following steps:

- ☐ Open the *Network Security > DPI > DNP3 Enforcer > Profile* dialog.
- ☐ Mark the checkbox in the *Profile active* column.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
dpi dnp3 profile enable 1
```

To activate the *DNP3 Enforcer* profile 1.
After activating the profile, you cannot add further objects to the profile.

Applying the DNP3 Enforcer profile to the data stream

Perform the following step:

- ☐ Click the ⬆ button.

```
dpi dnp3 profile commit
```

To apply the *DNP3 Enforcer* profiles.

```
show dpi dnp3 profiletable
```

To display the *DNP3 Enforcer* profiles.

```
Profile Index    Sanity Check  CRC Check  TCP Reset  Outstation-Traffic  Description   Enabled
Function Code List
Default Object List
-------------- ------------ ------------------------------------ --------------------
1              [x]          [x]       [x]        [ ]                 my-dnp3      [x]
1,2,3,23
6
```

```
show dpi dnp3 objectlist 1
```

To display the *object* list that the device applies to *DNP3 Enforcer* profile 1.

```
Index       Object Type  Group Number  Variation  Function Code  Function Name  Function Length
Qualifier List
--------- ------------ ----------------------------------- ----------------------------
1         request      5            1          2             write          1
0x17,0x28
```

10.10 Deep Packet Inspection - IEC104 Enforcer function

The *IEC104 Enforcer* function activates the Deep Packet Inspection (DPI) firewall capabilities for the IEC104 data stream. The protocol is based on a profile that contains the following parameters:

- *Type IDs*
- *Originator Address*
- *Common Address*
- *Cause of transmission size*
- *Common Addresses* size
- *IO Address* size
- *IEC101 Type IDs*
- *Sanity check*

The device uses the *DPI* function to discard data packets that violate the specified profiles. When the checkbox in the *TCP reset* column is marked, then the device terminates the *TCP* connection if it detects any of the following conditions:

- Violation of the IEC104 standard as specified in the *Sanity check* column.
- Violation of the allowed *Type ID* values as specified in the *Function type* and *Advanced type ID list* columns.
- Violation of the allowed addresses as specified in the *Originator address list* and *Common address list* columns.
- Violation of the allowed sizes as specified in the *Cause of transmission size*, *Common address size* and *IO address size* columns.
- Violation of the allowed *IEC101 Type ID* values as specified in the *Allow IEC_60870_5_101* column.

10.10.1 Application example for the IEC104 Enforcer function

The device uses the *DPI* function to monitor the data stream between the *IEC104 control station* (client) and *substation* (server). The *DPI* function inspects the data packets for the specified characteristics.

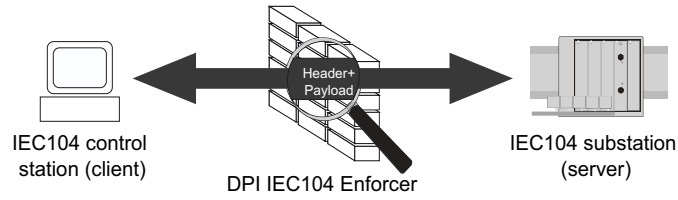


Figure 28: Inspection of data packets

The network administrator wants the device to forward data packets from the *IEC104 control station* (client) to *substation* (server). The data packets contain the following characteristics:

- *Function type* = `readOnly`
  (corresponding *Type IDs* = `1,3,5,7,9,11,13,15,20,21,30-40,70,100-102`)
- *Advanced type ID list*:
  - `2 (Single point information with time tag M_SP_TA_1)`
  - `4 (Double point information with time tag M_DP_TA_1)`
  - `6 (Step position information with time tag M_ST_TA_1)`
- *Originator address list* = `254,255`
- *Common address list* = `254,255`
- *Allow IEC_60870_5_101* = marked
  (corresponding *Type IDs* = `2,4,6,8,10,12,14,16,17,18,19,103,104,105,106`)
- *Sanity check* = marked

Creating an IEC104 Enforcer profile

For the purpose described in the application example, add the *IEC104 Enforcer* profile with the above values and name `my-iec104`.

Perform the following steps:

- ☐ Open the *Network Security > DPI > IEC104 Enforcer* dialog.
- ☐ Click the ➕ button.
  The dialog displays the *Create* window.
- ☐ In the *Index* field, specify the value `1`.
- ☐ Click the *Ok* button.
  The device adds a profile.
- ☐ Specify the following settings for the profile:
  - *Description* column = `my-iec104`
  - *Function type* column = `readOnly`
    The device assigns the *Type ID* values `1,3,5,7,9,11,13,15,20,21,30-40,70,100-102` corresponding to the *function type* = `readOnly`.
  - *Advanced type ID list* column = `2,4,6`
  - *Originator address list* column = `254,255`
  - *Common address list* column = `254,255`
  - *Allow IEC_60870_5_101* column = marked
    The device assigns the *IEC101 Type ID* values `2,4,6,8,10,12,14,16,17,18,19,103,104,105,106`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
enable
```
To change to the Privileged EXEC mode.

```
configure
```
To change to the Configuration mode.

```
dpi iec104 add 1 description my-iec104
function-type readonly adv-type-id-list
2,4,6 originator-addr-list 254,255 common-
addr-list 254,255 allow-101 enable
```
To add the *IEC104 Enforcer* profile.

- `dpi iec104 add 1`
  To add the *IEC104 Enforcer* profile with index = `1`.
- `description my-iec104`
  To specify the user-specific name `my-iec104`.
- `function-type readonly`
  To specify the *function type* `readonly`.
- `adv-type-id-list 2,4,6`
  To specify advanced type IDs `2,4,6`.
- `originator-addr-list 254,255`
  To specify originator addresses `254,255`.
- `common-addr-list 254,255`
  To specify common addresses `254,255`.
- `allow-101 enable`
  To enable the *IEC101*.

Activating the IEC104 Enforcer profile

Perform the following steps:

- ☐ Mark the checkbox in the *Profile active* column.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
dpi iec104 enable 1
```

To activate the *IEC104 Enforcer* profile 1.
After activating the profile, the device helps prevent profile modifications.

Applying the IEC104 Enforcer profile to the data stream

Perform the following step:

- ☐ Click the ⬆ button.

```
dpi iec104 commit
```

To apply the *IEC104 Enforcer* profiles.

10.11 Deep Packet Inspection - AMP Enforcer function

10.11.1 Description

The *AMP Enforcer* function supports the Common ASCII Message Protocol (CAMP) and the Non-Intelligent Terminal Protocol (NITP) using the Transmission Control Protocol (TCP). The *AMP Enforcer* function applies the Deep Packet Inspection (DPI) to the CAMP and NITP data stream. The ASCII Message Protocol (AMP) is used to monitor and control industrial automation equipment such as Programmable Logic Controllers (PLCs), sensors, and meters.

The device performs the *DPI* function based on the *Program and mode protect* function and the specified profiles. Every profile contains the following parameters:

- *Protocol*
- *Message type*
- *Address class*
- *Device class*
- *Memory address*
- *Data word*
- *Task codes (config and non-config)*
- *Task code data*
- *Error check character*
- *Block check character*
- *Sanity check*

The device discards the data packets that violate the specified profiles. When the checkbox in the *TCP reset* column is marked, the device terminates the *TCP* connection if it detects any of the following conditions:

- Violation of the AMP standard as specified in the *Sanity check*, *Error check characters* and *Block check characters* columns.
- Violation of the values as specified in the following columns:
  - *Protocol*
  - *Message type*
  - *Address class*
  - *Device class*
  - *Memory address*
  - *Data word*
  - *Task code*
  - *Task code data*

10.11.2 Program and mode protect function

The device uses the *Program and mode protect* function to forward or discard data packets that contain *task codes* with the `config` mode. The *task codes* with the `config` mode, are the command or response messages. These messages are associated with modification of the configuration, application program, or the operational mode of the equipment.

Depending on the status of the *Program and mode protect* function, the device behaves as follows:

- The function is active:
  The device forwards the data packets that match the parameters specified in the profiles except the data packets that contain the *task codes* with the `config` mode.
- The function is inactive:
  The device forwards the data packets that match the parameters specified in the profiles including the data packets that contain the *task codes* with the `config` mode.

In both the active and inactive states of the *Program and mode protect* function, the device lets you add and apply profiles that contain the following characteristics:
- A *task code* with the value `config` in the *Mode* column.
- A *task code* with the value `non-config` in the *Mode* column.

In the default setting, the *Program and mode protect* function is active.

10.11.3 Hardware LAN bypass

The Hardware LAN bypass function is used to maintain the data communication in case of a power loss or a detected failure. See section "Hardware LAN bypass" on page 107.

10.11.4 Application examples for the AMP Enforcer function

The device uses the *DPI* function to monitor the data stream between the AMP control station (client) and PLC (server). The *DPI* function inspects the data packets for the specified characteristics.

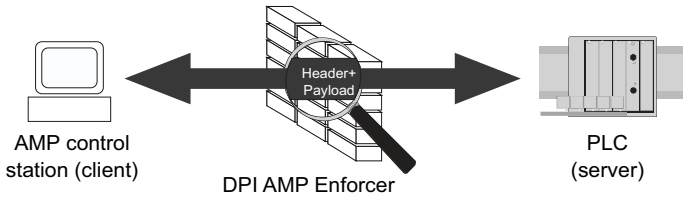


Figure 29: Inspection of data packets

The following sections describe how to set up a *AMP Enforcer* profile:
- Setting up a profile for data packets (camp)
- Setting up a profile for data packets (nitp)

Setting up a profile for data packets (camp)

The network administrator wants the device to forward data packets from the AMP control station (client) to PLC (server). The data packets contain the following characteristics:
- *Protocol* = `camp`
- *Message type*:
  - `04` (corresponding message = `Read Data Command`)
  - `06` (corresponding message = `Write Data Command`)
- *Address class* = `0001,0004`
- *Memory address* = `0003,0006`
- *Block check characters* = `marked`
- *Sanity check* = `marked`

For the purpose described above, add the *AMP Enforcer* profile with the above values and name `accept-camp`.

Perform the following steps:

☐ Create an *AMP Enforcer* profile.

☐ Open the *Network Security > DPI > AMP Enforcer > Profile* dialog.

☐ Click the button.
The dialog displays the *Create* window.
- ☐ In the *Index* field, specify the value `1`.
- ☐ Click the *Ok* button.
  The device adds a profile.

☐ Specify the following settings for the profile:
- *Description* column = `accept-camp`
- *Protocol* column = `camp`
- *Message type* column = `04,06`
- *Address class* column = `0001,0004`
- *Memory address* column = `0003,0006`

☐ Apply the settings temporarily. To do this, click the ✓ button.

```
enable
configure
dpi amp profile add 1 description accept-
camp protocol camp message-type 04,06
address-class 0001,0004 memory-address
0003,0006
```

To change to the Privileged EXEC mode.

To change to the Configuration mode.

To add an *AMP Enforcer* profile.

- `dpi amp profile add 1`
  To add the *AMP Enforcer* profile with index = `1`.
- `description accept-camp`
  To specify the description `accept-camp`.
- `protocol camp`
  To specify the *Protocol* `camp`.
- `message-type 04,06`
  To specify the *message type* `04,06`.
- `address-class 0001,0004`
  To specify the *address classes* `0001,0004`.
- `memory-address 0003,0006`
  To specify the *Memory addresses* `0003,0006`.

☐ Activate the *AMP Enforcer* profile.

☐ Open the *Network Security > DPI > AMP Enforcer > Profile* dialog.

☐ Mark the checkbox in the *Profile active* column.

☐ Apply the settings temporarily. To do this, click the ✓ button.

`dpi amp profile enable 1`	To activate the *AMP Enforcer* profile `1`. After activating the profile, the device helps prevent profile modifications.

☐ Apply the *AMP Enforcer* profile to the data stream.

☐ Open the *Network Security > DPI > AMP Enforcer > Global* dialog.

☐ Click the button.

`dpi amp commit`	To apply the *AMP Enforcer* profiles.

Setting up a profile for data packets (nitp)

The network administrator wants the device to forward data packets from the AMP control station (client) to PLC (server) to modify the settings of the PLC (server). The data packets contain the following characteristics:

- *Protocol* = `nitp`
- *Task code*:
  - `02 (Write Word Memory Area Random)`
  - `30 (Read Operational Status)`
  - `50 (Read User Word Area Block)`
  - `9B` (user-specific *task code* with value `config` in the *Mode* column)
- *Error check characters* = `marked`
- *Sanity check* = `marked`

For the purpose described above, add the *AMP Enforcer* profile with the above values and name `accept-nitp`.

Perform the following steps:

☐ Create an *AMP Enforcer* profile.

☐ Open the *Network Security > DPI > AMP Enforcer > Global* dialog.

☐ Deactivate the *Program and mode protect* function. To do this, unmark in the *Protect mode* frame the *Program and mode protect* checkbox.

☐ Apply the settings temporarily. To do this, click the ✓ button.

☐ Create a user-specific *task code*. To do this, click the button.
The dialog displays the *Create* window to add a *task code*.
  ☐ In the *Task code* field, specify the value `9B`.
  ☐ Click the *Ok* button.
  ☐ In the *Description* column, specify the value `modify-configuration`.

☐ Open the *Network Security > DPI > AMP Enforcer > Profile* dialog.

- ☐ Click the button.
  The dialog displays the *Create* window.
  - ☐ In the *Index* field, specify the value `1`.
  - ☐ Click the *Ok* button.
    The device adds a profile.
- ☐ Specify the following settings for the profile:
  - *Description* column = `accept-nitp`
  - *Protocol* column = `nitp`
  - *Task code* column = `02,30,50,9B`
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`no dpi amp protect-mode`	To deactivate the *Program and mode protect* function.
`dpi amp task-code add 9B description modify-configuration`	To add a user-specific *task code*. • `dpi amp task-code add 9B` To add a *task code* `9B`. • `description modify-configuration` To specify the description `modify-configuration`.
`dpi amp profile add 1 description accept-nitp protocol nitp task-code 02,30,50,9B`	To add an *AMP Enforcer* profile. • `dpi amp profile add 1` To add the *AMP Enforcer* profile with index = `1`. • `description accept-nitp` To specify the description `accept-nitp`. • `protocol nitp` To specify the *protocol* `nitp`. • `task-code 02,30,50,9B` To specify the *task codes* `02,30,50,9B`.

- ☐ Activate the *AMP Enforcer* profile.

- ☐ Mark the checkbox in the *Profile active* column.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`dpi amp profile enable 1`	To activate the *AMP Enforcer* profile `1`. After activating the profile, the device helps prevent profile modifications.

- ☐ Apply the *AMP Enforcer* profile to the data stream.

- ☐ Open the *Network Security > DPI > AMP Enforcer > Global* dialog.
- ☐ Click the button.

`dpi amp commit`	To apply the *AMP Enforcer* profiles.

10.12 Deep Packet Inspection - ENIP Enforcer function

The Ethernet Industrial Protocol (ENIP) is part of the Common Industrial Protocol (CIP). The Common Industrial Protocol (CIP) defines the object structure and specifies the message transfer. The *ENIP Enforcer* function applies the Deep Packet Inspection (DPI) function to the ENIP and CIP data stream. The Ethernet Industrial Protocol (ENIP) is used to monitor and control industrial automation equipment such as PLCs (Programmable Logic Controllers), sensors, and meters.

The device performs the DPI function based on the specified profiles. Every profile contains the following parameters:
- *Function types*
- Allow embedded PCCC
- *Sanity check*
- *Objects*

To control how the device processes the data packets during inspection, you specify the *Class IDs*, *Service codes*, or the combination of both in the following fields in the Graphical User Interface:
- *Default object list*
- *Wildcard service codes*
- *Class ID*
- *Service codes*

The device uses the *DPI* function to discard data packets that violate the specified profiles. When the *TCP reset* function is enabled, then the device terminates the *TCP* connection if it detects any of the following conditions:
- Violation of the ENIP standard as specified in the *Allow embedded PCCC* and *Sanity check* columns.
- Violation of the allowed *Function types* as specified in the *Function type* column.
- Violation of the allowed *Objects* as specified in the following fields in the Graphical User Interface:
  - *Default object list*
  - *Wildcard service codes*
  - *Class ID*
  - *Service codes*

10.12.1 Application example for the ENIP Enforcer function

The device uses the *DPI* function to monitor the data stream between the ENIP control station (server) and the PLC (client). The *DPI* function inspects the data packets for the specified characteristics.

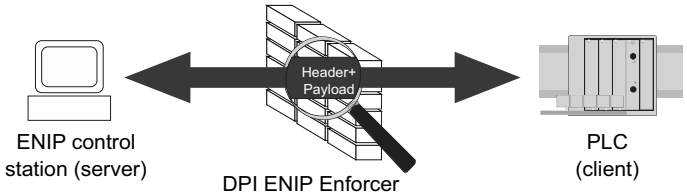


Figure 30: Inspection of data packets

The network administrator wants the device to forward data packets from the ENIP control station (server) to the PLC (client). The data packets contain the following characteristics:
- *Function type* = *advanced*
- *Allow embedded PCCC* column = marked

- *Sanity check* column = marked
- *Objects*:
  - *Default object list* = `6`
  - *Wildcard service codes* = `0x01`
  - *Class ID* = `0x100`
  - *Service codes* = `0x0E`

Creating an ENIP Enforcer profile

For the purpose described in the application example, add the *ENIP Enforcer* profile with the above values and name `my-enip`.

Perform the following steps:

- ☐ Open the *Network Security > DPI > ENIP Enforcer > Profile* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *Index* field, specify the value `1`.
- ☐ Click the *Ok* button.
  The device adds a profile.
- ☐ Specify the following settings for the profile:
  - *Description* column = `my-enip`
  - *Function type* column = *advanced*
  - *Allow embedded PCCC* column = marked
  - *Default object list* column = `6`
  - *Wildcard service codes* column = `0x01`
    The device applies the *Wildcard service code* to every *Class ID* available in the *Default object list* and the *Service codes* columns.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Create and apply the *Objects* to the *ENIP Enforcer* profile. To do this, open the *Network Security > DPI > ENIP Enforcer > Object* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
  - ☐ From the *Index* drop-down list, select the item `1 - enip`.
  - ☐ In the *Class ID* field, specify the value `0x100`.
  - ☐ In the *Service codes* field, specify the value `0x0E`.
  - ☐ In the *Description* field, specify the value `my-enip-object`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dpi enip profile add 1 description my-enip function-type advanced def-list 6 wildcard-list 0x01 allow-emb-pccc enable`	To add the *ENIP Enforcer* profile. • `dpi enip profile add 1` To add the *ENIP Enforcer* profile with index = `1`. • `description my-enip` To specify the user-specific name `my-enip`. • `function-type advanced` To specify the *function type* `advanced`. • `def-list 6` To specify the *default object list* `6`. • `wildcard-list 0x01` To specify the *Wildcard service code* `0x01`. • `allow-emb-pccc enable` To enable the inspection of PCCC messages.
`dpi enip object add 1 0x100 0x0E description my-enip-object`	To add the user-specific *objects* to the *ENIP Enforcer* profile `1`. • `dpi enip object add 1` To add the object to the *ENIP Enforcer* profile `1`. • `0x100` To specify the *Class ID* `0x100`. • `0x0E` To specify the *Service code* `0x0E`. • `description my-enip-object` To specify the description `my-enip-object`.

Activating the ENIP Enforcer profile

Perform the following steps:

- ☐ Open the *Network Security > DPI > ENIP Enforcer > Profile* dialog.
- ☐ Mark the checkbox in the *Profile active* column.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`dpi enip profile enable 1`	To activate the *ENIP Enforcer* profile `1`. After activating the profile, you cannot add further objects to the profile.

Applying the ENIP Enforcer profile to the data stream

Perform the following steps:

- ☐ Click the ⬆ button.

`dpi enip profile commit`	To apply the *ENIP Enforcer* profiles.
`show dpi enip profiletable`	To display the *ENIP Enforcer* profiles.
`show dpi enip objecttable`	To display the *ENIP Enforcer* objects.

10.13 Deep Packet Inspection - S7 Enforcer function

S7comm is a communication protocol based on a master-slave model. Using the S7comm protocol, a master device, such as a Programmable Logic Controller (PLC) or a Human Machine Interface (HMI), initiates communication with one or more slave devices, such as I/O modules, drives, or other PLCs. The S7comm protocol is used for exchanging data, such as reading and writing variables and sending control commands.

The S7comm protocol has an advanced variant called S7comm Plus. In comparison to S7comm, S7comm Plus provides compatibility with modern PLCs and higher flexibility according to various communication requirements. The S7comm Plus protocol offers improved performance and additional features like improved security and scalability.

Using the *S7 Enforcer* function, the device performs Deep Packet Inspection (DPI) on the data stream to monitor and validate conformity with S7comm and S7comm Plus protocol standards. This process involves:

- Creating a template
  You specify specific rules that include the following parameters:
  - *Protocol type*
  - *Function type*
  - *Function group* (only S7comm)
  - *Sub-function group* (only S7comm)
- Creating a profile
  That includes the following additional parameters:
  - *Sanity check*
  - *Debug*
  - *TCP reset*
- Associating the template with the profile
- Applying the profile to the data stream
  The device blocks the data packets that violate the specified profile. The device permits only data packets containing the values specified in the profile.

The device supports up to 40 templates for inspecting the data packets:

- 14 predefined templates
  The device restricts you from deleting predefined templates.
- a maximum of 26 user-defined templates

10.13.1 Application example

The device uses the *DPI* function to monitor the data stream between the *S7 Master (Control station)* and the *S7 Slave (Substation)*. The device inspects the data packets for the specified characteristics.

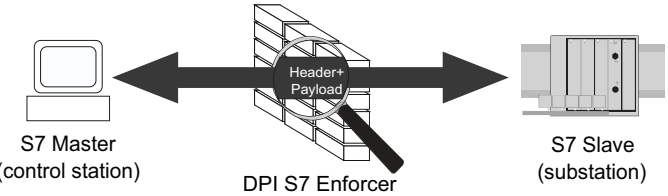


Figure 31: Inspection of data packets

The following sections describe how to set up an *S7 Enforcer* profile:
- “Setting up a profile for S7comm data packets” on page 170
- “Setting up a profile for S7comm Plus data packets” on page 172

10.13.2 Setting up a profile for S7comm data packets

The network administrator wants the device to forward data packets from the *S7 Master (Control station)* to the *S7 Slave (Substation)*.

The data packets should have the following characteristics:
- *Protocol type* = `s7comm`
- *Function type* = `0x00 (CPU services)`
- *Function group* = `0x02 (Cyclic services)`
- *Sub-function group* = `0x01 (Cyclic transfer)`, `0x05 (Change driven transfer)`

The device should perform the following checks:
- *Sanity check*
  To check the plausibility of the data packets regarding format and specification
- *Debug*
  To send a reset packet along with the information related to the termination of the TCP connection
- *TCP reset*
  To terminate the TCP connection, if the device detects a protocol violation or a plausibility check error

For the purpose described above, setup an *S7 Enforcer* profile:
- Create a template in the device with the above characteristics and name `my-s7comm-template`.
  See “Creating an S7 Enforcer template” on page 170.
- Create an *S7 Enforcer* profile with the above checks and the name `my-s7comm-profile`.
  See “Creating an S7 Enforcer profile” on page 171.
- Activate the *S7 Enforcer* profile.
  See “Activating the S7 Enforcer profile” on page 172.
- Apply the *S7 Enforcer* profile to the data stream.
  See “Applying the S7 Enforcer profile to the data stream” on page 172.

Creating an S7 Enforcer template

Perform the following steps:

- ☐ Open the *Network Security > DPI > S7 Enforcer > Template* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
  - ☐ In the *Index* field, specify the value `15`, then click the + button.
  - ☐ From the *Protocol type* drop-down list, select the `s7comm` item.
  - ☐ In the *Rule index* field, specify the value `1`.
- ☐ Click the *Ok* button.
  The device adds a template with *Index* = `15`.

- ☐ In the *Template name* column, specify the value `my-s7comm-template`.
- ☐ Specify the following settings for the rule with *Rule index* = `1`, associated with the template with *Index* = `15`:
  - *Status* column = marked
  - *Function type* column = `0x00 (CPU services)`
  - *Function group* column = `0x02 (Cyclic services)`
  - *Sub-function group* column = `0x01 (Cyclic transfer)`, `0x05 (Change driven transfer)`
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dpi s7 template add 15 description my-s7comm-template protocol-type s7comm`	To add an *S7 Enforcer* template. • `dpi s7 template add 1` To add the *S7 Enforcer* template with index = `15`. • `description my-s7comm-template` To specify the description `my-s7comm-template`. • `protocol-type s7comm` To specify the *Protocol type* `s7comm`.
`dpi s7 rule add 15 1 function-type 0x00 function-group 0x2 sub-function-group 0x01,0x05`	To add a rule to the *S7 Enforcer* template. • `dpi s7 rule add 15 1` To add the rule with rule index = `1` to the *S7 Enforcer* template with index = `15`. • `function-type 0x00` To specify the *Function type* `0x00`. • `function-group 0x2` To specify the *Function group* `0x2`. • `sub-function-group 0x01,0x05` To specify the *Sub-function group* `0x01,0x05`.
`dpi s7 rule enable 15 1`	To activate rule `1` associated with template `15`.

Creating an S7 Enforcer profile

Perform the following steps:

- ☐ Open the *Network Security > DPI > S7 Enforcer > Profile* dialog.
- ☐ Click the ⊞ button.
  The dialog displays the *Create* window.
- ☐ In the *Index* field, specify the value `1`.
- ☐ Click the *Ok* button.
  The device adds a profile with *Index* = `1`.
- ☐ Specify the following settings for the profile with *Index* = `1`:
  - *Description* column = `my-s7comm-profile`
  - *Template list* column = `15-my-s7comm-template-S7COMM`
  - *Debug* column = marked
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
dpi s7 profile add 1 description my-s7comm-
profile template-list 15 debug enable
```

To add an *S7 Enforcer* profile.

- `dpi s7 profile add 1`
  To add the *S7 Enforcer* profile with index = `1`.
- `description my-s7comm-profile`
  To specify the description `my-s7comm-profile`.
- `template-list 15`
  To specify the template list with index = `15`.
- `debug enable`
  To enable `debugging`.

Activating the S7 Enforcer profile

Perform the following steps:

- ☐ Open the *Network Security > DPI > S7 Enforcer > Profile* dialog.
- ☐ Mark the checkbox in the *Profile active* column for the profile with *Index* = `1`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
dpi s7 profile enable 1
```

To activate the *S7 Enforcer* profile `1`.
After activating the profile, the device helps prevent profile modifications.

Applying the S7 Enforcer profile to the data stream

Perform the following steps:

- ☐ Open the *Network Security > DPI > S7 Enforcer > Profile* dialog.
- ☐ Click the ⤒ button.

```
dpi s7 profile commit
```

To apply the *S7 Enforcer* profiles.

10.13.3 Setting up a profile for S7comm Plus data packets

The network administrator wants the device to forward data packets from the *S7 Master (Control station)* to the *S7 Slave (Substation)*.

The data packets should have the following characteristics:

- *Protocol type* = `s7commplus`
- *Function type* = `0x04ca (CreateObject)`

The device should perform the following checks:

- *Sanity check*
  To check the plausibility of the data packets regarding format and specification

- *Debug*
  To send a reset packet along with the information related to the termination of the TCP connection
- *TCP reset*
  To terminate the TCP connection, if the device detects a protocol violation or a plausibility check error

For the purpose described above, setup an *S7 Enforcer* profile:
- Create a template in the device with the above characteristics and name `my-s7commplus-template`.
  See section “Creating an S7 Enforcer template” on page 173.
- Create an *S7 Enforcer* profile with the above checks and name `my-s7commplus-profile`.
  See section “Creating an S7 Enforcer profile” on page 174.
- Activate the *S7 Enforcer* profile.
  See section “Activating the S7 Enforcer profile” on page 175.
- Apply the *S7 Enforcer* profile to the data stream.
  See section “Applying the S7 Enforcer profile to the data stream” on page 175.

Creating an S7 Enforcer template

Perform the following steps:

- ☐ Open the *Network Security > DPI > S7 Enforcer > Template* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
  - ☐ In the *Index* field, specify the value `15`, then click the + button.
  - ☐ From the *Protocol type* drop-down list, select the `s7commplus` item.
  - ☐ In the *Rule index* field, specify the value `1`.
- ☐ Click the *Ok* button.
  The device adds a template with *Index* = `15`.
- ☐ In the *Template name* column, specify the value `my-s7commplus-template`.
- ☐ Specify the following settings for the rule with *Rule index* = `1`, associated with the template with *Index* = `15`:
  - *Status* column = marked
  - *Function type* column = `0x04ca (CreateObject)`
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.

```
dpi s7 template add 15 description my-
s7commplus-template protocol-type
s7commplus
```

To add an *S7 Enforcer* template.

- `dpi s7 template add 1`
  To add the *S7 Enforcer* template with index = `15`.
- `description my-s7commplus-template`
  To specify the description `my-s7commplus-template`.
- `protocol-type S7commplus`
  To specify the *Protocol type* `s7commplus`.

```
dpi s7 rule add 15 1 function-type 0x04ca
function-group 0xFF sub-function-group -
```

To add a rule to the *S7 Enforcer* template.

- `dpi s7 rule add 15 1`
  To add the rule with rule index = `1` to the *S7 Enforcer* template with index = `15`.
- `function-type 0x04ca`
  To specify the *Function type* `0x04ca`.
- `function-group 0xFF`
  To specify the *Function group* `none`.
- `sub-function-group -`
  To specify the *Sub-function group* `none`.

```
dpi s7 rule enable 15 1
```

To activate rule `1` associated with template `15`.

Creating an S7 Enforcer profile

Perform the following steps:

- ☐ Open the *Network Security > DPI > S7 Enforcer > Profile* dialog.
- ☐ Click the  button.
  The dialog displays the *Create* window.
- ☐ In the *Index* field, specify the value `1`.
- ☐ Click the *Ok* button.
  The device adds a profile with *Index* = `1`.
- ☐ Specify the following settings for the profile with *Index* = `1`:
  - *Description* column = `my-s7commplus-profile`
  - *Template list* column = `15-my-s7commplus-template-S7COMM_PLUS`
  - *Debug* column = marked
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
dpi s7 profile add 1 description my-
s7commplus-profile template-list 15 debug
enable
```

To add an *S7 Enforcer* profile.

- `dpi s7 profile add 1`
  To add the *S7 Enforcer* profile with index = `1`.
- `description my-s7commplus-profile`
  To specify the description `my-s7commplus-profile`.
- `template-list 15`
  To specify the template list with index = `15`.
- `debug enable`
  To enable debugging mode.

Activating the S7 Enforcer profile

Perform the following steps:

- ☐ Open the *Network Security > DPI > S7 Enforcer > Profile* dialog.
- ☐ Mark the checkbox in the *Profile active* column for the profile with *Index* = 1.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
dpi s7 profile enable 1
```

To activate the *S7 Enforcer* profile 1.
After activating the profile, the device helps prevent profile modifications.

Applying the S7 Enforcer profile to the data stream

Perform the following steps:

- ☐ Open the *Network Security > DPI > S7 Enforcer > Profile* dialog.
- ☐ Click the ⤒ button.

```
dpi s7 profile commit
```

To apply the *S7 Enforcer* profiles.

11 Network load control

The device features a number of functions that can help you reduce the network load:
- Direct packet distribution
- Rate limiter
- Prioritization - QoS
- Flow control

11.1 Direct packet distribution

The device reduces the network load with direct packet distribution.

On each of its ports, the device learns the sender MAC address of received data packets. The device stores the combination “port and MAC address” in its MAC address table (forwarding database).

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 corrupt data packets.

11.1.1 Learning MAC addresses

When the device receives a data packet, it checks if the MAC address of the sender is already stored in the MAC address table (forwarding database). When the MAC address of the sender is unknown, the device generates an entry. The device then compares the destination MAC address of the data packet with the entries stored in the MAC address table (forwarding database):
- The device forwards packets with a known destination MAC address directly to ports that have already received data packets from this MAC address.
- The device floods data packets with unknown destination addresses, that is, the device forwards these data packets to every port.

11.1.2 Aging of learned MAC addresses

Addresses that have not been detected by the device for an adjustable period of time (aging time) are deleted from the MAC address table (forwarding database) by the device. A reboot or resetting the MAC address table (forwarding database) deletes the entries in the MAC address table (forwarding database).

11.1.3 Static address entries

In addition to learning the sender MAC address, the device also provides the option to set MAC addresses manually. These MAC addresses remain set up and survive resetting of the MAC address table (forwarding database) 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 *MAC address* field, specify the destination MAC address.
– In the *VLAN ID* field, specify the VLAN ID.
– 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 *MAC address* field, select only one port.
When you have defined a Multicast MAC address in the *MAC 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.

☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mac-filter <MAC address> <VLAN ID>`	To add the MAC address filter, consisting of a MAC address and VLAN ID.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`mac-filter <MAC address> <VLAN ID>`	To assign the port to a previously added MAC address filter.
`save`	To 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.

☐ Apply the settings 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, remove it from the table. To do this, select the table row that contains the value *Permanent* in the *Status* column, then click the button.

☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`no mac-filter <MAC address> <VLAN ID>`	To cancel the assignment of the MAC address filter on the port.
`exit`	To change to the Configuration mode.
`no mac-filter <MAC address> <VLAN ID>`	To delete the MAC address filter, consisting of a MAC address and a VLAN ID.
`exit`	To change to the Privileged EXEC mode.
`save`	To 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 (forwarding database), click the button.
As an alternative, open the *Basic Settings > Restart* dialog and click the *Clear FDB* button.

`clear mac-addr-table`	To delete the learned MAC addresses from the MAC address table (forwarding database).

11.2 Rate limiter

The rate limiter function helps ensure stable operation even with high data volumes by limiting the amount of data packets on the ports. The rate limitation is performed individually for each port, as well as separately for inbound and outbound data packets.

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 data packets.

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 amount of outbound data packets instead of the inbound data packets. 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 separated according to the type of the data packets:
  - 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 *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.

☐ Apply the settings temporarily. To do this, click the ✓ button.

11.3 QoS/Priority

QoS (Quality of Service) is a procedure defined in IEEE 802.1D which is used to distribute resources in the network. QoS lets you prioritize the data of necessary applications.

When there is a heavy network load, prioritizing helps prevent data packets with lower priority from interfering with delay-sensitive data packets. Delay-sensitive data packets include, for example, voice, video, and real-time data.

11.3.1 Handling of received priority information

Applications label data packets with the following prioritization information:

- VLAN priority according to IEEE 802.1Q (Layer 2)

11.3.2 VLAN tagging

For the VLAN and prioritizing functions, IEEE 802.1Q 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”).

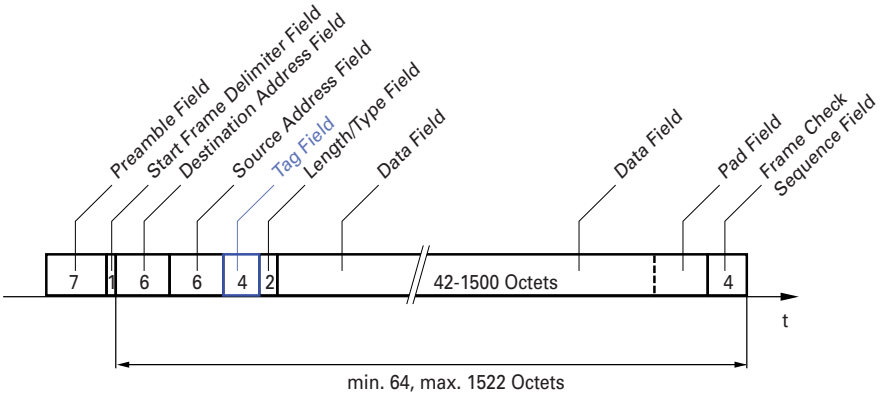


Figure 32: Ethernet data packet with tag

For data packets with VLAN tags, the device evaluates the following information:
- Priority information
- When VLANs are set up, VLAN tagging

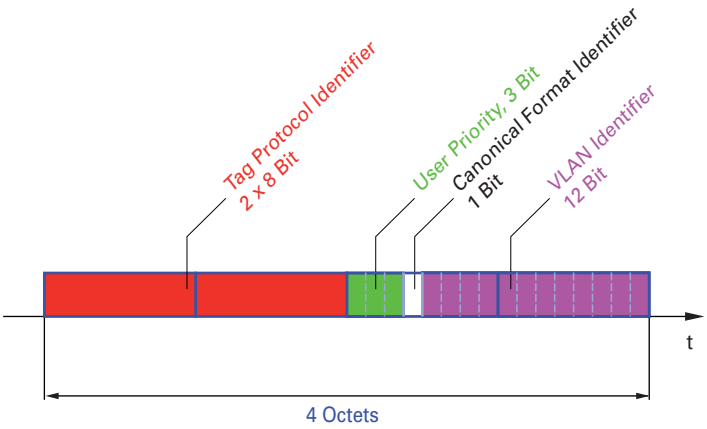


Figure 33: Structure of the VLAN tagging

A data packets with VLAN tag containing priority information but no VLAN information (VLAN ID = 0), is known as a *Priority Tagged* frame.

Note:
Network protocols and redundancy mechanisms use the highest *traffic class* 7. Therefore, select other *traffic classes* for application data.

When using VLAN prioritizing, consider the following special features:
- End-to-end prioritizing requires the VLAN tags to be transmitted to the entire network. The prerequisite is that every network component is VLAN-capable.
- Routers are not able to send and receive packets with VLAN tags through port-based router interfaces.

11.3.3 Setting prioritization

Assigning the Port priority

Perform the following steps:

- ☐ 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.

`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`vlan priority 3`	To assign interface `1/1` the *Port priority* `3`.
`exit`	To 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`classofservice dot1p-mapping 0 2`	To assign a VLAN priority of `0` to *traffic class* `2`.
`classofservice dot1p-mapping 1 2`	To assign a VLAN priority of `1` to *traffic class* `2`.
`exit`	To change to the Privileged EXEC mode.
`show classofservice dot1p-mapping`	To display the assignment.

11.4 Flow control

If a large number of data packets are received in the priority queue of a port at the same time, then this can cause the port memory to overflow. This happens, for example, when the device receives data on a Gigabit port and forwards it to a port with a lower bandwidth. The device discards superfluous data packets.

The flow control mechanism defined in IEEE 802.3 helps ensure that no data packets are lost due to buffer overflow on a port. Shortly before the buffer memory of a port 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 data packets.

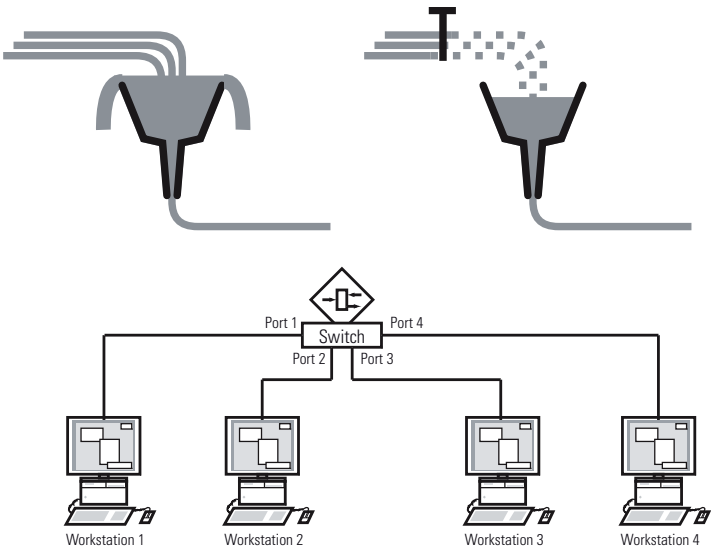


Figure 34: Example of flow control

11.4.1 Flow Control with a half-duplex link

In the example, there is a half-duplex 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.

11.4.2 Flow Control with a full-duplex link

In the example, there is a full-duplex link between Workstation 2 and the device.

Before the send queue of port 2 overflows, the device sends a request to Workstation 2 to include a small break in the sending transmission.

11.4.3 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

12 VLANs

In the simplest case, a virtual LAN (VLAN) consists of a group of network participants in one network segment who can communicate with each other as though they belonged to a separate LAN.

More complex VLANs span out over multiple network segments and are also based on logical (instead of only physical) connections between network participants. VLANs are an element of flexible network design. It is easier to reconfiguring logical connections centrally than cable connections.

The device supports independent VLAN learning according to IEEE 802.1Q 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 the data packets as normal.
- Flexibility
  You have the option of forming user groups based on the function of the participants apart from their physical location or medium.
- Clarity
  VLANs give networks a clear structure and make maintenance easier.

12.1 Examples of VLANs

The following practical examples provide a quick introduction to the structure of a VLAN.

Note:
When configuring VLANs you use an interface for accessing the device management that will remain unchanged. For this example, you use either interface 1/6 or the serial connection to set up the VLANs.

12.1.1 Application example of a simple port-based VLAN

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.

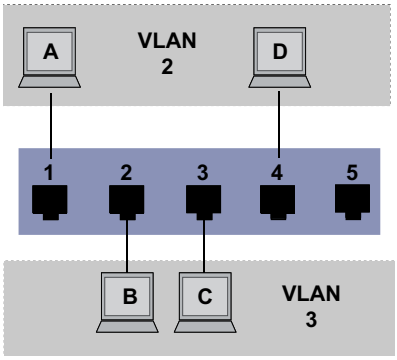


Figure 35: Example of a simple port-based VLAN

When setting up the VLANs, you add communication rules for every port, which you set up 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 15: Ingress table

Terminal	Port	Port VLAN identifier (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
	5	1

Table 16: 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 add VLAN `3` with the name `VLAN3`.

`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 2`	To add VLAN `2`.
`name 2 VLAN2`	To assign the name `2` to the VLAN `VLAN2`.
`vlan add 3`	To add VLAN `3`.
`name 3 VLAN3`	To assign the name `3` to the VLAN `VLAN3`.
`name 1 VLAN1`	To assign the name `1` to the VLAN `VLAN1`.
`exit`	To change to the Privileged EXEC mode.
`show vlan brief`	To display the current VLAN configuration.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 64
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 > Configuration* dialog.
- ☐ To assign the port to a VLAN, specify the desired value in the corresponding column.
  Possible values:
  - `T`
    The port is a member of the VLAN.
    The port transmits tagged data packets.
  - `U`
    The port is a member of the VLAN.
    The port transmits untagged data packets.
  - `F`
    The port is not a member of the VLAN.
  - `-`
    The port is not a member of the VLAN.

  Because end devices usually interpret untagged data packets, you specify the value `U`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ In the *Port-VLAN ID* column, specify 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 ports connected to an end device.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

The value in the *Ingress filtering* column has no affect on how this example functions.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To 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`	To assign the Port VLAN ID 1/1 to port 2.
`exit`	To change to the Configuration mode.
`interface 1/2`	To 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`	To assign the Port VLAN ID 1/2 to port 3.
`exit`	To change to the Configuration mode.
`interface 1/3`	To 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`	To assign the Port VLAN ID 1/3 to port 3.
`exit`	To change to the Configuration mode.
`interface 1/4`	To 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`	To assign the Port VLAN ID 1/4 to port 2.
`exit`	To change to the Configuration mode.
`exit`	To change to the Privileged EXEC mode.
`show vlan id 3`	To display 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
```

12.1.2 Application example of a complex VLAN setup

The second example displays a more complex configuration with 3 VLANs (1 to 3). Along with the Switch from example 1, you use a second Switch (on the right in the example).

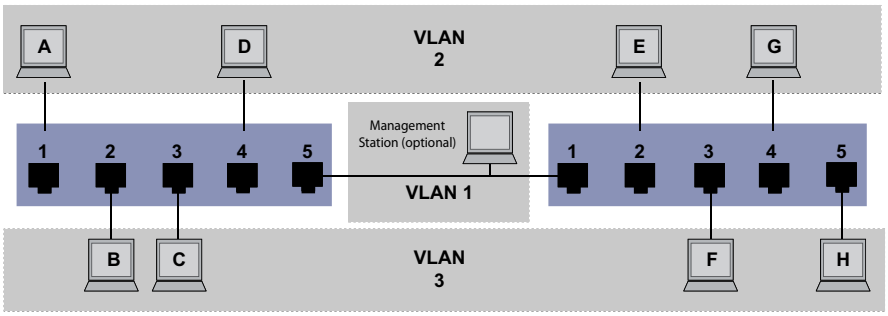


Figure 36: Example of a more complex VLAN configuration

The terminal devices (A to H) of the individual VLANs are spread over 2 transmission devices (Switches). Such VLANs are therefore known as distributed VLANs. An optional network management station is also shown, which has access to the device management of each network component if the associated VLAN is set up correctly.

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 through 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 both 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 17: 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 18: 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 19: 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 20: 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 specified above to adapt the previously set up 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, 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 add VLAN 3 with the name VLAN3.

`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 2`	To add VLAN 2.
`name 2 VLAN2`	To assign the name 2 to the VLAN VLAN2.
`vlan add 3`	To add VLAN 3.
`name 3 VLAN3`	To assign the name 3 to the VLAN VLAN3.
`name 1 VLAN1`	To assign the name 1 to the VLAN VLAN1.
`exit`	To change to the Privileged EXEC mode.
`show vlan brief`	To display the current VLAN configuration.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 64
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 > Configuration* dialog.
- ☐ To assign the port to a VLAN, specify the desired value in the corresponding column.
  Possible values:
  - T
    The port is a member of the VLAN.
    The port transmits tagged data packets.
  - U
    The port is a member of the VLAN.
    The port transmits untagged data packets.
  - F
    The port is not a member of the VLAN.
  - -
    The port is not a member of the VLAN.

  Because end devices usually interpret untagged data packets, you specify the value U.
  You specify the T setting on the uplink port on which the VLANs communicate with each other.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ In the *Port-VLAN ID* column, specify 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 ports connected to an end device.

- ☐ 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To 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`	To assign the Port VLAN ID 1 to port 1/1.
`vlan ingressfilter`	To activate ingress filtering on port 1/1.
`vlan acceptframe vlanonly`	Port 1/1 only forwards packets with a VLAN tag.
`exit`	To change to the Configuration mode.
`interface 1/2`	To 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`	To assign the Port VLAN ID 2 to port 1/2.
`exit`	To change to the Configuration mode.
`interface 1/3`	To 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`	To assign the Port VLAN ID 3 to port 1/3.
`exit`	To change to the Configuration mode.
`interface 1/4`	To 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`	To assign the Port VLAN ID 2 to port 1/4.
`exit`	To change to the Configuration mode.
`interface 1/5`	To 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`	To assign the Port VLAN ID 3 to port 1/5.

```
exit                                                    To change to the Configuration mode.
exit                                                    To change to the Privileged EXEC mode.
show vlan id 3                                          To display 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
```

13 Routing

13.1 Configuration

Because the configuration of a router is very dependent on the conditions in the 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 the network so that you can clearly see the division into subnets and the related distribution of the IP addresses. This step is necessary. Good planning of the subnets with the corresponding netmasks 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 netmasks to the router interfaces.

Note:
Match 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 subnet 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 using the IP address of the router interface.
Activate the routing globally before you assign an IP address from the subnet 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 using the IP address of the router interface. The device management VLAN is the VLAN by means of which you access the device management of every device.

Note:
Depending on your configuration steps, it can be necessary to change the IP parameters of your configuration computer to enable access to the Layer 3 devices.

- Selecting a routing procedure
  On the basis of the network plan and the communication requirements of the connected devices, you select the optimal routing procedure (static routes, OSPF) for your situation. In doing so, consider which routing procedures the routers can use along a route.
- Configuring a routing procedure
  Set up 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 21: 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 through physical media

What does the data exchange on the Layer 3 mean in comparison with the data exchange on the Layer 2?

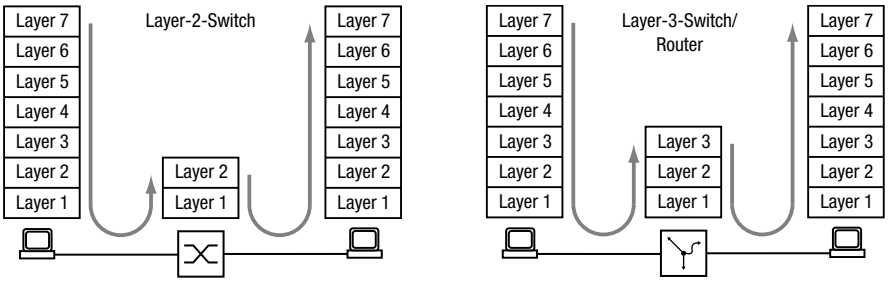


Figure 37: Data Transport by a Switch and a Router in the OSI Reference Model's Layers

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 packets are 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 stream 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, the network administrator can thus structure the network, breaking it down into subnets (see on page 201 “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.

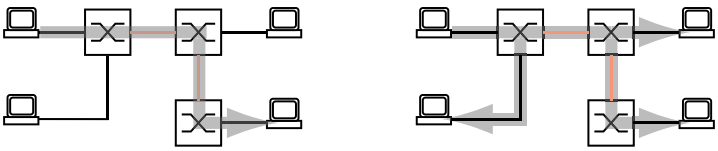


Figure 38: MAC Data Transmission: Unicast Data Packet (left) and Broadcast Data Packet (right)

This illustration clearly shows that broadcast data packets can cause a significant load on larger networks. You also make the 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

Using the Address Resolution Protocol (ARP), the device learns the MAC address that belongs to an IP address. What is the benefit of this?

Let's suppose that you want to set up the device using the Graphical User Interface. You enter the IP address of the device in the address line of your web browser. But which MAC address will your PC now use to display the information in the device in your web browser?

If the IP address of the device is in the same subnet 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.

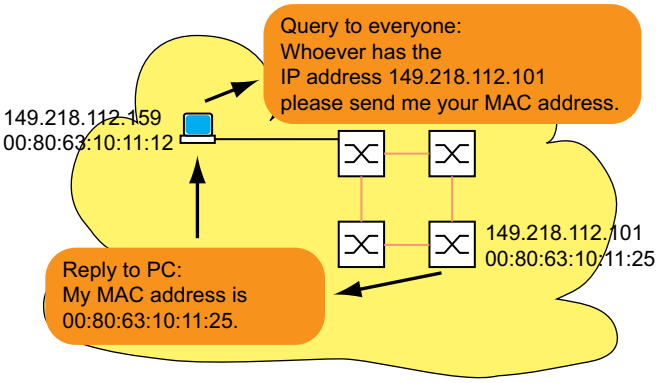


Figure 39: ARP request and reply

When the IP address of the device is in a different subnet, 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.

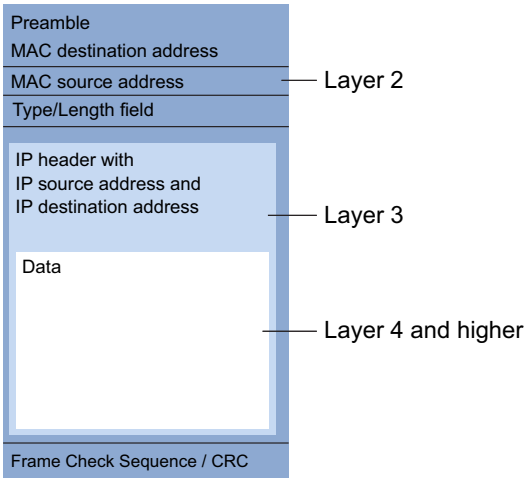


Figure 40: Structure of a data packet from the ISO/OSI reference model perspective

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 netmask 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.

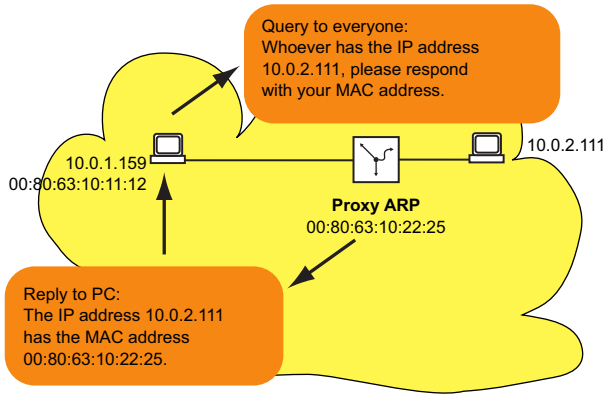


Figure 41: Proxy ARP function

The *Proxy ARP* function is available on the router interfaces on which you enable the proxy ARP.

Note:
The *1:1 NAT* function also lets you integrate the devices into a larger L3 network.

13.2.2 CIDR

The original class allocation of the IP addresses only planned for three address classes to be used by the users.

Since 1992, five classes of IP address have been defined in the RFC 1340.

Table 22: IP address classes

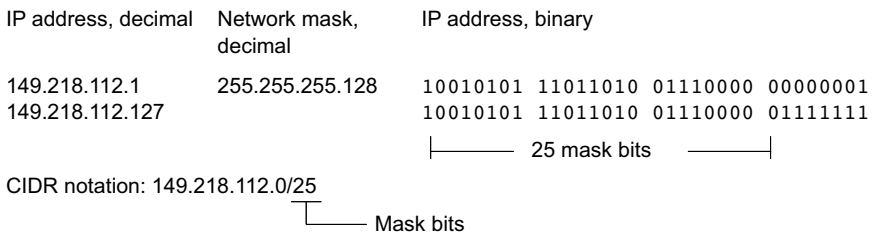
Class	Network part	Host part	Address range
A	1 byte	3 bytes	1.0.0.0 … 126.255.255.255
B	2 bytes	2 bytes	128.0.0.0 … 191.255.255.255
C	3 bytes	1 byte	192.0.0.0 … 223.255.255.255
D			224.0.0.0 … 239.255.255.255
E			240.0.0.0 … 255.255.255.255

Class C with a maximum of 254 (2^8-2) addresses was too small, and class B with a maximum of 65534 $(2^{16}-2)$ 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 issues. The CIDR overcomes these class boundaries and supports classless address ranges.

With CIDR, you specify the number of bits that designate the netmask. You represent the IP address range in binary form and count the 1 bits that comprise the netmask. The netmask length 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 lets you subdivide class B address ranges to a very fine degree.

Using mask bits simplifies the routing table. The router determines in that direction in which most of the mask bits match (longest prefix match).

13.2.3 Multinetting

Multinetting lets you connect a number of subnets to one router port. When you want to connect existing subnets to a router within a physical medium, multinetting provides a solution. In this case you can use multinetting to assign a number of IP addresses for the different subnets to the routing port to which you are connecting the physical medium.

For a long-term solution, other network design strategies provide more advantages regarding resolving issues and bandwidth management.

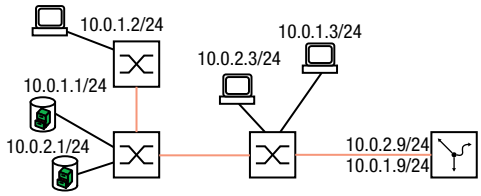


Figure 42: Example of multinetting

13.3 Static Routing

Static routes are user-defined routes which the router uses to transmit data from one subnet to another.

You specify to which router (next hop) the local router forwards data for a particular subnet. Static routes are kept in a table which is permanently stored in the router.

Compared to dynamic routing, the advantage of this transparent route selection is offset by the increased workload involved in configuring the static routes. Static routing is therefore suited to very small networks or to selected areas of larger networks. Static routing makes the routes transparent for the administrator and can be easily set up 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 set up 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 set up the router interfaces.

The device lets you define port-based and VLAN-based router interfaces.

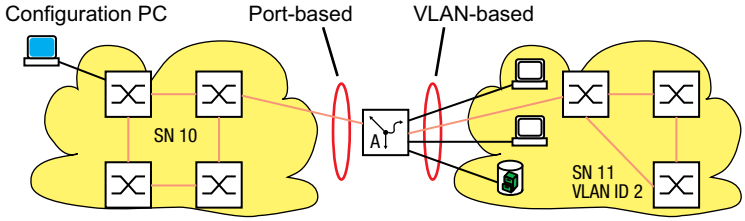


Figure 43: Static routes: Example of connecting two production cells

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 43 on page 203.

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.

In the following section you find an example of the simplest case of a routing application with port-based router interfaces.

Configuration of the router interfaces

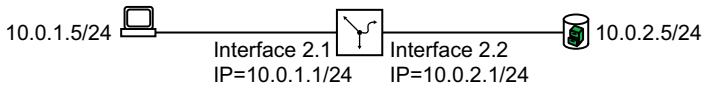


Figure 44: Simplest case of a route

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 2/1`	To change to the Interface Configuration mode of interface `2/1`.
`ip address primary 10.0.1.1 255.255.255.0`	To assign the interface its primary IP parameters.
`ip routing`	To activate the *Routing* function on this interface.
`exit`	To change to the Configuration mode.
`interface 2/2`	To change to the Interface Configuration mode of interface `2/2`.
`ip address primary 10.0.2.1 255.255.255.0`	To assign the interface its IP parameters.
`ip routing`	To activate the *Routing* function on this interface.
`exit`	To change to the Configuration mode.
`ip routing`	To enable the *Routing* function globally.
`exit`	To change to the Privileged EXEC mode.
`show ip interface 2/1`	To 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..........................  enabled
Admin State...............................  enabled
Link State................................  up
```

`show ip route all` — To check 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.

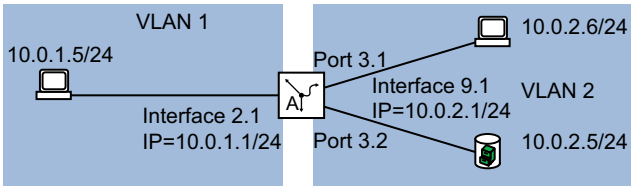


Figure 45: VLAN-based router interface

Set up 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`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 2`	To add a VLAN by entering the VLAN ID. The VLAN ID needs to be in the range `1..4042`.
`name 2 VLAN2`	To assign the name `VLAN2` to the VLAN.
`routing add 2`	To add a virtual router interface. To activate the *Routing* function on this interface.
`exit`	To change to the Privileged EXEC mode.
`show ip interface`	To check the entry for the virtual router interface.

`Interface IP Address IP Mask`
`--------- --------------- ---------------`
`vlan/2 0.0.0.0 0.0.0.0`	

`configure`	To change to the Configuration mode.
`interface vlan/2`	To change to the Interface Configuration mode of interface `vlan/2`.
`ip address primary 10.0.2.1 255.255.255.0`	To assign the IP parameters to the virtual router interface.
`ip routing`	To activate the *Routing* function on this interface.
`exit`	To change to the Configuration mode.
`interface 3/1`	To change to the Interface Configuration mode of interface `3/1`.
`vlan participation exclude 1`	To remove port `3/1` from VLAN `1`. In the default setting, every port is assigned to VLAN `1`.
`vlan participation include 2`	To declare port `3/1` a member of VLAN `2`.
`vlan pvid 2`	To specify port VLAN ID `2`. Therefore, the device assigns data packets that the port receives without a VLAN tag to VLAN `2`.
`exit`	To change to the Configuration mode.

```
interface 3/2
```
To change to the Interface Configuration mode of interface 3/2.

```
vlan participation exclude 1
```
To remove port 3/2 from VLAN 1. In the default setting, every port is assigned to VLAN 1.

```
vlan participation include 2
```
To declare port 3/2 a member of VLAN 2.

```
vlan pvid 2
```
To specify port VLAN ID 2. Therefore, the device assigns data packets that the port receives without a VLAN tag to VLAN 2.

```
exit
```
To change to the Configuration mode.

```
ip routing
```
To enable the *Routing* function globally.

```
exit
```
To change to the Privileged EXEC mode.

```
show vlan id 2
```
To 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
```
To 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 *ARP* 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 settings, 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`.
- Apply the settings temporarily. To do this, click the ✓ button.

You delete a router interface selected 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 through the router B (next hop). It can obtain this information using a dynamic routing protocol or a static routing entry. With this information, router A can transmit data from subnet 10.0.1.0/24 through 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.

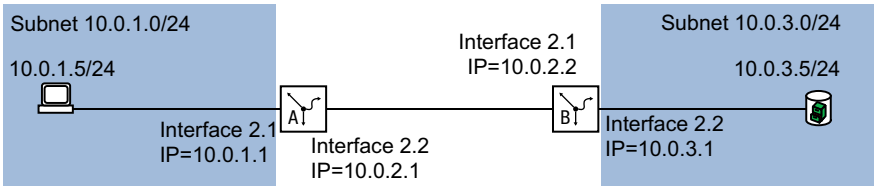


Figure 46: Static Routing

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 44 on page 204.

To do this, perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ip route add 10.0.3.0 255.255.255.0 10.0.2.2`	To add the static routing entry.
`ip routing`	To enable the *Routing* function globally.

```
exit
```
To change to the Privileged EXEC mode.

```
show ip route all
```
To check 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 44 on page 204.

☐ Set up 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.

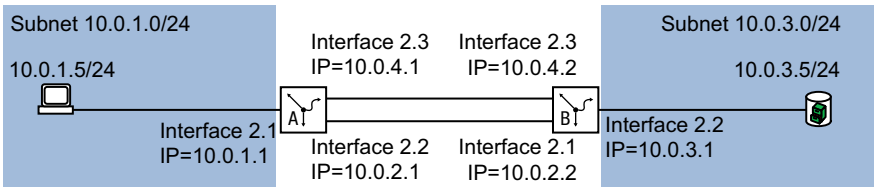


Figure 47: Redundant static route

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
```
To change to the Privileged EXEC mode.

```
configure
```
To change to the Configuration mode.

```
interface 2/3
```
To select the port at which you want to connect the redundant route.

```
ip address primary 10.0.4.1 255.255.255.0
```
To assign the IP parameters to the port.

```
ip routing
```
To activate the *Routing* function on this interface.

```
exit
```
To change to the Configuration mode.

```
ip route add 10.0.3.0 255.255.255.0
10.0.4.2 preference 2
```
To add the static routing entry for the redundant route. The value `2` at the end of the command indicates the preference value.
When both routes are available, the router uses the route through subnet `10.0.2.0/24`, because this route has the higher preference (see on page 207 “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
```
To set the default preference for static routes. (default setting: 1)

```
show ip route all
```
To check 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]
```

Set up router B in the same way, using the values for router B.

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
```
To change to the Privileged EXEC mode.

```
configure
```
To change to the Configuration mode.

```
ip route modify 10.0.3.0 255.255.255.0
10.0.2.2 preference 2
```
To assign a Preference of 2 to the existing static routing entry (see on page 207 “Configuration of a simple static route”).
When both routes are available, the router uses both routes for the data transmission.

```
show ip route all
```
To check 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]
```

13.4 NAT – Network Address Translation

The Network Address Translation (NAT) protocol describes a procedure for automatically and transparently changing IP address information in data packets while still transmitting the data packets to their precise destination.

When you do not want IP addresses of an internal network to be visible from outside, use NAT. The reasons for this can include, for example:
- Keeping the structure of the internal network hidden from the outside world.
- Keeping private IP addresses hidden.
- Using IP addresses multiple times – by forming identical production cells, for example.

Depending on your reason for using NAT, it offers you various procedures for using the IP address information. In the following sections, you will find additional information on this process.

13.4.1 Applying the NAT Rules

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

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

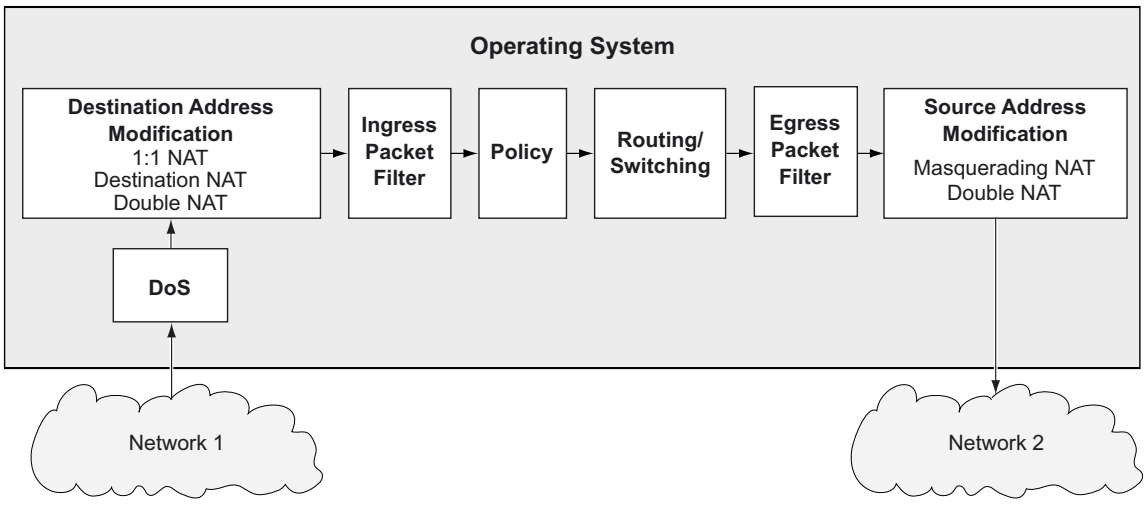


Figure 48: Processing sequence of the data packets in the device

13.4.2 1:1 NAT

The *1:1 NAT* function lets you establish communication links within a local network to devices that are actually located in other networks. The NAT router virtually “shifts” the devices into the public network. For this, the NAT router replaces the virtual with the actual IP address in the data packet while sending it. A typical application is the connecting of several identically structured production cells with the same IP address to a server farm.

The prerequisite for the *1:1 NAT* process is that the NAT router itself responds to ARP requests. To do this, activate the *Proxy ARP* function for the relevant interface in the *Routing > Interfaces >* Configuration dialog or in the *Routing > L3-Redundancy > VRRP > Configuration* dialog.

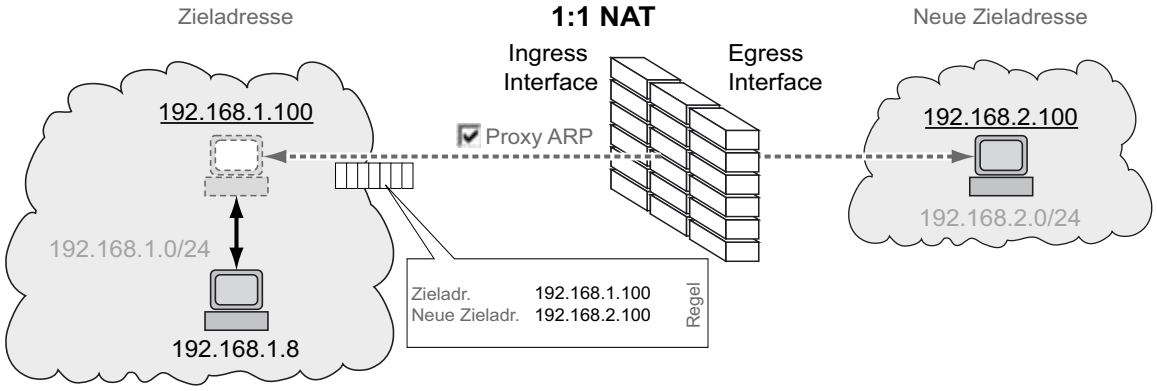


Figure 49: How the 1:1 NAT function works

Note:
With the *1:1 NAT* function the device responds to ARP requests from the external network to addresses which it maps from the internal network. This is also the case where no device with the IP address exists in the internal network. Therefore, only assign IP addresses to devices in the external network that are outside the range that the *1:1 NAT* function maps from the internal network to the external network.

Application example for the 1:1 NAT function

You have multiple identical production cells and want to connect them with the host computer. As even the IP addresses used in the production cells are identical, you convert the IP addresses using the *1:1 NAT* function.

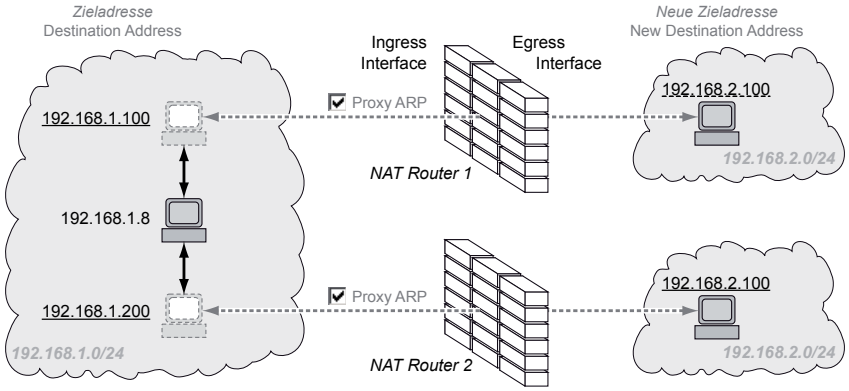


Figure 50: Connect identical production cells with the host computer (application example)

Prerequisites for further configuration:

- You need two NAT routers.
- The *Routing* function is enabled in every device.
- Two router interfaces are set up in every device. One router interface is connected to the company network and one to the network of the production cell.
- The IP address and gateway are set in the devices of the production cell. The devices use the IP address of the egress interface of the NAT router as the gateway.

Perform the following steps:

☐ Activate the *Proxy ARP* function on the ingress interfaces.

- ☐ Open the *Routing > Interfaces > Configuration* dialog or the *Routing > L3-Redundancy > VRRP > Configuration* dialog.
- ☐ On the router interface that is connected to the company network, mark the checkbox in the *Proxy ARP* field.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

☐ Add a rule.

- ☐ Open the *Routing > NAT > 1:1 NAT > Rule* dialog.
- ☐ Add a table row. To do this, click the button.
  The dialog displays the *Create* window.
- ☐ In the *Destination address* field, specify the virtual IP address of the device in the production cell. In the example this is `192.168.1.100` in NAT router 1 and `192.168.1.200` in NAT router 2.
- ☐ In the *New destination address* field, specify the IP address of the device in the production cell. In the example this is `192.168.2.100` in NAT router 1 and NAT router 2.
- ☐ Click the *Ok* button.
- ☐ In the *Rule name* column, specify the name of the NAT rule.
- ☐ In the *Priority* column, specify any value between `1` and `6500`.
- ☐ In the *Ingress interface* column, select the router interface that is connected to the company network.
- ☐ In the *Egress interface* column, select the router interface connected with the production cell.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

☐ Activate the rule.

- ☐ Mark the checkbox in the *Active* column.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

☐ Apply the rule to the data stream.

- ☐ Open the *Routing > NAT > NAT Global* dialog.
- ☐ Click the button.

When changes to the rules affect existing entries in the state table of the firewall, it helps to clear the state table. See the *Clear firewall table* button in the *Basic Settings > Restart* dialog. It is possible, that the device interrupts open communication connections.

13.4.3 Destination NAT

The *Destination NAT* function lets you divert the data stream of outgoing communication links to or through a server in a local network.

A special form of the *Destination NAT* function is *port forwarding*. You use *port forwarding* to hide the structure of a network from the outside while still allowing communication links from the outside into the network. A typical application is remote control of a PC in a production cell. The maintenance station establishes the communication link to the NAT router, and the *Destination NAT* function takes care of the routing to the production cell.

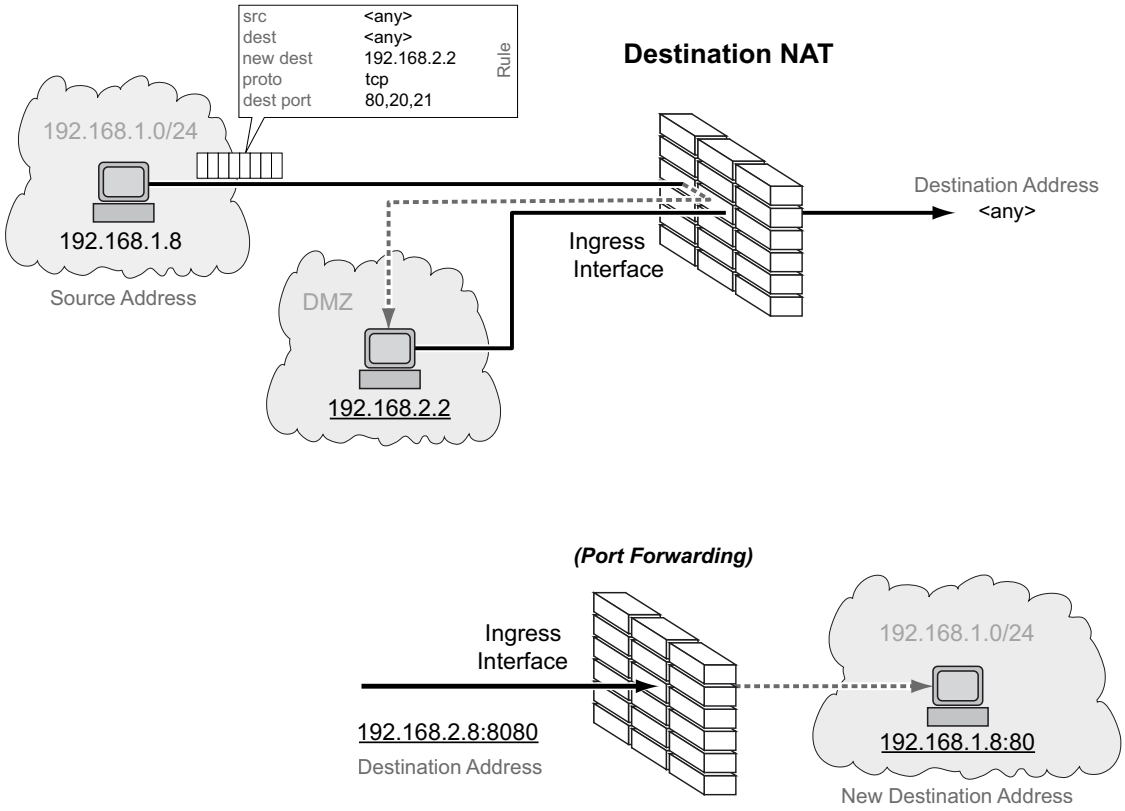


Figure 51: How the Destination NAT function works

Application example for port forwarding

You have a production cell. The network of the production cell is not visible on the company network. The NAT router establishes the connection between the production cell and the company network. To allow an administrator from the company network to manage a server in the production cell, use the *port forwarding* function.

Parameter	Administrator PC	NAT router	Server
IP address Port 1		192.168.1.1	
IP address Port 4		192.168.2.8	
IP address	192.168.2.55		192.168.1.8
Gateway	192.168.2.8		192.168.1.1

Prerequisites for further configuration:

- The *Routing* function is enabled in the device.
- In the device, a router interface is set up and connected to the company network.
- In the devices in the production cell, the IP address and gateway are defined. The devices use the IP address of port 1 of the NAT router as the gateway.

Perform the following steps:

☐ Add a rule.

- ☐ Open the *Routing > NAT > Destination NAT > Rule* dialog.
- ☐ Add a table row. To do this, click the button.
  The dialog displays the *Create* window.
- ☐ In the *New destination address* field, specify the IP address of the server in the production cell. In the example this is `192.168.1.8`. The NAT router forwards the connection to this address.
- ☐ Click the *Ok* button.
- ☐ In the *Rule name* field, specify the name of the NAT rule.
- ☐ In the *Destination address* field, specify the IP address of the router interface in the company network. In the example this is `192.168.2.8`. The PC of the administrator establishes the connection to this address.
- ☐ In the *Destination port* field, specify the port number. In the example this is `8080`. The PC of the administrator establishes the connection to this port.
- ☐ In the *New destination port* field, specify the port number. In the example this is `80`. The NAT router forwards the connection to this port.
- ☐ To forward connections only from the PC of the administrator to the server in the production cell, change the value in the *Source address* field to the IP address of the PC. In the example this is `192.168.2.55`. Otherwise, leave the value `any`.
- ☐ To forward only TCP data packets to the server in the production cell, change the value in the *Protocol* field to `tcp`. Otherwise, leave the value `any`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

☐ Activate the rule.

- ☐ Mark the checkbox in the *Active* column to enable the added rule.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

☐ Assign rule to a router interface.

- ☐ Open the *Routing > NAT > Destination NAT > Mapping* dialog.
- ☐ Click the *Assign* button.
- ☐ In the *Port* field, select the router interface that is connected to the company network.
- ☐ Select the added rule in the *Rule index* field.
- ☐ Click the *Ok* button.

☐ Activate assignment of the rule to the router interface.

- ☐ Mark the checkbox in the *Active* column to activate assignment of the rule to the router interface.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

☐ Apply the rule to the data stream.

- ☐ Open the *Routing > NAT > NAT Global* dialog.
- ☐ Click the ⬆ button.

When changes to the rules affect existing entries in the state table of the firewall, it helps to clear the state table. See the *Clear firewall table* button in the *Basic Settings > Restart* dialog. It is possible, that the device interrupts open communication connections.

13.4.4 Masquerading NAT

The *Masquerading NAT* function hides any number of devices behind the IP address of the NAT router and thus hides the structure of a network from other networks. For this, the NAT router replaces the sender address in the data packet with its own IP address. In addition, the NAT router replaces the source port in the data packet with its own value to send the response data packets back to the original sender at a later point.

Adding the port information also gave the IP Masquerading the name “Network Address Port Translation” (NAPT).

The devices establish communication links to the outside from the hidden network by converting the IP address. However, it is not possible to establish a connection in the other direction, because the devices outside only know the external IP address of the NAT router.

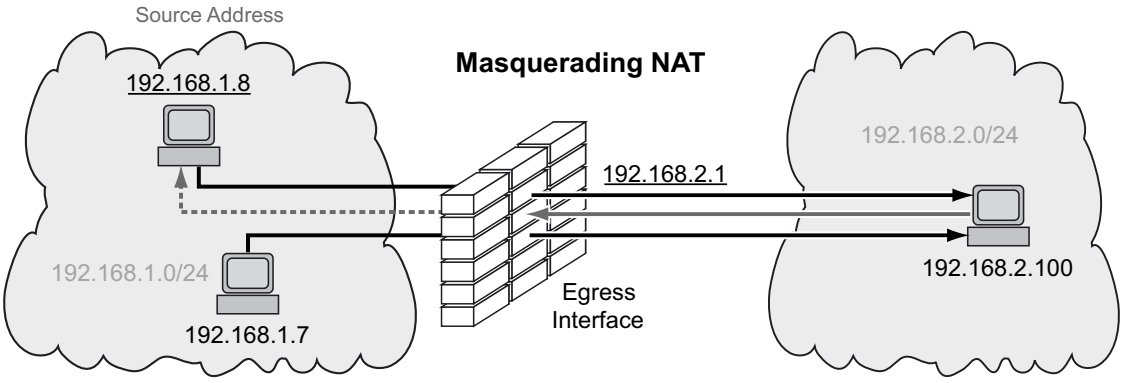


Figure 52: How the Masquerading NAT function works

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

13.4.5 Double NAT

The *Double NAT* function lets you establish communication links between end devices located in different IP networks, which have no way to specify a *default gateway* or *default route*. The NAT router virtually “shifts” the devices into the other network. For this, the NAT router replaces the source address and the destination address in the data packet during sending. A typical application is the linking of controllers located in different networks.

The *Double NAT* function requires that the NAT router itself responds to ARP requests from the respective network. To make this happen, activate the *Proxy ARP* function on the ingress interface and on the egress interface.

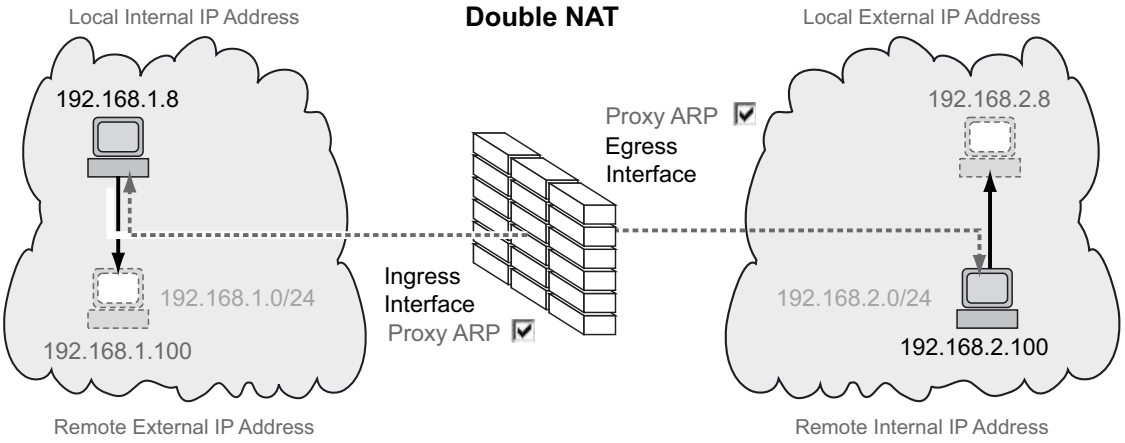


Figure 53: How the Double NAT function works

The figure shows which IP addresses the devices use to communicate with each other and how the NAT router changes the IP addresses:

- The device on the left sends a data packet to the device on the right.
  - The data packet contains the source address `192.168.1.8` and the destination address `192.168.1.100`.
  - The NAT router replaces both addresses.
  - The data packet that the device on the right receives contains the source address `192.168.2.8` and the destination address `192.168.2.100`.
- In the reverse direction, the device on the right sends a data packet to the device on the left.
  - The data packet contains the source address `192.168.2.100` and the destination address `192.168.2.8`.
  - The NAT router replaces both addresses.
  - The data packet that the device on the left receives contains the source address `192.168.1.100` and the destination address `192.168.1.8`.

The NAT router changes the source and destination addresses in the data packets. Both devices communicate with each other in the same network, even though they are actually in different networks.

Application example for the Double NAT function

You want to connect the device on the left (a workstation in the company network, for example) with the device to the right (a robot controller in the production cell, for example). The robot controller only communicates with devices on the same logical network. When communicating between the networks, the NAT router translates the IP addresses.

Parameter	Device on the left	Device on the right
Local internal IP address	192.168.1.8	
Local external IP address	192.168.2.8 (virtual)	
Remote internal IP address		192.168.2.100
Remote external IP address		192.168.1.100 (virtual)

Prerequisites for further configuration:

- The *Routing* function is enabled in the device.
- Two router interfaces are set up in the device. One router interface is connected to the company network and one to the network of the production cell.
- The IP address is set in the device on the left and in the device on the right.

Perform the following steps:

☐ Activate the *Proxy ARP* function on the router interfaces.

- ☐ Open the *Routing > Interfaces > Configuration* dialog.
- ☐ On the router interfaces that are connected to the company network and to the production cell, mark the checkbox in the *Proxy ARP* field.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

☐ Add a rule.

- ☐ Open the *Routing > NAT > Double NAT > Rule* dialog.
- ☐ Add a table row. To do this, click the button.
  The dialog displays the *Create* window.
- ☐ In the *Local internal IP address* field, specify the IP address of the device on the left in the company network. In the example this is `192.168.1.8`.
- ☐ In the *Local external IP address* field, specify the virtual IP address of the device on the left in the production cell. In the example this is `192.168.2.8`.
- ☐ In the *Remote internal IP address* field, specify the IP address of the device on the right in the production cell. In the example this is `192.168.2.100`.
- ☐ In the *Remote external IP address* field, specify the virtual IP address of the device on the right in the company network. In the example this is `192.168.1.100`.
- ☐ Click the *Ok* button.
- ☐ In the *Rule name* field, specify the name of the NAT rule.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

☐ Activate the rule.

- ☐ Mark the checkbox in the *Active* column to enable the added rule.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

☐ Assign the rule to the ingress interface connected to the company network.

- ☐ Open the *Routing > NAT > Double NAT > Mapping* dialog.
- ☐ Click the *Assign* button.
- ☐ In the *Port* field, select the router interface that is connected to the company network.
- ☐ Select the value `ingress` in the *Direction* field.
- ☐ Select the added rule in the *Rule index* field.
- ☐ Click the *Ok* button.

☐ Assign the rule to the egress interface connected to the production cell.

- ☐ Open the *Routing > NAT > Double NAT > Mapping* dialog.
- ☐ Click the *Assign* button.
- ☐ In the *Port* field, select the router interface connected with the production cell.
- ☐ Select the value *egress* in the *Direction* field.
- ☐ Select the added rule in the *Rule index* field.
- ☐ Click the *Ok* button.

☐ Activate assignment of the rule to the router interface.

- ☐ Mark the checkbox in the *Active* column to activate assignment of the rule to the router interface.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

☐ Apply the rule to the data stream.

- ☐ Open the *Routing > NAT > NAT Global* dialog.
- ☐ Click the ⤒ button.

When changes to the rules affect existing entries in the state table of the firewall, it helps to clear the state table. See the *Clear firewall table* button in the *Basic Settings > Restart* dialog. It is possible, that the device interrupts open communication connections.

13.5 VRRP

End devices usually let you specify one *default gateway* for forwarding data packets in external subnets. Here the term “Gateway” applies to a router with which end devices communicate with other subnets.

If this router fails, then the end device cannot send any more data to the external subnets.

In this case, the Virtual Router Redundancy Protocol (VRRP) provides assistance.

VRRP is a type of “gateway redundancy”. VRRP describes a process that groups multiple routers into one virtual router. End devices constantly address the virtual router, and VRRP helps ensure that a physical router belonging to the virtual router transmits the data.

When a physical router fails, VRRP helps ensure that another physical router continues to route the data as part of the virtual router.

When a physical router fails, VRRP has a typical failover time of 3 to 4 seconds.

Note:
The device supports only VRRP packets without authentication information. To operate the device 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*.

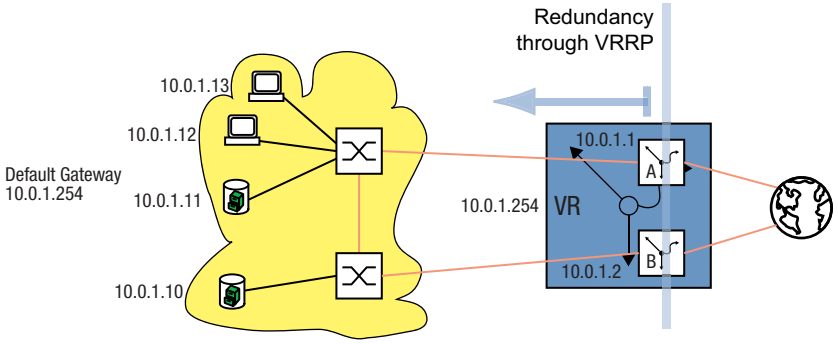


Figure 54: Illustration of the virtual router

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.

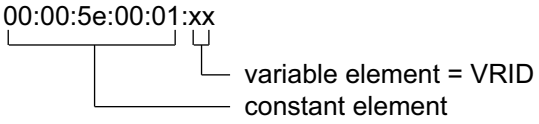


Figure 55: Virtual MAC address

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.

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 23: 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 55 on page 223.
- 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 s.
- 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`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ip routing`	To enable the *Routing* function globally.
`ip vrrp operation`	To enable VRRP globally.
`interface 1/3`	To change to the Interface Configuration mode of interface `1/3`.
`ip address primary 10.0.1.1 255.255.255.0`	To specify the primary IP address and the netmask of the router interface.
`ip routing`	To enable the *Routing* function on this interface.
`ip vrrp add 1`	To add the VRID for the first virtual router on this port.
`ip vrrp virtual-address add 1 10.0.1.100`	To assign virtual router `1` its IP address.
`ip vrrp 1 priority 200`	To assign 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 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 specify different *default gateways* on the connected end devices and thus steer the data flow.

When both routers are active, the data flows through the router on which the IP address of the *default gateway* has the higher VRRP priority. When a router fails, the data flows through the remaining routers.

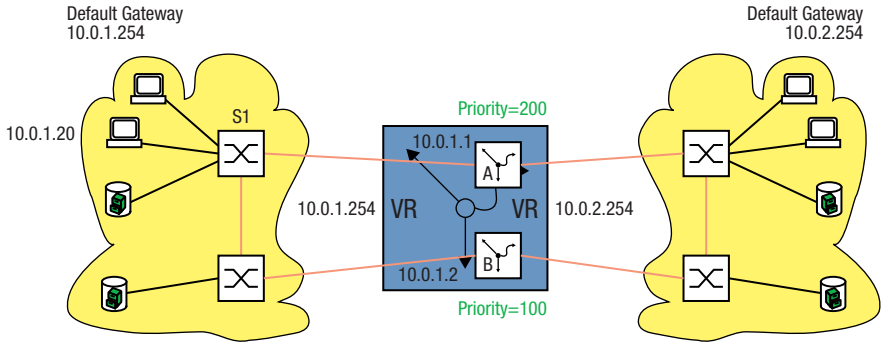


Figure 56: Virtual router with load sharing

Set up 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*.

13.5.3 VRRP with Multinetting

The router lets you combine VRRP with Multinetting.

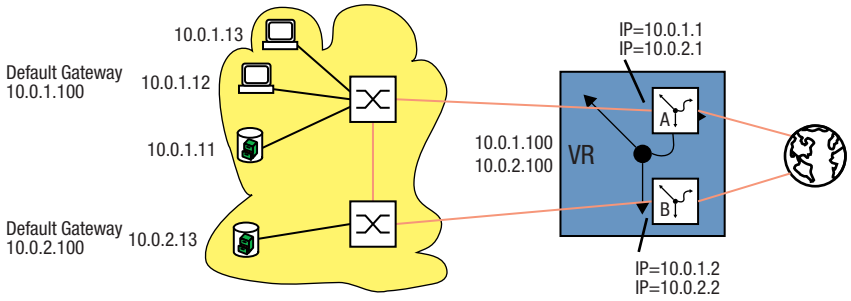


Figure 57: Virtual router with multinetting

Set up VRRP with multinetting on the basis of an existing VRRP configuration. See figure 54 on page 222.

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`	To select the port at which you want to set up multinetting.
`ip address secondary 10.0.2.1 255.255.255.0`	To assign the second IP address to the port.
`ip vrrp virtual-address add 1 10.0.2.100`	To assign a second IP address to the virtual router with the VRID 1.

- ☐ Perform the same configuration on the backup router.

13.6 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 subnet remain within the subnet, 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 to update 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 24: 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 generates its routing table.

13.6.1 OSPF-Topology

OSPF is hierarchically structured to limit the scope of the OSPF information to be exchanged in large networks. You divide up the network using what are known as areas.

Autonomous System

An Autonomous System (AS) is a number of routers that are managed by a single administration and use the same Interior Gateway Protocol (IGP). Exterior Gateway Protocols (EGP), on the other hand, are used to connect a number of autonomous systems. OSPF is an Interior Gateway Protocol.

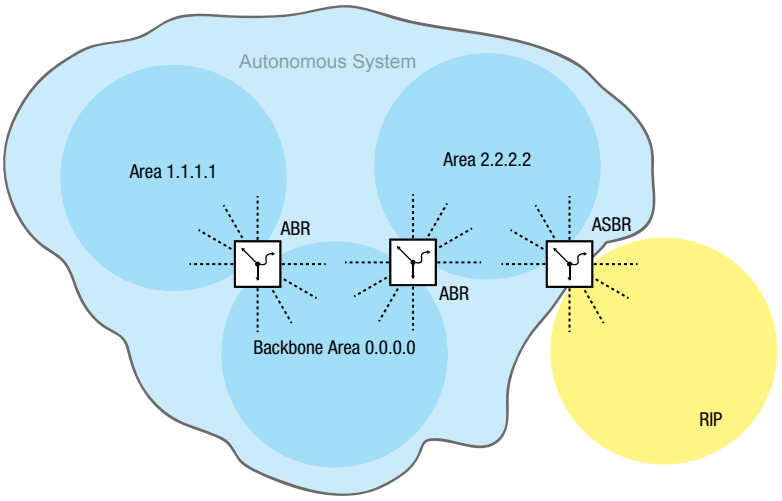


Figure 58: Autonomous System

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 set up 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`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ip ospf router-id 192.168.1.2`	To assign the router ID, for example `192.168.1.2`.
`ip ospf operation`	To enable the *OSPF* function 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 (see figure 59 on page 229). 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.

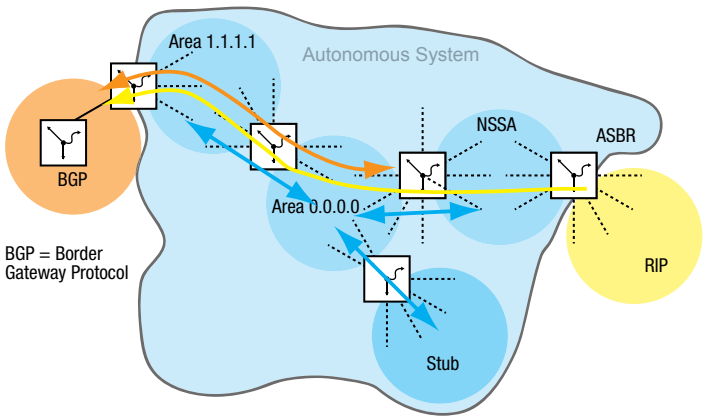


Figure 59: LSA distribution into the area types

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ip ospf area 2.2.2.2 nssa add import-nssa`	To specify area `2.2.2.2` as NSSA.
`ip ospf area 3.3.3.3 stub add 0`	To specify area `3.3.3.3` as stub area.
`ip ospf area 3.3.3.3 stub modify 0 default-cost 10`	To 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. A VL even lets you connect an area that is connected with the backbone area through another area.

Configuration for expanding the backbone area:

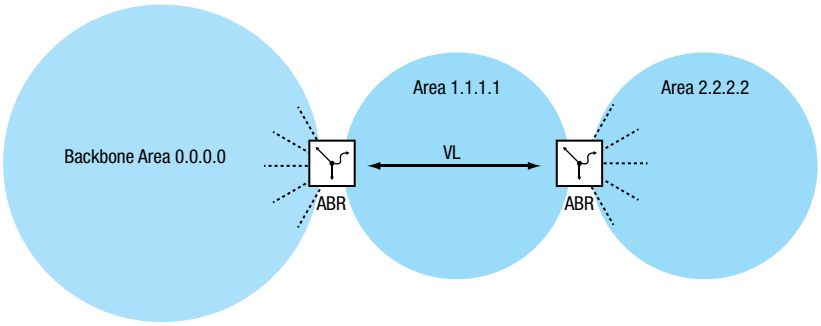


Figure 60: Linking a remote area to the backbone area using a virtual link (VL)

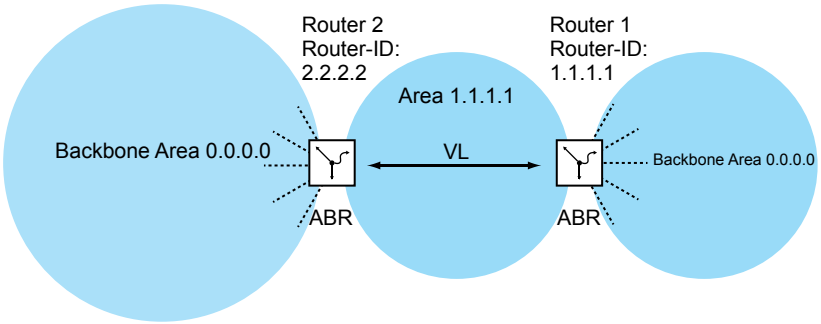


Figure 61: Expanding the backbone area using a virtual link (VL)

Set up router 1. To do this, perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ip ospf area 1.1.1.1 virtual-link add 2.2.2.2`	To enter the neighboring router ID for a virtual link in area `1.1.1.1`.

Set up router 2. To do this, perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ip ospf area 1.1.1.1 virtual-link add 1.1.1.1`	To 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 subnets on which OSPF is not switched on)
  - *`static`* (static routes)

Link State Advertisement

As a basis for building up a database using the link states, OSPF uses Link State Advertisements (LSA).

An LSA contains the following information:
- the router
- the connected subnets
- the routes that can be reached
- the netmasks
- 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 233 “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 you can also specify it manually.

13.6.2 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 generation, maintenance and distribution of what is called the link state database.

The database describes the following parameters:
- every router within a routing domain (area)
- the active interfaces and routes
- how the routers are linked to each other
- the costs of the 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

13.6.3 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 specify this router ID manually during booting of the OSPF router “Router ID” on page 228.

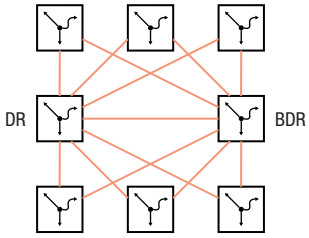


Figure 62: LSA distribution with designated router and backup designated router

To exchange information, OSPF uses reserved multicast addresses.

Table 25: 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 set up for each router interface. When reconfiguring the timers, verify that they are uniform within an area.

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface 1/1.
`ip ospf hello-interval 20`	To specify the Hello interval as 20 seconds.
`ip ospf dead-interval 60`	To specify the Dead interval as 60 seconds.
`exit`	To change to the Configuration mode.

```
exit                                    To change to the Privileged EXEC mode.
show ip ospf neighbor 1/1               To display 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

13.6.4 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                                  To change to the Privileged EXEC mode.
show ip ospf database internal          To display 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` — To display the external Adjacencies of the router.

```
Area ID         Adv Router       Age    Sequence   Checksum
-----------     ---------------  -----  --------   ------
1.1.1.1         192.169.1.1      178    80000002   0xcalc
```

13.6.5 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 lets you differentiate between Fast Ethernet and Gigabit Ethernet. To do this, perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`ip ospf cost 2`	To assign the value `1/1` to port `2` for the OSPF costs.

13.6.6 Configuring OSPF

In the delivery state, the default values are selected so that you can set up simple *OSPF* functions with a few steps. After you specify the router interface and enable the *OSPF* function, *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 support OSPF, so you do not have to activate the *OSPF* function on the corresponding router interface. By activating the *Redistribution* function, you can inject the routes to the end devices into OSPF.

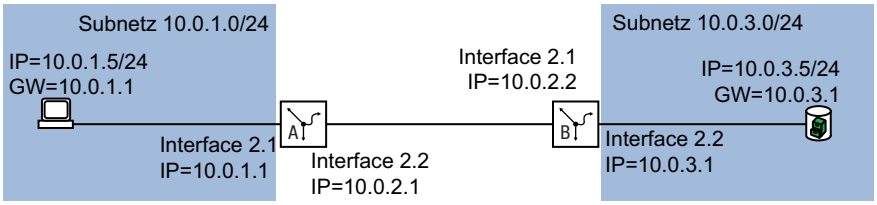


Figure 63: Application example of an OSPF setup

Set up the *OSPF* functions. To do this, perform the following steps:

- ☐ Set up router interfaces – assign IP address and netmask.
- ☐ Activate the *OSPF* function on the port.
- ☐ Enable the *OSPF* function globally.
- ☐ Enable routing globally (if this has not already been done).

Configuration for Router B

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 2/2`	To change to the Interface Configuration mode of interface `2/2`.
`ip address primary 10.0.3.1 255.255.255.0`	To assign the IP parameters to the port.
`ip routing`	To activate routing on this port.
`ip ospf operation`	To activate the *OSPF* function on this port.
`exit`	To change to the Configuration mode.
`interface 2/1`	To change to the Interface Configuration mode of interface `2/1`.
`ip address primary 10.0.2.2 255.255.255.0`	To assign the IP parameters to the port.
`ip routing`	To activate routing on this port.
`ip ospf operation`	To activate the *OSPF* function on this port.
`exit`	To change to the Configuration mode.
`ip ospf router-id 10.0.2.2`	To assign router ID `10.0.2.2` to router B.
`ip ospf operation`	To enable the *OSPF* function globally.
`ip ospf re-distribute connected [subnets]`	To specify the OSPF parameters for the following actions: • send the routes of the locally connected interfaces • include subnets without OSPF in *OSPF* (CIDR).
`exit`	To change to the Configuration mode.
`exit`	To change to the Privileged EXEC mode.
`show ip ospf global`	To display the settings for the *Global* 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`	To display the settings for the *Interfaces* 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`	To change to the Configuration mode.
`ip routing`	To enable the *Routing* function globally.
`exit`	To change to the Privileged EXEC mode.

☐ Also perform the corresponding configuration on the other OSPF routers.

`show ip ospf neighbor brief` To 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` To 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]
```

13.6.7 Limiting the distribution of the routes using an ACL

With Redistributing enabled, the *OSPF* function distributes every static route set up 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.

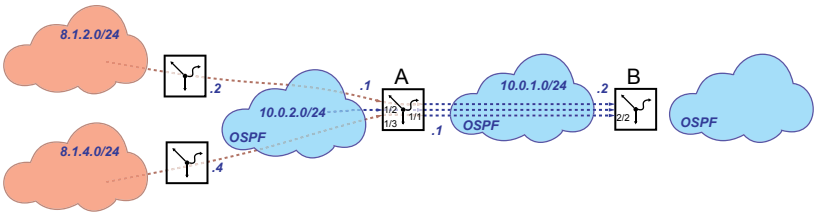
Using IP rules, you specify which routes the device distributes to other devices in OSPF:
- To distribute a few routes in OSPF, you use the explicit `permit` rules. Using the `permit` rules, you specify exactly which routes the device distributes in OSPF.
- To distribute many routes in OSPF, you use 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 set-up on router A.



Router A

☐ Enable routing globally.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ip routing`	To enable routing globally.

☐ Setting up the first router interface `10.0.1.1/24`.
Activate routing.
Activate the *OSPF* function on the router interface.

`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`ip address primary 10.0.1.1 255.255.255.0`	To specify the IP address and subnet mask.
`ip routing`	To activate routing.
`ip ospf operation`	To activate the *OSPF* function on the router interface.
`exit`	To change to the Configuration mode.

☐ Setting up the second router interface `10.0.2.1/24`.
Activate routing.
Activate the *OSPF* function on the router interface.

`interface 1/2`	To change to the Interface Configuration mode of interface `1/2`.
`ip address primary 10.0.2.1 255.255.255.0`	To specify the IP address and subnet mask.
`ip routing`	To activate routing.
`ip ospf operation`	To activate the *OSPF* function on the router interface.
`exit`	To change to the Configuration mode.

☐ Enable the *OSPF* function globally.

`ip ospf router-id 10.0.1.1`	To assign the router ID (for example 10.0.1.1).
`ip ospf operation`	To enable the *OSPF* function 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]
```

☐ Set up and distribute static routes

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ip route add 8.1.2.0 255.255.255.0 10.0.2.2`	To set up 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`	To set up the static route `8.1.4.0` through the gateway `10.0.2.4`.
`ip ospf re-distribute static subnets enable`	To distribute the set-up routes in the *OSPF* function.

Router B

☐ Enable routing globally.

```
enable                                  To change to the Privileged EXEC mode.
configure                               To change to the Configuration mode.
ip routing                              To enable routing globally.
```

☐ Setting up the router interface 10.0.1.2/24.
Activate routing.
Activate the *OSPF* function on the router interface.

```
interface 2/2                           To change to the Interface Configuration mode of
                                        interface 2/2.
ip address primary 10.0.1.2 255.255.255.0   To specify the IP address and subnet mask.
ip routing                              To activate routing.
ip ospf operation                       To activate the OSPF function on the router
                                        interface.
exit                                    To 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 the *OSPF* function globally.

```
ip ospf router-id 10.0.1.2              To assign the router ID (for example 10.0.1.2).
ip ospf operation                       To enable the OSPF function 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                   To check 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 set-up on router A
Router A distributes both set-up routes.

```
show ip route all                       To check 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]
```

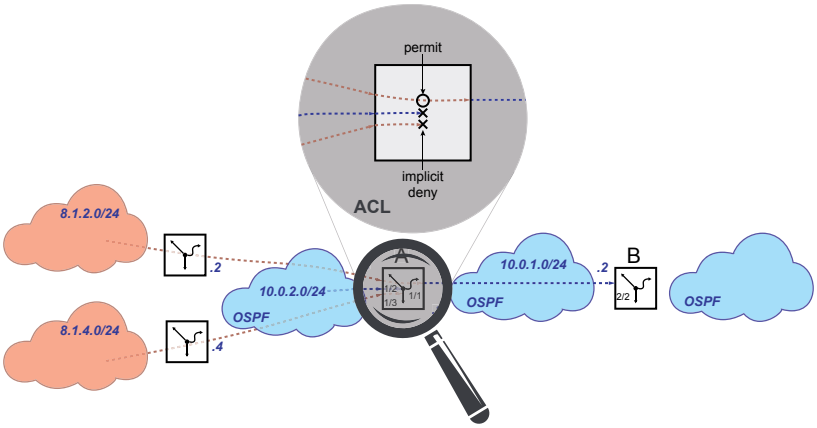
To explicitly enable a route with a permit rule, refer to the “Explicitly enabling a route using a permit rule” on page 242 section.

To explicitly disable a route with a deny rule, refer to the “Explicitly disabling a route using a deny rule” on page 244 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
```

To add the `OSPF-rule` Access Control List. To 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 set-up rules.

```
show access-list ip
```

To display the set-up 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
```

To 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 the *OSPF* function.

```
ip ospf distribute-list out static OSPF-
rule
```

To apply the `OSPF-rule` Access Control List to the *OSPF* function.

Router B

☐ Check the distribution of the routes set-up on router A
Router A only distributes the route for the subnet `8.1.2.0/24` due to the set-up Access Control List.

To check the router table:

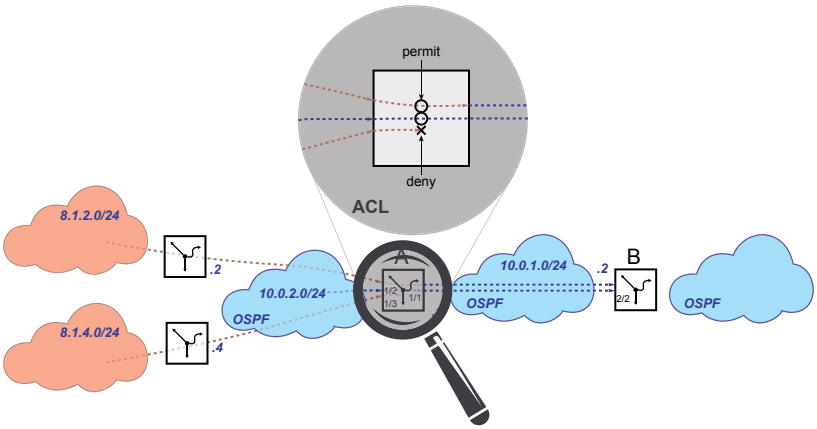
```
show ip route all

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 set up a `permit` rule, as described in section “Explicitly enabling a route using a permit rule” on page 242.

```
no ip ospf distribute-list out static OSPF-rule
```
To separate the `OSPF-rule` Access Control List from the *OSPF* function.

```
ip access-list extended del OSPF-rule
```
To 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
```
To add the `OSPF-rule` Access Control List. To set up a `deny` rule for the `8.1.4.0` subnet.
- `src 8.1.4.0-0.0.0.0` = 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.

☐ Apply the Access Control List to the *OSPF* function.

```
ip ospf distribute-list out static OSPF-rule
```
To apply the rule `OSPF-rule` to the *OSPF* function.

Router B

☐ Check the distribution of the routes set-up on router A
Due to the implicit `deny` rule embedded in the device, Router A does not distribute routes.

```
show ip route all
```
To check 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
```

To add a `permit` rule for every subnet to the `OSPF-rule` Access Control List.

☐ Check the set-up rules.

```
show access-list ip
```

To display the set-up 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
```

To 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
```

To 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 set-up on router A
Router A only distributes the route for the subnet `8.1.2.0/24` due to the set-up Access Control List.

To check 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]
```

13.7 Entering the IP Parameters

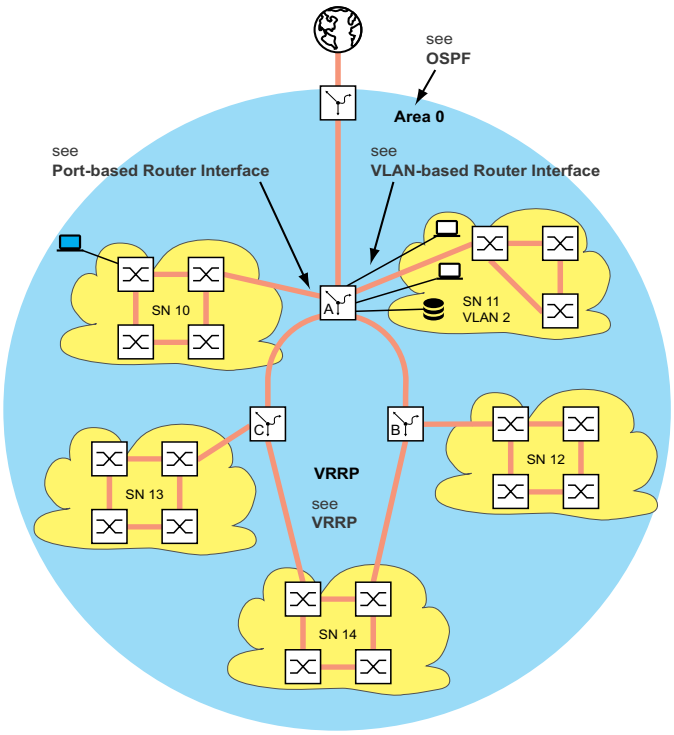


Figure 64: Network plan

To set up the Layer 3 function, you require access to the device management.

Depending on your own application, you will find many options for assigning IP addresses to the devices. The following example describes one option that often arises in practice. Although you have other prerequisites, this example shows the general method for entering the IP parameters and points out significant things that you should note.

The prerequisites for the following example are:

- All Layer 2 and Layer 3 devices have the IP address 0.0.0.0 (= default setting)
- The IP addresses of the devices and router interfaces and the gateway IP addresses are specified in the network plan.

- The devices and their connections are installed.
- Redundant connections are open (see VRRP). To help avoid loops in the configuration phase, close the redundant connections only after the configuration phase.

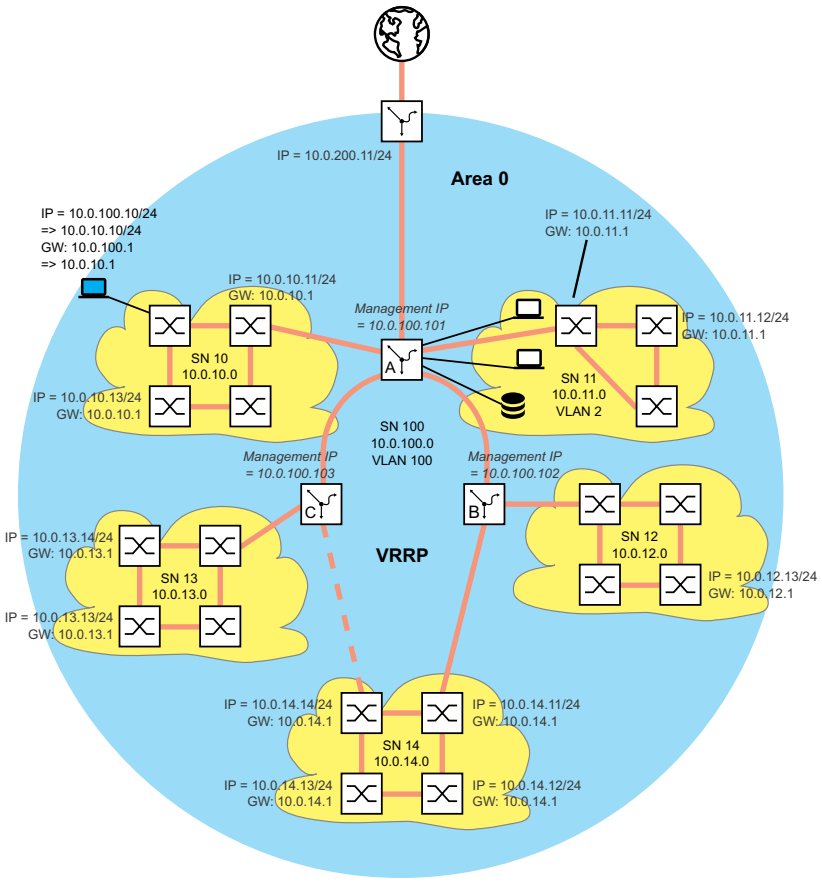


Figure 65: Network plan with management IP addresses

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.
- ☐ Set up 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 subnet 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 using the IP address of the router interface.

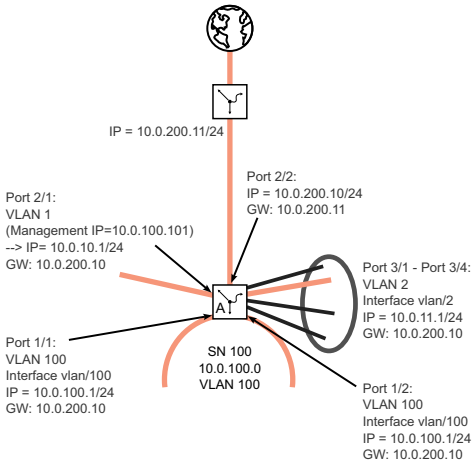


Figure 66: IP parameters for Layer 3 device A

Perform the following steps:

- ☐ Set up the *Routing* function for Layer 3 device A.
  You first set up the router interface at the port to which the configuration computer is connected.
  The result of this is that in future you will access the Layer 3 device using subnet 10.
- ☐ Change the IP parameters of your configuration computer to the values for subnet 10. You thus access Layer 3 device A again, namely using the IP address of the router interface set up beforehand.
- ☐ Finish the router configuration for Layer 3 device A. See the previous figures.

After configuring the *Routing* function on every Layer 3 device, you have access to every device.

14 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

14.1 Interface tracking

With interface tracking the device monitors the link status of:
- Physical ports
- VLAN router interfaces

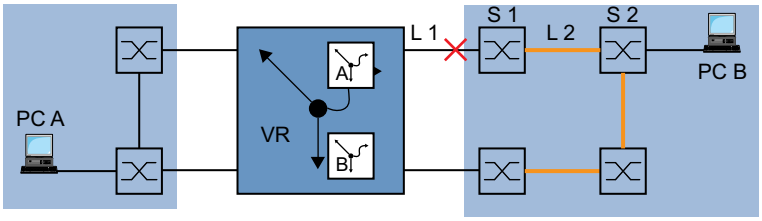


Figure 67: Monitoring a line with interface tracking

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 lets you 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.

14.2 Ping tracking

With ping tracking, the device uses ping requests to monitor the link status to other devices.

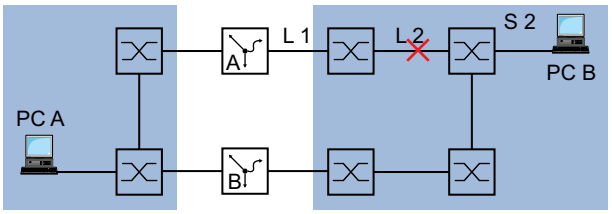


Figure 68: Monitoring a line with ping tracking

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 specify 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 lets you set the sensitivity of the ping behavior of the device. The device informs the application about an object status change.

Ping tracking lets you 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.

14.3 Logical tracking

Logical tracking lets you 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 section “Application example for logical tracking” on page 259.

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.

14.4 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.

14.4.1 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 *Advanced > 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`

☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`track add interface 11`	To add a tracking object to the table.
`track modify interface 11 ifnumber 1/1 link-up-delay 3 link-down-delay 0`	To specify the parameters for this tracking object.
`track enable interface 11`	To 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                                    To change to the Privileged EXEC mode.
show track interface                    To display the set-up tracking objects.
Name     If-Number  Link-Up-Delay  Link-Down-Delay  State  Active
-------- ---------- -------------  ---------------  -----  ------
if-11     1/1                   0                3   up       [x]
```

14.4.2 Application example for ping tracking

The interface tracking monitors the directly connected link. See figure 67 on page 253.

The ping tracking monitors the entire link to device S2. See figure 68 on page 255.

Perform the following steps:

☐ Set up ping tracking at port `1/2` for IP address `10.0.2.53` with the preset parameters.

☐ Open the *Advanced > Tracking > Configuration* dialog.

☐ To add a table row, click the button.

Select type:

☐ Enter the values you desire, for example:
Type: `ping`
Track ID: `21`

☐ 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`

☐ Apply the settings temporarily. To do this, click the ✓ button.

```
enable                                  To change to the Privileged EXEC mode.
configure                               To change to the Configuration mode.
track add ping 21                       To add a tracking object to the table.
track modify ping 21    ifnumber  1/2   To specify the parameters for this tracking object.
   address   10.0.2.53
   interval  500
   miss      3
   success   2
   timeout   100
track enable ping 21                    To 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                                        To change to the Privileged EXEC mode.
show track                                  To display the set-up tracking objects.
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..................................
```

14.4.3 Application example for logical tracking

The following figure 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 set up. See section “Application example for ping tracking” on page 258.

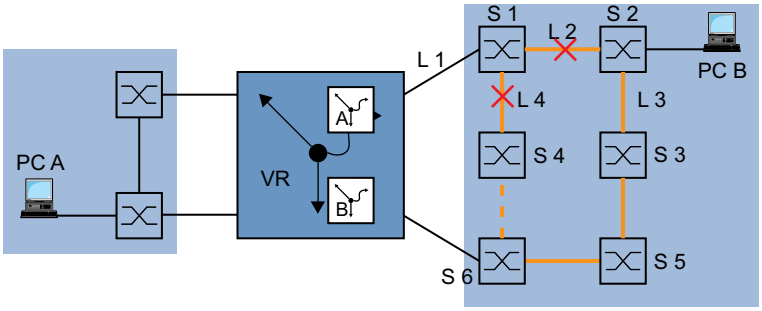


Figure 69: Monitoring the accessibility of a device in a redundant ring

☐ Set up a logical tracking object as an OR link. To do this, perform the following steps:

☐ Open the *Advanced > Tracking > Configuration* dialog.

☐ Click the button.
The dialog displays the *Create* window.

Select type:

☐ Enter the values you desire, for example:
Type: `logical`
Track ID: `31`

☐ Click the *Ok* button.

Properties:

☐ Enter the values you desire, for example:
Logical operand A: `ping-21`
Logical operand B: `ping-22`
Operator: `or`

☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`track add logical 31`	To add a tracking object to the table.
`track modify logical 31 ping-21 or ping-22`	To specify the parameters for this tracking object.
`track enable logical 31`	To 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`	To change to the Privileged EXEC mode.
`show track ping 21`	To display the set-up tracking objects.

```
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` To display the set-up tracking objects.

```
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` To display the set-up tracking objects.

```
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..................................
```

14.5 Static route tracking

14.5.1 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 through L 2 can be interrupted. In this case, the router continues transmitting through the interrupted route.

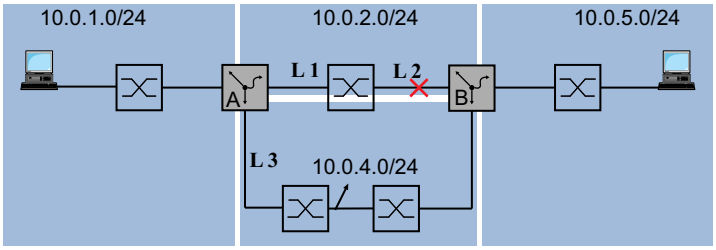


Figure 70: Example of static route tracking

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.

14.5.2 Application example for the static route tracking function

The following figure displays an example of the static route tracking function.

Router A monitors the best route through 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`

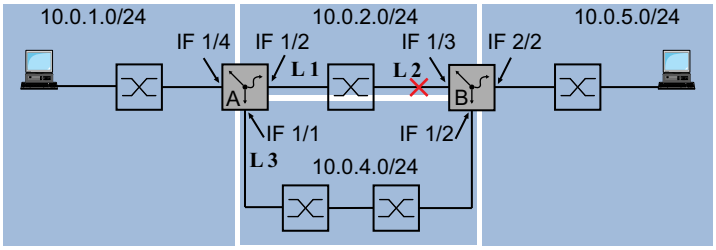


Figure 71: Configuring static route tracking

The following list contains prerequisites for further configuration:

- The IP parameters of the router interfaces are set up.
  See section "Configuration of the router interfaces" on page 204.
- The *Routing* function is enabled in the device and also active on the router interface.
- Ping tracking on interface `1/2` of router A is set up. See section "Ping tracking" on page 255.

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 *Advanced > 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` table row, *IP address* column, specify the IP address `10.0.2.53`.

☐ In the `ping-1` table row, *Ping port* column, specify the interface `1/2`.

☐ To activate the table row, mark the checkbox in the *Active* column.

☐ Click the button.
The dialog displays the *Create* window.

☐ Specify the settings for the first static route:
Type: `ping`
Track ID: `2`

☐ Click the *Ok* button.

☐ In the `ping-2` table row, *IP address* column, specify the IP address `10.0.4.2`.

☐ In the `ping-2` table row, *Ping port* column, specify the interface `1/1`.

☐ To activate the table row, mark the checkbox in the *Active* column.

☐ Apply the settings temporarily. To do this, click the ✓ button.

```
enable                                      To change to the Privileged EXEC mode.
configure                                   To change to the Configuration mode.
track add ping 1                            To add a tracking object with track ID 1.
track modify ping 1 address 10.0.2.53       To modify the ping 1 entry with the IP address
                                            10.0.2.53.
track modify ping 1 interface 1/2           To set the source interface number of the ping
                                            tracking instance to 1/2.
track enable ping 1                         To activate the tracking object.
track add ping 2                            To add a tracking object with track ID 2.
track modify ping 2 address 10.0.4.2        To modify the ping 2 entry with the IP address
                                            10.0.4.2.
track modify ping 2 interface 1/1           To set the source interface number of the ping
                                            tracking instance to 1/1.
track enable ping 2                         To activate the tracking object.
exit                                        To change to the Privileged EXEC mode.
show track ping                             To check 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:
To activate the table row, first 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.
- ☐ Specify the settings 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.
- ☐ Specify the settings 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.

☐ Apply the settings temporarily. To do this, 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`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ip route add 10.0.5.0 255.255.255.0 10.0.2.53`	To add 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`	To add a static routing entry with preference 2.
`exit`	To change to the Privileged EXEC mode.
`show ip route all`	To check 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, add 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 26: 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	

15 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
- Event counter at port level
- Link flap
- Detecting non-matching duplex modes
- Displaying the SFP status
- Topology discovery
- Reports
- Syslog
- Event log

15.1 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 specified in the trap destination table. The device lets you set up the trap destination table with the network management station using SNMP.

15.1.1 List of SNMP traps

The following table displays possible SNMP traps sent by the device.

Table 27: Possible SNMP traps

Name of the SNMP trap	Meaning
authenticationFailure	When a station attempts to access an agent without authorisation, the device sends this trap.
coldStart	Sent after the system startup.
hm2DevMonSenseExtNvmRemoval	When the external memory has been removed, the device sends this trap.
linkDown	When the connection on a port is interrupted, the device sends this trap.

Table 27: Possible SNMP traps (cont.)

Name of the SNMP trap	Meaning
linkUp	When connection is established to a port, the device sends this trap.
hm2DevMonSensePSState	When the status of a power supply unit changes, the device sends this trap.
hm2SigConStateChange	When the status of the signal contact changes in the operation monitoring, the device sends this trap.
newRoot	When the sending agent becomes the new root of the spanning tree, the device sends this trap.
topologyChange	When the port changes from blocking to forwarding or from forwarding to blocking, the device sends this trap.
alarmRisingThreshold	When the *RMON input* exceeds its upper threshold, the device sends this trap.
alarmFallingThreshold	When the *RMON input* goes below its lower threshold, the device sends this trap.
hm2AgentPortSecurityViolation	When a MAC address detected on this port does not match the current settings of the parameter hm2AgentPortSecurityEntry, the device sends this trap.
hm2DiagSelftestActionTrap	When a self test for the four categories *task*, *resource*, *software*, and *hardware* is performed according to the specified settings, the device sends this trap.
hm2MrpReconfig	When the configuration of the MRP Ring changes, the device sends this trap.
hm2DiagIfaceUtilizationTrap	When the actual value of the interface exceeds the specified upper threshold value or falls below the specified lower threshold value, the device sends this trap.
hm2LogAuditStartNextSector	When the audit trail after completing one sector starts a new one, the device sends this trap.
hm2ConfigurationSavedTrap	After the device has successfully saved its settings locally, the device sends this trap.
hm2ConfigurationChangedTrap	When you change the settings of the device for the first time after it has been saved locally, the device sends this trap.
hm2PlatformStpInstanceLoopInconsistentStartTrap	When the port in this STP instance changes to the *Loop Inconsistent* status, the device sends this trap.
hm2PlatformStpInstanceLoopInconsistentEndTrap	When the port in this STP instance leaves the *Loop Inconsistent* status receiving a BPDU packet, the device sends this trap.

15.1.2 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 transferring a configuration file onto 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.

15.1.3 SNMP trap setting

The device lets you send an SNMP trap as a reaction to specific events. Set up 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, select the entries that the device takes into account when it sends SNMP traps.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

For example, in the following dialogs you specify when the device triggers an SNMP trap:

- *Basic Settings > Port* dialog
- *Network Security > Packet Filter > Routed Firewall Mode > Rule* dialog
- *Routing > OSPF > Global* dialog
- *Advanced > Tracking > Configuration* dialog
- *Routing > L3-Redundancy > VRRP > Configuration* dialog
- *Routing > NAT > 1:1 NAT > Rule* dialog
- *Routing > NAT > Destination NAT > Rule* dialog
- *Routing > NAT > Masquerading NAT > Rule* dialog
- *Routing > NAT > Double NAT > Rule* dialog
- *Diagnostics > Status Configuration > Device Status* dialog
- *Diagnostics > Status Configuration > Security Status* dialog
- *Diagnostics > Status Configuration > Signal Contact* dialog
- *Diagnostics > System > Selftest* dialog

15.1.4 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.

15.2 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 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 lets you:
- 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 set up 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 you operate the device outside of the user-specified temperature threshold values
- The interruption of link connection(s)
  Set up at least one port for this feature. In the table of the *Port* tab, *Propagate connection error* column, you specify for which ports the device will propagate a link interruption to the device status. In the default setting, link connection monitoring is inactive.
- The removal of the external memory
  The configuration profile in the external memory does not match the settings in the device.

Select the corresponding entries to decide which events the device status includes.

Note:
With a non-redundant voltage supply, the device reports the absence of a supply voltage. To disable this message, feed the supply voltage over both inputs or ignore the monitoring.

15.2.1 Events which can be monitored

Table 28: Device Status events

Name	Meaning
Connection errors	Activate this function to monitor every port link event in which the *Propagate connection error* checkbox is marked.
Temperature	Activate this function to monitor if the temperature exceeds the specified upper threshold value or falls below the specified lower threshold value.
External memory removal	Activate this function to monitor the presence of an external storage device.
External memory not in sync	The device monitors synchronization between the device settings and the configuration profile stored in the external memory (*ENVM*).
Power supply	Activate this function to monitor the power supply.

15.2.2 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, add at least one trap destination that receives SNMP traps.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Basic Settings > System* dialog.
- ☐ To monitor the temperature, in the *System data* frame, you specify the temperature threshold values.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`device-status trap`	To send an SNMP trap when the device status changes.
`device-status monitor envm-not-in-sync`	To monitor the configuration profiles in the device and in the external memory. The *Device status* 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.
`device-status monitor envm-removal`	To monitor 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`	To monitor 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 temperature`	To monitor the temperature in the device. When the temperature exceeds the specified upper threshold value or falls below the specified lower threshold value, the value in the *Device status* frame changes to `error`.

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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`device-status monitor link-failure`	To monitor 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`	To change to the Interface Configuration mode of interface 1/1.
`device-status link-alarm`	To monitor the port/interface link. When the link interrupts on a monitored 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.

15.2.3 Displaying the Device Status

Perform the following steps:

- ☐ Open the *Basic Settings > System* dialog.

`enable`	To change to the Privileged EXEC mode.
`show device-status all`	To display the device status and the setting for the device status determination.

15.3 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 lets you:
- 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

15.3.1 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 29: 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 shorter than 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.
HTTP server active	Activate this function to monitor when the *HTTP* function is active.
SNMP unencrypted	Activate this function to monitor when the *SNMPv1* or *SNMPv2* function is active.
Access to System Monitor 1 through the serial interface possible	The device monitors the System Monitor 1 status.
Saving the configuration profile on the external memory possible	The device monitors the possibility to save settings to the external non-volatile memory.
Link interrupted on enabled device ports	The device monitors the link status of active ports.

Table 29: Security Status events (cont.)

Name	Meaning
Access with HiDiscovery possible	Activate this function to monitor when the HiDiscovery function has write access to the device.
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-generated digital certificates.

15.3.2 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ In the *Diagnostics > Status Configuration > Alarms (Traps)* dialog, add at least one trap destination that receives SNMP traps.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`security-status monitor pwd-change`	To monitor the password for the locally set up user account `admin`. When the password for the `admin` user account is the default setting, the value in the *Security status* frame changes to *`error`*.
`security-status monitor pwd-min-length`	To monitor 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`	To monitor 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`*. • *Upper-case characters (min.)* • *Lower-case characters (min.)* • *Digits (min.)* • *Special characters (min.)*
`security-status monitor pwd-policy-inactive`	To monitor 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 http-enabled`	To monitor the HTTP server. When you enable the HTTP server, the value in the *Security status* frame changes to *`error`*.

`security-status monitor snmp-unsecure`	To monitor the SNMP server. When at least one of the following conditions applies, the value in the *Security status* frame changes to *error*: • The *SNMPv1* function is enabled. • The *SNMPv2* function is enabled. • The encryption for SNMPv3 is disabled. You enable the encryption in the *Device Security > User Management* dialog, in the *SNMP encryption type* field.
`security-status monitor sysmon-enabled`	To monitor the activation of the *System Monitor 1* function in the device.
`security-status monitor extnvm-upd-enabled`	To monitor the activation of the external non volatile memory update.
`security-status trap`	To send an SNMP trap when the device status changes.

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.
- ☐ Apply the settings 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`security-status monitor no-link-enabled`	To monitor 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`	To change to the Interface Configuration mode of interface `1/1`.
`security-status monitor no-link`	To monitor the link on interface/port `1`.

15.3.3 Displaying the Security Status

Perform the following steps:

- ☐ Open the *Basic Settings > System* dialog.

`enable`	To change to the Privileged EXEC mode.
`show security-status all`	To display the security status and the setting for the security status determination.

15.4 Out-of-Band signaling

The device uses the signal contact to control external devices and monitor device functions. Function monitoring lets you 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 you operate the device outside of the user-specified temperature threshold values
- The interruption of link connection(s)
  Set up 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 profile in the external memory does not match the settings in the device.

Select the corresponding entries to decide which events the device status includes.

Note:
With a non-redundant voltage supply, the device reports the absence of a supply voltage. To disable this message, feed the supply voltage over both inputs or ignore the monitoring.

15.4.1 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 from the *Mode* drop-down list.
- ☐ Open the signal contact.
  Select the *open* radio button in the *Configuration* frame.
- ☐ Close the signal contact.
  Select the *close* radio button in the *Configuration* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`signal-contact 1 mode manual`	To select the manual setting mode for signal contact 1.
`signal-contact 1 state open`	To open signal contact 1.
`signal-contact 1 state closed`	To close signal contact 1.

15.4.2 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ In the *Diagnostics > Status Configuration > Alarms (Traps)* dialog, add at least one trap destination that receives SNMP traps.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ You specify the temperature threshold values for the temperature monitoring in the *Basic Settings > System* dialog.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`signal-contact 1 monitor temperature`	To monitor the temperature in the device. When the temperature exceeds the specified upper threshold value or falls below the specified lower threshold value, the signal contact opens.
`signal-contact 1 monitor ring-redundancy`	To monitor the ring redundancy. The signal contact opens in the following situations: • The device operates as a Redundancy Manager. The redundancy function of the device uses the alternative connection. There is no longer a redundancy reserve. • The device, as a ring participant, has detected an error in its ring redundancy settings.
`signal-contact 1 monitor link-failure`	To monitor the ports/interfaces link. When the link interrupts on a monitored port/interface, the signal contact opens.

`signal-contact 1 monitor envm-removal`	To monitor 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`	To monitor the configuration profiles in the device and in the external memory. 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.
`signal-contact 1 monitor power-supply 1`	To monitor 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`	To monitor module 1. When you remove module 1 from the device, the signal contact opens.
`signal-contact 1 trap`	To send an SNMP trap when the status of the operation monitoring changes.
`no signal-contact 1 trap`	To disable the SNMP trap

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`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`signal-contact 1 monitor link-failure`	To monitor the ports/interfaces link. When the link interrupts on a monitored port/interface, the signal contact opens.
`interface 1/1`	To change to the Interface Configuration mode of interface 1/1.
`signal-contact 1 link-alarm`	To monitor the port/interface link. When the link interrupts on the port/interface, the signal contact opens.

Events which can be monitored

Table 30: Device Status events

Name	Meaning
Connection errors	Activate this function to monitor every port link event in which the *Propagate connection error* checkbox is marked.
Temperature	Activate this function to monitor if the temperature exceeds the specified upper threshold value or falls below the specified lower threshold value.
External memory removed	Activate this function to monitor the presence of an external storage device.
External memory not in sync with NVM	The device monitors synchronization between the device settings and the configuration profile stored in the external memory (*ENVM*).
Power supply	Activate this function to monitor the power supply.

Displaying the signal contact 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.

```
show signal-contact 1 all
```

To display the settings for the specified signal contact.

15.5 Port event counter

The port statistics table assists experienced network administrators in identifying potential network interruptions.

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 31: Examples indicating known weaknesses

Counter	Indication of known possible weakness
Received fragments	• Non-functioning controller of the connected device • Electromagnetic interference in the transmission medium
CRC Error	• Non-functioning controller of the connected device • Electromagnetic interference in the transmission medium • Inoperable component in the network
Collisions	• Non-functioning controller of the connected device • Network over extended/lines too long • 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.

15.5.1 Detecting non-matching duplex modes

Potential problems occur when 2 ports directly connected to each other have mismatched duplex modes. These potential problems are difficult to detect. The automatic detection and reporting of this situation has the benefit of recognizing mismatched duplex modes before potential 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 data stream level the local device records a lot of detected 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 detected 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:

- Duplex problem detected
  Mismatched duplex modes.

- EMI
  Electromagnetic interference.
- Network extension
  The network extension is too great, or too many cascading hubs.
- Collisions, *Late Collisions*
  In half-duplex mode, collisions mean normal operation.
  In full-duplex mode, no incrementation of the port counters for collisions or *Late Collisions*.
- CRC Error
  The device evaluates these detected errors as non-matching duplex modes in the manual full-duplex mode.

Table 32: 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	Potential 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	Potential 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	Potential duplex problem, EMI

15.6 Link flap function

The *Link flap* function assists in managing link changes. You can therefore use the function to speed up convergence if a Layer 2 redundancy protocol based on IEEE 802.3 Ethernet packets is active in the network, for example, Rapid Spanning Tree Protocol (RSTP). Convergence is the time required to adjust the network to topology changes, for example when the link status on a port changes.

The *Link flap* function is intended for use in networks with an active Layer 2 redundancy protocol such as RSTP. However, the device itself does not support a redundancy protocol and is not part of the redundant topology.

Using the *Link flap* function, the device replicates link changes that it detects on one port to another port. You can therefore use the function to speed up convergence if a switch device with an active Layer 2 redundancy protocol is connected as a direct neighbor. The prerequisite is that both ports are connected to the same Layer 2 network.

The *Link flap* function exclusively affects the physical ports `1/1` and `1/3`.

If the *Link flap* function is enabled, then the device disables the following port in case of the condition mentioned:

- Port `1/1`, if the link on port `1/3` becomes inoperable
- Port `1/3`, if the link on port `1/1` becomes inoperable

As soon as the condition no longer exists and the link is operational again, the device re-enables the port that it had previously deactivated. During this period, the device management remains accessible through the management port.

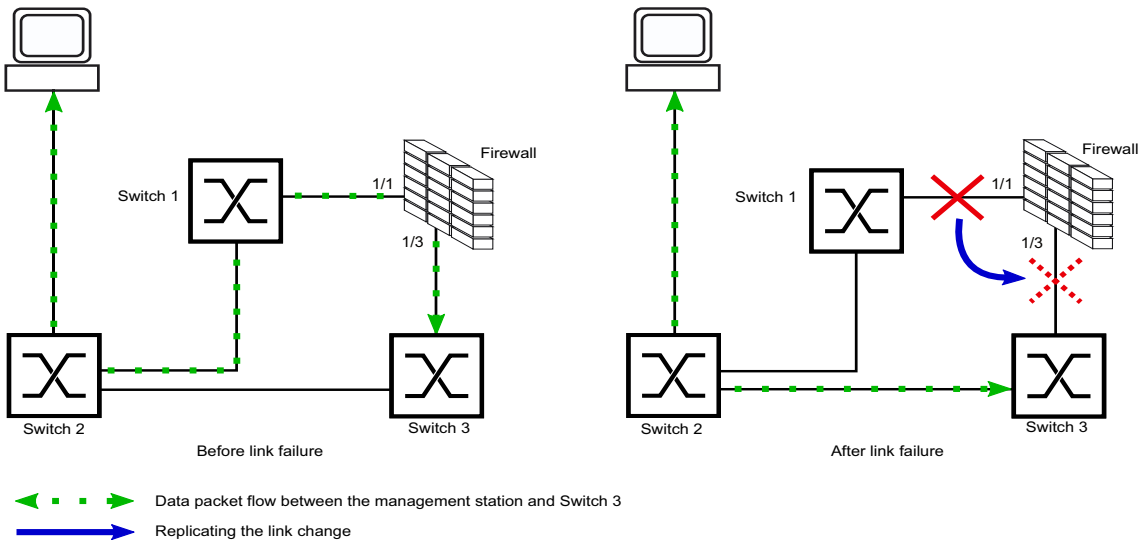


Figure 72: Data packet flow before and after a link failure

15.6.1 Enabling the Link flap function

In the default setting, the *Link flap* function is disabled. To enable the *Link flap* function, perform the following steps.

Prerequisites:
- The physical ports 1/1 and 1/3 are connected to the same Layer 2 network.
- In the *Basic Settings > Port* dialog, *Configuration* tab, the *Port on* checkbox is marked for ports 1/1 and 1/3.

- ☐ Activate the *802.3 Frames forwarding* function. To do this, in the *Network Security > DoS > Global* dialog, *Layer 2 frames* frame, mark the *802.3 Frames forwarding* checkbox.
  With this setting, the device replicates detected link changes between ports 1/1 and 1/3.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Diagnostics > Ports > Port Monitor* dialog, *Link flap* tab.
- ☐ Enable the *Link flap* function.
  Select the *On* radio button in the *Operation* frame.

  Note:
  If a link on the device becomes inoperable, RSTP or another Layer 2 redundancy protocol will find an alternative path by bypassing the device and excluding it from the network path. This scenario poses a potential security risk. Therefore, enable the *Link flap* function only if you are aware of the effects.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos l2-frame-forwarding`	To activate the *802.3 Frames forwarding* function.
`link-flap operation`	To enable the *Link flap* function.

15.7 Displaying the SFP status

The SFP status display lets you look at the current SFP module connections and their properties. The properties include:

- module type
- serial number of media module
- temperature in ° C
- transmission power in mW
- receive power in mW

Perform the following step:

- ☐ Open the *Diagnostics > Ports > SFP* dialog.

15.8 Topology discovery

IEEE 802.1AB defines the Link Layer Discovery Protocol (LLDP). LLDP lets you automatically detect the LAN network topology.

Devices with LLDP active:
- broadcast their connection and management information to neighboring devices on the shared LAN. When the receiving device has its *LLDP* function active, evaluation of the devices occur.
- receive connection and management information from 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 lets the network management station map the topology of the network.

Non-LLDP-capable devices normally block the special Multicast LLDP IEEE MAC address used for information exchange. Non-LLDP-capable 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.

15.8.1 Displaying the Topology discovery results

Display the topology of the network. To do this, perform the following step:

- ☐ Open the *Diagnostics > LLDP > Topology Discovery* dialog, *LLDP* tab.

When you use a port to connect several devices, for example through a hub, the table contains a line for each connected device.

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 MAC address table (forwarding database) contains MAC addresses of devices that the topology table hides for the sake of clarity.

15.9 Reports

The following lists reports and buttons available for diagnostics:

- System Log file
  The device logs device-internal events in the System Log file.
- 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 remain available even after powering off the device. 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 number of files set up. 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.

15.9.1 Global settings

Using this dialog you enable or disable where the device sends reports, for example, to a Console, a syslog server, or a connection to the Command Line Interface. You also set at which severity level the device writes events into the reports.

Perform the following steps:

- ☐ Open the *Diagnostics > Report > Global* dialog.
- ☐ To send a report to the console, specify the desired level in the *Console logging* frame, *Severity* field.
- ☐ Enable the *Console logging* function.
  Select the *On* radio button in the *Console logging* frame.
- ☐ Apply the settings 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.
- ☐ Apply the settings 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 setup 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 to send SNMP Read requests as events to the syslog server.
  Select the *On* radio button in the *SNMP logging* frame.
- ☐ Enable the *Log SNMP set request* function for the device to send SNMP Write requests as events to the syslog server.
  Select the *On* radio button in the *SNMP logging* frame.
- ☐ Choose the desired severity level for the get and set requests.
- ☐ Apply the settings 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 IEEE 1686 for Substation Intelligent Electronic Devices.

Perform the following steps:

- ☐ Open the *Diagnostics > Report > Global* dialog.
- ☐ Enable the *CLI logging* function.
  Select the *On* radio button in the *CLI logging* frame.
- ☐ Apply the settings 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`
- `config.xml`
- `defaultconfig.xml`
- `script`
- `runningconfig.xml`
- `supportinfo.html`
- `systeminfo.html`
- `systemlog.html`

The device names the ZIP archive automatically in the format `<IP_address>_<system_name>.zip`.

Perform the following steps:

- ☐ Click the button.
  After a while, you can download the ZIP archive.
- ☐ Select the directory in which you want to save the support information.
- ☐ Click the *Ok* button.

15.9.2 Syslog

The device lets you 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 row, click the button.
- ☐ In the *IP address* column, enter the IP address or *Hostname* of the syslog server.
- ☐ In the *Destination UDP port* column, specify the UDP port on which the syslog server expects the log entries.
- ☐ In the *Min. severity* column, specify the minimum severity level that an event requires for the device to send a log entry to this syslog server.
- ☐ Mark the checkbox in the *Active* column.
- ☐ Enable the *Syslog* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

In the *SNMP logging* frame, set up the following settings for SNMP read and write requests:

Perform the following steps:

- ☐ Open the *Diagnostics > Report > Global* dialog.
- ☐ Enable the *Log SNMP get request* function for the device to send SNMP Read requests as events to the syslog server.
  Select the *On* radio button in the *SNMP logging* frame.
- ☐ Enable the *Log SNMP set request* function for the device to send SNMP Write requests as events to the syslog server.
  Select the *On* radio button in the *SNMP logging* frame.
- ☐ Choose the desired severity level for the get and set requests.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging host add 1 addr 10.0.1.159 severity 3`	To add a 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`	To enable the *Syslog* function.
`exit`	To change to the Privileged EXEC mode.
`show logging host`	To display the syslog host settings.

```
No.    Server IP      Port   Max. Severity   Type        Status
-----  -------------- -----  --------------  ----------  -------
1      10.0.1.159     514    error           systemlog   active
```

`configure`	To change to the Configuration mode.
`logging snmp-requests get operation`	To log the reception of *SNMP Get requests*.
`logging snmp-requests get severity 5`	The value `5` specifies the severity level of the event that the device logs when it receives an *SNMP Get request*. The value `5` means `notice`.
`logging snmp-requests set operation`	To log the reception of *SNMP Set requests*.
`logging snmp-requests set severity 5`	The value `5` specifies the severity level of the event that the device logs when it receives an *SNMP Set request*. The value `5` means `notice`.
`exit`	To change to the Privileged EXEC mode.
`show logging snmp`	To 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
```

15.9.3 System Log

The device lets you call up a System Log file of the system events. The table in the *Diagnostics* > Report > *System Log* dialog lists the logged events.

You have the following options:
- View and refresh the System Log file
- Searching for content
- Downloading a copy of the System Log file
- Clearing the System Log file on the device

You have the option to also send the logged events to one or more syslog servers.

View and refresh the System Log file

The device continuously logs events in the System Log file. The display of events in the Graphical User Interface does not update automatically. If the dialog is already open for a while, refresh the display to also display the recently logged events.

Perform the following steps:

- ☐ Refresh the display of the System Log file in the Graphical User Interface. To do this, click the ↻ button.

`enable`	To change to the Privileged EXEC mode.
`show logging buffered`	To display the buffered log entries.

Searching for content

The device continuously logs events in the System Log file. After a while, the file may contain a large number of events.

Perform the following steps:

- ☐ Look for a keyword in the System Log file. To do this, use the search function of your web browser.

`enable`	To change to the Privileged EXEC mode.
`show logging buffered <filter>`	To display the buffered log entries. You can enter keywords for the severity level, digits, or ranges, separated by a comma. Example: `emergency,alert-error,4,5-6`

Downloading a copy of the System Log file

The device continuously logs events in the System Log file. After a while, the file may contain many events. In the Graphical User Interface, you can download a copy of the System Log file to analyze the logged events on your computer. Using the Command Line Interface, you can save a copy of the System Log file in the external memory or on a remote server.

Perform the following steps:

- ☐ Download a copy of the System Log file onto your computer. To do this, click the button.
- ☐ Select the desired file format, either HTML or CSV.
- ☐ The web browser saves the file on the computer according to its download settings. If necessary, select the file location.

`enable`	To change to the Privileged EXEC mode.
`copy eventlog buffered envm EXAMPLE`	To save a copy of the System Log file with filename `EXAMPLE` in the external memory.
`copy eventlog buffered remote ftp://1.2.3.4/EXAMPLE`	To save a copy of the System Log file with filename `EXAMPLE` on a remote server.

Clearing the System Log file on the device

The device continuously logs events in the System Log file. After a while, the file may contain many events. If you are no longer interested in the logged events, you can clear the System Log file in the device.

Perform the following steps:

- ☐ Delete the content of the System Log file. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`clear logging buffered`	To clear the log file.

15.9.4 Audit Trail

The *Diagnostics > Report > Audit Trail* dialog contains system information and changes to the device settings performed through the Command Line Interface and SNMP. In the case of a change in the device settings, 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 device software update
- Configuration changes using HiDiscovery
- Automatic configuration or device software 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

16 Advanced functions of the device

16.1 Using the device as a DHCP client

The Dynamic Host Configuration Protocol (DHCP) lets a server assign the IP settings to the devices on the network (clients). This reduces the effort required for manual setup.

When operating as a DHCP client, the device retrieves the following settings for its physical interfaces from a DHCP server:

- IP address
- Netmask
- Default gateway

In the following example, you enable the *DHCP client* function on interface `1/1`. To do this, perform the following steps:

- ☐ Open the *Routing > Interfaces > Configuration* dialog.
- ☐ In the table row for interface `1/1`, mark the checkbox in the *DHCP client* column.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`dhcp-client`	To enable the *DHCP client* function on `interface 1/1`.
`exit`	To change to the Configuration mode.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

16.2 DHCP server

The Dynamic Host Configuration Protocol (DHCP) lets a server assign the IP settings to the devices on the network (clients). This reduces the effort required for manual setup. The DHCP server stores and assigns the available IP addresses and further settings, if specified.

The procedure for assigning the IP settings consists of 4 phases:
- *DISCOVER* sent by the DHCP client
- *OFFER* sent by the DHCP server
- *REQUEST* sent by the DHCP client
- *ACKNOWLEDGE* sent by the DHCP server

The DHCP server in the device listens for requests on UDP port 67 and responds to the client devices on UDP port 68. When the device receives a DHCP request, it validates the IP address to be assigned before leasing the IP address and other IP settings to the requesting client device.

The device lets you activate the *DHCP Server* function on single physical ports.

16.2.1 Settings that the server assigns to the clients

When operating as a DHCP server, the device assigns the IP settings to the client devices based on the following parameters:
- MAC address of the client device
- Physical port to which the client device is connected

The device assigns the following IP settings to the client devices:
- IP address
- Subnet mask
- Default gateway, if specified
- Further network settings, if specified

16.2.2 Pools

The device stores the IP settings in two types of pools.
- Static pools
  To assign the same IP address to a specific device each time, the device stores the relevant IP settings in a pool whose address range is exactly one IP address.
  Static pools are useful, for example, to assign a fixed IP address to a server, NAS, or printer.
- Dynamic pools
  To assign IP addresses from a certain address range, the device stores the relevant IP settings in a pool whose address range includes multiple IP addresses.

Setting up a static pool

In the following example, you set up the device to assign IP settings from a certain static pool to a certain client device connected to a certain port.

The static pool is to be set up based on the following parameters:
- MAC address of the client device: `ec:e5:55:d6:50:01`
- Physical port to which the client device is connected on the server device: `1/1`

- IP address that the device should assign to the client device: `192.168.23.42`
- The assigned IP settings are valid for 2 days: `172800`

Perform the following steps:

- ☐ Open the *Advanced > DHCP > DHCP Server > Pool* dialog.
- ☐ Add a table row. To do this, click the button.
- ☐ Specify the following settings for the table row:
  - *IP range start* column = `192.168.23.42`
  - *Port* column = `1/1`
  - *MAC address* column = `ec:e5:55:d6:50:01`
  - *Lease time [s]* column = `172800`
  - *Active* column = marked
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Advanced > DHCP > DHCP Server > Global* dialog.
- ☐ Verify that the DHCP function is active on port `1/1`.
  If not already done, mark the checkbox in the *DHCP server active* column for port `1/1`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dhcp-server pool add 1 static 192.168.23.42 interface 1/1`	To add a static pool with index `1` with the IP address `192.168.23.42` to physical port `1/1`.
`dhcp-server pool modify 1 mode mac EC:E5:55:D6:50:01`	To assign the static pool with index `1` to a client device with MAC address `EC:E5:55:D6:50:01`.
`dhcp-server pool modify 1 leasetime 172800`	To specify the lease time of the static pool with index `1`.
`dhcp-server pool mode 1 enable`	To enable the static pool with index `1`.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`dhcp-server operation`	To activate the DHCP server function on this port.

Setting up a dynamic pool

In the following example, you set up the device to assign an IP address from a certain address range to client devices connected to a certain port.

The dynamic pool is to be set up based on the following parameters:
- MAC address of the client device is not to be evaluated.
- Physical port to which the client devices are connected on the server device: `1/2`
- Address range from which the device assigns an IP address to the client devices: `192.168.23.92..192.168.23.142`
- The assigned IP settings are valid for 2 days: `172800`

Perform the following steps:

- ☐ Open the *Advanced > DHCP > DHCP Server > Pool* dialog.
- ☐ Add a table row. To do this, click the button.
- ☐ Specify the following settings for the table row:
  - *IP range start* column = `192.168.23.92`
  - *IP range end* column = `192.168.23.142`
  - *Port* column = `1/2`
  - *Lease time [s]* column = `172800`
  - *Active* column = `Marked`
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Advanced > DHCP > DHCP Server > Global* dialog.
- ☐ Verify that the DHCP function is active on port `1/2`.
  If not already done, mark the checkbox in the *DHCP server active* column for port `1/2`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dhcp-server pool add 2 dynamic 192.168.23.92 192.168.23.142 interface 1/2`	To add a dynamic pool with index `2` with a range from `192.168.23.92` to `192.168.23.142` to physical port `1/2`.
`dhcp-server pool modify 2 leasetime 172800`	To specify the lease time of the dynamic pool with index `2`.
`dhcp-server pool mode 2 enable`	To enable the dynamic pool with index `2`.
`interface 1/2`	To change to the Interface Configuration mode of interface `1/2`.
`dhcp-server operation`	To activate the DHCP server function on this port.

16.3 Using the device as a DNS client

As a DNS client, the device queries a DNS server to resolve the hostname of a device in the network to the related IP address.

The device lets you specify up to 4 DNS servers to which it forwards a request to resolve a hostname (*DNS request*).

When the device receives a request to resolve a hostname (*DNS request*), it first tries to find the related IP address internally. If the device cannot resolve the hostname by itself, it forwards the request to a DNS server. The DNS server returns the associated IP address to the device.

16.3.1 Setting up the DNS client function

The device has the option to contact a DNS server assigned by the DHCP server. This example describes how to set up the device to contact a user-defined DNS server instead. To do this, perform the following steps:

- ☐ Open the *Advanced* > *DNS* > *Client* > *Static* dialog.
- ☐ In the *Configuration* frame, select the `user` item from the *Source* drop-down list.
- ☐ In the *Configuration* frame, *Domain name* field, specify the value `example.com`.
- ☐ In the table, click the ⊞ button.
  The dialog displays the *Create* window.
- ☐ In the *Index* column, specify the value `1` as the sequential number. You can only assign unique values.
- ☐ In the *IP address* column, specify the IPv4 address of the DNS server, for example `192.168.3.5`.
- ☐ Click the *Ok* button.
  The device adds a table row.
- ☐ Open the *Advanced* > *DNS* > *Client* > *Global* dialog.
- ☐ Enable the *Client* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dns client source user`	To specify that the device contacts a user-defined DNS server.
`dns client domain-name example.com`	To specify the string `example.com` as a domain name. The device adds this domain name to hostnames without a domain suffix.
`dns client servers add 1 ip 192.168.3.5`	To add a DNS server with the IPv4 address `192.168.3.5` as index `1`.
`dns client adminstate`	To enable the *Client* function globally.

A Setting up the configuration environment

A.1 Preparing access using SSH

You can connect to the device using SSH. To do this, perform the following steps:

- Generate a key in the device.
  or
- Transfer your own key onto the device.
- Prepare access to the device in the SSH client program.

Note:
In the default setting, the key is already existing and access using SSH is enabled.

A.1.1 Generating a key in the device

The device lets you generate the key directly in the device. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *SSH* tab.
- ☐ Disable the *SSH* server.
  Select the *Off* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ To generate a RSA key, in the *Signature* frame, click the *Create* button.
- ☐ Enable the *SSH* server.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ssh key rsa generate`	To generate a new RSA key.

A.1.2 Transferring your own key onto the device

OpenSSH gives experienced network administrators the option of generating their own key. To generate the key, enter the following commands on your PC:

```
ssh-keygen -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.
- ☐ Disable the *SSH* server.
  Select the *Off* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ When the file is located on your PC or on a network drive, drag and drop it onto the  area. As an alternative, click in the area to select the file.
- ☐ To transfer the file to the device, click the *Start* button.
- ☐ Enable the *SSH* server.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings 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`	To change to the Privileged EXEC mode.
`copy sshkey envm <file name>`	To transfer your own key onto the device from the external memory.

A.1.3 Preparing the SSH client program

The *PuTTY* program lets you access the device using SSH. You can download the software from www.chiark.greenend.org.uk/~sgtatham/putty/.

Perform the following steps:

- ☐ Start the program by double-clicking on it.

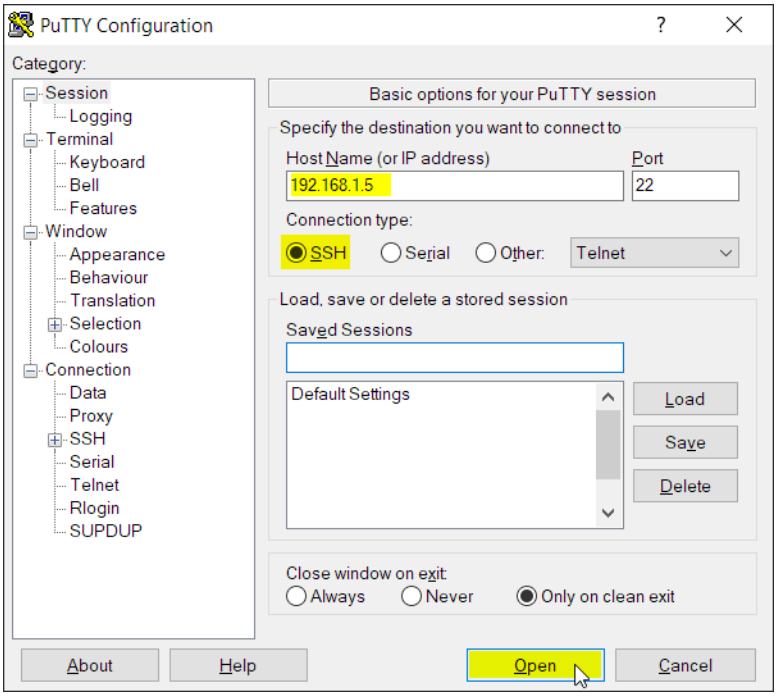


Figure 73: PuTTY input screen

- ☐ 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.

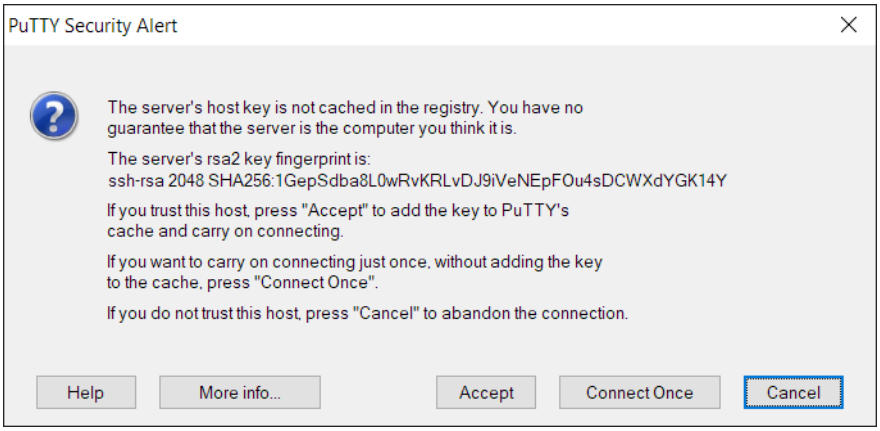


Figure 74: Security alert prompt for the fingerprint

Before the connection is established, the *PuTTY* program displays a security alarm message and lets you check the key fingerprint.

- ☐ Check the fingerprint of the key to help ensure that you have actually connected to the desired device.
- ☐ When the fingerprint matches your key, click the *Yes* button.

For experienced network administrators, another way of accessing your device through an SSH is by using the OpenSSH Suite. To set up the data connection, enter the following command:

```
ssh admin@10.0.112.53
```

`admin` is the user name.

`10.0.112.53` is the IP address of your device.

A.2 SSH algorithms

Secure Shell (SSH) algorithms are cryptographic algorithms used in the SSH protocol to help provide secure communication over a potentially unsecured network. These algorithms help ensure the confidentiality, integrity, and authenticity of a data connection between a client and the server.

The device supports the following classes of SSH algorithms:
- Key Exchange (KEX)
- Host key-based
- Encryption (Ciphers)
- Hash-based Message Authentication Code (HMAC)

A.2.1 Enabling the SSH algorithms in the device

In the default setting, the most commonly used algorithms are enabled in the device. If a required algorithm is disabled, you can enable this and further algorithms using the Simple Network Management Protocol (SNMP). To do this, you typically use a Linux computer.

The following example explains how to enable the algorithms in the device.

The example is based on the following specifications:
- `192.168.1.1`
  IP address of the device
- `admin`
  User account with access role `administrator` on the device
- `welcome123`
  User account password

Prerequisites:
- The access role `administrator` is assigned to the user account you use to perform the actions on the device.
- You need a Linux computer with the `snmp` and `nmap` packages installed.

Perform the following steps on the Linux computer:
- ☐ Open a terminal application.
- ☐ Download the ZIP archive, which contains the device software and the MIB files from hirschmann-support.belden.com/en-US/downloads.
- ☐ Extract the contents of the ZIP archive to a temporary directory.
- ☐ Copy the `standard-mibs` and `released-mibs` folders to the desired directory, for example, to `/home/workspace/mibs/`.
- ☐ Create an environment variable containing the paths to the MIB files.
  ```
  export MIBDIRS=/home/workspace/mibs/standard-mibs/:/home/workspace/mibs/released-mibs/
  ```

☐ Enable the algorithms in the device.

```
snmpset -Ln -u admin -a SHA-1 -A welcome123 -x AES-128 -X welcome123 -l authPriv 192.168.1.1 <MIB variable for algorithm> b '<algorithm indexes>'
```

Explanation:

`-Ln`
No logging

`-u admin`
User account name

`-a SHA-1`
Protocol for SNMPv3 authentication
For increased security, use SHA-1.

`-A welcome123`
User account password
If the password is shorter than 8 characters, then enter the password twice. For example, instead of `welcome`, enter `welcomewelcome`.

`-x AES-128`
Protocol for SNMPv3 privacy
For increased security, use AES-128.

`-X welcome123`
User account password
If the password is shorter than 8 characters, then enter the password twice. For example, instead of `welcome`, enter `welcomewelcome`.

`-l authPriv`
Security level

`192.168.1.1`
IP address of the device

`<MIB variable for algorithm>`
MIB variable that specifies the algorithm class
You can find the value to be entered in the section of the desired algorithm.

`<algorithm indexes>`
Index number by which the device identifies the desired algorithm
You can find the value to be entered in the section of the desired algorithm.

- See “Key Exchange (KEX)” on page 306.
- See “Host key-based” on page 307.
- See “Encryption (Ciphers)” on page 308.
- See “Hash-based Message Authentication Code (HMAC)” on page 309.

☐ Check the algorithms enabled in the device.

```
nmap --script ssh2-enum-algos 192.168.1.1
```

A.2.2 Key Exchange (KEX)

In the initial connection phase, the client and server negotiate a KEX algorithm to generate a strong, unique key used to establish the SSH session. The KEX algorithm helps ensure that the key remains confidential and undisclosed to potential unauthorized access.

The device identifies each algorithm by an index number. Use the index number to enable the desired algorithm on the device.

Table 33: Supported KEX algorithms

Index	Algorithm	Default setting
0	diffie-hellman-group1-sha1	disabled
1	diffie-hellman-group14-sha1	disabled
2	diffie-hellman-group14-sha256	disabled
3	diffie-hellman-group16-sha512	enabled

Table 33: Supported KEX algorithms

Index	Algorithm	Default setting
4	diffie-hellman-group18-sha512	enabled
5	diffie-hellman-group-exchange-sha256	enabled
6	ecdh-sha2-nistp256	enabled
7	ecdh-sha2-nistp384	disabled
8	ecdh-sha2-nistp521	enabled
9	curve25519-sha256	enabled
10	curve25519-sha256@libssh.org	enabled

You can enable the algorithms that you need or disable those that you do not need. To do this, follow the instructions in section "Enabling the SSH algorithms in the device" on page 305.

- The MIB variable `HM2-MGMTACCESS-MIB::hm2SshKexAlgorithms.0` specifies that you enable the KEX algorithms.
- The device will enable each algorithm you specify in the `snmpset` command.
- The device will disable each algorithm you do not specify in the `snmpset` command, even if it was previously enabled.

Perform the following steps to enable, for example, the `diffie-hellman-group1-sha1` and `diffie-hellman-group14-sha1` algorithms:

☐ Enable the algorithms in the device.

```
snmpset -Ln -u admin -a SHA-1 -A welcome123 -x AES-128 -X welcome123 -l authPriv 192.168.1.1 HM2-MGMTACCESS-MIB::hm2SshKexAlgorithms.0 b '0 1'
```

☐ Check the algorithms enabled in the device.

```
nmap --script ssh2-enum-algos 192.168.1.1
```

Look at the `kex_algorithms` section:

```
kex_algorithms: (5)
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
ecdh-sha2-nistp521
curve25519-sha256
curve25519-sha256@libssh.org
```

The last three algorithms in the list are permanently enabled and cannot be disabled.

A.2.3 Host key-based

Host key-based algorithms let the SSH server authenticate itself to an SSH client by sending its public key during a connection handshake. Subsequently, the client verifies this key against a trusted source to help ensure a secure and valid connection. This verification process helps ensure secure authentication.

The device identifies each algorithm by an index number. Use the index number to enable the desired algorithm on the device.

Table 34: Supported Host key-based algorithms

Index	Algorithm	Default setting
6	rsa-sha2-256	enabled
7	rsa-sha2-512	enabled
13	ssh-rsa	disabled

You can enable the algorithms that you need or disable those that you do not need. To do this, follow the instructions in section “Enabling the SSH algorithms in the device” on page 305.

- The MIB variable `HM2-MGMTACCESS-MIB::hm2SshHostKeyAlgorithms.0` specifies that you enable the Host key-based algorithms.
- The device will enable each algorithm you specify in the `snmpset` command.
- The device will disable each algorithm you do not specify in the `snmpset` command, even if it was previously enabled.

Perform the following steps to enable, for example, the `rsa-sha2-512` and `ssh-rsa` algorithms:

☐ Enable the algorithms in the device.

```
snmpset -Ln -u admin -a SHA-1 -A welcome123 -x AES-128 -X welcome123 -l authPriv 192.168.1.1 HM2-MGMTACCESS-MIB::hm2SshHostKeyAlgorithms.0 b '7 13'
```

☐ Check the algorithms enabled in the device.

```
nmap --script ssh2-enum-algos 192.168.1.1
```

Look at the `server_host_key_algorithms` section:

```
server_host_key_algorithms: (2)
rsa-sha2-512
ssh-rsa
```

A.2.4 Encryption (Ciphers)

Encryption algorithms encrypt data transmitted over an SSH connection. The algorithm the device uses keeps the data private on its way between the client and server.

The device identifies each algorithm by an index number. Use the index number to enable the desired algorithm on the device.

Table 35: Supported Encryption algorithms

Index	Algorithm	Default setting
0	aes128-ctr	enabled
1	aes192-ctr	enabled
2	aes256-ctr	enabled

You can enable the algorithms that you need or disable those that you do not need. To do this, follow the instructions in section “Enabling the SSH algorithms in the device” on page 305.

- The MIB variable `HM2-MGMTACCESS-MIB::hm2SshEncryptionAlgorithms.0` specifies that you enable the Encryption algorithms.
- The device will enable each algorithm you specify in the `snmpset` command.
- The device will disable each algorithm you do not specify in the `snmpset` command, even if it was previously enabled.

Perform the following steps to enable, for example, the `aes128-ctr` and `aes192-ctr` algorithms:

☐ Enable the algorithms in the device.

```
snmpset -Ln -u admin -a SHA-1 -A welcome123 -x AES-128 -X welcome123 -l authPriv 192.168.1.1 HM2-MGMTACCESS-MIB::hm2SshEncryptionAlgorithms.0 b '0 1'
```

☐ Check the algorithms enabled in the device.

```
nmap --script ssh2-enum-algos 192.168.1.1
```

Look at the `encryption_algorithms` section:

```
encryption_algorithms: (2)
aes128-ctr
aes192-ctr
```

A.2.5 Hash-based Message Authentication Code (HMAC)

HMAC algorithms help detect any modifications to transmitted data. The device uses an HMAC algorithm to verify the integrity and authenticity of transmitted data.

The device identifies each algorithm by an index number. Use the index number to enable the desired algorithm on the device.

Table 36: Supported HMAC algorithms

Index	Algorithm	Default setting
0	hmac-sha1	enabled
1	hmac-sha2-256	enabled
2	hmac-sha2-512	enabled

You can enable the algorithms that you need or disable those that you do not need. To do this, follow the instructions in section “Enabling the SSH algorithms in the device” on page 305.

- The MIB variable `HM2-MGMTACCESS-MIB::hm2SshHmacAlgorithms.0` specifies that you enable the HMAC algorithms.
- The device will enable each algorithm you specify in the `snmpset` command.
- The device will disable each algorithm you do not specify in the `snmpset` command, even if it was previously enabled.

Perform the following steps to enable, for example, the `hmac-sha1` and `hmac-sha2-256` algorithms:

☐ Enable the algorithms in the device.

```
snmpset -Ln -u admin -a SHA-1 -A welcome123 -x AES-128 -X welcome123 -l authPriv 192.168.1.1 HM2-MGMTACCESS-MIB::hm2SshHmacAlgorithms.0 b '0 1'
```

☐ Check the algorithms enabled in the device.

```
nmap --script ssh2-enum-algos 192.168.1.1
```

Look at the `mac_algorithms` section:

```
mac_algorithms: (2)
hmac-sha1
hmac-sha2-256
```

A.3 HTTPS certificate

Your web browser establishes the connection to the device using the Hypertext Transfer Protocol Secure (HTTPS). The prerequisite is that you enable the *HTTPS server* function in the*Device Security > Management Access > Server* dialog, *HTTPS* tab.

A.3.1 Conflicts in certificate validation

Web browsers and other third-party software routinely validate digital certificates.

If your web browser displays a message indicating a conflict in validating the digital certificate of the device, perform the following steps:

- ☐ Verify if the digital certificate has expired.
- ☐ Verify if your web browser no longer regards the algorithm used for generating the digital certificate as trustworthy.

To solve the conflict in certificate validation, update the digital certificate on the device. See section “HTTPS certificate management”.

A.3.2 HTTPS certificate management

To establish a secure connection, a digital certificate in X.509 format is required. In the default setting, the device uses a self-signed digital certificate.

You can regenerate the self-signed digital certificate using the latest device software. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *HTTPS* tab.
- ☐ To generate a self-signed digital certificate, in the *Certificate* frame, click the *Create* button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ For the changes to take effect after transferring a digital certificate onto the device, disable and re-enable the HTTPS server. Restart the HTTPS server using the Command Line Interface.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`https certificate generate`	To generate a digital certificate for the HTTPS server.
`no https server`	To disable the *HTTPS* function.
`https server`	To enable the *HTTPS* function.

As an alternative, generate a digital certificate externally, using up-to-date signature algorithms. Transfer the new digital certificate onto the device. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *HTTPS* tab.
- ☐ When the file is located on your PC or on a network drive, drag and drop it onto the  area. As an alternative, click in the area to select the file.
- ☐ To transfer the file to the device, click the *Start* button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`copy httpscert envm <file name>`	To transfer the digital certificate for the HTTPS server from the external memory onto the device.
`configure`	To change to the Configuration mode.
`no https server`	To disable the *HTTPS* function.
`https server`	To enable the *HTTPS* function.

Note:
To activate the digital certificate after the device generated or you transferred it, reboot the device or restart the HTTPS server. Restart the HTTPS server using the Command Line Interface.

A.3.3 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.
- ☐ Enable the *HTTPS* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ To access the device by HTTPS, enter HTTPS instead of HTTP in your web browser, followed by the IP address of the device.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`https port 443`	To specify the number of the TCP port on which the web server receives HTTPS requests from clients.
`https server`	To enable the *HTTPS* function.
`show https`	To display 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 to make the changes effective.

The device uses Hypertext Transfer Protocol Secure (HTTPS) 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, Axel Schneider
  Wiley, 2018
  ISBN 978-1-119-52791-6 (Print), ISBN 978-1-119-52799-2 (eBook)
- *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, 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 device software that provides you with additional benefits. You find information and software downloads on the Hirschmann product pages on the Internet at .

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` (`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) numerical value = integer in the range $0..2^{32}-1$
Timeout	Time value in hundredths of a second 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`.

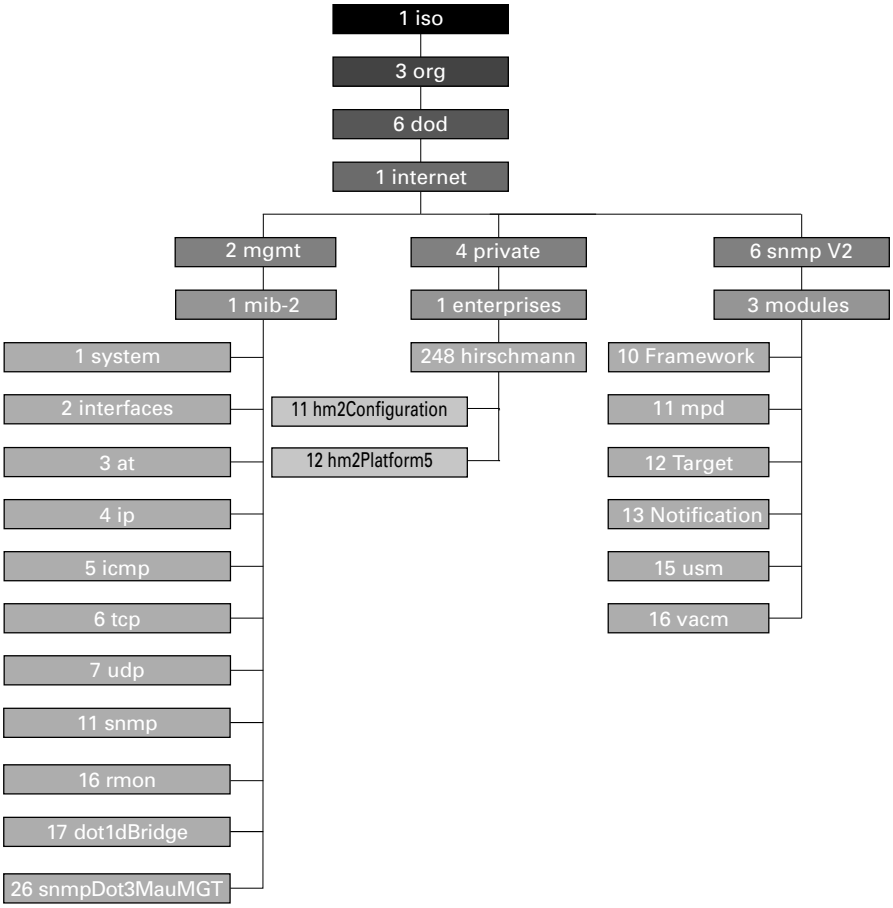


Figure 75: Tree structure of the Hirschmann MIB

When you have downloaded updated device software from the product pages on the Internet, the ZIP archive contains not only the device software but also the MIBs.

B.4 List of RFCs

RFC 768	UDP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1191	Path MTU Discovery
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1493	Dot1d
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 2233	The Interfaces Group MIB using SMI v2
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 2578	SMIv2
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance statements for SMI v2
RFC 2618	RADIUS Authentication Client MIB
RFC 2620	RADIUS Accounting MIB
RFC 2663	IP Network Address Translator (NAT) Terminology and Considerations
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 3022	Traditional IP Network Address Translator
RFC 3164	The BSD syslog protocol
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 3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
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 4363	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions
RFC 4836	Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
RFC 5905	NTPv4

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 802.3	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3x	Flow Control
IEEE 802.3af	Power over Ethernet

B.6 Underlying ANSI Norms

ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices, April 2006

B.7 Technical Data

16.3.2 Switching

Size of the MAC address table (forwarding database) (incl. static filters)	16384
Max. number of statically set-up MAC address filters	100
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)	1996 Bytes

16.3.3 VLAN

VLAN ID range	1..4042
Number of VLANs	max. 64 simultaneously per device max. 64 simultaneously per port

16.3.4 Routing/Switching

MTU (Max. allowed length of over-long packets a router interface can receive or transmit)	1500
Number of loopback interfaces	8
Max. number of Secondary IP addresses (Multinetting)	1
Max. number of VLAN router interfaces	64
Max. number of static routing entries	256

16.3.5 Firewall

Max. number of Routed Firewall Mode packet filter rules	2048
Max. number of Transparent Firewall Mode packet filter rules	999

16.3.6 NAT

Max. number of 1:1 NAT rules	255
Max. number of Destination NAT rules	255
Max. number of Double NAT rules	255
Max. number of Masquerading NAT rules	128
Max. number of Connection Tracking entries	7768

B.8 Copyright of integrated Software

The product contains, among other things, Open Source Software files developed by third parties and licensed under an Open Source Software license.

You can find the license terms in the Graphical User Interface in the *Help > Licenses* dialog.

B.9 Abbreviations used

ACA	Name of the external memory
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
NMS	Network Management System
NTP	Network Time Protocol
PC	Personal Computer
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
SCP	Secure Copy
SFP	Small Form-factor Pluggable
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TP	Twisted-pair
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

C Index

R

S

D Technical 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.belden.com.

For technical support, visit 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 decide against any compromise in any case. 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 IRD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen
  Germany

HIRSCHMANN

A BELDEN BRAND